



## **3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022**



**2 - 4 November 2022**

**International Conference Centre, Lead City University, Ibadan, Oyo State, Nigeria**

# **2022 Proceedings**



## Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Venue: International Conference Centre, Lead City University, Ibadan, Oyo State, Nigeria

Date: 2 - 4 November 2022

Copyright © 2023 by LCU Press. All rights reserved. No part of this publication may be reproduced, stored or distributed commercially in any form or by any means, electronic or mechanical, including photocopying, without permission from the publisher. Product or company names used are for identification purposes only. The inclusion of the names of the products or companies does not indicate a claim of ownership by LCU Press of the trademark or registered trademark.

### Publication Information

Title:	3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022
Proceedings Format:	Printed / eProceedings
eISBN:	978-978-799-394-1
Date of print:	July 2023
Version:	First Edition
Editor-in-Chief:	Wilson Sakpere, PhD

All works contributed to this proceeding are new, previously unpublished material. The views expressed in this proceeding are those of the authors, but not necessarily of the publisher.

## FASCON 2022 Conference Partners

The FASCON 2022 Committee would like to recognise the following partners:



# Editorial Board

## Editor-in-Chief

Dr W. Sakpere

*Head, Department of Computer Science, Lead City University, Ibadan*

## Advisory Editor

Professor Olusola Ladokun

*Dean, Faculty of Natural and Applied Sciences, Lead City University, Ibadan*

## Reviewers

Professor S. O. Akinola

*Department of Computer Science, University of Ibadan, Ibadan*

Professor P. A. Idowu

*Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife*

Professor B. A. Adebo

*Department of Physics, Lead City University, Ibadan*

Professor O. M. Ighodaro

*Department of Chemical Sciences, Lead City University, Ibadan*

Dr (Mrs) B. A. Bamkefa

*Department of Biological Sciences, Lead City University, Ibadan*

Dr O. O. Ogunlaja

*Department of Chemical Sciences, Lead City University, Ibadan*

Dr A. A. Waheed

*Department of Computer Science, Lead City University, Ibadan*

Dr (Mrs) O. K. Sindiku

*Department of Biological Sciences, Lead City University, Ibadan*

## FASCON Logo Designer

Olalekan Olabisi

*Department of Computer Science, Lead City University, Ibadan*

# FASCON 2022 Review Process

A formal 'Call for Abstracts' was issued, inviting anyone interested to submit an abstract within categories specified by the Organising Committee. Abstracts were assigned to the review panel in the field to judge the possible acceptance of the submission for presentation at the conference, based on the scope and depth of the subject matter. Selected paper presentations were invited for full paper publication in the conference proceedings. The selected papers were assigned to the review panel in the field to judge the possible acceptance of the paper for publication in the conference proceedings, based on the scope and depth of the subject matter.

The review process is based on the international de facto standard for blind paper reviews. In the blind peer-review process, papers were scrutinised by a panel of respected University academics and experts. The reviewers were asked to provide specific feedback, both positive and negative. This was the only information from the review process disclosed to the authors; all other information were kept confidential.

Reviewers used a 10-point scale to rate the following criteria:

- Originality
- Technical Quality
- Presentation Style
- References

Reviewers gave comprehensive reviewer comments and an overall rating, which assists the authors in improving and correcting their papers. The reviewers submitted their scoring and comments online via Google Forms. The Editor-in-Chief drew reports based on the reviewers scoring and comments and ranked the papers for acceptability or non-acceptability. The papers were submitted to the Turnitin online plagiarism database.

The reviewers' comments and plagiarism results were forwarded to the author(s), with a request to submit a final revised version before being accepted. Only those papers of high quality as recommended by the reviewers were included in the FASCON 2022 Proceedings as full papers.

W. Sakpere, PhD

*Chairman, Local Organising Committee, FASCON 2022*

# Local Organising Committee

Dr W. Sakpere, *Chairman, Local Organising Committee*

Dr T. S. Faniran, *Secretary, Local Organising Committee*

## Scientific/Technical Programme Committee

- i. Professor B. A. Adebo (Chair)
- ii. Professor S. O. Akinola
- iii. Professor O. M. Ighodaro
- iv. Dr O. O. Ogunlaja
- v. Dr (Mrs) F. C. Adesina
- vi. Dr A. A. Waheed
- vii. Dr H. Otobrise
- viii. Dr (Mrs) O. K. Sindiku

## Finance/Fund-raising Committee

- i. Dr (Mrs) Nike Bakare (Chair)
- ii. Dr (Mrs) V. B. Oyekunle
- iii. Mr O. Agboola
- iv. Miss I. M. Fatoki

## Publicity and Protocol Committee

- i. Dr (Mrs) B. Bamkefa (Chair)
- ii. Dr Fope Owojori
- iii. Mrs O. F. Afe
- iv. Mrs S. Oni
- v. Mr A. Ogunleye
- vi. Mrs L. Aiyelabola
- vii. Mr K. Adegbehingbe
- viii. Mr Adeluwoye
- ix. Mr E. Umezurike

## Web, Multimedia and Tech Committee

- i. Dr A. M. Ayoade (Chair)
- ii. Dr (Mrs) F. M. Adedeji
- iii. Dr R. O. Kolapo
- iv. Mr A. Abiodun
- v. Mr E. Adediran

## Welfare and Hospitality Committee

- i. Professor Arojoye (Chair)
- ii. Dr (Mrs) N. Abiola-Olagunju
- iii. Mrs A. T. John-Dewole
- iv. Mrs Ola-Babalola
- v. Miss B. Ekeolu

## Accommodation and Logistics Committee

- i. Dr O. John-Dewole (Chair)
- ii. Dr (Mrs) T. Ekanade
- iii. Dr Aliu Olabamiji
- iv. Mr F. Ero
- v. Mr O. D. Ogunsanwo

## Exhibition and Workshop Committee

- i. Dr O. A. Bamisaye (Chair)
- ii. Dr K. Adediran
- iii. Dr (Mrs) O. Nwaechefu
- iv. Mrs K. I. Okesola

# Table of Contents

FASCON 2022 Conference Partners.....	iii
Editorial Board .....	iv
FASCON 2022 Review Process.....	v
Local Organising Committee .....	vi
Table of Contents.....	vii
Adopting Nutrition-Based Measures in Managing COVID-19 Pandemic: Perspectives of Medical Practitioners and Nutritionists .....	1
<i>Bello Monsurat, Olarewaju Cecilia Abiodun and Oluwagbemileke Feranmi Boluwatife – Department of Home Economics, Adeyemi College of Education, Ondo, Nigeria</i>	
Cybercrime Monitoring System for Online Security Experts.....	9
<i>Bello Latifat and Sakpere Wilson – Department of Computer Science, Lead City University, Ibadan, Nigeria</i>	
Face Recognition-based Intelligent System for Effective Students' Class Attendance (FARBSAS) .....	18
<i>Olagunju Korede Solomon – University of Ibadan and National Open University of Nigeria, Nigeria</i>	
Web-Based Payroll System for Fixed-Term Employees .....	28
<i>Ajibade Olalekan A. and Sakpere Wilson – Department of Computer Science, Lead City University, Ibadan, Nigeria</i>	
Analysis of the Emotional and Psychological Health of the Nigerian Military During COVID-19 .....	38
<i>Oyewale Christianah T. – Department of Computer Science, University of Ibadan, Oyo State, Nigeria</i> <i>Ibitoye Ayodeji O. – Department of Computing and Mathematical Sciences, Koladai University, Oyo State, Nigeria</i>	
Intrusion Detection System in Cloud Computing: A Review .....	45
<i>Awodele Simon O. and Sakpere Wilson – Department of Computer Science, Lead City University, Ibadan, Nigeria</i>	
Big Data Concept, Analytics and Hadoop Technology: A Systematic Survey .....	59
<i>Adelodun Felicia O. and Sakpere Wilson – Department of Computer Science, Lead City University, Ibadan, Nigeria</i>	
Haptoglobin Phenotype, Serum Iron Levels and Severity in Multi-Drug Resistant Mycobacterium Tuberculosis Patients in Ibadan.....	65
<i>Ojika Obianuju Ibifuro and Muhammed Jamiu Aasia – Department of Biotechnology, Baze University, Abuja, Nigeria</i> <i>Ochayi Okwute Michael – Department of Physiology, Baze University, Abuja, Nigeria</i> <i>Nze Okechukwu – Department of Chemistry, Baze University, Abuja, Nigeria</i>	





Editorial

---

# Adopting Nutrition-Based Measures in Managing COVID-19 Pandemic: Perspectives of Medical Practitioners and Nutritionists

---

Bello Monsurat, Olarewaju Cecilia Abiodun and Oluwagbemileke Feranmi Boluwatife

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Bello, M., Olanrewaju, C. A., & Oluwagbemileke, F. B. (2023). Adopting Nutrition-Based Measures in Managing COVID-19 Pandemic: Perspectives of Medical Practitioners and Nutritionists. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 2-8). Ibadan. <https://doi.org/10.5281/zenodo.8121054>.

# Adopting Nutrition-Based Measures in Managing COVID-19 Pandemic: Perspectives of Medical Practitioners and Nutritionists

Bello Monsurat, Olarewaju Cecilia Abiodun and \*Oluwagbemileke Feranmi Boluwatife

Department of Home Economics,

Adeyemi College of Education, Ondo, Nigeria

\*lekeferanmi2019@gmail.com

**Abstract:** Coronavirus disease (also called COVID-19, 2019-nCov or 2019 Novel Coronavirus) is associated with respiration-related symptoms such as cough, fever, pneumonia, and sometimes death. This study examined the comparison in the perceptions of medical practitioners and nutritionists on the relationship between good nutrition and the coronavirus disease. Three research hypotheses were postulated and tested at a 0.05 level of significance. A descriptive survey research approach was adopted. Ninety-one medicals and nutritionists were selected in Ondo West Local Government as respondents. A self-developed and validated questionnaire titled "Utilization of Good Dietary Pattern in the Management of COVID-19 Pandemic Questionnaire" was the instrument used for data collection. Data collected were analysed with mean, standard deviation and t-test of significance difference. Findings revealed that both classes of respondents agreed with no significant difference that the possible consequences of the COVID-19 pandemic on the health of the populace include a breakdown in the immune system, inflammation of the respiratory tract, multi-organ failure, and mortality ( $\bar{x} \geq 2.50$ ) and that good nutrition can aid in the management of COVID-19 pandemic through immune boosting and increased resistance against infections. Their responses are slightly different regarding the roles of high biological value proteins and lipids in COVID-19 Management as well as about the facts that multi-organ failure upon the advancement of COVID-19 and that COVID-19 complications can be prevented through the exertion of anti-inflammatory effect in the gut. The study concluded that the consumption of a good nutritious diet can aid the management of COVID-19 before and after the infection, as it will boost individuals' immune systems. It was therefore recommended that the consumption of nutrient-dense diets and immune-boosting food should be prioritized in managing COVID-19.

**Key Words:** COVID-19, disease management, immune boosting, medical practitioners, nutritionists, nutrition

## I. INTRODUCTION

Coronavirus disease (also called COVID-19, 2019-nCov or 2019 Novel Coronavirus) is an infectious disease caused by a new strain of coronavirus, which until its discovery was not identified in humans. It is associated with flu-like symptoms such as cough, fever, pneumonia, and sometimes, death. Its novelty has put the members of the scientific community on their heels as effective and sustainable vaccines to mitigate the hydra-headed virus and drugs to treat the pathology are being sourced for. Reducing inflammation and ensuring that patients can give necessary immune responses at the same time was a critical challenge. Facts such as the one reported

by Handu *et al.* (2021) that adults infected with coronavirus disease 2019 (COVID-19) showed a significant impact of malnutrition on health outcomes, should inform the search for remedies to the global malady. In other words, scientists needed to explore the potential of foods and much as in drugs. The eventualities of the COVID-19 pandemic have reflected the indispensable need for good and adequate nutrition and dietary habits. They are expedient to minimize the occurrence of Non-Communicable Diseases (NCDs) and modulate the inflammatory status of infected individuals. From another perspective, the health status of recovered patients can be affected by improper nutrition during infection (Brugliera *et al.*, 2020; Fernández-Quintela *et al.*, 2020; Zabetakis *et al.*, 2020).

Based on the available information on the treatment given to coronavirus disease patients, the nutritional remedy is the first-line treatment. First, nutrition is essential for the survival of man—hale, invalid and convalescent. Further from this, nutrition care is identified as a means of addressing malnutrition to treat and prevent further adverse health outcomes from COVID-19 infection. Since the disease spontaneously overpowers the immune system and unleashes infections in the respiratory system, appropriate intake of a well-balanced diet which constitutes all essential nutrients in the right proportion will be of great help to the immune system. Also, the intake of certain micronutrients in amounts exceeding their recommended dietary allowances is recommended since infections and other stressors can reduce micronutrient status (Fernández-Quintela *et al.*, 2020).

Studies have established the importance of nutrition in the building of the body's immunity to infections. Protein deficiency is said to negatively affect the number of functional immunoglobulins and gut-associated lymphoid tissue, thus impairing the immune system function. The quality and quantity of proteins consumed are also important here. Therefore, high biological value proteins (such as those present in eggs, lean meat, fish, and dairy) which contain all the essential amino acids and can exert anti-inflammatory effects in the body should be included in the diets of COVID-19 patients. Also, amino acids like arginine and glutamine can positively influence the immune system (Iddir *et al.*, 2020). Similarly, omega-3 fatty acids – docosahexaenoic acid (DHA) and eicosapentaenoic acid (EPA) – can render enveloped viruses inactive and prevent viral replication. These two essential fatty acids (DHA and EPA) suppress the production of prostaglandin which could cause inflammation, by inhibiting the activity of cyclooxygenase enzymes (COX) (Zabetakis *et al.*, 2020). They can lower the rate of Platelet-Activating Factors (PAF) biosynthesis, as

well as increase the rate of those involved in its degradation. Also, Platelet activation may be blocked as a way of preventing thrombosis (the blockage of blood vessels by blood clots) associated with COVID-19 (Lordan *et al.*, 2021; Zabetakis *et al.*, 2020).

Carbohydrates and dietary fibres are not left out in this all-important role of nutrition in COVID-19 management. The consumption of highly processed carbohydrates which have higher glycemic indexes can overload the mitochondrion and lead to the synthesis of free radicals. On the other hand, the consumption of highly caloric foods can help reduce inflammation, while sufficient fibre consumption (about 25–35 g/day) can facilitate correct metabolic functioning and reduce both gut and systemic inflammation (particularly, by lowering the number of inflammatory cytokines such as CRP, TNF- $\alpha$  and IL-6) (Iddir *et al.*, 2020). Vitamins A, C, D, E, B<sub>6</sub> and B<sub>12</sub> minerals (such as folate, iron, and magnesium) and trace elements like zinc, selenium and copper help reduce disease susceptibility (Maggini *et al.*, 2008, 2018) and the maintenance of immune function (Calder, 2013). Deficiencies in these nutrients negatively affect the immune system, resulting in decreased resistance against infections. Vitamins and minerals are essential for adaptive immunity as they are involved in cytokine production, lymphocyte differentiation and proliferation, antibody production, and generation of memory cells.

This study, therefore, seeks to study the comparison in the perceptions of medical practitioners and nutritionists on the relationship between good nutrition and the coronavirus disease.

## II. STATEMENT OF THE PROBLEM

Good nutrition has been identified as one of the most effective approaches to addressing the effects of COVID-19 on human physical and mental health. However, there remains an observable gulf in the coherence of facts held by medical practitioners and nutritionists in this regard. This may be because the first class of people handle nutrition as only a supplement to remedies or cures expected to be supplied by pharmaceutical products, while the latter group believe strongly in the cogency of nutrition in treating, or in a more ideal sense, preventing or protecting against ailments including such ones as the dreaded COVID-19. Meanwhile, these disparities will only continue to threaten the credibility ascribed to the information supplied by the two groups of professionals. It becomes therefore necessary to compare (and if necessary, contrast) the perspectives of the duo on the role of good nutrition in the management of the COVID-19 pandemic. Also, there is a need to create more awareness among the populace of the importance of good and immune-boosting nutrition in combating COVID-19.

## III. PURPOSE OF THE STUDY

The main purpose of the study is to juxtapose the perspectives of medical practitioners and nutritionists about the adoption of nutrition-based measures in managing the COVID-19 pandemic. Specifically, the study documented the comparative perceptions of medical practitioners and nutritionists on the:

1. consequences of the COVID-19 pandemic on the health of the populace,
2. general roles of good nutrition in the management of the

- COVID-19 pandemic, and
3. specific nutrition-based measures in the management of the COVID-19 Pandemic.

## IV. RESEARCH HYPOTHESES

The following null hypotheses shall be tested at a 0.05 level of significance.

H<sub>01</sub>: The perspectives of medical practitioners and nutritionists on the consequences of the COVID-19 pandemic on the health of the populace are not significantly different.

H<sub>02</sub>: There is no significant difference in the perspectives of medical practitioners and nutritionists on the general role of good nutrition in the management of the COVID-19 pandemic.

H<sub>03</sub>: The perspectives of medical practitioners and nutritionists on the specific nutrition-based measures in the management of the COVID-19 Pandemic are not significantly different.

## V. METHODOLOGY

The design used for this study was the descriptive survey design as it allows for the examination of the interaction between the variables under study (profession, nutrition and coronavirus disease) and the implications of the findings. The population of the study consisted of Health Workers and Nutritionists in Ondo State. The simple random sampling technique was used to select a total of ninety-one (91) respondents: forty-six (46) males and forty-five (45) females.

A self-structured questionnaire was used to elicit information from the respondents. It consisted of five sections: 'A' to 'E'. Section A was meant to elicit information on the personal data of the respondents while Sections B, C, D and E contained question items intended to obtain information to answer the four research questions raised for the study. The questionnaire was constructed on a four-point Likert scale of Strongly Agree (SA), Agree (A), Disagree (D) and Strongly Disagree (SD). The research instrument for the study was validated by three experts in the Department of Home Economics, Adeyemi College of Education, Ondo. Their observations, suggestions and comments were used to make constructive corrections in the final copy of the instrument. Copies of the questionnaire were administered electronically to elites (using Google form) and in person to other respondents.

The data collected was analyzed using mean, standard deviation and t-test. The decision rule was that any mean value equal to or greater than 2.50 is regarded as agreed, while any mean value below 2.50 is considered as disagreed. Further, when the 2-tailed significant value at 0.05 level of significance is less than 0.05, the difference in the mean responses of the two categories of respondents is taken to be significant. Else, the difference is said not to be statistically significant. This is done for every single item under each hypothesis and for the summation of the responses needed to test each hypothesis.

## VI. RESULTS

Research Hypothesis 1: The perspectives of medical practitioners and nutritionists on the consequences of the COVID-19 pandemic on the health of the populace are not significantly different.

Table 1: Mean, Standard Deviation and T-test Analysis of the Perspective of Medical Practitioners and Nutritionists on the Consequences of the COVID-19 Pandemic on the Health of the Populace

nM = 57; nN = 34; df = 89; COP = 2.50; $\rho$ = 0.05							
S/N	ITEMS	Respondents	$\bar{x}$	SD	t	Sig. (2-tailed)	Decision
1.	Coronavirus disease (COVID-19) may cause interstitial pneumonia and respiratory distress syndrome, which can lead to multi-organ failure.	Medicals	3.60	0.495	-1.644	0.104	NS
		Nutritionists	3.76	0.431			
2.	COVID-19 can lead to break down of the immune system of the body	Medicals	3.84	0.492	0.909	0.366	NS
		Nutritionists	3.74	0.618			
3.	COVID-19 can cause acute inflammation of the respiratory tract	Medicals	3.91	0.285	1.966	0.052	NS
		Nutritionists	3.76	0.431			
4.	Multi-organ failure occurs as the disease advances	Medicals	3.89	0.310	3.378	0.001	S
		Nutritionists	3.59	0.557			
5.	Lung capacity is reduced by damage to pulmonary tissues	Medicals	3.67	0.852	0.752	0.454	NS
		Nutritionists	3.53	0.825			
6.	COVID-19 leads to the stigmatization of patients which in turn affect their psychological health	Medicals	3.16	0.922	-1.206	0.231	NS
		Nutritionists	3.38	0.739			
7.	Complications can result from damage to the blood vessels	Medicals	3.65	0.612	1.305	0.195	NS
		Nutritionists	3.47	0.662			
8.	The pandemic can lead to mortality.	Medicals	3.79	0.559	-0.300	0.765	NS
		Nutritionists	3.82	0.459			
	Grand	Medicals	29.51	2.361	0.802	0.425	NS
		Nutritionists	29.06	2.933			

Source: Field Survey (2021)

**Keys:** nM = Number of Medical Practitioners  
df = Degree of Freedom  
 $\rho$  = Level of Significance  
SD = Standard Deviation  
S = Significant

nN = Number of Nutritionists  
COP = Cut-Off-Point  
 $\bar{x}$  = Mean Value of Responses  
NS = Not Significant  
t = Calculated t-value

Table 1 shows the mean responses of medical practitioners and nutritionists on the possible consequences of the COVID-19 pandemic on the health of the populace. The means of the responses range from 3.16 to 3.91 which is greater than the cut-off point of 2.50. This indicates that both sets of respondents agreed that COVID-19 can lead to acute inflammation of the respiratory tract, breakdown of the immune system, mortality, multi-organ failure upon the advancement of the disease, pulmonary tissue damage, interstitial pneumonia and respiratory distress syndrome, damage in the blood vessels, and stigmatization of patients. The standard deviations of the responses ranged from 0.310 to 0.922 indicating that the responses clustered around the mean. However, the t-test analysis revealed that the responses of the

medical practitioners and nutritionists are not significantly different on the foregoing points, except for the point that multi-organ failure upon the advancement of COVID-19. The medicals gave a mean response that is much higher than that of the nutritionists on the point. Summarily, there is no significant difference between the perspectives of medical practitioners and nutritionists on the consequences of the COVID-19 pandemic on the health of the populace.

Research Hypothesis 2: There is no significant difference in the perspectives of medical practitioners and nutritionists on the general role of good nutrition in the management of the COVID-19 pandemic.

Table 2: Mean, Standard Deviation and T-test Analysis of the Perspective of Medical Practitioners and Nutritionists on the General Role of Good Nutrition in the Management of the COVID-19 Pandemic

nM = 57; nN = 34; df = 89; COP = 2.50; $\rho = 0.05$							
S/N	ITEMS	Respondents	$\bar{x}$	SD	t	Sig. (2-tailed)	Decision
1.	Immune boosting, which is an important step in fighting against COVID-19 infection	Medicals	3.88	0.327	-0.365	0.716	NS
		Nutritionists	3.84	0.591			
2.	Exertion of anti-inflammatory effects in the gut helps prevent COVID-19 complications.	Medicals	3.88	0.327	-3.264	0.002	S
		Nutritionists	2.84	0.978			
3.	An increase in resistance to infections such as COVID-19 can be achieved through a good diet	Medicals	3.53	0.961	-1.634	0.106	NS
		Nutritionists	3.51	0.928			
4.	Control of metabolic functions to prevent multi-organ dysfunction	Medicals	3.79	0.538	-1.472	0.145	NS
		Nutritionists	3.33	1.006			
5.	Prevention of damage to the blood vessels that commonly exist in COVID-19 patients	Medicals	3.62	0.652	-0.996	0.322	NS
		Nutritionists	3.51	0.848			
Grand		Medicals	17.04	2.927	-2.528	0.013	S
		Nutritionists	18.50	2.178			

Source: Field Survey (2021)

**Keys:** nM = Number of Medical Practitioners  
df = Degree of Freedom  
 $\rho$  = Level of Significance  
SD = Standard Deviation  
S = Significant

nN = Number of Nutritionists  
COP = Cut-Off-Point  
 $\bar{x}$  = Mean Value of Responses  
NS = Not Significant  
t = Calculated t-value

Table 2 shows the mean responses of medical practitioners and nutritionists on the general role of good nutrition in the management of the COVID-19 pandemic. The mean values of the responses range from 2.84 to 3.88 which are greater than the cut-off point of 2.50. This means both sets of respondents agreed that the general role of good nutrition in COVID-19 management includes immune boosting, increase in resistance against infections, prevention of damage to the blood vessels, control of metabolic functions and exertion of anti-inflammatory effect in the gut as to prevent COVID-19 complications. The standard deviations of the responses ranged from 0.538 to 1.006 indicating that the responses are slightly scattered around the mean. However, the t-test analysis revealed that the responses of the medical

practitioners and nutritionists are not significantly different on the foregoing points, except for the point that exerting anti-inflammatory effect in the gut to prevent COVID-19 complications, where the responses of the medicals deviate very highly from the mean value, unlike those of the nutritionists. On a cumulative ground, there is a significant difference between the perspectives of medical practitioners and nutritionists on the general role of good nutrition in the management of the COVID-19 pandemic.

Research Hypothesis 3: The perspectives of medical practitioners and nutritionists on the specific nutrition-based measures in the management of the COVID-19 Pandemic are not significantly different.

Table 3: T-test Analysis of the Perspective of Medical Practitioners and Nutritionists on the Specific Nutrition-Based Measures in the Management of the COVID-19 Pandemic

nM = 57; nN = 34; df = 89; COP = 2.50; p = 0.05							
S/N	ITEMS	Respondents	$\bar{x}$	SD	t	Sig. (2-tailed)	Decision
1.	High biological value proteins (in lean meat, fish and dairy products) exert anti-inflammatory effects in the gut to prevent COVID-19 complications	Medicals	3.44	1.000	2.083	0.040	S
		Nutritionists	3.00	0.921			
2.	Amino acids (such as arginine and glutamine) in walnuts, peanuts, almonds and cashew nuts can facilitate immunity	Medicals	3.44	1.118	-0.425	0.672	NS
		Nutritionists	3.53	0.706			
3.	Omega-3 fatty acids (in fish and fish oil) can help reduce	Medicals	2.82	0.928	-2.711	0.008	S
		Nutritionists	3.35	0.849			
4.	Limiting the consumption of high glycemic carbohydrates (i.e., highly processed carbohydrate foods) such as refined wheat, white rice, breakfast cereals, cakes, watermelon, pineapple, and dried fruits and soon been reported to be related to the proper immune system functioning	Medicals	3.18	1.020	-0.143	0.887	NS
		Nutritionists	3.21	0.914			
5.	Food sources of dietary fibre such as fruits, vegetables, nuts and seeds, and potatoes with peels are of importance in metabolic functions.	Medicals	3.75	0.786	-1.122	0.265	NS
		Nutritionists	3.91	0.288			
6.	Mineral elements (such as zinc and selenium) obtained from food sources such as meats, fish, cereals, dairy products, fruits, vegetables, and nuts are important in increasing resistance against infections.	Medicals	3.65	0.876	-1.489	0.140	NS
		Nutritionists	3.88	0.327			
	Grand	Medicals	20.28	3.904	-0.818	0.415	NS
		Nutritionists	20.88	2.280			

Source: Field Survey (2021)

**Keys:** nM = Number of Medical Practitioners  
df = Degree of Freedom  
p = Level of Significance  
SD = Standard Deviation  
S = Significant

nN = Number of Nutritionists  
COP = Cut-Off-Point  
 $\bar{x}$  = Mean Value of Responses  
NS = Not Significant  
t = Calculated t-value

Table 3 shows the mean responses of medical practitioners and nutritionists on the specific nutrition-based measures in the management of the COVID-19 Pandemic. The mean values of the responses ranged from 2.82 to 3.91 which is greater than the cut-off point of 2.50. This means both sets of respondents agreed that the specific dietary habit necessary for managing COVID-19 infection include the consumption of food sources of dietary fibre, mineral elements (such as zinc and selenium), amino acids (arginine and glutamine), high biological value proteins, lipids like the Omega -3 fatty acids, and limiting the consumption of high glycemic carbohydrates. The standard deviations of the responses range from 0.288 to 1.118 indicating that the responses are slightly scattered around the mean. However, the t-test analysis revealed that the responses of the medical practitioners and nutritionists are not significantly different on the foregoing points, except for their perspectives on the roles played by high biological value proteins and lipids in COVID-19 Management. On a cumulative ground, there is no significant difference between the perspectives of medical practitioners and nutritionists on the specific nutrition-based measures in the management of the COVID-19 Pandemic.

## VII. DISCUSSION

The result of the study revealed that coronavirus has consequences such as interstitial pneumonia and respiratory distress syndrome, breakdown of the immune system, acute inflammation of the respiratory tract, multi-organ failure upon advancement of the disease, pulmonary tissue damage, stigmatization of patients, damage in the blood vessels, and mortality. The studies carried out by Ding *et al.* (2020), Guan *et al.* (2020), Zangrillo *et al.* (2020) and Zhou *et al.* (2020) confirmed these findings. Furthermore, Maguire and Stone (2021), while reviewing the alliance between nurses and dietitians, discovered that more cases of advanced diseases are associated with COVID-19, and that the greater risk is that of malnutrition which then became increasingly difficult to manage by conventional means.

It was equally discovered that the general role of good nutrition in COVID-19 management includes immune boosting, increase in resistance against infections, prevention of damage to the blood vessels, control of metabolic functions and exertion of anti-inflammatory effects in the gut to prevent COVID-19 complications. Also, the specific dietary habit

necessary for managing COVID-19 infection includes the consumption of food sources of dietary fibre, mineral elements (such as zinc and selenium), amino acids (arginine and glutamine, high biological value proteins, lipids like the Omega-3 fatty acids, and limiting the consumption of high glycemic carbohydrates. Good dietary habits can help in immune boosting, exert anti-inflammatory effects in the gut to prevent COVID-19 complications, increase resistance against infections, control metabolic functions, and prevent damage to the blood vessels. This is supported by the report of Iddir *et al.* (2020), Monnier *et al.* (2006) and Zabetakis *et al.* (2020). This is in line with the position of Maguire and Stone (2021) that the standard care of COVID-19 patients (especially for those living with cancer) included routine monitoring of their nutrition, dissemination of receive targeted nutrition information, and administration of therapeutic diets. In other words, the comprehensive nutritional intervention was helpful in optimising outcomes for this highly vulnerable patient group.

However, the perspectives of medicals and nutritionists are significantly different on the general role of nutrition in the management of COVID-19, while their perspectives on the specific roles are not significantly different. Maguire and Stone (2021) explained that nurses and dietitians collaborated to provide nutritional care for COVID-19 patients, particularly those living with cancer. The first point of contact for the patients was the nurses, who liaised between patients and their respective family members during admission. The family members furnished the nurses with information such as the usual feeding habits and practices of the patients, their food allergies and preferences, and necessary home nutrition histories. This information is then used by the dietitians to recommend and deliver appropriate food services and nutritional care, as well as to carry out a comprehensive nutritional assessment of the patients.

## VIII. CONCLUSION

Based on the findings of this study, it can be concluded that COVID-19 is a pandemic that has come to stay and whose effect can never be forgotten in the history of the whole world. Apart from the medications given to COVID-19 patients and the advocacy for proper hygiene, the consumption of an adequate, nutrient-dense diet can aid the management of COVID-19 before and after the infection as it will boost individuals' immune systems, thus reducing the impact of the infection on infected individuals.

## IX. RECOMMENDATIONS

1. The public should be made aware of the positive implications of good dietary habits on the management of the COVID-19 pandemic through newsletters and other print channels, personal contacts, billboards, social media, community and town hall meetings, sensitization on market days, and Mass media such as radio, television, internet sites.
2. Further research studies should be carried out on the effect of the coronavirus on various age groups and the nutritional requirement to manage the effects of the disease on them.
3. Government should be up and doing by assisting in the cultivation of food sources of the nutrients needed by the populace during the crisis caused by the pandemic.

## REFERENCES

- Brugliera, L., Spina, A., Castellazzi, P., Cimino, P., Arcuri, P., Negro, A., Houdayer, E., Alemanno, F., Giordani, A., Mortini, P., & Iannaccone, S. (2020). Nutritional management of COVID-19 patients in a rehabilitation unit. *European Journal of Clinical Nutrition*, 74(6), 860–863. <https://doi.org/10.1038/s41430-020-0664-x>
- Calder, P. C. (2013). Omega-3 polyunsaturated fatty acids and inflammatory processes: Nutrition or pharmacology? *British Journal of Clinical Pharmacology*, 75(3), 645–662. <https://doi.org/10.1111/j.1365-2125.2012.04374.x>
- Ding, L., Wang, L., Ma, W., & He, H. (2020). Efficacy and safety of early prone positioning combined with HFNC or NIV in moderate to severe ARDS: A multi-center prospective cohort study. *Critical Care*, 24(28), 1–8. <https://doi.org/10.1186/s13054-020-2738-5>
- Fernández-Quintela, A., Milton-Laskibar, I., Trepiana, J., Gómez-Zorita, S., Kajarabille, N., Léniz, A., González, M., & Portillo, M. P. (2020). Key aspects in nutritional management of COVID-19 patients. *Journal of Clinical Medicine*, 9(8), 1–24. <https://doi.org/10.3390/jcm9082589>
- Guan, W., Ni, Z., Hu, Y., Liang, W., Ou, C., He, J., Liu, L., Shan, H., Lei, C., Hui, D. S. C., Du, B., Li, L., Zeng, G., Yuen, K.-Y., Chen, R., Tang, C., Wang, T., Chen, P., Xiang, J., ... Zhong, N. (2020). Clinical characteristics of coronavirus disease 2019 in China. *New England Journal of Medicine*, 382(18), 1708–1720. <https://doi.org/10.1056/nejmoa2002032>
- Handu, D., Moloney, L., Rozga, M., & Cheng, F. (2021). Malnutrition care during the COVID-19 pandemic: Considerations for registered dietitian nutritionists. *Journal of the Academy of Nutrition and Dietetics*, 121(5), 979–987. <https://doi.org/10.1016/j.jand.2020.05.012>
- Iddir, M., Brito, A., Dingo, G., Del Campo, S. S. F., Samouda, H., La Frano, M. R., & Bohn, T. (2020). Strengthening the immune system and reducing inflammation and oxidative stress through diet and nutrition: Considerations during the COVID-19 crisis. *Nutrients*, 12(6), 1–43. <https://doi.org/10.3390/nu12061562>
- Lordan, R., Tsoupras, A., & Zabetakis, I. (2021). Platelet activation and prothrombotic mediators at the nexus of inflammation and atherosclerosis: Potential role of antiplatelet agents. *Blood Reviews*, 45, 1–18. <https://doi.org/10.1016/j.blre.2020.100694>
- Maggini, S., Beveridge, S., Sorbara, P. J. P., & Senatore, G. (2008). Feeding the immune system: The role of micronutrients in restoring resistance to infections. *CABI Reviews: Perspectives in Agriculture, Veterinary Science, Nutrition and Natural Resources*, 2008(98), 1–21. <https://doi.org/10.1079/PAVSNNR20083098>
- Maggini, S., Pierre, A., & Calder, P. C. (2018). Immune function and micronutrient requirements change over the life course. *Nutrients*, 10(10), 1–27. <https://doi.org/10.3390/nu10101531>
- Maguire, F., & Stone, S. (2021). The cancer nurse-dietitian alliance in the era of COVID-19: Why the role of nurses in the nutritional care of patients must not be undervalued. *The Australian Journal of Cancer Nursing*, 22(3), 2–3. <https://doi.org/10.33235/ajcn.22.3.2-3>

- Monnier, L., Mas, E., Ginet, C., Michel, F., Villon, L., Cristol, J. P., & Colette, C. (2006). Activation of oxidative stress by acute glucose fluctuations compared with sustained chronic hyperglycemia in patients with type 2 diabetes. *JAMA*, 295(14), 1681–1687. <https://doi.org/10.1001/jama.295.14.1681>
- Zabetakis, I., Lordan, R., Norton, C., & Tsoupras, A. (2020). COVID-19: The inflammation link and the role of nutrition in potential mitigation. *Nutrients*, 12(5), 1–28. <https://doi.org/10.3390/nu12051466>
- Zangrillo, A., Beretta, L., Silvani, P., Colombo, S., Scandroglio, A. M., Dell'acqua, A., Fominskiy, E., Landoni, G., Monti, G., Azzolini, M. L., Monaco, F., Oriani, A., Belletti, A., Sartorelli, M., Pallanch, O., Saleh, O., Sartini, C., Nardelli, P., Lombardi, G., ... Tresoldi, M. (2020). Fast reshaping of intensive care unit facilities in a large metropolitan hospital in Milan, Italy: Facing the COVID-19 pandemic emergency. *Critical Care and Resuscitation: Journal of the Australasian Academy of Critical Care Medicine*, 22(2), 91–94. <https://doi.org/10.51893/2020.2.pov1>
- Zhou, F., Yu, T., Du, R., Fan, G., Liu, Y., Liu, Z., Xiang, J., Wang, Y., Song, B., Gu, X., Guan, L., Wei, Y., Li, H., Wu, X., Xu, J., Tu, S., Zhang, Y., Chen, H., & Cao, B. (2020). Clinical course and risk factors for mortality of adult inpatients with COVID-19 in Wuhan, China: A retrospective cohort study. *The Lancet*, 395(10229), 1054–1062. [https://doi.org/10.1016/S0140-6736\(20\)30566-3](https://doi.org/10.1016/S0140-6736(20)30566-3)



Editorial

---

# Cybercrime Monitoring System for Online Security Experts

---

Bello Latifat O. and Sakpere Wilson

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Bello, L. O., & Sakpere, W. (2023). Cybercrime Monitoring System for Online Security Experts. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 10-17). Ibadan. <https://doi.org/10.5281/zenodo.8121056>.

# Cybercrime Monitoring System for Online Security Experts

\*Bello Latifat O. and Sakpere Wilson  
Department of Computer Science,  
Lead City University Ibadan, Nigeria  
\*bellolatifat05@gmail.com

**Abstract:** Cyberspace is increasingly attacked and there are limited means of mitigating this act. This is usually due to a shifted degree of security attributes and management schemes within the cloud entity in cyberspace. The challenges are due to improvements in methods and the utilisation of new technologies in committing crimes by cybercriminals. The threat of cybercrime will continue to evolve and grow as cybercriminals adapt to new security solutions and take advantage of the changes in online behaviour. Hence, it is still challenging to identify and track down cyber criminals. This study focuses on implementing a cybercrime monitoring system for online data experts. After an in-depth understanding of cyber users' attacks, a possible solution is proposed. A web application portal is designed using WordPress development tools that will serve as a platform to monitor and present possible vulnerabilities discovered. Tawk.to is integrated into the website for the implementation of real-life monitoring and My Structured Query Language (MySQL) is used as the database for storing and retrieval of information. This system captures the digital signature of each piece of information sent to cyberspace, the user login parameter, date, time, the location of the user, the Media Access Control address of the system used, and activities carried out by the user while online. It also aids cyber security experts in ascertaining the extent of activities carried out by cybercriminals in the domain. The outcome demonstrated that the system could identify cyber users and their activities online.

**Key Words:** Cybercrime, Cyberspace, Cyber Criminals, Security Expert

## I. INTRODUCTION

Security of life and property is very vital to human life. Human life needs to be protected from critical and pervasive threats. The rate of security threats in the world is increasing at an exponential rate (Walker-Roberts *et al.*, 2020). Due to this challenge, individuals and governments have designed means to safeguard and protect themselves and their citizens against such threats. These security threats may include physical and cybercrime threats (Chatfield & Reddick, 2019).

Crime is a major issue in the world today. One of the factors influencing crime incidents is the technological advancement we are experiencing globally (Sadiku *et al.*, 2022). Burglary, internet crime, theft, and fraud are all examples of crime. Typically, criminal behaviour is motivated by greed, rage, jealousy, retaliation, or pride, which negatively impacts other law-abiding citizens (Paul & Aithal, 2018). Also, committing a crime can result in the dissolution of an organisation's structure and governance, which necessitates the implementation of security measures in every aspect of our lives. Cybersecurity is essential for containing this threat.

Cyber security plays an important role in Information

Technology (IT). In the modern day, information protection has grown to be a major issue. Cybersecurity has grown to be a significant issue in the information technology (IT) industry during the past ten years. Cybercrime causes a lot of issues for people, organisations, and the government, and many steps are being made to combat it. Notwithstanding these precautions, there are still concerns about cyber security because a cybercrime attack can result in anything from widespread fraud to the blackmail of major corporations (Kalakuntla *et al.*, 2019).

A crime that involves a computer and a network is referred to as cybercrime (Agana & Inyama, 2015). It's possible that the computer was used in the crime or that it was the subject of a cyberattack. A concerted attack on a computer system to touse hardware operations, alter processing control, or corrupt stored data can be described as a computer attack (Aiken *et al.*, 2022). Cybercrime is the term used to describe any crime perpetrated through computer networks. These crimes are done against specific people or groups of people to damage the victim's reputation, either directly or indirectly. This is done with the use of advanced media transmissions systems such as the Internet, trojan, hacking, phishing, website cloning, copyright infringement and many more. The rate at which cybercrime is growing in the current environment is concerning and has increased security threats (Prakash *et al.*, 2019). Cybercrime investigation is a very challenging process since it is challenging to identify or track cybercrime perpetrators. Criminals have used computers and the internet to conduct crimes while remaining anonymous (Javed *et al.*, 2022). To safeguard users from cyberterrorism, computer-based monitoring systems are required. These systems make it simple to record evidence of hackers who infiltrate a network. It is worth noting that cybercrime has been of great benefit to its Practitioners and their benefactors. While it has been dysfunctional to the victims of the scammers, their dependents, and to a large extent society, it has become an image nightmare for most countries and their citizens. With the Internet creating limitless opportunities for commercial, social, and educational activities today, many businesses and personal transactions are conducted electronically. For this reason, cybercrime must be taken seriously by industry experts and academics at large.

This study focuses on developing a cost-effective model of a cybercrime monitoring system for online security experts. The specific objectives of the study are to develop a navigable and usable website suitable for monitoring threats, integrate Tawk.to to the website and evaluate the performance of the system.

## II. STATEMENT OF THE PROBLEM

Cybercrime is challenging because of the shifted degree of security attributes and management schemes within the cloud entity in cyberspace (Agana & Inyama, 2015). The threat

posed by cybercrime will continue to evolve and grow as criminals adapt to new security solutions and take advantage of the changes in online behaviours (Eddolls, 2016). Additionally, because of the nature of cybercrime, which is domiciled in cyberspaces, it is difficult for law enforcement to identify and bring cybercriminals to justice (Rogers & Seigfried, 2004). Although several cyber monitoring systems have been in existence, it is still difficult to identify and track cybercriminals. The problem is the cost implication and difficulty in integrating a Web Application Firewall into a website (Mihai, 2017). Also, monitoring large user groups is tedious (Ba, 2017). The humongous cost and difficulty in implementing an automated monitoring device discourage individuals and organisations from effectively monitoring their websites. As a result, Cybercrime continues to increase. This has raised concerns. This study is work-in-progress research that will aid in monitoring internet users' actions, the recovery of digital proof of cybercrime, and the protection of users from hacking.

### III. SYSTEM DESIGN

After determining and understanding how users are attacked online, a suitable method and methodology for developing an enhanced Cyber Crime Monitoring System for Online Security Expert is implemented. A web application portal is designed using WordPress development tools that will serve as a platform to monitor the activities of users visiting the web Gateway. Tawk.to API is integrated into the website for the implementation of a real-life Monitoring System, and MySQL is used as the database for the storage of information of users that visits the website. This application will keep track of a user's online activity and index.dat file content by taking screenshots, allowing online security professionals to better defend their domain.

This system will record the digital signatures of every piece of information transferred into cyberspace, the user's login credentials, the user's geographic location, the MAC address of the computer they are using, the date, time, and the actions they took online. It will support forensic professionals' investigations and efforts to catch cybercriminals.

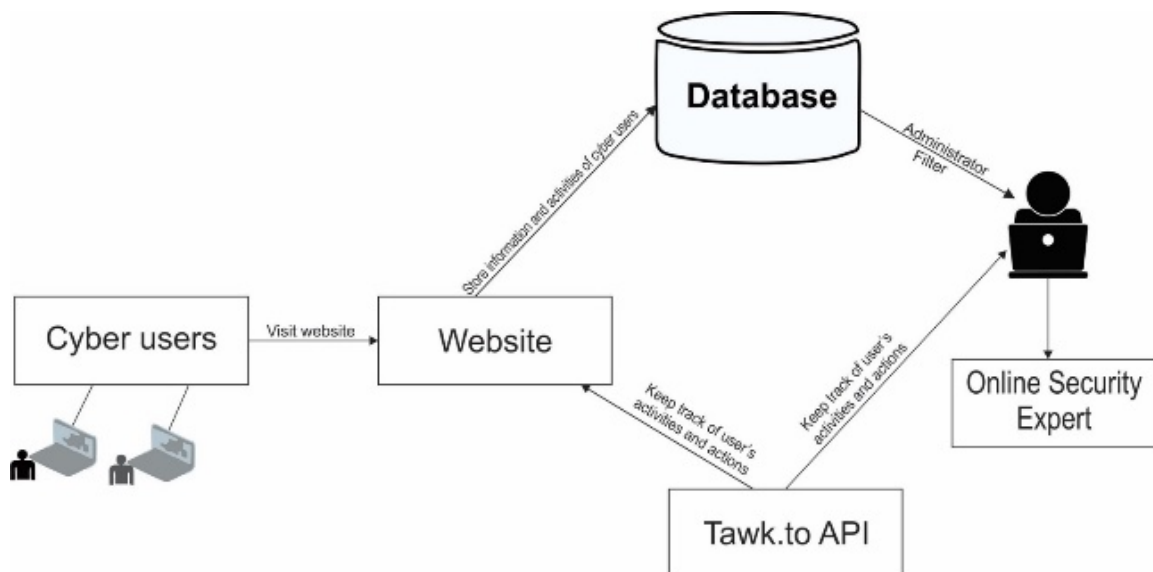


Figure 1: System Architecture

#### A. Research Method

The research methods adopted in this study are as follows:

1. Software Development: A navigable and usable website is developed using WordPress development tools and PHP is used as the programming language. MySQL database is integrated into the website for storage of information of users that visit the website. Tawk.to is integrated into the website for proper monitoring.
2. Experiment: In this phase, all the components of the system are tested to ascertain the aim of the study.
3. Evaluation: The System Usability Scale is adopted for the evaluation performance of the system. It is a standardised survey-based method for the assessment of perceived usability. The questionnaire is distributed to twenty (20) participants to get their feedback about the functionality of the system. The usability of a system takes the level of satisfaction, effectiveness and efficiency into consideration. While the usability test is carried out because of the user, the outcome of the test is focused on the system and not the user (Sakpere *et al.*, 2017).

### IV. IMPLEMENTATION

A temporary website is designed and hosted online which serves as the platform to be monitored. The monitoring dashboard is launched which pops up a login page. On the login page, the administrator enters a username and password to gain access to the system. The administrator was able to view two users on the website and the actions they are carrying out while online. The system was able to capture the location of the users and the Media Access Control address of the system used, and any suspected user would be immediately banned from the website. The website is developed to serve as a platform in which the activities would be easily monitored. It is structured in four categories to present information about:

- Cybercrime Monitoring System
- Monitor Control Login
- WordPress Admin
- Developer



Figure 2: The research website

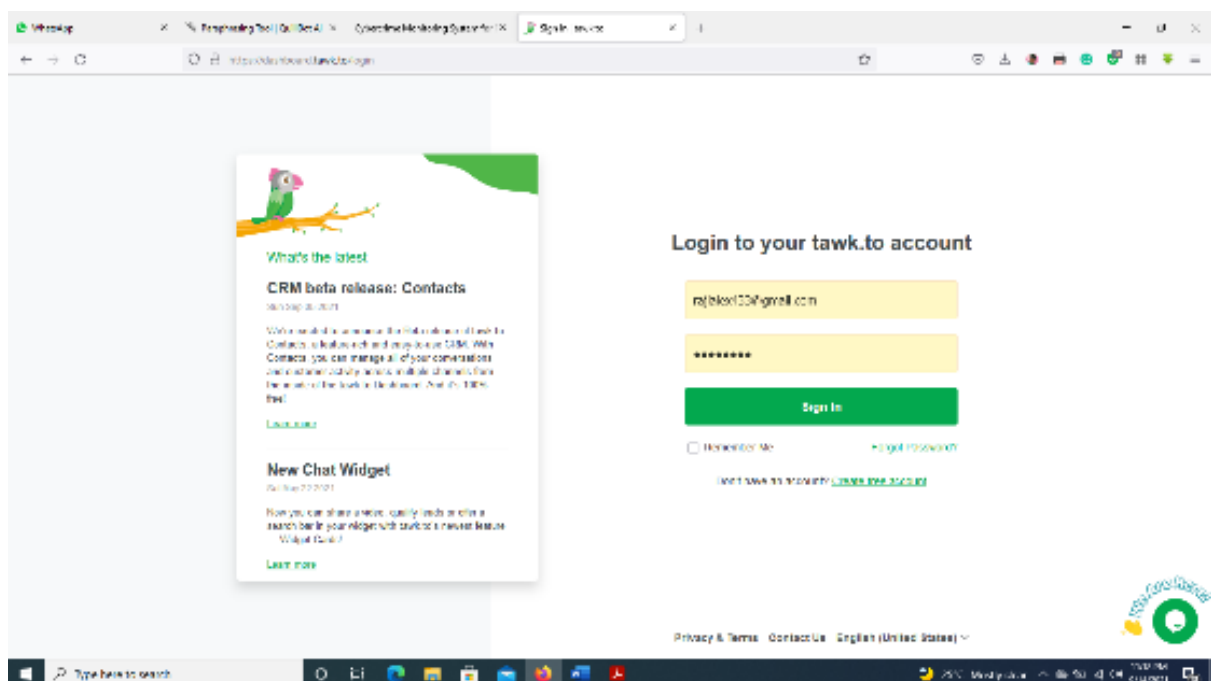


Figure 3: Cybercrime Monitoring Dashboard Login Portal

The Cybercrime Monitoring Dashboard Login Portal as shown in Figure 3, is the screenshot system login page. The login page contains two basic and necessary information, the username and password to have access to the system. The

username is the name of the administrator or any user authorised or allowed to gain access to the application, while the password is used to verify the identity of the user during the authentication procedure.

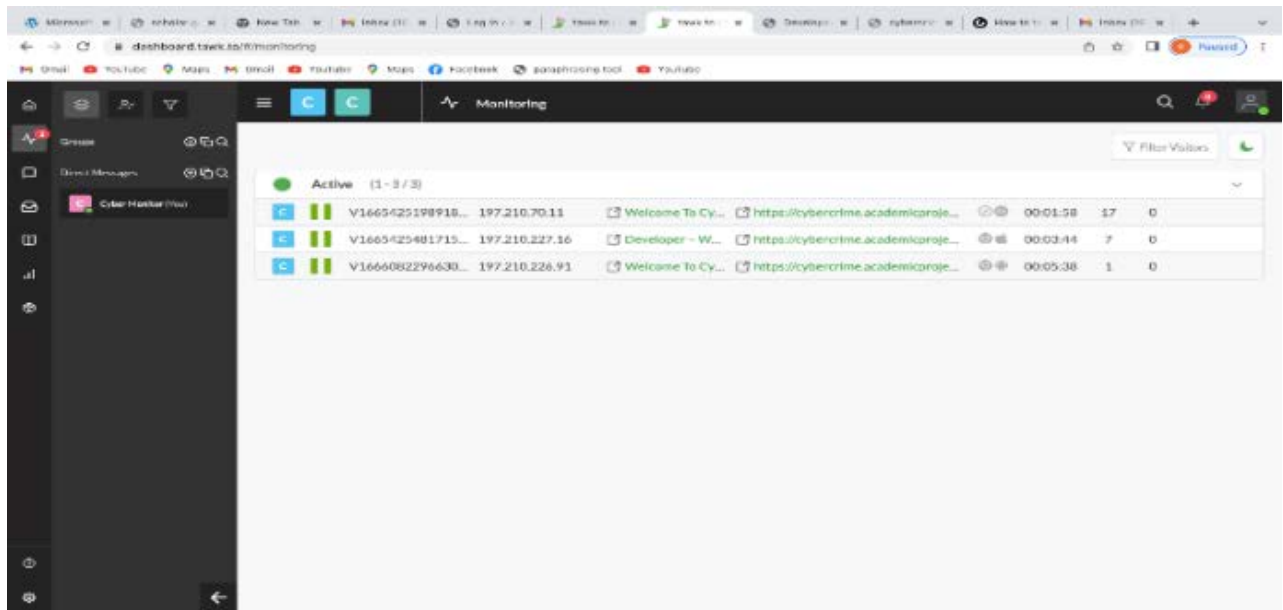


Figure 4: Three users detected on the Monitoring System

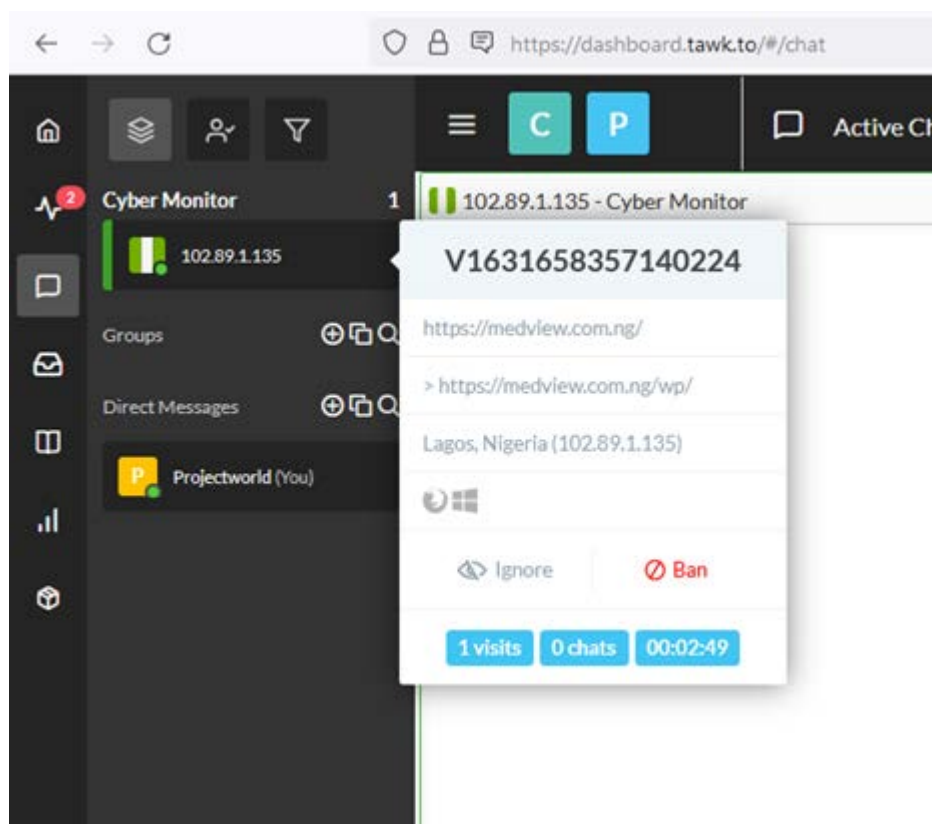


Figure 5: User Location and IP Address Detected

Three users were detected on the monitoring system as shown in Figure 4, the administrator was able to view three users on the website and the actions they are carrying out while online. Screenshot of the User Location and IP address detected as shown in Figure 5. The system was able to capture the location of the users and the Media Access Control address of the system used, and any suspected user would be immediately barred from the website.

## V. EVALUATION

Software testing is an inspection done to tell stakeholders about the calibre of the software product or service that is

being tested. Product testing can also give an objective, unbiased impression of the software, enabling the business to recognise and understand the risks related to the adoption of software. The testing technique is the act of running a programme or application to find software bugs (errors or other problems) and confirm that the software is suitable for usage (Cayola & Macías, 2018). After the completion of the system, Unit testing was carried out to check the functionality of each component of the system to know if the component is integrated as planned. The whole system testing was done when all the modules had been successfully integrated and tested. System testing made sure that the requirements and design complied.

### A. Performance Evaluation

The performance evaluation of the system is done using System Usability Scale (SUS). SUS is a standardised questionnaire-based method for the assessment of perceived usability. It has proven to be quick but not dirty (Lewis, 2018). SUS was developed by John Brooke in the year 1996. It demonstrated how urgently the usability community needed a tool to get consumers' subjective ratings of a product's usability (Bangor *et al.*, 2008).

### B. Evaluation using the System Usability Scale

The evaluation questionnaire was given to twenty (20) participants to get their feedback about the usability of the application. SUS is used to determine the level of satisfaction, effectiveness and efficiency. SUS consists of ten (10)

standardised questions based on a 4-point Likert Scale where Strongly Disagree = 1, Disagree = 2, Agree = 3, and Strongly Agree = 4.

SUS uses a complex scoring system because it comprises five (5) positive odd-numbered questions and five (5) negative even-numbered questions. SUS score =  $(X + Y) * 2.5$ , where X = Add up the total score of all odd-numbered questions then subtract 5.

Y = Add up the total score of all even-numbered questions then subtract from 25.

$$\text{Average} = \frac{\sum \text{of all SUS Scores}}{\text{Number of Participants}}$$

### C. SUS Scores for Participants of the Cybercrime Monitoring System

Table 1: SUS Score for Users of the Cybercrime Monitoring System Using 4-Point Likert Scale

Users	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	SUS Score	NPS
1	4	1	3	1	3	1	4	1	4	1	87.5	Promoter
2	4	1	4	2	4	2	4	2	4	1	80.0	Passive
3	4	1	3	2	4	2	4	1	4	1	80.0	Promoter
4	3	1	4	2	4	1	4	1	4	1	82.5	Promoter
5	4	1	4	1	4	1	4	1	4	1	87.5	Promoter
6	4	1	4	2	4	1	3	1	3	2	77.5	Passive
7	4	1	4	1	4	1	4	1	4	1	87.5	Promoter
8	4	2	4	1	4	2	4	1	4	1	82.5	Promoter
9	3	1	4	2	4	2	4	2	4	2	75.0	Passive
10	4	1	3	2	3	1	4	2	3	2	72.5	Passive
11	4	2	4	2	3	1	4	1	4	2	77.5	Passive
12	3	1	4	2	4	2	3	2	4	1	75.0	Passive
13	4	2	4	1	4	2	4	1	4	1	82.5	Promoter
14	3	1	3	1	4	2	4	2	3	1	75.0	Passive
15	4	1	4	1	3	1	3	1	4	2	80.0	Promoter
16	4	1	3	2	4	1	4	1	4	1	82.5	Promoter
17	4	1	3	1	4	1	4	1	4	1	85.0	Passive
18	4	1	4	1	4	2	4	1	3	1	82.5	Promoter
19	3	1	4	1	4	1	4	2	4	1	82.0	Promoter
20	3	1	4	1	4	1	4	1	4	2	82.5	Passive

User 1 = 87.5, User 2 = 80.0, User 3 = 80.0,  
 User 4 = 82.5, User 5 = 87.5, User 6 = 77.5,  
 User 7 = 87.5, User 8 = 82.5, User 9 = 75.0,  
 User 10 = 72.5, User 11 = 77.5, User 12 = 75.0,  
 User 13 = 82.5, User 14 = 77.5, User 15 = 80.0,  
 User 16 = 82.5, User 17 = 85.0, User 18 = 82.5,  
 User 19 = 85.0, User 20 = 82.5

Sum of all SUS Scores for all Participants = 87.5 + 80.0 + 80.0 + 82.5 + 87.5 + 77.5 + 87.5 + 82.5 + 75.0 + 72.5 + 77.5 + 75.0 + 82.5 + 75.0 + 80.0 + 82.5 + 85.0 + 82.5 + 82.0 + 82.5 = 1617

$$\text{The Average SUS score} = \frac{1617}{20} = 80.9$$

$$\text{Average} = \frac{\sum \text{of all SUS Scores}}{\text{Number of Participants}}$$

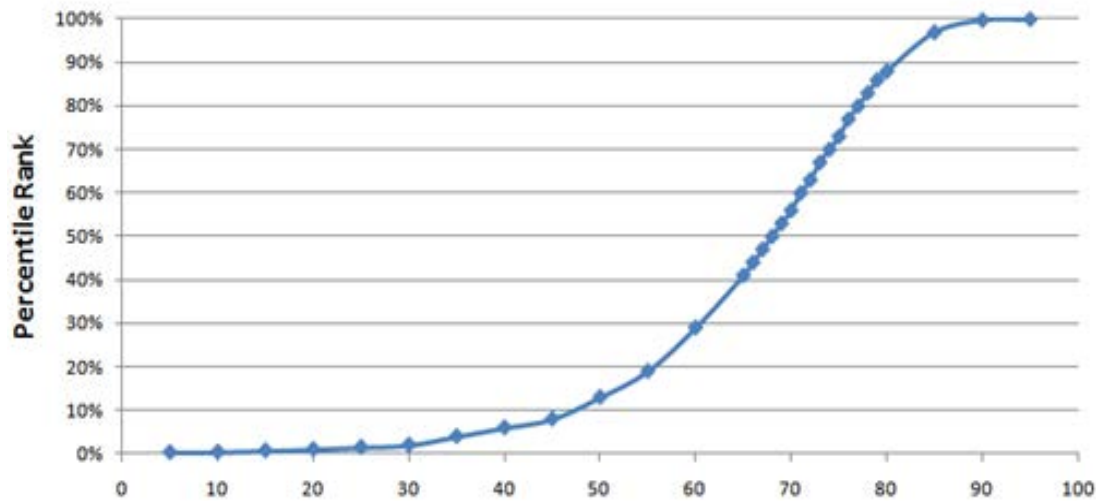


Figure 6: Percentile Ranking for Common SUS Scores

Table 2: Percentiles, Grades, Adjectives, and NPS Categories to Describe Raw SUS Scores

Grade	SUS	Percentile Range	Adjective	Acceptable	NPS
A+	84.1 – 100	96 – 100	Best Imaginable	Acceptable	Promoter
A	80.8 – 84.0	90 – 95	Excellent	Acceptable	Promoter
A-	78.9 – 80.7	85 – 89		Acceptable	Promoter
B+	77.2 – 78.8	80 – 84		Acceptable	Passive
B	74.1 – 77.1	70 – 79		Acceptable	Passive
B-	72.6 – 74.0	65 – 69		Acceptable	Passive
C+	71.1 – 72.5	60 – 64	Good	Acceptable	Passive
C	65.0 – 71.0	41 – 59		Marginal	Passive
C-	62.7 – 64.9	35 – 40		Marginal	Passive
D	51.7 – 62.6	15 – 34	OK	Marginal	Detractor
E	25.1 – 51.6	2 – 14	Poor	Not Acceptable	Detractor
F	0 – 25	0 – 1.9	Worst Imaginable	Not Acceptable	Detractor

#### D. Usability Evaluation

The normalisation of System Usability Scale (SUS) scores to obtain percentile ranking makes the scores relevant.

The raw and mean SUS score is 80.9 for the cybercrime monitoring system. It was normalised to a percentile ranking of 90. The percentile rank of 90 for the System was interpreted to be grade A. This indicates that the system was excellent and acceptable, and the users were promoters. Users won't dissuade others from utilising the proposed system as shown above.

#### E. Comparative Evaluation Analysis

The system has undergone a comparative analysis to determine its functionality, which is documented in Table 3; the graphical analysis of the system is shown by the bar chart in Figure 7. The study was compared with the Initial System and the result shows that the cybercrime monitoring system has an edge over the existing system.

4	82.5	80.0
5	87.5	72.5
6	77.5	77.5
7	87.5	70.0
8	82.5	70.0
9	75.0	72.5
10	72.5	77.5
11	77.5	80.0
12	75.0	75.0
13	82.5	70.0
14	75.0	72.5
15	80.0	77.5
16	82.5	70.0
17	85.0	72.5
18	82.5	70.0
19	82.0	75.0
20	82.5	80.0

Table 3: SUS Score for Cybercrime Monitoring System

Users	SUS Score (CMS)	SUS Initial System
1	87.5	70.0
2	80.0	72.5
3	80.0	75.0

From the result in Table 3, the raw and mean SUS score is 80.9 for the cybercrime monitoring system. It was normalised to a percentile ranking of 90. This indicates that the system was excellent and acceptable, and the users were promoters. The users will not deter others from utilising the proposed system while the mean SUS score for the initial system is 75.25 and was normalised to a percentile ranking of 72. This indicates

that the system was acceptable and the users were passive. The system's users will deter others from utilising it.

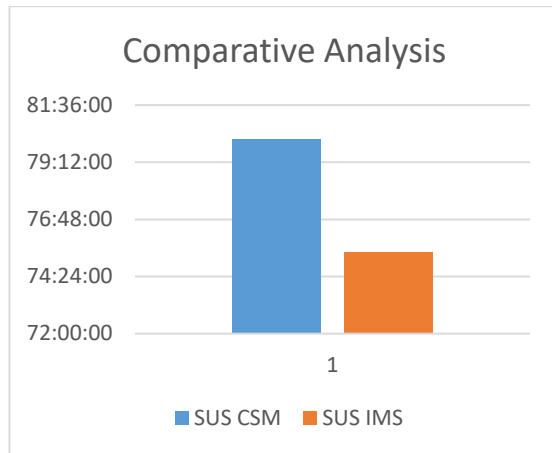


Figure 7: Graphical Representation of the Comparative Analysis

## VI. CONCLUSION

Cyber security is a continual process that must be updated regularly. Network defenders are continuously fighting back as new applications and cybercriminals find and exploit new weaknesses in computer programmes and systems. The underlying ideas behind physical and general security also apply to cyber security. An evaluation of vulnerability kicks off the procedure. Risk evaluation, threat identification, findings documentation, and action plan development are all parts of vulnerability assessment. The vulnerability of the internet is one of the most serious threats to cyber security. Due to the use of email, online browsers, and other technologies, any web-based system has serious security problems. Governments across the world keep massive amounts of personal data and records on their residents, as well as sensitive government secrets, making them easy targets. Despite this, many government institutions face challenges such as inadequately secured infrastructure, a lack of awareness, and competing budget and resource objectives. Better security enables government agencies to deliver dependable services to the public, maintain citizen-to-government communications, safeguard sensitive information, and defend national security. Taking into consideration the increase in the rate of crimes using computers, one has to take every security measure to protect his cyberspace. This study contributes theoretically to the existing body of knowledge through a more extensive understanding of emerging technologies, with potential for future research. In addition, the system was executed at a minimal cost and reduces the difficulty of integrating a monitoring system into a website that will make individuals, organisations and government agencies find it easier to protect their websites effectively.

## VII. SUGGESTED AREAS FOR FURTHER RESEARCH

This work has been able to accomplish its objectives with certain observations noted. For future studies, the points below are proposed.

1. To combat cybercrime, you need to establish a special "cybercrime police" and train them on the use of information technology in cybercrime.
2. Cybersecurity education should be implemented at all

levels of education to educate Internet users and their outlook on the threats they may face when using the Internet.

3. Developers of hardware and software should provide technical remedies for typical cyber concerns in their new products.
4. All websites should include monitoring software for security checks against threats so that cyber police can identify and arrest criminals.
5. Organisations need to take strict security measures to protect their digital data.

## REFERENCES

- Agana, M. A., & Inyama, H. C. (2015). Cyber crime detection and control using the cyber user identification model. *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS)*, 5(5), 354–368.
- Aiken, M., Farr, R., & Witschi, D. (2022). Cyberchondria, coronavirus, and cybercrime: A perfect storm. In H. Aker & M. Aiken (Eds.), *Handbook of Research on Cyberchondria, Health Literacy, and the Role of Media in Society's Perception of Medical Information* (pp. 16–34). IGI Global. <https://doi.org/10.4018/978-1-7998-8630-3.ch002>
- Ba, Y. (2017). *Understanding cybercrime and developing a monitoring device*. Bachelor's Thesis, Turku University of Applied Sciences.
- Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An empirical evaluation of the system usability scale. *International Journal of Human-Computer Interaction*, 24(6), 574–594. <https://doi.org/10.1080/10447310802205776>
- Cayola, L., & Macías, J. A. (2018). Systematic guidance on usability methods in user-centered software development. *Information and Software Technology*, 97, 163–175. <https://doi.org/10.1016/j.infsof.2018.01.010>
- Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, 36(2), 346–357. <https://doi.org/10.1016/j.giq.2018.09.007>
- Eddolls, M. (2016). Making cybercrime prevention the highest priority. *Network Security*, 2016(8), 5–8. [https://doi.org/10.1016/S1353-4858\(16\)30075-7](https://doi.org/10.1016/S1353-4858(16)30075-7)
- Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. *IEEE Access*, 10, 11065–11089. <https://doi.org/10.1109/ACCESS.2022.3142508>
- Kalakuntla, R., Vanamala, A. B., & Kolipyaka, R. R. (2019). Cyber Security. *HOLISTICA – Journal of Business and Public Administration*, 10(2), 115–128. <https://doi.org/10.2478/hjbpa-2019-0020>
- Lewis, J. R. (2018). The system usability scale: Past, present, and future. *International Journal of Human-Computer Interaction*, 34(7), 577–590. <https://doi.org/10.1080/10447318.2018.1455307>
- Mihai, I.-C. (2017). *Procedure for detecting cybercrime activities on websites*. Master's Dissertation, European Union Agency for Law Enforcement Training.

- Paul, P. K., & Aithal, P. S. (2018). Cyber crime: Challenges, issues, recommendation and suggestion in Indian context. *International Journal of Advanced Trends in Engineering and Technology*, 3(1), 59–62. <https://doi.org/10.5281/zenodo.1171079>
- Prakash, F., Sadawarti, H. K., & Baskar, K. (2019). Cyber crime: Challenges and its classification. *International Multi-Disciplinary Academic Research Conference (IMARC-2019)*, 1–3.
- Rogers, M. K., & Seigfried, K. (2004). The future of computer forensics: A needs analysis survey. *Computers and Security*, 23(1), 12–16. <https://doi.org/10.1016/j.cose.2004.01.003>
- Sadiku, I. B., Ajayi, W., Sakpere, W., John-Dewole, T., & Badru, R. A. (2022). Effect of traditional and software-defined networking on performance of computer network. *Scientific Journal of Informatics*, 9(2), 111–122. <https://doi.org/10.15294/sji.v9i2.31315>
- Sakpere, W. E., Mlitwa, N. B. W., & Oshin, M. A. (2017). Towards an efficient indoor navigation system: a Near Field Communication approach. *Journal of Engineering, Design and Technology (JEDT)*, 15(4), 505–527. <https://doi.org/10.1108/JEDT-10-2016-0073>
- Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., & Dehghantanha, A. (2020). Threats on the horizon: Understanding security threats in the era of cyber-physical systems. *Journal of Supercomputing*, 76, 2643–2664. <https://doi.org/10.1007/s11227-019-03028-9>



Editorial

---

# Face Recognition-based Intelligent System for Effective Students' Class Attendance (FARBSAS)

---

Olagunju Korede Solomon

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Olagunju, K. S. (2023). Face Recognition-based Intelligent System for Effective Students' Class Attendance (FARBSAS). In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 19-27). Ibadan. <https://doi.org/10.5281/zenodo.8121058>.

# Face Recognition-based Intelligent System for Effective Students' Class Attendance (FARBSAS)

Olagunju Korede Solomon

University of Ibadan and National Open University of Nigeria,  
Nigeria

solomonkore09@gmail.com

**Abstract:** Students' class attendance is considered very important in many higher institutions of learning. However, some institutions' current system for determining students' attendance has certain loopholes. The current system enables the practice of impersonation, does not curb lateness to class effectively and the present attendance model is not designed to capture attendance in the real sense of it. This article aims to provide a solution to the identified problems by proposing an effective student class attendance system using a prototype called Facial Recognition-Based Students' Attendance System (FARBSAS). Face recognition technology is a type of biometric technology that is emerging in the modern world. The method used to gather data includes a survey to determine students' and lecturers' views of the current attendance system. A survey conducted on 45 students and 11 lecturers from the Department of Computer Science, University of Ibadan (UI) shows that there is a need to change the existing students' class attendance model.

**Key Words:** Attendance model, facial recognition, biometrics

## I. INTRODUCTION

"Attendance is usually considered to reflect students' level of engagement with their course and to be critical to student success..." says Moores *et al.* (2019). Basically this 'engagement with course' is done when students are physically present during a class session to learn. Some lecturers ensure that the students write their names and details on a sheet of paper that must be passed around for the students to provide proof that they were physically present in the class. Sutabri *et al.* (2019) described this pen-and-paper method of conducting the student attendance system in Indonesia that is similar to what is being done in many universities in Nigeria and India (Patel & Priya, 2014). In fact, the physical presence of students in the class had been considered so important that a lecturer quoted what a student wrote saying: "As long as you don't fall asleep, you will be alright" (Dirk, 2010). But we need to readjust this thinking because there is a big difference between being physically present in the class and being actively present in the class.

Fagbenle and Elegbeleye (2014) referred to the definition of attendance as "...not merely being bodily present but including actual participation in the work and activities of the school". This definition clearly defines attendance in a way that captures the purpose of students' attendance in the real sense. To fulfil the purpose of class attendance for students, being physically present is only the beginning of the process. When the combination of students' physical presence and their participation in the class had been recorded, then students' attendance had been taken. After all the actual essence of being in the class is to acquire knowledge and

understanding. Students that practice this type of attendance are the ones that can transform acquired knowledge into solutions which can be scientifically, technically and effectively used to transform society. This is what class attendance should constitute.

## II. LITERATURE REVIEW

Some have the view that a compulsory attendance policy in higher institutions is not the way to go. St. Clair (1999) holds a position against class attendance based on factors that she built on Pintrich's theoretical model of motivation. The position is that, while many have provided some methods of constructing empirical results in finding out whether class attendance has a positive impact on student performance or not, and have largely favoured the conclusion that it does, they did not factor in the importance of student motivation in determining their results. Büchele (2021) also alludes to the fact that prevalent findings and results show that there is a positive correlation between students' class attendance and performance. However, he also holds a contrary view. He says that these findings are usually poorly conducted and would be considered to have been based on weak grounds. Yet on a positive note, he concluded by mentioning that "cognitive engagement partly and behavioural engagement fully mediated the link between attendance and performance". In a nutshell, while motivation needs to be considered as St. Clair pointed out, and cognitive engagement of the students and their behavioural engagement are important as postulated by Büchele, it can only be said that the importance of student's attendance has not been ruled out completely. Quite frankly, the argument does not seem to be about students' attendance, as much as it reflects a stand against administrative policies that demand students' attendance, and in some instances, even grade students based on their attendance performance. So, should the school administration make student attendance compulsory?

Moores *et al.* (2019) provided what can be called an all-angle perspective on various given answers. While some have the opinion that compulsory policies asserted by school administration need not be enforced, with their points raised, the irresistible and irrevocable positions of writers who favour the idea that school authority should make student attendance compulsory are too germane that they cannot be denied.

If one thinks about it, what is the point of the class timetable, if students are not expected to be in the class? What is the point of having class-based schools, if students do not come to class but only show up on the examination day and they eventually have high scores? What is the point of school in which students can learn by themselves and teach themselves by themselves? What is the point of paying school fees or

funding education if students can do as they like without any proper administrative policy on their class attendance? What is the point of graduating students based on character and academic performance when the only way to determine their cognitive strength is by the examination they passed? Is school all about passing examinations? Obviously, the main reason why there is various divergence of opinions anchors on the current understanding of class attendance that focuses mainly on students' physical presence in the class. This forms a major reason why our current understanding of school attendance needs to be modified and properly aligned with the current reality.

#### A. Related Works

The reality is that many academic projects and works of literature are giving attention to the deployment of biometrics as a way to improve the management of students' attendance systems. In fact, various designs and developments of software had been done. In Nigeria, Okokpuije *et al.* (2017) developed a biometric attendance system using iris recognition technology for student attendance. The main aim is to eliminate the issues of forgery and impersonation. A very good part is that it is a web-based application. Isinkaye *et al.* (2020) developed an Android-based face recognition system for attendance and malpractice control. Their focus was to curtail examination malpractices as it also checks whether a student's attendance record qualifies him or her to sit for the examination. In India, Verma and Gupta (2013) developed a fingerprint-based recognition technology for the student attendance system. This requires the use of an external device called a fingerprint scanner as well the use of a mobile phone to allow parents to monitor the attendance activities of the students. In China, some students also developed a voice recognition-based system for student attendance (Uddin *et al.*, 2016). One good aspect of their work was that they integrated the lecturer's interface into the system. Sunaryono *et al.* (2021) also developed a face recognition-based attendance system in which the students can use their Android

smartphones to connect to the school Wi-Fi in an intranet system. The purpose was to ensure that students who are not on campus will not be able to forge attendance and they allow for quick response (QR) codes generation in addition to their face recognition system.

Quite notably, all the aforementioned projects are good works. However, they have their main focus on the physical presence of students in the class. It is important to understand that the main crux of the issue is not just the management of the physical presence of the students in class. The implementation of an attendance system that will recognize the amalgamation of the physical presence of the students and their class activities as attendance is the way to go. This is the focus of this article.

The choice of using a face recognition system instead of the other options mentioned earlier is based on the considerations that it is less costly to implement (Kawaguchi *et al.*, 2005), convenient to use for the students and face detection can be done from a distance. In a simple description, face recognition is based on computer vision technology whereby facial features are analysed for identification. Basically, three important actions must be taken by the computer: face detection, feature extraction and face recognition matching in the database.

### III. METHODOLOGY

A survey was conducted among 45 students and 11 lecturers in the Department of Computer Science at the University of Ibadan (UI) to determine their view of the current pen and paper-based students' attendance system and their view of the adoption of the use of face-based recognition technology instead. The survey was done by issuing a questionnaire to the participants through an online Google document. The questions asked and the result of the survey is as shown in Table 1.

Table 1: Responses from 45 Students and 11 Lecturers at the University of Ibadan towards the current attendance system and adoption of a face-based recognition system for attendance

QUESTIONS	YES	NO
Do you consider the pen-and-paper method of taking class attendance as effective or outdated?	60% say Outdated	40% say Effective
Do you consider the percentage of a student's class attendance as an effective measure to determine a student's level of understanding of a course and the ability to transfer the acquired knowledge into the solution domain?	20%	80 %
Do you think that an attendance system that incorporates scores for a student that attended a class and stayed in the class all through can be called an effective class attendance system?	55.6%	44.4%
Do you think that an attendance system that incorporates features like class performance, short presentations, group work or product development can boost students' sense of value for the course of study?	100%	0%
Do you think that an attendance system that awards scores for class participation, presentation, group work or product development can demonstrate a reason to conclude that no student will fail the course as long they are active in class?	66.7%	33.3%
Do you think that using software that can capture your face to take class attendance for you is an effective model or undesirable model?	80%	20%

The result of the survey shows that there is a need to change the way the attendance system is currently being conducted in some higher institutions. There is a need to redefine attendance and instead of continuing the archaic pen-and-paper attendance system, the emergence of biometric technology can provide a better approach to the exercise.

As discussed by Abdulrahman and Alhayani (2023), biometric technologies are gaining popularity in various human endeavours as a way to do human identification and verification by deploying the technology in many ways. Some of these ways include iris recognition, fingerprint recognition, face recognition, and signature, among others. Abdulrahman and Alhayani write further that “face recognition can be considered as a standout amidst the most fruitful biometric discernible verification methods ...”. This expression forms a major factor that influenced the choice of selecting face recognition technology for this study to conduct students’ attendance system.

The article uses the Use Case diagram to provide a system design to explain the features of the proposed face recognition software. An activities diagram is also used to present the flow of actions and activities within the proposed attendance model. The desktop software version of the face recognition software prototype called FARBSAS was developed using Swing in Java programming language,

OpenCV library for face recognition technology and MySQL Workbench 8.0 for relational database management system. OpenCV is a large open-source library that is used for image processing, computer vision, and machine learning.

#### IV. RESULT

A digital system that can use facial recognition technology to take class attendance for students and track their performance in class is here proposed. The software application is called FARBSAS (Face Recognition-Based Software for Student Attendance System). It would be installed on students’ smartphones or computers or tablets. The students will launch the application when they enter a class, input their access details, select the course code from the menu option, click on the “Attendance” button and the camera of the phone or computer must be actively on until the end of the class session. When the class is over, the application can be stopped, and the attendance for a particular course on a particular day would be recorded. The student can save the feedback in printable formats.

The Activity Diagram in Figure 1 shows how the FARBSAS app that is developed for the students is designed to carry out a series of actions. The Use Case diagram in Figure 2 also shows how the students will interact with the FARBSAS app designed for them.

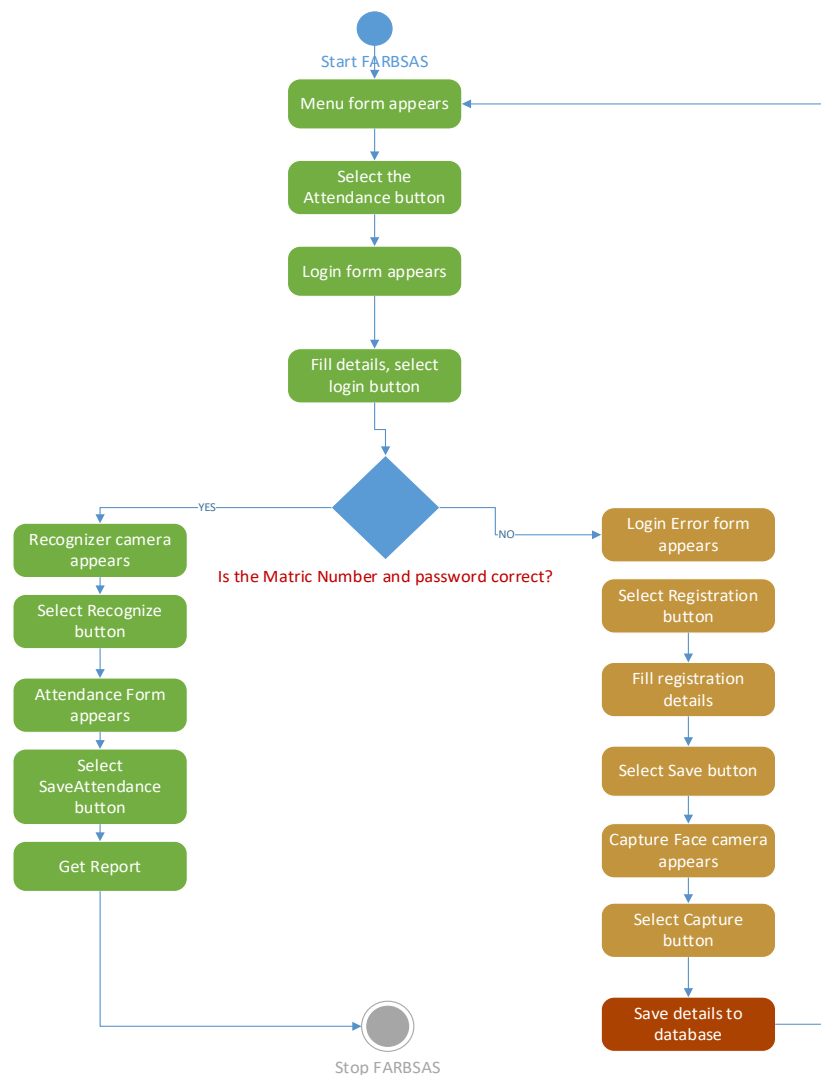


Figure 1: Activity Diagram showing the activities and actions that would be performed by FARBSAS

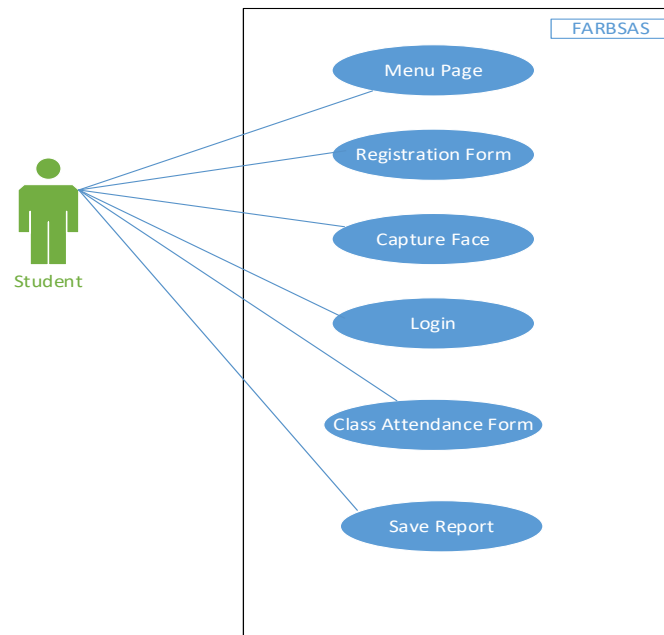


Figure 2: Use Case Diagram showing how the student will use the features of FARBSAS

#### A. Structure of FARBSAS Network

FARBSAS is structured in a way that allows the lecturer and students to interface through their smart devices for attendance-taking. Firstly, the lecturers have their separate graphical user interface (GUI) where they will start a server, a simple server socket, that will listen on protocols for clients to be attached to it. Clients in this instance refer to the students' devices. So, when the students start their GUI, they will select the Attendance button from their application's Main Menu. This will trigger Login GUI. After the students input their Matriculation Numbers and Password, then the student device can connect to the lecturer's server. The lecturer will be able to see all connected devices. This first stage of FARBSAS operation is entirely based on Network architecture as described in Figure 3 below. Of course, there is also database connectivity at the student login menu as can be seen in Figure 6. This means that FARBSAS had already

provided a section where students can register their details and capture their faces. You will see this Register GUI section in Figure 9.

#### B. Graphical User Interfaces for FARBSAS

Figure 4 shows that the lecturers will start the server on their smart electronic devices. This will allow students to connect. The students will simply need to start FARBSAS on their smart devices, and then select the Attendance button from the main menu as shown in Figure 5. Students will then input their Matric Number and password as shown in Figure 6. If the matric number and password provided are correct, then the Attendance Form in Figure 7 will come up for the student to use face recognition to capture attendance. If the details provided by the student are not correct or one of the details is not correct, the Login Error Page (Figure 8) alert will come out.

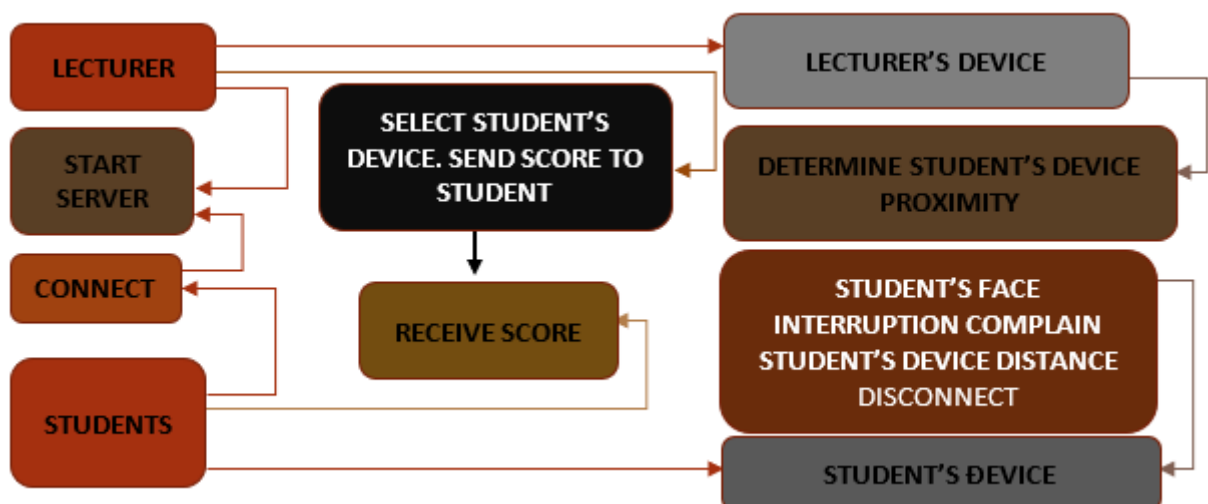


Figure 3: Network architecture between lecturer and student

Figure 4: Lecturer's interface to allow students to connect to the class and give scores to students' performance in class

The Attendance Form page (Figure 10) is the page where the student will take their attendance. Basically, this page will allow the student to select the course code that he or she is attending at the moment. Then the name of the student and the matric number as well as the date will come up automatically. The additional features that make the FARBSAS attendance system an effective model are the portions of the form where the student will indicate class performance and the lecturer will award a score. The student's attendance quality will also be tracked by ensuring that once a student's device is a distance away from the specified location coordinates set by the lecturer for all connected devices, the Leave class check box will automatically indicate a mark and the time the student leaves the class will show. If the student stays all through the class, the FARBSAS can determine this since the student's device was connected to the lecturer's set by location distance. When the class is over, the student can select Save Attendance to end the attendance process for the class. The attendance form also allows the students to indicate what they did in the class and the lecturer's score for the performance will show immediately.

Figure 5: FARBSAS Menu Page

Figure 6: FARBSAS Login Page

Figure 7: Attendance Form page

Remember that on the Login page, Figure 6, when a student types in his/her details and either one of the two options provided is wrong or the two options are wrong, then the Login Error page (Figure 8) will show up. If the student is sure that he/she had already registered, the Back button can be used to go back to the Login page to re-enter the correct details. However, if the student is only using the FARBSAS for the first time, the Menu button will allow the student to call the Registration form (Figure 9) page to able to register. When a student selects the Register button on the Login page (Figure 5), the Registration Form (Figure 9) will appear. This is the page where a student can register personal details. Then the student will select the place his face to be close to the

camera.

Figure 8: FARBSAS Login Error Page

Figure 9: FARBSAS Registration page

The Capture Face area on the Figure 9 page is the area where the student will do face capturing. The camera will turn on and a rectangular shape will appear on the face of the student on the Capture Face page. When the student selects the Capture button, the Capture Face page will count the number of grey pictures that were captured. The FARBSAS is

programmed to count 25 grey pictures. The counting will show up in the area where 00 is written. After 25 counts, the face capturing will take effect and all the details of the students that were provided in the Registration Page (Figure 9) will be saved into the database along with the face.

Figure 10: Output for a student's class performance

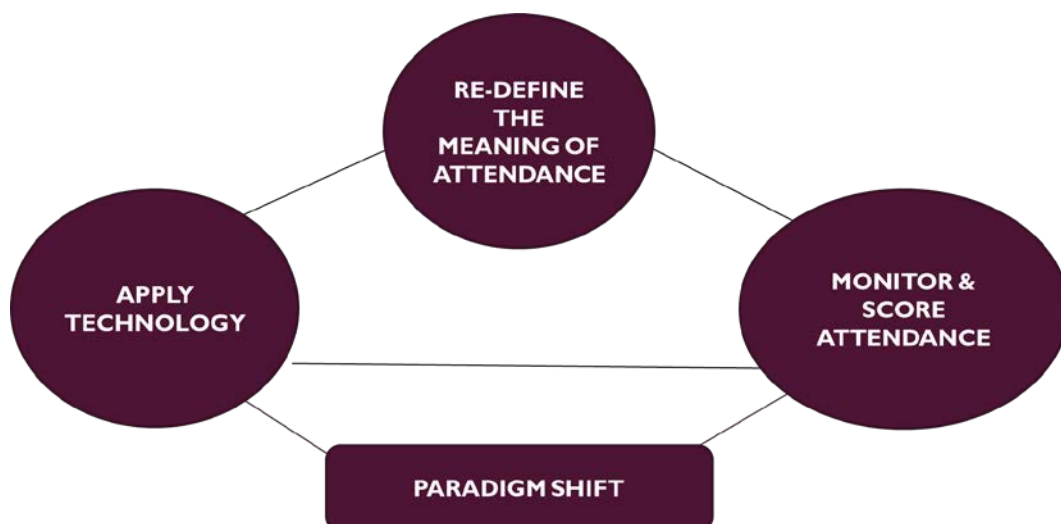


Figure 11: Three major actions to achieve effective students attendance

Figure 10 shows how to capture a student's class performance beyond being merely physically present in the class. This output will capture what a student did in the class; it could be an oral presentation of a project or assignment or group presentation that needs to be defended in the class, and it could also be actual project work that the lecturer required the students to carry out and any other activities that were

idealized to ensure that students participate while they attended class. The lecturer can award a score for each attribute of the student. Some of the attributes of the student could be the ability to explain the subject, good writing skills, neat presentation and even the ability to implement concepts into products as they may relate to the course of study.

Students can see the output per class session and be able to develop anticipation for success. The scores awarded for each class will help a student to have feedback on areas for improvement and areas of strength. This can even help in developing interest in certain skills that a student may eventually turn into an economic development of the society.

## V. DISCUSSION

Based on the result of the survey carried out in Table 1, it can be deduced that there is a need to carry out three important activities which will lead to a complete paradigm shift in the way we currently conduct student attendance. Figure 11 gives a summary of the proposed activities that can produce an effective student attendance paradigm shift. Redefining our current understanding of student attendance will help to shift focus beyond our present views that had been fixated only on the physical presence of students in the classroom. Indeed, defining attendance in a way that includes students' physical presence and their class performances during a class session will reflect the purpose of learning and reposition the educational system in the light of being the productive institution that they are supposed to be.

Monitoring and scoring attendance will also provide a motivational factor for students to realize the value of the institutional policy regarding attendance regulations. The scoring of attendance will boost the participatory level of students in the classes. As FARBSAS has shown, a student who failed to attend a class, or left the class uncompleted for frivolous reasons can readily assess and accept the consequences of such actions. FARBSAS also shows that it is important to redesign students' participation in such a way that the abilities of students will manifest, earn them progress and be nurtured. By this, a student who is gifted in oral presentation can grow their ability, those that are stunning in writing skills will also grow their gift, other students who may be very good in the practice can demonstrate their own and others who may be very good in answering questions in the examinations can also grow their abilities. This is very important because people have various abilities. Hence an attendance system that put these peculiarities into consideration will reduce the failure rate and may even reduce out-of-school issues in society. Using technology to drive these initiatives will take away the pen-and-paper process that is slow, boring and even archaic. One of the best-known technologies is the use of a face recognition system.

## VI. CONCLUSION

An attendance system that goes beyond focusing on physical presence is needed for students' attendance. Hence, the amalgamation of physical presence and the class work that students are expected to do, are the combinations that form effective class attendance. It is only when a student does not fulfil this kind of attendance system that it can be concluded that the student is not teachable and so cannot be considered to sit for the examination. This paradigm shift can do more good in attaining the overall purpose of the educational system so that more employable and capable problem-solving students would be produced in higher institutions of the modern age.

Of course, there will be a need to review the ratio of lecturers to students. This is important because, in a situation where a lecturer is teaching a large number of students, it would be

difficult or unrealistic to expect a quality attendance system. But when attention is given to a proper proportion of students by a lecturer, excellent output can be achieved.

It is also important to ensure that there are ports where students would be able to charge their smart electronic devices. FARBSAS can still be scaled up to include features whereby lecturers can load questions for students as assignments, create groups for students to assign short works to them and award scores for students at a later time other than class period to allow for flexibility and ease of labour for them.

## REFERENCES

- Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, 80(3), 2642–2646. <https://doi.org/10.1016/j.matpr.2021.07.005>
- Büchele, S. (2021). Evaluating the link between attendance and performance in higher education: The role of classroom engagement dimensions. *Assessment and Evaluation in Higher Education*, 46(1), 132–150. <https://doi.org/10.1080/02602938.2020.1754330>
- Dirk, K. (2010). "I hope it's just attendance": What does participation mean to freshman composition students and instructors? *Composition Studies*, 38(1), 88–107.
- Fagbenle, A. O., & Elegbeleye, A. O. (2014). Attendance dilemma and its effects on the academic performance of secondary schools' students in Osun State, Nigeria. *International Journal of Humanities Social Sciences and Education (IJHSSE)*, 1(4), 13–20.
- Isinkaye, F. O., Soyemi, J., & Arowosegbe, O. I. (2020). An Android-based face recognition system for class attendance and malpractice control. *International Journal of Computer Science and Information Security (IJCSIS)*, 180(1), 78–83.
- Kawaguchi, Y., Shoji, T., Lin, W., Kakusho, K., & Minoh, M. (2005). Face recognition-based lecture attendance system. *The 3rd AEARU Workshop on Network Education*, 65–69.
- Moore, E., Birdi, G. K., & Higson, H. E. (2019). Determinants of university students' attendance. *Educational Research*, 61(4), 371–387. <https://doi.org/10.1080/00131881.2019.1660587>
- Okokpuije, K. O., Noma-Osaghae, E., Okesola, O. J., John, S. N., & Robert, O. (2017). Design and implementation of a student attendance system using Iris biometric recognition. *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, 563–567. <https://doi.org/10.1109/CSCI.2017.96>
- Patel, U. A., & Priya, S. (2014). Development of a student attendance management system using RFID and face recognition: A review. *International Journal of Advance Research in Computer Science and Management Studies*, 2(8), 109–119.
- St. Clair, K. L. (1999). A case against compulsory class attendance policies in higher education. *Innovative Higher Education*, 23(3), 171–180. <https://doi.org/10.1023/A:1022942400812>
- Sunaryono, D., Siswantoro, J., & Anggoro, R. (2021). An android based course attendance system using face recognition. *Journal of King Saud University* -

- Computer and Information Sciences*, 33(3), 304–312.  
<https://doi.org/10.1016/j.jksuci.2019.01.006>
- Sutabri, T., Pamungkur, Kurniawan, A., & Saragih, R. E. (2019). Automatic attendance system for university student using face recognition based on deep learning. *International Journal of Machine Learning and Computing*, 9(5), 668–674.  
<https://doi.org/10.18178/ijmlc.2019.9.5.856>
- Uddin, N., Rashid, M. M., Mostafa, M. G., Belayet, H., Salam, S. M., Nithe, N. A., Rahman, M. W., & Halder, S. (2016). Development of voice recognition for student attendance. *Global Journal of Human-Social Science*, 16(1), 1–6.
- Verma, P., & Gupta, N. (2013). Fingerprint based student attendance system using GSM. *International Journal of Science and Research (IJSR)*, 2(10), 128–131.



Editorial

---

# Web-Based Payroll System for Fixed-Term Employees

---

Ajibade Olalekan A. and Sakpere Wilson

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Ajibade, O. A., & Sakpere, W. (2023). Web-Based Payroll System for Fixed-Term Employees. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 29-37). Ibadan. <https://doi.org/10.5281/zenodo.8121060>.

# Web-Based Payroll System for Fixed-Term Employees

\*Ajibade Olalekan A. and Sakpere Wilson  
Department of Computer Science,  
Lead City University Ibadan, Nigeria  
\*aoajii@yahoo.com

**Abstract:** Web-based Payroll System for Fixed Term Employees is a simple web-based attendance system that was developed for manufacturing industries. It was specifically designed to calculate the payroll of fixed-term employees whose wages were calculated based on the number of hours worked at an agreed amount paid per hour. The significance of this application is to be able to determine the actual amount to be paid to each employee devoid of cheating by making use of a biometric machine to capture the actual time employees come to work and the time they leave. Many organisations nowadays are battling for survival because of fraud perpetrated by employees. This study helps to bridge this gap by helping organisations to manage employee productivity and prevent cheating as it cannot be manipulated. The Software Development Kit (SDK) of the digitalPersona fingerprint scanner was integrated with the system using J-Query. The fingerprint scanner communicates with the system using the serial port of a computer system. Also, J-Query was made to interact with the fingerprint scanner, scan the print signature of the employee and save it in the database using MySQL. It is from the database that attendance is estimated while VB.NET and PHP were used to develop the payroll system. The System Usability Scale (SUS) was used to evaluate the program after ten respondents were sampled and given questionnaires to fill out.

**Key Words:** Attendance, Biometric, Fingerprint, Employee, Software, Payroll

## I. INTRODUCTION

The term “payroll” refers to the number of workers that get compensation from a company (R. Patra & Teja, 2023; Yulisfan *et al.*, 2021). Even though, most companies generally use the term to refer to the money that is paid to the employees or the records that shows how much each employee has collected. Payroll may also refer to the company, department, or software which is used to process paycheques and taxes or to the process of calculating and distributing employee paycheques. Processing payroll is a very important function of any business which necessitates an understanding of current regulations, detailed tax knowledge to ensure proper withholding and filing, and a highly organised system that can be relied upon to pay each employee the right amount of money. For many organisations, using payroll systems can help to mitigate stress and minimise errors.

### A. Payroll Deductions and Processing

Payroll deductions include many different items, including:

- i. Federal income taxes
- ii. Social Security taxes
- iii. State income taxes
- iv. Local tax withholdings
- v. Health insurance

Patra and Teja (2023) state that Payroll must be processed repeatedly, that is on a weekly or monthly basis and at such times, it must be accurate. Since payroll is the single largest expense for most companies, it is very important that payroll is processed in a way that is efficient and can be relied upon. There are several options for processing payroll. Processing payroll manually is an inexpensive option but can be manipulated. The Internal Revenue Service (IRS) provides tax tables used in calculating withholdings, but voluntary deductions must be figured out as well. Keeping good records, organising information, and ensuring consistent accuracy may be more difficult when payroll is processed manually. Outsourcing payroll is expensive but may save labour time and prevent errors. A payroll company will take care of all taxes and other payroll issues, ensuring that it is accurate and reliable and may also be able to help answer questions that may arise. Payroll software is a good middle-of-the-road option, affordable for most companies and simple to use so it saves some labour time. Many different payroll software options enable the selection of the amount of assistance needed with payroll. Since payroll is still taken care of in-house with payroll software, it may be easier to make changes and retrieve data, which may also be a bonus over payroll outsourcing.

### B. Employment Types

This is like an agreement between an employer and an employee. There are several ways staff can be employed, with each having peculiar arrangements for wages and leave entitlements. The different employment types include full-time employees, part-time employees, casual employees, fixed-term or contract employees, apprentices and trainees. While full-time employees work regularly for an average of 38 hours per week, part-time employees usually work less than 38 hours per week and generally have regular hours. Part-time employees receive the same wages and conditions as full-time employees on a proportionate or pro-rata basis, according to the number of hours worked. However, the conditions are different for other employees type. For example, casual employees are engaged on an irregular basis according to business demands while fixed-term or contract employees can be engaged for an agreed length of time to perform a specific task or work on a particular project or replace an employee on leave, for example. Fixed-term employees can work full or part-time and, in most cases, do not enjoy the benefits enjoyed by permanent staff. It is outsourced to a contractor who takes care of their wages and is paid either on a weekly or monthly basis.

Furthermore, apprentices and trainees are working towards a nationally recognised qualification or working towards having a certain knowledge about the job. They must be formally registered, usually through a contract between a registered training provider, the employee, and the employer. Apprentices and trainees get paid according to their award or

registered agreement. In addition, one can pay piece rates or commission payments to employees in certain circumstances. This means that they get paid based on the results they achieve instead of an hourly or weekly pay rate. This is applied majorly in sales where an employee's pay will be based on a percentage of the total number of goods sold. Requirements vary for this arrangement depending on which industrial relations system one belongs to.

### C. Attendance Timing

Most organisations across the world run a 40-hour shift/week for employees which is an 8-hour/day shift, while some run a 45-hour shift/week. Any extra hour is calculated as overtime. While some organisations run 3 shifts/day which is not quite common here in Nigeria, the majority of the organisations here run 2 shifts/day day and night. The day shift runs from 8am to 5pm and the night shift runs from 8pm to 5am. In some situations, however, workers in production lines where machines run 24 hours each day can work from 7am to 7pm while those on night shift work from 7pm to 7am. Overtime is simply an additional number of hours worked by an employee daily. If an employee is supposed to work from 8am to 5pm and such employee ended up working from 8am to 6pm, the extra one hour is overtime and any amount agreed between the employer and employee is to be paid as overtime will be paid to such employee.

This study focuses on developing a hybridised web-based biometric system for the attendance and payroll of fixed term employees in a manufacturing environment. Specifically, the study intends to develop a web-based attendance system, develop a web-based payroll system, develop a database to store the attendance and payroll systems, and integrate and evaluate the systems for robust performance. The study deals mainly with the payroll of fixed term employees in a soap manufacturing company in the south-western part of Nigeria. It does not cover permanent employees.

Due to the use of manual processes or minimal adoption of technology in attendance and payroll processing, an avenue where fixed term employees cheat employers via various means is created. For example, conniving with HR staff or with one another by helping one another to sign the attendance register when they are not at their jobs. Solving this challenge is necessary. The widespread prevalence, adoption and usage of biometrics have opened its adoption in the workplace for attendance and payroll of employees.

### D. Problem Statement

Years back, industries and institutions take attendance manually, which is time and paper-consuming, all in the process of keeping records. The first attendance machine is very simple and works by workers inserting an attendance paper or a timesheet into a machine with the time of insertion printed on the timesheet. This is also time-consuming and causes long queues while doing attendance. Also, the data on the timesheet is processed manually by HR to do Payroll. Nowadays, various automated attendance systems are used for attendance taking and even remotely. However, with the existing systems on attendance and payroll and with it not being implemented for fixed term employees, there are lots of fraudulent manipulations in some companies in Nigeria. If this is not checked, it will lead to the collapse of many organisations in a country where there is unemployment already. Hence, the need to have an efficient system that

saves time and pays for the exact number of hours of work done by an employee.

## II. REVIEW OF RELATED WORKS

Singh *et al.* (2017) proposed a web-based leave and payroll system. The system integrates with other systems using APIs. In such an establishment where it is implemented, new features can be added which might not have been there at the beginning when the system is being deployed and it will not affect the integrity of the system. It is also deployed in a way that it will automatically work and link with the biometric attendance system.

In the work of Rahman *et al.* (2017), they proposed an automated system. The system comprises six different modules. The modules range from the employee management system to the employee attendance management system, employee leave management system, employee performance management system, employee payroll system and employee monitoring system. The system is used by an admin, an operator and the employees. Each has separate access to the system according to what is required of them.

Tharanya and SenthilRaja (2020) introduced a web-based smart attendance and payroll system where employee details are captured into a database and each employee is assigned a unique employee number. An admin logs into the system to log an employee in and out daily. This step captures workers' time and provides a day-to-day activity of time records as a report or for further usage such as the monthly wage calculation by finance department programming attendance management.

In the work of Prasad *et al.* (2019), each employee gets a secured identification number that they use to authenticate, which along with other information like the coordinates and images are saved on their smartphones that run on Android, which also have the required APK Files installed on it. The employees log into the system on their smartphones with their credentials and take an image for security purposes. Employees are required to turn on their GPS on their Android smartphones as the process won't go if it is turned off. Each employee's smartphone on getting to work connects to an access point WIFI and does attendance and the records are used to calculate their pay.

Patra *et al.* (2021) introduced a system that collects the attendance of workers with a biometric scanner. The collected attendance data is at the same time uploaded on the cloud. This data can be accessed by both the organisation and workers by making use of their respective applications. The organisation will be able to work on the employee's data with the aid of attendance taking and all other things performed in the software application to calculate Payroll.

Kimani and Nyatuka (2018) used barcodes to authenticate users for attendance. Users scan the barcode on their pass ID in and out, which serves as input for the payroll calculation. PHP, MySQL, HTML and notepad++ were used as tools, and software prototyping methodology was used.

## III. SYSTEM DESIGN

Every system has its way of identifying hardware using the

hardware's unique ID. Figure 1 shows the system design under discussion.

- WordPress was installed on the system for the front-end and back-end program design for web applications. Sublime text was also installed to write the PHP, CMS, and jQuery codes. PersonaDigita Fingerprint device and API were installed on the system to enable smooth communication between the fingerprint scanner and the software.
- VB.NET framework was installed on the PC. This was used to develop the standalone system application. The standalone system application communicates with the web application.
- Xamp server application was installed on the PC. Xamp was used to create the MqSQL application stand as an offline server for the program to be executed on it. It is compatible with WordPress and PHP.
- The codes were compiled, test run and deployed to WordPress.

#### IV. IMPLEMENTATION

The system was implemented in a manufacturing company in Nigeria. The company employs the services of consultants

in the recruitment and management of fixed term employees. The user's attendance records from biometrics were used in generating the payroll.

##### A. System Interface

The System interface opens when the payroll program is launched. On the interface, there are seven buttons as seen in Figure 2. It is on this interface that the admin logs in to the program, new employee fingerprints are captured, and employees also clock in and clock out. Before users can clock into the program, the admin has to log in to secure the program. After the admin login, new users' fingerprints must be captured and saved into the database before being allowed to clock in and out according to the shift schedule using the fingerprint scanner. Figure 2 shows the interface where a new employee is registered. The payroll dashboard is presented in Figure 3. It opens after the admin logs in to the program. In the payroll dashboard, one can navigate to attendance. Attendance was captured when users clock in with their registered fingerprints in the morning and clocked out after work. The attendance dashboard shows the time employees come in and out, the list of employees and other vital information relating to attendance.

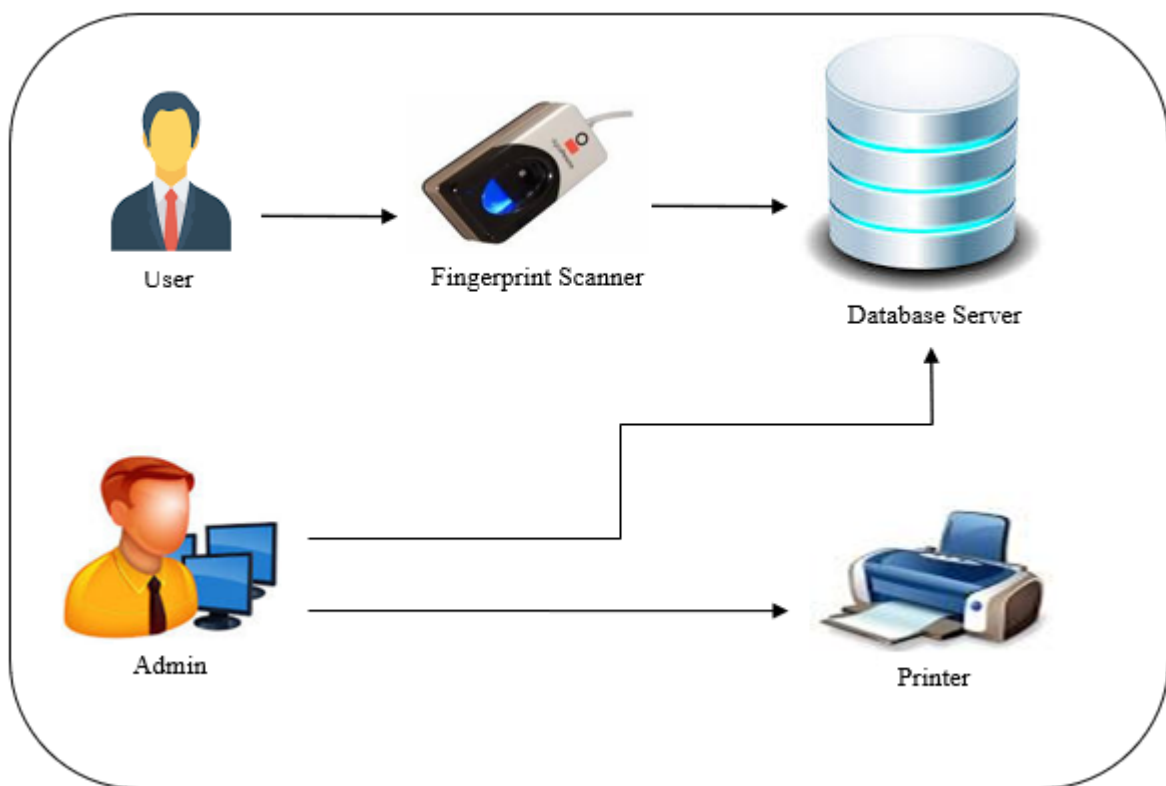


Figure 1: System Design of the System

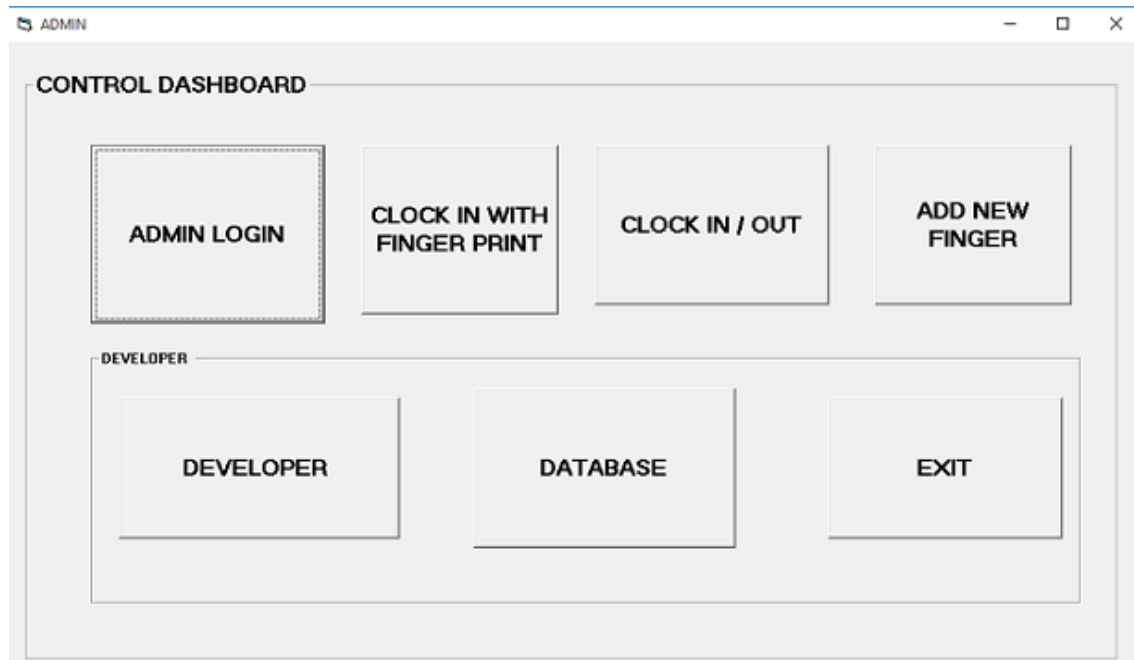


Figure 2: Control Dashboard of the System

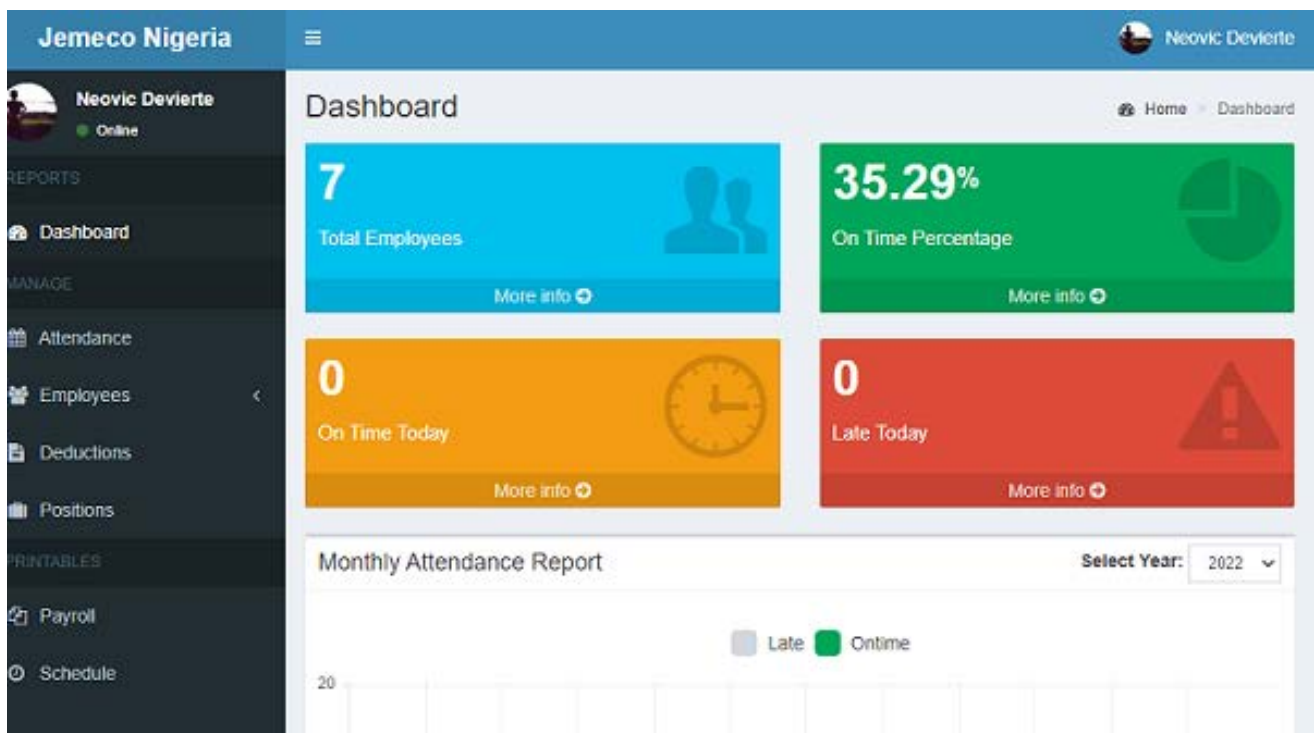


Figure 3: Payroll Dashboard of the System

### B. Shift Schedule

These are a set of rules that govern the resumption of work, closing at work, and overtime. Some organisations run 3 shifts, some 2 shifts and some 1 shift. In this program, we make use of 2 shifts from 8am to 5pm (morning shift) and 8pm to 5am (night shift). Any additional hours worked are overtime, which is added to the total amount for a day's work. Figure 4 shows the screenshot of the schedule.

### C. Payroll Component

These are the required information needed to generate the payroll. We present a detailed explanation of what they mean as regards the computation of the payroll of a fixed-term employee ranging from the hourly pay, overtime pay, gross pay and the government tax, which is a mandatory deduction accruing to the government and deducted from the monthly pay of each employee.

**Jemeco Nigeria** | Neovic Devierte | Online

**Schedules** | Home > Employees > Schedules

+ New

Show 10 entries | Search:

Time In	Time Out	Tools
08:00 AM	05:00 PM	<a href="#">Edit</a> <a href="#">Delete</a>
08:00 PM	05:00 AM	<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1 to 2 of 2 entries | Previous 1 Next

Figure 4: Screenshot of Shift Schedule of Fixed-Term Employees in a Soap Factory

**Jemeco Nigeria** | Neovic Devierte | Online

**Positions** | Home > Positions

+ New

Show 10 entries | Search:

Position Title	Rate per Hour	Tools
Fixed-Term	200.00	<a href="#">Edit</a> <a href="#">Delete</a>
Supervisor	300.00	<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1 to 2 of 2 entries | Previous 1 Next

Figure 5: Screenshot of Payroll of Fixed-Term Employees in a Soap Factory

**Hourly Pay:** This is how much an employee is entitled to collect per hour. If an employee is placed on a 200 naira per hour pay, such employee working on an 8-hour shift will earn 1,600 naira per day.

**Overtime Pay:** The stipulated number of hours worked per day is 8 hours and per week is 40 hours. Any employee whose working period exceeds the stipulated number of hours backed by law is entitled to overtime pay. The overtime pay is calculated and added to the gross pay which an employee is entitled to at the end of the month. In the past, overtime pay was calculated and paid separately to avoid it being taxed. But nowadays, with government directives, overtime pay is added to gross pay and taxed accordingly.

**Gross Pay:** This is the total amount an employee earns at the end of the month before deductions. An employee who for example is on a 200 naira per hour per day earns 1,600 naira per day. If he works Monday through Friday, it becomes 8,000 naira and if it's 4 weeks in the month, 8,000 naira multiplied by 4 will give us 32,000 naira as the gross pay.

**Deductions:** For fixed-term employees earning from 40,000 naira and above per month, a 2% personal income tax is deducted from their salary per month. Therefore, if an employee earns 40,000 naira in a month, 2% of 40,000 naira is 800 naira. Such an employee at the end of the month will earn 39,200 naira. After the tax deduction, admin charges are also deducted. If 3,000 naira is fixed as admin charges, 3,000 naira will be deducted from 39,200 which gives us 36,200 as

the net pay. But for employees earning below 40,000 naira per month, the deduction will only be the 3,000 naira admin charges.

**Pay Schedule:** The input to the program comes from the fingerprint scanner. It captures for each employee their sign-in and sign-out time, which calculates the number of hours worked in a day plus overtime, if any. This calculation gives the gross pay for a month, and the net pay for the same month after all necessary deductions have been made. Below is a payroll of employees from June 6, 2022, to August 5, 2022, based on the number of times the employees were present at work. The various tabs and icons on the interface are explained below.

**Date:** This shows the period of the payroll i.e., from one day of the month to another.

**Employee Name:** This is the name of an employee.

**Employee ID:** This is a unique ID that the program assigns to each employee.

**Gross:** This is the total amount of money accruing to an employee at the end of a particular period.

**Deductions:** Deductions are the total of the admin charges and tax. Deductions go to Jemeco Nigeria Ltd for their administrative duties while Tax goes to the government.

**Cash Advance:** This is the money given to employees in the form of a small loan that will be deducted from the employee pay at the end of a particular period.

**Net Pay:** This is the take-home of the employees. It is the amount left for the employee after deductions have been made.

The sum of what the recruitment consultant pays to all employees for a particular period can be seen and printed as shown in Figure 7.

**Payslip:** For clarity, employees are expected to know what they get and how the figures were arrived at. A payslip contains all the necessary information as regards how much was paid and how much was deducted. This can be printed out and given to each employee at the end of a particular pay period. An example is shown in Figure 8.

Employee Name	Employee ID	Gross	Deductions	Cash Advance	Net Pay
.		0.00	3,250.00	0.00	-3,250.00
Ajayi, Seun	BJV876510243	9,670.00	3,250.00	0.00	6,420.00
Ajibade, Olalekan	POZ359201867	16,015.00	3,250.00	0.00	12,765.00
Akinyele, Olawale	FSD549120736	10,756.67	3,250.00	0.00	7,506.67
Anthony, Adebayo	ABC123456789	3,883.33	3,250.00	0.00	633.33
Jimoh, Adewale	LRH076548231	8,123.33	3,250.00	0.00	4,873.33
Sunday, Temiloluwa	GPW569017342	10,763.33	3,250.00	0.00	7,513.33

Figure 6: Screenshot of Payroll Report of Fixed-Term Employees in a Soap Factory

Employee Name	Employee ID	Net Pay
.		-3,250.00
Ajayi, Seun	BJV876510243	6,420.00
Ajibade, Olalekan	POZ359201867	12,765.00
Akinyele, Olawale	FSD549120736	7,506.67
Anthony, Adebayo	ABC123456789	633.33
Jimoh, Adewale	LRH076548231	4,873.33
Sunday, Temiloluwa	GPW569017342	7,513.33
<b>Total</b>		<b>36,461.67</b>

Figure 7: Screenshot of the total amount payable to Employees for a period in a Soap Factory

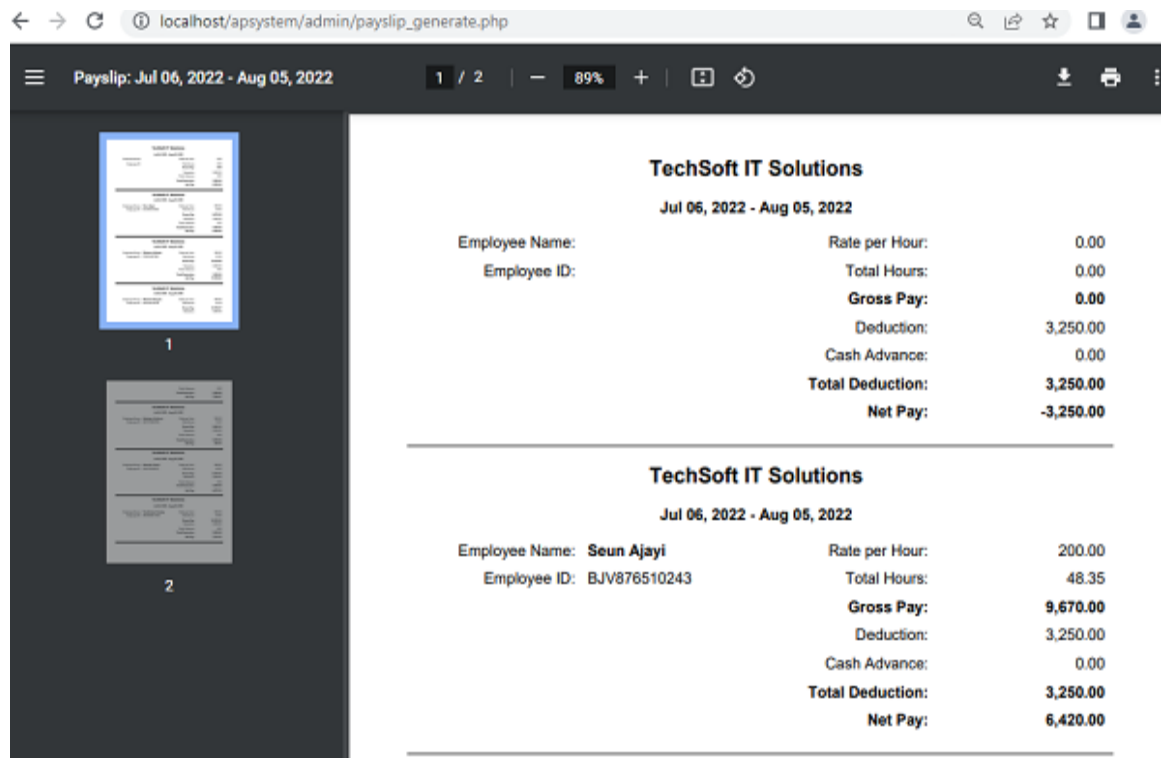


Figure 8: Screenshot of Employee Payslip in a Soap Factory

## V. EVALUATION

The program was evaluated by using the System Usability Scale (SUS). The usability of a system takes the level of satisfaction, effectiveness and efficiency into consideration (Sakpere *et al.*, 2017). In SUS, a score of above 68 means that the program is usable while a score of below 68 means that there are some inhibitions and there's a need to modify the program. The score was calculated based on the user's response to the use of the program (Pal & Vanijja, 2020; Vlachogianni & Tselios, 2022).

### A. Distribution of Respondents by Employment Type

Ten employees were selected while evaluating the program. The respondents were selected according to their employment type and their interaction with the program. They were drawn majorly from the records of a recruitment consultant that manages the fixed-term employees employed by the soap factory and from the permanent staff in the soap factory.

Table 1: Respondents' Distribution by Employment Type

Employment Type	Size
Fixed-Term	8
Full Staff	2
Total	10

### B. Distribution of Respondents' Statements on Attendance Timing and Payroll

Ten questions were formulated. The questions were formed based on attendance timing and payroll. The questions were formulated in relation to the research objectives as shown in Table 2.

### C. Distribution of Respondents' Answers to Questions

In Table 3, the number of respondents was tabulated against each question according to their responses. Ten questions were asked of the respondents. The sum of the total response on each column against each question is ten, which is equivalent to the ten respondents.

Table 2: Respondents' Statements on Attendance and Payroll

S/N	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Fingerprint takes less time to do Attendance					
2	Fingerprint Biometrics is better than manual					
3	Attendance is easy to capture with Biometrics					
4	Fingerprint Biometrics gives accurate time in and time out					
5	Biometrics clocking makes employee timing easy to audit					
6	Biometrics is the best input for payroll calculation					
7	Biometrics gives accurate data for payroll					
8	Biometrics gives accurate overtime data					
9	Biometrics makes payroll easy to calculate					
10	Biometrics Clocking makes payroll process to be faster					

Table 3: Respondents' Answers to Questions

S/N	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Fingerprint takes less time to do Attendance				2	8
2	Fingerprint Biometrics is better than manual				2	8
3	Attendance is easy to capture with Biometrics	1			2	7
4	Fingerprint Biometrics gives accurate time in and time out	1			4	5
5	Biometrics clocking makes employee timing easy to audit				3	7
6	Biometrics is the best input for payroll calculation	2			4	4
7	Biometrics gives accurate data for payroll				2	8
8	Biometrics gives accurate overtime data				2	8
9	Biometrics makes payroll easy to calculate	1			2	7
10	Biometrics Clocking makes payroll process to be faster				5	5

Table 4: Respondents' Point Numbers for Questions

S/N	Statement	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	Fingerprint takes less time to do Attendance				8	40
2	Fingerprint Biometrics is better than manual				8	40
3	Attendance is easy to capture with Biometrics	1			8	35
4	Fingerprint Biometrics gives accurate time in and time out	1			16	25
5	Biometrics clocking makes employee timing easy to audit				12	35
6	Biometrics is the best input for payroll calculation	2			16	20
7	Biometrics gives accurate data for payroll				8	40
8	Biometrics gives accurate overtime data				8	40
9	Biometrics makes payroll easy to calculate	1			8	35
10	Biometrics Clocking makes payroll process to be faster				20	25

#### D. System Usability Scale (SUS) for the Program

The System Usability Scale does not tell the specific problem but gives a pointer to where the problem is. The average scale score is 68 and anything less than 68 points to the fact that there's a need for modifications. Using the system usability scale, respondents will rank each question from 1 to 5 based on how much they agree with the statement they are reading, where 5 means they agree, 4 means they agree, 3 means neutral, 2 means disagree and 1 means they disagree totally.

Using the first statement in Table 3 above as an example where 2 people agreed and 8 people strongly agreed, 2 multiplied by 4 equals 8 and 8 multiplied by 5 equals 40 as seen in the first statement in Table 4. For each of the odd-numbered questions, 1 was subtracted from the score and for each of the even-numbered questions, 5 was subtracted from their value. These new values for all odd-numbered questions were added to get X while the new values for all even-numbered questions were added to get Y. The new figures of X and Y were added and multiplied by 2.5.

From Table 4 above:

$$X = 47 + 43 + 46 + 47 + 43 = 226$$

$$Y = -43 - 37 - 33 - 43 - 40 = -196$$

$$X + Y = 226 - 196 = 30$$

$$30 \times 2.5 = 75$$

The average System Usability Scale score is 68. Since the score derived is 75, above 68, then the application's usability is acceptable. Going by the result obtained in evaluating the

system, the usability assessment measurement characteristics have been achieved by its:

- Effectiveness – users were able to achieve their objective.
- Efficiency – minimal effort and resources are expended to achieve the objectives.
- Satisfaction – users were satisfied using the system.

## VI. CONCLUSION

This research proves that the problem of ghost workers can be solved using technology and the fraud being carried out in public and private establishments in Nigeria can stop with the use of biometrics. Also, the era where workers sit at home and, at the end of the month, receive wages for the work they didn't do, no longer exists. Below are the contributions of this study:

- The system eliminates cheating where someone can claim he came to work whereas he does not but might have connived with another employee who will write his name, sign in and sign out for him and at the end of the day, such employee will be paid fully for what he did not do. Such issue of paying ghost workers is very rampant and if not checked can lead to the collapse of an organisation. With the level of unemployment in the country, there should be measures to protect the few firms that are still running and employing labour.
- It prevents time cheating where an employee who only works for a few hours in a day can claim a full day wage, all because he altered the attendance register to

his favour.

- It can be used to calculate accurate overtime pay for workers so that an employee who does not work overtime will not claim overtime pay at the end of the month just because the system can be manipulated.
- It prevents time wastage where employees queue behind each other to fill and sign the attendance register. A lot of time is wasted in the process which in turn affects their productive hours because of the delay in filling and signing of the attendance register.
- It provides a reliable system of attendance that is storable and information can be retrieved at any point in time as damage to the hard cover can damage a record of many years since it is not electronic where records can be backed up and kept in different storage devices and different locations, it produces only one copy which can be easily damaged either to miss handling where the pages begin to tear off or if there is a fire outbreak.

#### REFERENCES

- Kimani, M., & Nyatuka, D. (2018). A web-based employee time tracking system: Enhancing operational efficiency in the workplace. *Research and Innovation Conference*, 1–11. <http://hdl.handle.net/11071/9524>
- Pal, D., & Vanijja, V. (2020). Perceived usability evaluation of Microsoft Teams as an online learning platform during COVID-19 using system usability scale and technology acceptance model in India. *Children and Youth Services Review*, 119, 1–12. <https://doi.org/10.1016/j.childyouth.2020.105535>
- Patra, R., & Teja, P. R. (2023). A study on payroll management system. *International Journal For Multidisciplinary Research*, 5(1), 1–26. <https://doi.org/10.36948/ijfmr.2023.v05i01.1419>
- Patra, S. R., Suthar, D., Rane, V., & Singh, V. (2021). *Attendance and salary management system for construction industry* (pp. 1–4). EasyChair Preprint 7016. <https://easychair.org/publications/preprint/6Tnf%0A>
- Prasad, K. M., Goru, R. S. N., Vamsi, D., & Mayan, J. A. (2019). Automated payroll using GPS tracking and image capture. *IOP Conference Series: Materials Science and Engineering*, 590(1), 1–6. <https://doi.org/10.1088/1757-899X/590/1/012026>
- Rahman, M. M., Mishu, T. I., Islam, M. S., & Akanda, M. S. (2017). Implement fingerprint authentication for employee automation system. *International Journal of Innovative Research in Information Security (IJIRIS)*, 4(9), 5–12. <https://doi.org/10.26562/IJIRIS.2017.SPIS10080>
- Sakpere, W. E., Mlitwa, N. B. W., & Oshin, M. A. (2017). Towards an efficient indoor navigation system: a Near Field Communication approach. *Journal of Engineering, Design and Technology (JEDT)*, 15(4), 505–527. <https://doi.org/10.1108/JEDT-10-2016-0073>
- Singh, M., Singh, P., Singh, R., Singh, S., & Gupta, S. (2017). Leave and Payroll Management System. *IOSR Journal of Computer Engineering (IOSR-JCE)*, 1, 62–66.
- Tharanya, V., & SenthilRaja, P. (2020). Web based employees smart attendance and payroll system. *International Journal of Advanced Science and Engineering Research*, 5(1), 613–621.
- Vlachogianni, P., & Tselios, N. (2022). Perceived usability evaluation of educational technology using the System Usability Scale (SUS): A systematic review. *Journal of Research on Technology in Education*, 54(3), 392–409. <https://doi.org/10.1080/15391523.2020.1867938>
- Yulisfan, Muda, I., & Nedelea, A.-M. (2021). The evolution of payroll software that can replace the manual method in Indonesia. *Ecoforum Journal*, 10(2), 1–6.



Editorial

---

# Analysis of the Emotional and Psychological Health of the Nigerian Military During COVID-19

---

Oyewale Christianah T. and Ibitoye Ayodeji O.

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Oyewale, C. T., & Ibitoye, A. O. (2023). Analysis of the Emotional and Psychological Health of the Nigerian Military During COVID-19. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 39-44). Ibadan. <https://doi.org/10.5281/zenodo.8121062>.

# Analysis of the Emotional and Psychological Health of the Nigerian Military During COVID-19

\*<sup>1</sup>Oyewale Christianah T. and <sup>2</sup>Ibitoye Ayodeji O.

<sup>1</sup>Department of Computer Science, University of Ibadan, Oyo State, Nigeria

<sup>2</sup>Department of Computing and Mathematical Sciences, Koladaisi University, Oyo State, Nigeria

\*oyewalechristianahtitilope@gmail.com

**Abstract:** This article considers the analysis of the effect COVID-19 had on Nigerian military personnel in terms of their psychological and emotional well-being. It identifies the reasons why outside there; the military personnel are termed rich which causes them to be a low priority during the era of COVID-19. Such affected them psychologically and emotionally. The methodology for the study revolves around the hybrid of questionnaires and interviews. Primary data coming from the methodology employed were analyzed and to consolidate responses from questionnaires, stakeholders considered relevant to the study were interviewed. Results analysis was carried out, using Microsoft Power Business Intelligence software. The study's major finding revealed that despite the work-at-home policies occasioned by the COVID-19 phenomenon, the Nigerian Military was still going to work making them more vulnerable to COVID-19 infection. The study also found out that the distribution of COVID-19 relief was given more to the Non-military than the Military which exacerbated negative emotional and psychological effects on them. Despondently, the Nigerian military was considered as being rich and this led to less than satisfactory attention on mitigating the effect of COVID-19 on them despite their unrelenting efforts in keeping the peace of the country. Based on the findings of this study, the study concludes that the Nigerian Military should be considered for better attention in the event of a pandemic such as COVID-19 for the sake of their psychological and emotional stability.

**Key Words:** Nigerian Military, COVID-19, Psychology, Emotional, Power BI

## I. INTRODUCTION

COVID-19 began towards the end of the year 2019, and according to the World Health Organization, it is a communicable disease that can be fatal (Castellnuovo *et al.*, 2020). No doubt, everybody's life became extremely tense as a result, and fear of death grew among all irrespective of one social or health status. Daily increases in the pandemic's transmission rate were accompanied by a rise in the number of reported fatalities. This accelerated the rate at which people were more frightened while compelling the majority to follow the instructions provided by (Güner *et al.*, 2020) the health professional on safety measures. In this instance, many were psychologically affected. While the goal of psychology is to understand how the mind works. An effective technique to determine if someone has a mental disease is to conduct a psychological examination of them. COVID-19 was a part of the psychological and mental distress that people experienced. This among others is because keeping people in one place for an extended time could cause some detrimental psychological issues, which can cause some people to lose their temper easily, become confused, experience post-traumatic stress, fear contracting

an infection, become bored and become frustrated (Bonati *et al.*, 2022). While an individual's emotions are influenced by the circumstances in which they are found. People's emotional reactions to the pandemic experience may have harmed a variety of people, including sleep issues, unwarranted anxiety, and other issues (Bera *et al.*, 2022). Similarly, some health challenges like obesity were acquired by people during the era of COVID-19 because it promoted some characteristics like eating too much and drinking too much and all these made the emotion of people to be worsened (Burnatowska *et al.*, 2022). This has shown that people suffered emotionally during the period of COVID-19. Some people were able to emotionally handle all of this, but others were not able to, which might have led to the death of some of them. To lessen the adverse effects of the stay-at-home regulations implemented by the majority of governments, including the Nigerian government, individuals and various bodies distributed relief materials to the populace. These materials allowed people to support themselves since they were unable to go out and earn a living for themselves. Here, money, food, soft drinks, and medical kits for COVID-19 were among the relieving goods that were distributed during the event (Ufua *et al.*, 2021).

Although, these kinds of gestures were generally heard especially on social media; this research wasn't able to see any records that pointed to palliative being distributed to Nigerian Military Officers. Since there was little to no research done to determine whether COVID-19 had an impact on the military, it was evident that the military may have been less focused and may not have even believed that they could be influenced (Wynn *et al.*, 2020). Consequently, the Nigerian military risks their life and leaves their loved ones behind to safeguard the countries and the people of Nigeria. Because Nigerian military personnel are also human, it's crucial to understand that they have the same needs as Nigerian civilians (Brouzos *et al.*, 2021).

Most research done on the effects of COVID-19 on the health of people was mainly done using the public, healthcare practitioners, less privileged, and so on but little or no right has been given to see the effect that COVID-19 had on the psychology and the emotions of the Nigerian Military. The study is out to interrogate the welfare effect of psychological and emotionally feeling of the military in the wake of COVID-19. Every effect stated earlier also applies to the Nigerian Military; if care is not taken, it may be more than that. Consequently, it has become important to analyze the effect that COVID-19 had on the Nigerian military by looking at it from the perspective of Nigerian Civilian to be able to see what the Civilians thinks about the Military in other to educate the public to give adequate support to the Nigerian Military in situations that the public was during

COVID-19.

The rest of this research work is as follows: Section 2 is a brief discussion of the past research that was already made. Section 3 explains the material and methods that were used in this research work. Section 4 is the test implementation and necessary discussions are made. The conclusion and future work are discussed in Section 5.

## II. LITERATURE REVIEW

Ammar *et al.* (2020) conducted a survey using seven languages to give clarity on the effects the restrictions that were put in place by the Government during COVID-19 had on the psychology and emotions of people. The method that was used by the authors is an online survey that was built using Google. This method used by the authors was used by us too because it became easier to reach a large number of people without seeing them physically. The only thing we finetuned to this method is that we didn't leave the filling of the Google form to the people, technical support was given to the ones that it became difficult for them to fill due to literacy issues and busy schedules. Also, the authors made their case study to fill the survey unlike us where we chose a sample size of people that were closely related or stayed closer to where the Military personnel stays. Due to military rules, it was difficult to survey the military personnel, we had to ask those that interacted with them to fill out the survey on their behalf. The authors' survey was extended to more than three countries making them have a larger dataset that was used for analysis and was able to get a result of the symptoms of depression from the respondents.

Olaseni *et al.* (2020) did about two similar studies where the statistical analysis of the psychological issues faced by Nigerians during COVID-19. The authors used a sample size of 502 Nigerians and were able to list out the different categories and levels of each of the psychological issues on the sample size and the study were able to conclude that Nigerians went through distress during COVID-19. The study didn't state if the survey was conducted with the civilian and the military, so we were forced to conclude that the result of the study spoke for both (Olaseni *et al.*, 2020). We could say of the truth that the Nigerian Military also went through distress during COVID-19.

Considering the study by (Kwaghe *et al.*, 2021), the fact that the health workers in Nigeria were affected both physically and psychologically during COVID-19 was established since they were involved in the care of people during COVID-19. The method used for this study is an interview and qualitative analysis was performed on the dataset. The result from the study was able to identify that part of what the health workers went through during COVID-19 was related to psychology and emotions. We could say that the sample size got into a such mental state because they served humanity. Using the same method of data analysis, can relate this experience to that of the Nigerian Military which despite the risky part of the job, the era of COVID-19 brought mental issues to them.

Nwafor *et al.* (2021) focused their study on pregnant women and used a sample size of 456 pregnant women which was analysed statistically. This shows that different groups of individuals got issues related to mental health during COVID-19. On the other hand, Ogbole *et al.* (2020)

statistically analyzed how the military perceived COVID-19 during the era using a sample size of 216. The study was able to directly collect data from the Nigerian Military which made it easier for them to do the analysis, but the study didn't go into how the Nigerian Military was psychologically and emotionally affected during COVID-19.

In the study conducted by Uford *et al.* (2022), Power BI was part of the tools that were used in the analysis. Power BI was used for the demographic data which showed the beauty of visualization of data using Power BI. Many of these reviewed publications focused on different individual civilian groups and other things, but none focused on the analysis of the psychological and emotional effects of COVID-19 on Nigerian Military personnel.

## III. MATERIALS AND METHODS

The method that was used in this research paper is the survey which involves the use of interviews and questionnaires as a means of gathering data (Esiefarienrhe & Mokeresete, 2022). There was no multiple-choice question in the survey but comprises 19 option-choice questions that permit only one answer for each specific question. The option-choice questions comprise some set of questions that were used to collect the demographic of the respondents to know details like the age range, the gender, and the likes. The other details that were also used in the option-choice questions are to know from the respondents' side of view the most populated between the military and the civilian. Also, to know the most populated Military force in Nigeria. We chose to also know if the respondent is a health worker or not. To also know what the civilians think about the income of the military, there was a question to know between the military and the civilian which of them were well paid by the Government. The last set of this category of question dived into asking if the military were affected by COVID-19 if they received and relieved materials, if there were psychological and emotional support from the Government and/or others put in place for the military, to know if there were measures put in place to combat stress for the military, if it was observed that parts of the COVID-19 recorded cases were also from the military, as one of the symptoms of psychological disorder we asked if the military were observed to be tired of their job during COVID-19 due to the stress the went through and been more exposed as they were still meant to go to work despite the stay at home rules by the Government and to also know if people were scared of going closer to the military during COVID-19 in which such could affect their mental health.

The open-ended questions that were in the survey were 9 questions. We chose to know the tribe of the respondent as it couldn't capture all the tribes for such a question to be an option-choice question. We allowed the respondent to enter the health challenges that they had for those that were selected to have any health challenges. We also needed to know the psychological and emotional state of the respondent, we asked to know if they were tested to have any and if they were to state such. We asked the respondent to state the psychological and emotional possible symptoms that they might have observed from the military during COVID-19. We asked the respondent to list the necessary measures that might have been provided to the military to combat stress and some other issues which might lead to psychological and emotional illness. The respondent was to

list what they observed about the precious things the military personnel might have lost during COVID-19. We also asked the respondents to advise to avoid military personnel having psychological and emotional issues.

The military men in Nigeria were to be used for this study, but it was restricted by stringent military regulations that had to be followed. Oyo State and Benue State were the two places we chose to conduct this investigation. This selection of both states was done based on the accessibility. To participate in the study, we selected persons who lived nearby the barracks or were closely related to the Nigerian military troops. We emailed a Google form link with questions that were created with the objective in mind to the respondents who were computer competent. Similarly, to this, those who needed assistance filling out the form were given people to assist them. The questionnaires were distributed by employing a Random sampling technique and the total number of the sample chosen was 500 respondents where 250 for Oyo State and 250 for Benue State. The survey was completed by 477 respondents in total where 280 from Oyo State and 197 from Benue State.

Before finally sending out the questionnaires, we had some selected people that we sent questionnaires to which made two of them volunteer to be interviewed. One had close relations with military personnel and the other was married to the military personnel. They booked an appointment for the interviews which were conducted using WhatsApp voice call and also messages (chats) with voice messages. The first interview lasted for more than one hour as the research got the interviewee to be much interested. The second interview took about 20 minutes. The interest they both developed made it easier for open-ended questions to be asked as they also promised to fill out the questionnaires. The interview made us restructure the questions in the questionnaires as it opened our eyes to some missing important aspects that we needed to consider.

We went through the responses gotten from the questionnaires to see if there were missing values and we noticed there were no missing values as there were validation tools on Google form which made the important fields be filled by the respondent. And those that filled themselves were literates in a task as such. The others were supported by the team members. It became easier for us to begin with the analysis of the dataset after the dataset was downloaded from the online Google Drive.

Since the responses were both in quantitative and qualitative form, we chose to use Microsoft Power Business Intelligence tool for the analysis of the dataset. For the qualitative analysis, the responses were text-based. That is, they were in sentences. The tool that is used for theming related words in Power BI was used in the analysis and visualization of them. The quantitative part of the dataset was visualized and analyzed using the various tools that Power BI has for such analysis.

Microsoft Power BI was chosen for the analysis of the dataset because it is a powerful tool for analysis and because of its ease of use for the analysis of the text. It was an easy tool for us since it is one of the popular tools, it can also be used for the analysis of any size of data and ease of understanding of insights by anyone irrespective of literacy level.

As the responses kept coming, we could follow as it was going because of the automated visualizing tool that Power BI has. We kept on monitoring the responses and seeing the different trends of the dataset. The richness of the dashboard in Power BI helps in having instant answers and it helped us to work locally and remotely. For the quantitative analysis, the responses that were not numeric were made numeric like using 1 for Yes, 0 for No, and 2 for Maybe.

Microsoft Power BI became a good tool for us as it was easier for us to use and learn within a few days for those with no prior knowledge of the user because it doesn't require knowledge of programming as the few codes that were written were less and was used in calculation of percentages which aid our analysis of the datasets. There was also an instant feel of activities when using tools that are used for click-and-drop or click-and-apply. This helped us to follow through during the design of the reports on the dashboard. The image below is the sample of the questionnaire that was used for data collection.

**ANALYSIS OF THE EMOTIONAL AND PSYCHOLOGICAL HEALTH OF THE NIGERIAN MILITARY DURING COVID 19**

Hi there, I'm Christianah Titilope Oyewale a Masters student of University of Ibadan. I'm conducting a research on the above topic. Thank you for helping out in filling the questionnaire.

Despite the sit at home law that was passed during Covid-19, there were still additional duties for the military personnel to ensure that the laws were obeyed. There were no record if they were properly taken care of during the pandemic. This project aimed at analyzing if what the military went through during the Covid-19 period had emotional and psychological effects on the them.

Please be transparent as much as possible.

NOTE: Details about your identity are not required in this questionnaire. A particular response won't be traced to any respondent.

oyewalechristianah@ttilope@gmail.com (not shared)  
Switch accounts

\*Required

1. Which age range do you belong to? \*

☐ Below 20  
☐ 21 - 30  
☐ 31-40  
☐ 41-50  
☐ 50 and above

2. What is your gender? \*

☐ Male  
☐ Female  
☐ I choose not to answer

3. What is your religion? \*

☐ Christianity

Figure 1: Image of the Questionnaire Used for Data Collection

#### IV. RESULTS AND DISCUSSION

As explained previously, the case study that we used in this research work was people that had close interaction with Nigerian Military personnel. After the proper formatting of

lives, health, and so on. This proved that it is not only civilians that lost precious things during COVID-19, but the military also. So, there is a reason why they needed to be taken care of during a pandemic like COVID-19.



**MILITARY CONTACT WITH COVID-19 DURING COVID-19**

Category	Percentage
%affected	48.63%
%notaffected	31.37%
%maybeaffected	20%

Figure 5: Military Contact with COVID-19



MILITARY WELL PAID  
**56%**

EMOTIONAL SUPPORT  
**59%**

Age	EmPsSupport (%)
31-40	95
Below 20	90
21 - 30	65
41-50	35
50 and above	5

Figure 6: Responses by Age

Figure 6 above shows the respondents that believed that the Nigerian Military personnel didn't receive emotional and psychological support from the Government and the general public where the people in the age range 31 to 40 agreed more and then follow by those below 20 years, then those between 21 and 30 years, follow by people between 41 to 50 years and then people that were above 50 years of age.

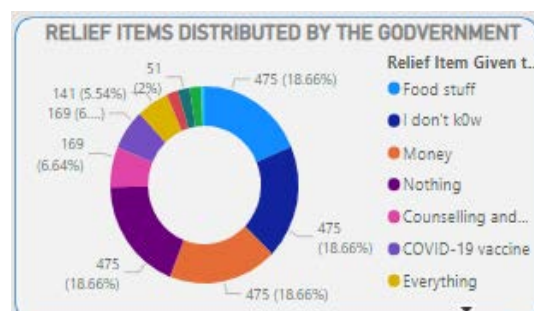


Figure 7: Relief Materials

Figure 7 above shows the relief materials that were distributed by the Government to the general public, this could have also been distributed to the Military Personnel in

other to show them that they were also loved by the Government.

## V. CONCLUSION

The focus of this study is on the analyses of the psychological and emotional effects of COVID-19 on Nigerian military personnel. The perverse nature of the effect of COVID-19 and the desire to interrogate how the pandemic affected the Nigerian military personnel psychologically and emotionally provided the motivation for the study. Granted that the government of the Federal of Nigeria deployed a wide range of palliative measures to address the pandemic to different sets of the people of Nigeria; the way and nature of palliatives channelled to the Nigerian military personnel as one of the highly vulnerable groups of people to the pandemic generated interesting findings. Hence, information was clustered from close relatives and interested members of the military community. With the hybrid, that is, a combination of questionnaire and transcribed interview data, the study generated a dataset that revealed the gender mix of the relatives of the Nigerian military personnel; the profile of palliative measures channelled to the Nigerian military personnel, and the extent of monetary compensation given to the Nigerian military person to cushion the effect of COVID-19 pandemic, the study found out that the Nigerian Military personnel were excluded from palliative interventions embarked upon by the Government. This finding invariably indicated that the Nigerian military personnel did not enjoy the appropriate volume of palliatives despite the high-risk nature of the works of military personnel during the COVID-19 era. To this effect, the observed neglect of the Nigerian military personnel adversely affected them psychologically and emotionally as respondents with different age categorizations maintained that the psychological and emotional being of the Nigerian military personnel was not taken care of. This finding appears unsatisfactory given the security services that Nigerian military personnel are assigned to perform with or without any pandemic. Thus, with this major finding, the study has revealed the need to address the abnormality inherent in the distribution of COVID-19 palliative measures by allowing such measures in the form of interventions meant to mitigate psychological and emotional adverse effects of any pandemics such as COVID-19 to flow to the Nigerian military personnel for the sake of their welfare consideration.

## REFERENCES

- Ammar, A., Mueller, P., Trabelsi, K., Chtourou, H., Boukhris, O., Masmoudi, L., Bouaziz, B., Brach, M., Schmicker, M., Bentlage, E., How, D., Ahmed, M., Aloui, A., Hammouda, O., Paineiras-Domingos, L. L., Braakmanjansen, A., Wrede, C., Bastoni, S., Pernambuco, C. S., ... Hoekelmann, A. (2020). Psychological consequences of COVID-19 home confinement: The ECLB-COVID19 multicenter study. *PLoS ONE*, 15(11), 1–13. <https://doi.org/10.1371/journal.pone.0240204>
- Bera, L., Souchon, M., Ladsous, A., Colin, V., & Lopez-Castroman, J. (2022). Emotional and behavioral impact of the COVID-19 epidemic in adolescents. *Current Psychiatry Reports*, 24(1), 37–46. <https://doi.org/10.1007/s11920-022-01313-8>
- Bonati, M., Campi, R., & Segre, G. (2022). Psychological impact of the quarantine during the COVID-19 pandemic on the general European adult population: A systematic review of the evidence. *Epidemiology and Psychiatric Sciences*, 31(e27), 1–19. <https://doi.org/10.1017/S2045796022000051>
- Brouzos, A., Vassilopoulos, S. P., Baourda, V. C., Tassi, C., Stavrou, V., Moschou, K., & Brouzou, K. O. (2021). “Staying Home – Feeling Positive”: Effectiveness of an on-line positive psychology group intervention during the COVID-19 pandemic. *Current Psychology*, 42(4), 2749–2761. <https://doi.org/10.1007/s12144-021-01613-x>
- Burnatowska, E., Surma, S., & Olszanecka-Glinianowicz, M. (2022). Relationship between mental health and emotional eating during the COVID-19 pandemic: A systematic review. *Nutrients*, 14(19), 1–15. <https://doi.org/10.3390/nu14193989>
- Castelnuovo, G., De Giorgio, A., Manzoni, G. M., Treadway, D. C., & Mohiyeddini, C. (2020). Psychological, behavioral, and interpersonal effects and clinical implications for health systems of the Coronavirus (COVID-19) pandemic: A call for research. *Frontiers in Psychology*, 11, 1–3. <https://doi.org/10.3389/fpsyg.2020.02146>
- Esiefarienrhe, B. M., & Mokeresete, M. (2022). Using software applications to enhance e-government service delivery in Botswana. *Journal of Information Systems and Informatics*, 4(3), 495–510. <https://doi.org/10.51519/journalisi.v4i3.262>
- Güner, R., Hasanoğlu, İ., & Aktaş, F. (2020). COVID-19: Prevention and control measures in community. *Turkish Journal of Medical Sciences*, 50(9), 571–577. <https://doi.org/10.3906/sag-2004-146>
- Kwaghe, A. V., Kwaghe, V. G., Habib, Z. G., Kwaghe, G. V., Ilesanmi, O. S., Ekele, B. A., Umeokonkwo, C. D., & Balogun, M. S. (2021). Stigmatization and psychological impact of COVID-19 pandemic on frontline healthcare Workers in Nigeria: A qualitative study. *BMC Psychiatry*, 21, 1–17. <https://doi.org/10.1186/s12888-021-03540-4>
- Nwafor, J. I., Okedo-Alex, I. N., & Ikeotuonye, A. C. (2021). Prevalence and predictors of depression, anxiety, and stress symptoms among pregnant women during COVID-19-related lockdown in Abakaliki, Nigeria. *Malawi Medical Journal*, 33(1), 54–58. <https://doi.org/10.4314/mmj.v33i1.8>
- Ogbole, A. J., Bisji, J. S., Umar, S. J., Jallo, I. M., Ezech, S. O., & James, A. L. (2020). Knowledge, attitudes and perception in regard to COVID-19 pandemic in Nigerian military population. *Advances in Social Sciences Research Journal*, 7(11), 231–249. <https://doi.org/10.14738/assrj.711.9254>
- Olaseni, A. O., Akinsola, O. S., Agberotimi, S. F., & Oguntayo, R. (2020). Psychological distress experiences of Nigerians during COVID-19 pandemic; the gender difference. *Social Sciences & Humanities Open*, 2(1), 1–7. <https://doi.org/10.1016/j.ssaho.2020.100052>
- Uford, I., Charles, I., & Ekong, J. E. (2022). The COVID-19 crisis and regular telework: The effect of stress on the Nigerian oil and gas employees’ work perception. *European Journal of Management and Marketing Studies*, 7(2), 179–199. <https://doi.org/10.46827/ejmms.v7i2.1252>
- Ufua, D. E., Osabuohien, E., Ogbari, M. E., Falola, H. O., Okoh, E. E., & Lakhani, A. (2021). Re-strategising

Government palliative support systems in tackling the challenges of COVID-19 lockdown in Lagos State, Nigeria. *Global Journal of Flexible Systems Management*, 22(1), S19–S32.

<https://doi.org/10.1007/s40171-021-00263-z>

Wynn, G., Morganstein, J. C., Jetly, R., Ford, S. C., Vance,

M. C., Meyer, E. G., West, J. C., Benedek, D. M., & Ursano, R. J. (2020). Military mental health and COVID-19. *Journal of Military, Veteran and Family Health*, 6(S2), 21–26. <https://doi.org/10.3138/jmvfh-2020-0048>



Editorial

---

# Intrusion Detection System in Cloud Computing: A Review

---

Awodele Simon O. and Sakpere Wilson

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Awodele, S. O., & Sakpere, W. (2023). Intrusion Detection System in Cloud Computing: A Review. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 46-58). Ibadan. <https://doi.org/10.5281/zenodo.8121064>.

# Intrusion Detection System in Cloud Computing: A Review

\*Awodele Simon O. and Sakpere Wilson  
Department of Computer Science,  
Lead City University Ibadan, Nigeria  
\*talk2ficky@gmail.com

**Abstract:** With greater flexibility and less infrastructure investment, cloud computing offers end customers scalable, virtualised on-demand services. These services are offered via the Internet while adhering to accepted networking protocols, standards, and file formats. Due to its distributed and scalable nature, cloud computing is currently preferred by the majority of IT firms. However, potential attackers for cyber threats are paying close attention to its flexible and open architecture. The Intrusion Detection System (IDS) is crucial in this situation for keeping an eye on hostile activity in cloud-based systems. This paper systematically reviews the existing methods for detecting intrusions based on various techniques and methods such as traditional techniques and soft computing methods.

**Key Words:** Intrusion detection system, cloud computing, cloud-based IDS, Signature IDS, Anomaly IDS, Hybrid IDS

## I. INTRODUCTION

With the widespread increase in technological advancement and the use of the internet, computing accessories and resources have become more readily available, more powerful, more resourceful, more common, and more accessible than ever before. This technological advancement has enabled connectivity, communication, collaboration, and access to remote devices. Information storage and accessibility are now easily possible with the use of computer systems, mobile devices, and other electronic devices (Jang-Jaccard *et al.*, 2013). Hence, individuals, business owners, firms, organisations, and government agencies are now embracing this fast-evolving digital infrastructure without considering the vulnerabilities it exhibits and sharing their

data and information without any thought of loss of privacy. However, as technology advances, new security threats and challenges regarding safety, trust, availability, and reliability emerge. Because cloud computing technology is internet-based, there is a high risk of intrusion and malicious attacks exploiting new vulnerabilities created by the transition from the common and traditional method of storing, processing, and accessing information, data, and communication to the new environment (Kosamkar, 2016; Sadiku *et al.*, 2022). Studies have shown that the innovation of many existing technologies, such as web services, web browsers, and virtualisation, has contributed to the development of cloud-based systems. Hence, any intrusions, threats, and attacks associated with these technologies also affect the cloud; they can even have a more dangerous effect in this environment (Hashizume *et al.*, 2013).

As a result, "cloud computing" can be defined as "an emerging technology that provides on-demand computing resources and services via the internet" (Samreen & Zaidi, 2012). That is, an Internet-based platform for data processing, storage, and sharing resources such as infrastructure, software, applications, and business processes (Sadiku *et al.*, 2022; Suthar, 2017). The National Institute of Standards and Technology (NIST) proposed a definition of cloud computing in its NIST Special Publication 800-145 as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (Mell & Grance, 2011). This cloud model is composed of five essential characteristics, three service models, and four deployment models.

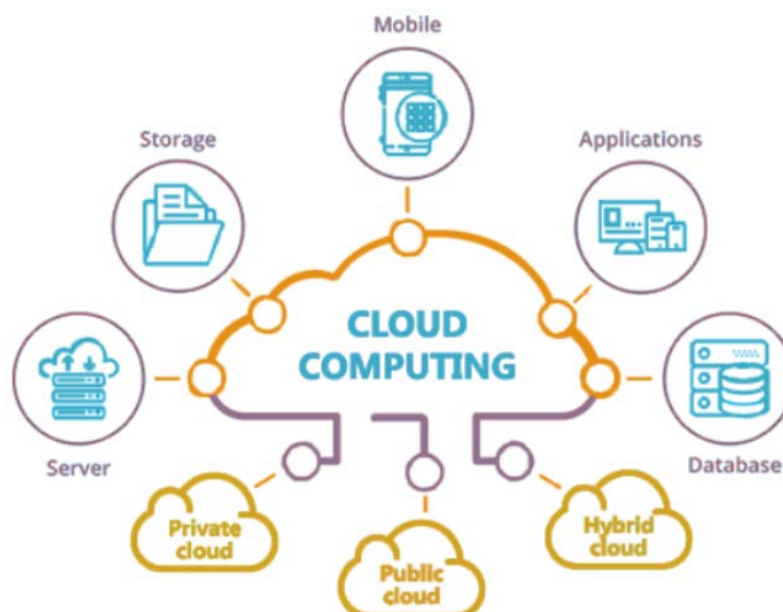


Figure 1: Architecture of Cloud Computing (MEGATEK ICT Academy, 2020)

In today's world, it is almost impossible to ponder the digital evolution of businesses and organisations without mentioning cloud computing technologies (Chaudhary, 2020). Cloud computing possesses some features that differentiate it from traditional web services. Some of these features are multitenancy, resource pooling, virtualisation, on-demand self-service, elasticity, automatic or easy resource deployment, and metered billing. When compared to using a typical web service provider, all of these enable cloud computing to provide users with more cost savings, automation, and flexibility. Communication in cloud computing technology can be separated into two sections: the front end and the back end. The client, or computer user, serves as the front end of the system, and the cloud is responsible for its back end (Ade, 2020; Odun-Ayo *et al.*, 2018). Based on the interface of the cloud services, the personal computer requires access to the coordination of cloud computing. Computers, a storage system, and servers make up the back-end infrastructure, which in turn generates the dedicated servers and cloud services required for these applications (Dinh *et al.*, 2013; Mansouri *et al.*, 2020; Sunyaev, 2020).

In cloud computing technology, computing resources are shared rather than having a local server or personal devices to handle applications. In other words, it enables consumers and businesses to use applications without installing them and to access their files from any computer or electronic device with internet access (Thakur *et al.*, 2017). In general, cloud computing technology is capable of delivering three types of services and four deployment models. Service delivery models include:

1. Infrastructure-as-a-Service (IaaS): Examples include Digital Ocean, Linode, Rackspace, and Amazon.
2. Platform-as-a-Service (PaaS): These include operating systems and developer platforms. OpenShift for the Google App Engine.
3. Software (apps) as a service (SaaS): For instance, GoToMeeting, Cisco Webx, Zoom, Drive, and Office 365.

Deployment models include public, private, community, and hybrid. Each of these models has different features, and the deployment model depends on the cloud user objectives. Before accepting a model deployment, the user is encouraged to review the security, reliability, and performance issues associated with the models (Mansouri *et al.*, 2020; Odun-Ayo *et al.*, 2018).

With the facts established and known that, in today's world, cloud computing is a technology that has been accepted and used by many, it is therefore vulnerable to various intrusions, attacks, and anomalies. As a result, the security of cloud systems is critical in protecting the data source from external and internal intruders and attacks. As a result, many security tools and techniques have been proposed to secure and prevent cloud attacks. One of these methods is intrusion detection systems (Krishnan, 2017) but in reality, there are various inadequacies and limitations to the existing traditional IDS methods and techniques used in detecting intrusion in cloud-based environments due to the nature of the cloud technology. Therefore, this necessitates the development of a new cloud-based IDS that can meet its security needs.

The focus of this paper is to review the various techniques for detecting intrusion in a cloud computing environment. This paper is organised as follows: Section 2 presents general background knowledge of intrusion and intrusion detection systems in cloud environments, and Section 3 presents the existing works. The conclusion is provided in the final section.

## II. INTRUSIONS IN THE CLOUD

Research on cloud security is ongoing, and numerous solutions have been put forth and improved. An intrusion is now a crucial area of cybersecurity data analytics and is defined as any action intended to compromise the security, confidentiality, integrity, or availability of a system, network or cloud (CIA), including any internet attack, attempts by authorised users to gain more access to the system, or by authorised users who abuse their access (Lata & Singh, 2022; Liu *et al.*, 2022; Modi *et al.*, 2013). Any of the following could constitute an intrusion:

1. Trojans, worms, and viruses that replicate in the network.
2. Sending specially designed packets to take advantage of any flaws.
3. Attacks that would render the services inoperable even for loyal customers.

Utilising a cloud-based intrusion detection system is one of the effective methods to stop such attempts (Elmasry *et al.*, 2021). In reality, the most known intrusions that affect the confidentiality, integrity, or availability of cloud services include the following.

### A. Insider attack

This frequently occurs when authorised users with access to an organisation's networks, systems, and data attempt to get and abuse the rights that have been or have not been legally granted to them. Since insiders could disclose information to adversaries, this attack is strongly tied to trust, and with this, the privacy of cloud users has been violated by this attack (Mehmood *et al.*, 2013).

### B. Attacks via backdoor channels

By taking advantage of this passive assault, hackers can breach the privacy of user information and get remote access to compromised workstations. To take over the victim's resources and use them as zombies in a DDoS assault, hackers can use backdoor channels (Modi *et al.*, 2013). The secrecy and accessibility of cloud users are the targets of this attack. Any mechanism by which authorised or unauthorised users can go beyond standard security precautions and obtain root access to take over the victim's resources and use them as zombies in a DDoS assault the secrecy and accessibility of cloud users are the targets of this attack. There are numerous methods for executing backdoor threats (Doan *et al.*, 2021; Li *et al.*, 2021, 2022; Nguyen & Tran, 2020). They include:

1. Taking advantage of security system flaws that permit unauthorised access to the system or data.
2. Putting malware on a machine that grants the attacker access to it.
3. Gaining access to systems using credentials that have been stolen or cracked.
4. By the covert insertion of messages that grant the attacker power over the systems or users into communications between systems or users.

### C. Hypervisor or Virtual Machine Attacks

An attacker might take over the virtual machines by getting access to the hypervisor. SubVirt, BLUEPILL and DKSM are the most frequent assaults on the virtual layer that provide hackers access to the host through the hypervisor (Bahram *et al.*, 2010; Khairkar *et al.*, 2013; King *et al.*, 2006). Attackers target zero-day vulnerabilities in virtual machines to get access to them before the developers are aware of such exploits. Numerous websites running on virtual servers were harmed because of a zero-day vulnerability in the HyperVM application being exploited (Mehmood *et al.*, 2013).

### D. Denial of Service (DoS) attack

To overwhelm the available resources, the attacker takes advantage of zombies to transmit a lot of network packets. As a result, authorised users are prevented from using the services provided online. DoS attacks—which involve sending a large number of requests to reach VMs through zombies in a cloud environment—are what render those VMs unavailable to authorised users (Modi *et al.*, 2013). The accessibility of cloud resources is the objective of this assault.

### E. Port Scanning

Port scanning can be used by attackers to gather a list of blocked, open, and unfiltered ports from which they can launch attacks against services using those open ports. SYN scanning, ACK scanning, TCP scanning, FIN scanning, UDP scanning, and other port scanning techniques are among them. Port scanning is a technique that attackers can employ to locate open ports in a cloud environment, after which they can focus on the services that are using them. This assault can result in the loss of integrity and secrecy on the cloud (Modi *et al.*, 2013).

### F. User-to-root attacks (U2R)

By using password sniffing, the attacker can access a valid user's account and utilise system weaknesses to get root access. Root shells can be created by utilising buffer overflows from a root-level process. In a cloud situation, an attacker gains access to legitimate user instances before gaining root rights on the host or virtual machines. The integrity of cloud-based systems has been violated by this attack (Modi *et al.*, 2013).

## III. INTRUSION DETECTION SYSTEMS

This section provides a quick review of the research that has been done on cloud-based IDS. An intrusion detection system is a software system or hardware device that scans all incoming and outgoing network traffic for unusual patterns that can point to a security breach in a network or system. The IDS scans traffic for signatures that correspond to recognised intrusion patterns and issues an alert when a match is discovered (Farsole *et al.*, 2010; Mukhopadhyay & Nath, 2014; Patil *et al.*, 2018). To keep an eye on suspicious traffic coming from outside or inside the network, the IDS is installed either inside or outside the firewall, depending on the traffic that has to be watched. IDS has many ways of working, but one of them is that it collects and examines data from a computer or a network to find any potential breaches of the security policy, including illegal access or misuse. An IDS analyses traffic for potential intrusions and issues a warning when such intrusions are found.

### A. Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network

Because people access cloud data over the Internet, the information there is vulnerable to numerous invasions. In the cloud, intrusion detection is thought to be a major problem. The currently available algorithms can identify well-known assaults but struggle to identify less frequent ones. The authors proposed an innovative intrusion detection system (IDS) in the cloud that combines kernel fuzzy c-means clustering (KFCM) and an ideal type-2 fuzzy neural network to address this problem (OT2FNN). To do this, we use the Lion optimisation algorithm (LOA) for weight optimisation to select the T2FNN parameters in the best possible way (Srilatha & Shyam, 2021).

### B. Cloud Intrusion Detection System Using Fuzzy Clustering and Artificial Neural Network

An intrusion detection system (IDS) is a security layer that monitors systems for suspicious activity and sends out notifications when it is discovered. Artificial Neural Networks (ANN) are capable of detecting system intrusions, although there is a slight issue with ANN's lack of detection precision for infrequent attacks and stability. To solve the problem, The authors chose to adopt the FC-ANN strategy, which is based on fuzzy clusters and artificial neural networks. The general process for FC-ANN is as follows: various training subsets are first created using the fuzzy clustering technique. Different ANN models are then trained to create various base models using various training subsets (Chormale & Ghatule, 2020).

### C. Application of Deep Learning Technique in an Intrusion Detection System

In this study, a hybrid network-based Intrusion Detection System (IDS) is employed to detect network intrusions using deep learning techniques. On the NSL-KDD and ISCXIDS 2012 datasets, the effectiveness of the suggested technique is assessed. Wireshark was used to do traffic visual analysis, and experiments were conducted to demonstrate the superiority of the suggested approach over the various base models (Sarajian & Golchi, 2020).

### D. Attacks and Intrusion Detection in Cloud Computing Using Neural Networks and Particle Swarm Optimisation Algorithms

Cloud computing has gained popularity among users in businesses and organisations nowadays. The two main problems facing cloud service providers and their clients are security and efficiency. Cloud-based services come with security threats since cloud computing is a virtual pool of resources offered in an open environment (the Internet). One of the main issues for cloud service providers and users alike is the detection of intrusions and attacks by unauthorised users. In the current study, intrusion and assault detection were accomplished using artificial intelligence approaches, such as the MLP Neural Network and particle swarm optimisation algorithms. Datasets for NSL-KDD and KDD-CUP were used to test the approaches (Saljoughi *et al.*, 2017).

### E. Network Intrusion Detection Method Combining CNN and BiLSTM in Cloud Computing Environment

In this paper, a CNN-Bi LSTM and C5.0-based network intrusion detection system is proposed. First, the original data set is processed using procedures including data

cleaning, data extraction, and data mapping before the data extraction method, SamExtract, is used to turn multiple traffic samples into grayscale images. Second, to make up for the insufficient extraction of local features, local parallel features are retrieved by CNN. To better understand the impact of the attributes before and after each attribute point in the sequence data, and to reduce FA, utilise bi-LSTM to extract long-distance-dependent features (Gao, 2022).

#### F. Application of data mining technology in detecting network intrusion and security maintenance

To detect network intrusion and maintain security, this work suggests an enhanced k-means algorithm and an improved *apriori* algorithm used in data mining technologies. The trial with the enhanced algorithms was carried out in this work using the traditional KDDCUP99 dataset. Comparisons are made between the algorithm's detection rate and false alarm rate and the experimental data from before the improvement. In terms of several simulation characteristics, such as average time, false alarm rate, absolute error, and accuracy value, the results of the proposed algorithms are examined. The findings demonstrate that the enhanced algorithm improves the detection model's designed detection efficiency and accuracy (Zhu *et al.*, 2021).

#### G. Intrusion Detection System with Snort in Cloud Computing: Advanced IDS

To guard against malicious packets, a Snort-based intrusion detection system was introduced in this work. Snort in IDS is efficient and more secure in identifying intrusions and has proven to be more advantageous to the user or organisations because security in cloud computing is essential to storing and moving the data over the internet. Data packets are more securely protected by Snort since they are thoroughly processed by network layer protocols (Mishra *et al.*, 2016; Modi *et al.*, 2012).

#### H. A fingerprinting system calls approach for intrusion detection in a cloud environment

Cloud-based systems are vulnerable to a wide range of assaults because of their distributed nature, with VM-based attacks being the most prevalent. Intrusion Detection System (IDS), which is used to monitor network traffic and policy breaches from unauthorised users, is necessary to defend against these attacks. Anomaly Detection is a method of Intrusion Detection that uses system activity monitoring to identify patterns that deviate from expected behaviour to uncover intrusions. This study presents a method for detecting anomalies in cloud environments that are based on system call sequence analysis from the virtual machines to the hypervisor (Gupta *et al.*, 2012).

### IV. INTRUSION DETECTION SYSTEMS IN THE CLOUD

Intrusion detection systems have become an important aspect of security measures to shield and protect computer resources and the entire network from any activities that are suspicious and dangerous to the computer systems. Hence, an intrusion detection system may be a hardware or software program that tracks, monitors, analyses, and reacts to hostile behaviour occurring on a computer system or network for indications of potential security policy violations (Khairkar *et al.*, 2013). If such activity is found, it issues a warning alarm and sends notifications to the system administrator. However, the

performance of the system may be impacted if the warning alerts sent by the IDS are false alarms or irrelevant to the real breach. IDS must be built so that it can identify false alarms in addition to intrusions.

A strong cloud security strategy must include cloud IDS as a key component. A cloud intrusion detection system is an IDS that has been built in a cloud-native form factor to monitor both on-premises and cloud-based assets as part of a cloud-delivered security strategy or for the protection of cloud-based resources under an IaaS security model (Kene & Theng, 2015; Lata & Singh, 2022). To detect and stop attacks that come from both within the cloud itself and from users accessing cloud technology from various locations via the Internet, a proper defence strategy in the cloud needs to be properly distributed.

As a result, IDS should be designed and implemented in such a way that they can detect all attacks connected to clouds across the entire cloud network with as few false alarms as possible. A cloud intrusion detection system (IDS) is essential for intrusion detection and incident response in cloud-based technology (Rani & Gagandeep, 2022). Key characteristics of a cloud IDS include (Kene & Theng, 2015; Lata & Singh, 2022):

1. Integrated Security: IDS capability is frequently included in other security products, including security gateways for cloud-native environments, next-generation FWaaS, SSE, and SASE. This security integration allows automatic threat detection and response while also streamlining security administration.
2. Threat Detection: An intrusion detection system's main objective is to detect threats. To find possible threats and produce alerts, an intrusion detection system may employ a range of various processes (machine learning, signature detection, anomaly detection, etc.).
3. Easy Installation: Cloud intrusion detection systems can be set up either utilising a service-based architecture or as virtual appliances. As a result, it is easy to roll out new solutions quickly to address shifting business needs.

An organisation can use a cloud IDS to efficiently and scalably identify potential threats to their cloud-based deployments. An organisation can gain from using cloud IDS in the following ways:

1. Cloud protection: Businesses are increasingly processing and storing data on cloud infrastructure. A corporation's security team may discover and address any threats to its cloud-based infrastructure because of a cloud IDS (Kene & Theng, 2015; Lata & Singh, 2022).
2. Flexibility: A cloud-based virtualised architecture that is shared by an IDS also has this benefit. Because the solution is built as a virtualised appliance or is used in a service-based paradigm, businesses can deploy, modify, or discontinue security monitoring capabilities as needed to meet shifting business needs.
3. Remote Access Support: Businesses are encouraging employees to work remotely more and more, and these remote employees need access to corporate cloud services. IDS can be used as a part of a SASE solution, which combines an IDS and secures remote access functionality into a single, cohesive package.
4. Managed Security: Cloud intrusion detection could be used with a service-based product like SASE or firewall as a service (FWaaS). This makes it possible for a

company to delegate to their security service provider the duties and costs associated with security management.

5. **Scalability:** Cloud-native IDS provides the scalability benefits of the cloud-based architecture. With the aid of a cloud IDS, an organisation's security monitoring capabilities may scale to meet demand and keep up with the expansion of cloud-based services.

#### A. Types of cloud-based IDS

Intrusion detection systems (IDSs), which are security technologies, are used to identify suspicious or malicious activities by both internal and external intruders. Such intrusive acts are seen as odd and against the security guidelines of the system. The IDS should sound an alarm when it detects these. This security concept is an active monitoring and defence solution that guards vital IT infrastructure against shady activities. IDS usage has expanded significantly because of the large number of data points and increasingly complicated system threats. Traditional IDS approaches do not meet cloud needs because most of the business and IT sectors are migrating toward decentralised architectures like cloud computing. IDS can be classified into four deployment categories in a cloud computing environment, (Rani & Gagandeep, 2022), as shown in Figure 2.

1. **Host-based IDS (HIDS):** It acquires and analyses data from a particular host to detect intrusive events. The data may be found in system logs or operating system audit trails. When a system or application behaves differently, HIDS analyses the data and alerts network management that the system is being attacked (Vieira *et al.*, 2010; Zouhair *et al.*, 2018). The effectiveness of HIDS can be improved by identifying the characteristics that provide it with additional information for detection (Mehmood *et al.*, 2013).
2. **Hypervisor-based:** A framework for communication across VMs is provided by the hypervisor. IDSs based on

hypervisors are installed at the hypervisor layer. It helps in the assessment of already-available information for the detection of unexpected behaviour. Information is reliant on communication at many different levels, including communication inside the virtual network created on a hypervisor, between VMs, and between VMs (Bharadwaja *et al.*, 2011; Modi *et al.*, 2013). Therefore, HCIDS examines system metrics for cloud instances directly from the hypervisor to search for probable patterns of misuse (Mehmood *et al.*, 2013).

3. **Network-based IDS (NIDS):** All network traffic is recorded and examined by NIDS to spot potential intrusions like port scanning and DoS attacks, among other things. NIDS typically performs intrusion detection when capturing network packets by processing the IP and transport layer headers (Gao, 2022; Hsu *et al.*, 2019; Sakr *et al.*, 2019). To locate intrusions, it uses anomaly-based and signature-based detection methodologies (Mehmood *et al.*, 2013). Network intrusion detection systems (NIDS) collect network packets and look for connections to well-known attack signatures, or they match real-time user behaviour to profiles that are already known about them (Chung *et al.*, 2013).
4. **Distributed IDS (DIDS):** It consists of multiple IDSs over a large network, all of which communicate with each other, or with a central server that facilitates advanced network monitoring, incident analysis, and instant attack data. By having these cooperative agents distributed across a network, incident analysts, network operations, and security personnel can get a broader view of what is occurring on the network (Kumar *et al.*, 2022). DIDS allows for efficient management of its incident analysis resources by centralizing its attack records and giving an analyst a quick and easy way to spot new trends and patterns and identify threats to the network across multiple network segments (Idhammad *et al.*, 2018).

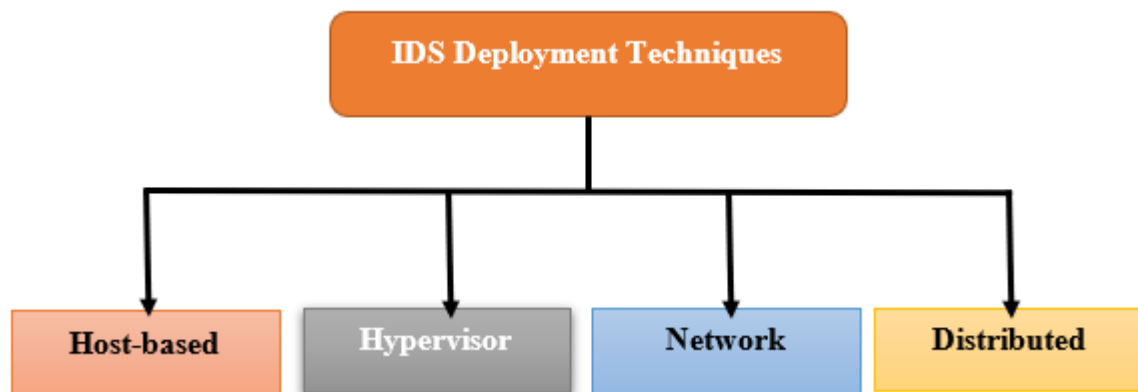
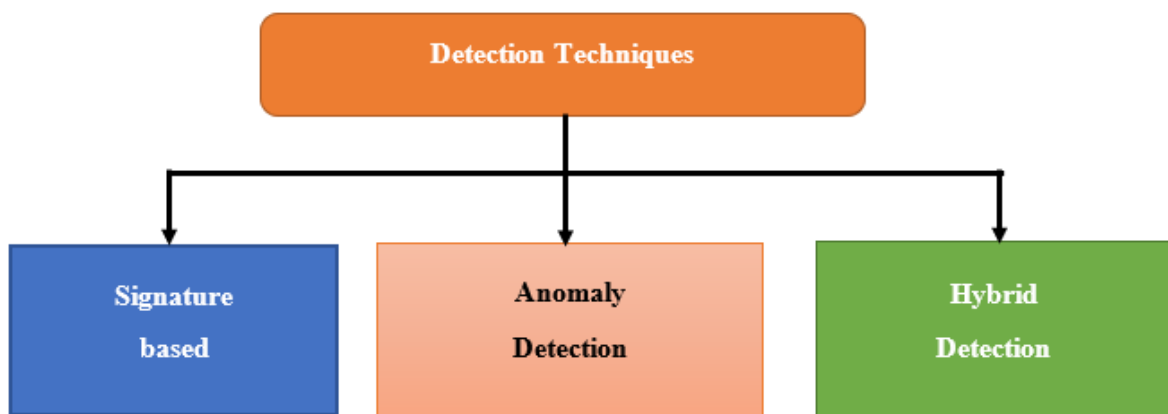


Figure 2: Deployment Techniques (Saljoughi *et al.*, 2017)

Table 1. The Summary of Deployment Techniques in Intrusion Detection Systems

IDS	Characteristic	Limitation	Positioning in Cloud	Deployment and monitoring authority
HIDS	Detect intrusions by keeping an eye on the file system, system calls, or network activity of the host.  No additional hardware is needed.	Installation of the host, hypervisor, or virtual machine software is required on each system.  It can only keep track of attacks on hosts where it is installed.	On every host, hypervisor, or VM system	Cloud Users on VMs.  Cloud provider on the hypervisor.
NIDS	Detect intrusions by keeping an eye on network activity.  Only the underlying network needs to be installed.  Multiple systems can be monitored simultaneously.	It only aids in detecting external intruders.  it is challenging to identify network intrusions in virtual networks.  it is difficult to detect intrusions from encrypted communications.	Either in a virtual or external network	Cloud service
Hypervisor	It enables users to track and examine communications within the hypervisor-based virtual network, between VMs, and between the hypervisor and a VM.	New and challenging to comprehend	The hypervisor	Cloud service
DIDS	utilises traits from both NIDS and HIDS and gains advantages from each of them as a result.	Expensive communication and processing costs.  Difficult to manage in a centralised DIDS.	External network, on a host, a hypervisor, or a virtual machine.	Cloud users on VMs. In other cases: cloud service provider

Figure 3: Detection Techniques (Saljoughi *et al.*, 2017)

### B. Techniques for detecting an intrusion.

In cloud environments, different methods and techniques for detecting intrusion are used, such as anomaly-based, signature-based, or a combination of both.

#### 1. Signature-based intrusion detection techniques

The signature-based intrusion detection system (IDS) will monitor network traffic packets and compare them to a database of known malicious threat signatures, or rules. Since they do not need to learn the environment, signature-based techniques are simple to deploy and work by merely searching, inspecting, and comparing the contents of captured network packets for known threat signatures (Kene

& Theng, 2015). Additionally, it contrasts behaviour signatures with those that are permitted. The system calls are also examined using a signature-based methodology for known risks. payload When used with known attacks and violations, the signature-based approach is quite effective, but unless it is updated with new signatures, it cannot identify new assaults (Mudzingwa & Agrawal, 2012). Attackers can easily get around signature-based detection systems by modifying known attacks and aiming for systems that have not been updated with fresh signatures that identify the alteration.

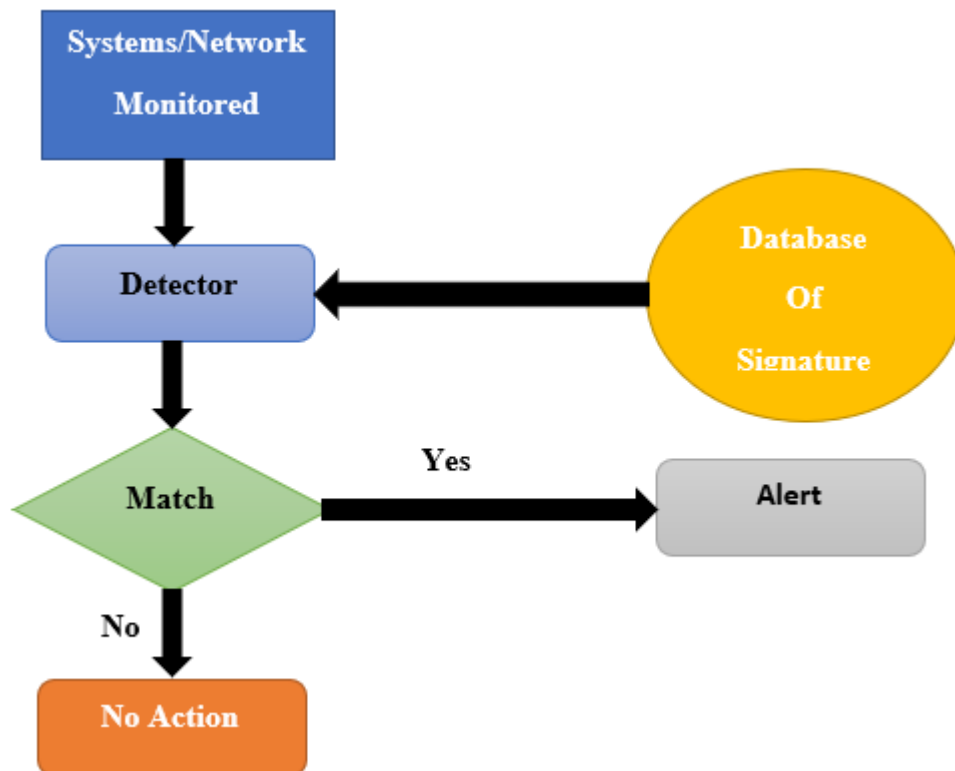


Figure 4: Signature-Based Methodology Architecture (Mudzingwa & Agrawal, 2012)

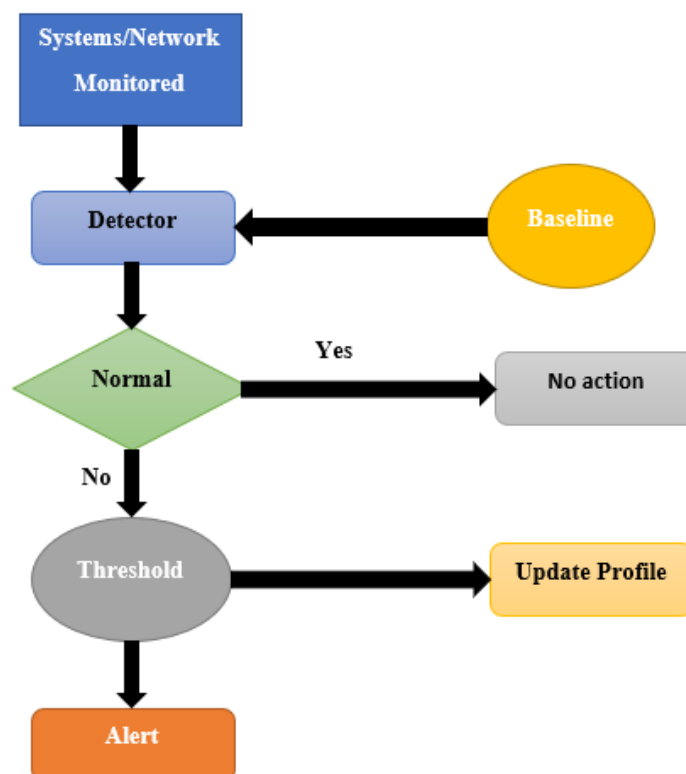


Figure 5: Anomaly-Based Methodology Architecture (Mudzingwa & Agrawal, 2012)

## 2. Anomaly-based intrusion detection techniques

Anomaly-Based Intrusion Detection System, also known as behaviour-based, monitors network traffic and compares it to the expected flow. Anomalous activity is alerted to the administrator or user by any deviation from typical traffic. Given that not all anomalies are intrusions, the rate of false positives is considerable. These IDS require system

administrators to distinguish between genuine attacks and false positives due to the possibility of many deviations in incoming traffic packets and known patterns. By contrasting observed activity with a reference profile, anomaly-based analysis analyses data. The baseline profile, which represents the monitored system's learned typical behaviour, is created during the learning phase, during which the IDS learns the

environment and creates a typical profile for the monitored system. Networks, people, and systems can all be parts of this ecosystem, and the anomaly itself may be static or dynamic. A dynamic profile varies as the systems being monitored develop, while a fixed profile remains constant after it has been set. Zero-day assaults on the environment can be found using anomaly-based approaches without the need for system updates (Mudzingwa & Agrawal, 2012). Three general methods, statistical anomaly detection, knowledge/data mining, and machine learning or deep learning, are used by anomalous intrusion detection methodologies to find anomalies. With the level at which the intruders are operating, a high-intelligence IDS is needed to protect the cloud environment.

The introduction of soft computing approaches is appealing to use in intrusion detection because of their capacity to deal with ambiguous and incomplete data (Modi *et al.*, 2012). To increase the effectiveness and detection accuracy of signature-based IDS or anomaly detection-based IDS, a variety of soft computing techniques, including Artificial Neural Networks (ANN), Fuzzy Logic, Association Rule Mining, Support Vector Machines (SVM), Genetic Algorithms (GA), etc., are used.

- **Artificial Neural Network (ANN):** ANNs are used for intrusion detection to generalise information from sparse data and to categorise data as either normal or intrusive. The following are the ANN kinds that are utilised in IDS: Multi-Layer Feed-Forward (MLFF) neural networks, Multi-Layer Perceptron (MLP), and Back Propagation (BP). Unstructured network data can be effectively handled by ANN-based IDS. The number of hidden layers and the ANN training phase determine the efficacy of this approach's intrusion detection (Modi *et al.*, 2012). To learn ANN effectively, though, additional training samples and time are needed. Since a speedy intrusion detection technique is needed for cloud intrusion detection, using just ANN-based IDS is not a viable option.

- **Support Vector Machines (SVM):** For binary classification, the SVM is already regarded as the top learning method. The SVM has been successfully used in a range of pattern recognition applications. It is a sort of pattern classifier that was initially based on a statistical learning technique for classification and regression with a variety of kernel functions. It has recently been used in information security for intrusion detection. Because of their high generalisability and capacity to escape the "dimensionality curse," support vector machines have emerged as one of the most widely used methods for anomaly intrusion detection (Jha & Ragha, 2013).
- **Genetic Algorithms (GA):** Another machine learning strategy built on the fundamentals of evolutionary computation is genetic algorithms. They combine the ideas of Darwin's theory and natural selection to produce a set of guidelines that may be used to categorise incursions on a testing set. The use of GAs in intrusion detection has been studied by researchers (Goyal *et al.*, 2011).

### 3. Hybrid-based intrusion detection techniques

This method combines anomaly-based and signature-based detection methods to find intrusions more rapidly and accurately than either method by itself. A hybrid approach takes advantage of the best features of both; it uses the misuse and anomaly approaches, respectively, to identify known and unknown dangers. Using a variety of soft computing techniques, it might be feasible to simultaneously identify any type of assault. The authors used signature-based techniques with fuzzy genetic algorithms to discriminate between external and internal threats. Figure 5 provides a general overview of a hybrid-based methodology that combines three distinct methodologies (Mudzingwa & Agrawal, 2012). The first methodology analyses the monitored environment before passing it on to the second and third methodologies. An improved system results from this.

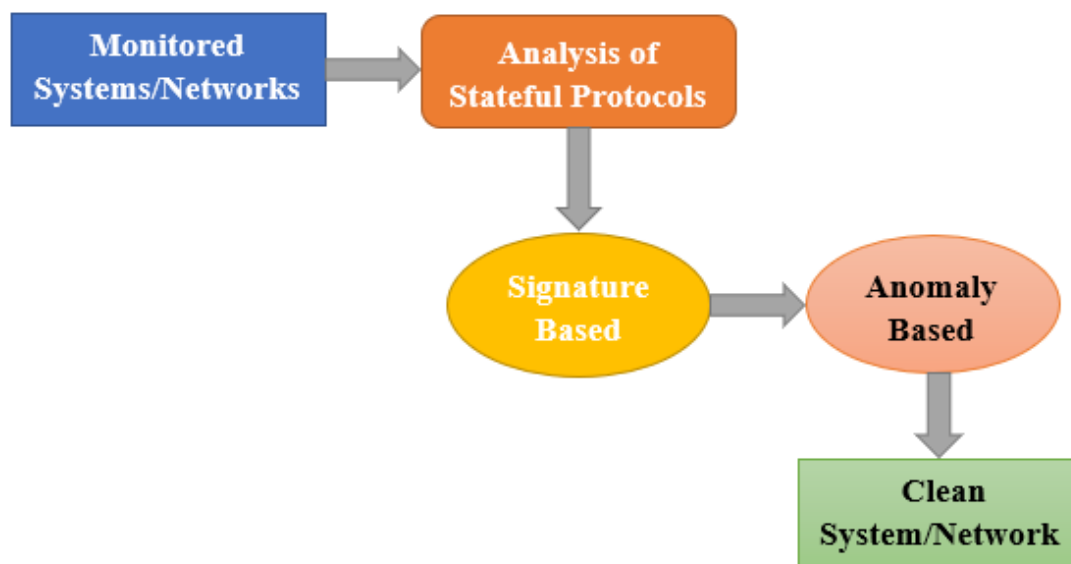


Figure 6: Hybrid-based methodology architecture (Mudzingwa & Agrawal, 2012)

### C. Analysis of related cloud-based intrusion detection systems (CIDS)

In this section, we will discuss different CIDS and categorise them into three groups according to the intrusion detection method that each system employs. The three types are hybrid, anomaly-based, and signature-based.

#### 1. Signature-based IDS

From the existing research based on signature IDS, to combat DoS and DDoS attacks, the authors suggested and modelled an IDS that functions cooperatively (Lo *et al.*, 2010). It consists of four parts, each having a distinct function. By capturing and examining network packets, the first one carries out intrusion detection. It immediately discards the packets that show a correlation with the block table rules, or else it forwards the anomalous packets that don't match these criteria to the alert clustering component, which determines the alert level of the received suspicious packet. The third element suppresses intrusion packets and notifies other IDS. The fourth part compiles warnings from other IDS and conducts a majority vote to decide on a packet. By implementing the suggested IDS, we can defend the system against single-point-of-failure attacks. However, because it uses signature-based detection approaches to find intrusions, it cannot detect unidentified attacks.

To identify denial-of-service (DoS) attacks on virtual SIP-based hosts, Mazzariello *et al.* (2010) examined the deployment of an intrusion detection system (IDS) at various locations within the cloud. The trials were carried out by the authors using Eucalyptus as a cloud and Snort as a network-based IDS. Eight virtual machines are being hosted by two of the six physical machines. There are two security groups set up, each with a SIP server, an Apache web server, and several RTP-based agents. To create background traffic, utilise distributed internet traffic generator (D-ITG). The SIP flood traffic is created using the "Invite Flood" program. The authors considered two scenarios to evaluate the IDS performance dependent on its cloud location. Findings from the assessment show that a single IDS instance placed close to the Cloud Controller (CC) will significantly increase the load on the CC when it comes to detecting DoS assaults. On the other hand, the deployment of a separate IDS instance at each virtual machine only affects the CPU burden of the attacked VM and has little to no effect on the other VMs. The suggested method relies on signatures and cannot identify unidentified attacks.

Another study by Bakshi and Dujodwala (2010) has proposed and implemented a distributed denial of service (DDoS) attack detection solution. Installing an IDS (such as Snort) on a virtual switch will enable the logging of incoming and outgoing traffic for auditing purposes into a database. The IDS detects specific threats (based on rules) in real-time by examining network packets. If IDS notices a lot of packets coming from a certain IP address (a DDoS attack), it notifies the virtual server, which bans the IP addresses of all the zombies in the botnet. The virtual server also updates routing tables and transfers the attacked apps to virtual machines (VMs) located in a different datacenter.

#### 2. Anomaly-based IDS

An intrusion prevention system with autonomous agents has been presented by Patel *et al.* (2010). The method of detection is based on anomalies. Autonomous sensors are

used to keep an eye on network activity and system activity to spot suspicious events (such as system calls, file access, and changes). The system is capable of self-management with minimal human involvement, and the agents can be changed in-flight without having to restart them. The prevention system manages these agents by giving them high-level orders, including the provision of rules to stop an impending attack before it occurs based on risk analysis and risk appraisal. The necessary features are accomplished via a tiered management paradigm. There are seven layers: resource managers, knowledge and learning managers, risk managers, autonomous element managers, autonomous coordinators, and an integrated interface.

According to the degree of user abnormality, Lee *et al.* (2011) have presented a novel method to discover intrusions for efficient resource use. The authentication, authorisation, and accounting (AAA) module of the suggested system is a crucial component. When a user tries to use cloud services, a AAA module-based authentication procedure is applied. After successful authentication, the user's anomaly level—which is based on current database information about the user—is sent to the user. In light of the user's level of abnormality, AAA selects the appropriate IDS with the appropriate security level. The host operating system (OS) is configured with the selected IDS, and AAA requests that it assign the user's guest OS. When a guest OS is assigned to a user, a connection is made between the guest OS and the user's data in the storage centre. IDS has three different security levels: high, which employs all known attack patterns as well as some anomaly techniques when extra security is needed; medium, which provides a moderate level of security using all known attack patterns; and low, which employs a subset of known attack patterns that are particularly risky, common, and seriously damaging to systems. As a result, the suggested method provides speedy attack detection and enables the assignment of many guest OSs because medium- and low-level IDS have low resource needs.

The Virtual Machine Monitor (VMM) has been presented as a method for identifying intrusions in a virtualised environment (Bharadwaja *et al.*, 2011). Every VMM has the "Collabra" system, which acts as a link between Dom0 of the Xen-based virtual network and the VMM. It maintains track of and checks for anomalies in hyper-calls made to VMM by guest virtual machines (VMs). The use of anomaly-based detection is made necessary by the lack of well-known hyper-call attacks that can be utilised as signatures. As a result, it can effectively detect unidentified attacks. The system functions cooperatively because it can communicate with every copy of itself that is installed on different VMMs. Logical domain channels (LDC) are utilised as soon as an intrusion is found to notify other instances of the attack's features and to seek the sanitisation of the specific VMM. The hyper-calls are split into normal and abnormal groups based on a threshold value. One of the two primary security features provided by the Collabra system is the hyper-call integrity check, which performs cross-verification for each hyper-call started by a guest VM based on a message authentication code (MAC) and a designated policy for that call. With the aid of the MAC, a network of virtual machines running on a hypervisor can be maintained securely. access to the hyper-call origin where the admin version of Collabra may identify the origin of approved hyper-calls. When a

guest VM hyper-call originates from a website other than an authorised application, it is flagged as untrusted, and the associated Collabra instance is informed of the details of the call. The proposed method enables rapid detection of coordinated and distributed attacks at the hypervisor layer.

### 3. Hybrid IDS

To defend against both known and unknown attacks, Modi *et al.* (2012) have created and deployed a network IDS that uses Snort to identify known attacks and a Bayesian classifier to detect unknown attacks. The primary components of the suggested system are as follows:

During packet preprocessing, information from network packets that is unrelated to detection is removed. To assess if a packet is normal or an intrusion, the analyser uses a signature-based or anomaly-based detection method. If the packet is an intrusion, it is recorded using a Bayesian classifier, Snort, and Alert Log. Other servers' NIDS receives alert logs, notifies them, and keeps them on their systems. In the knowledge base and behaviour base, respectively, of the storage module are stored the rules of known attacks and frequent or invasive network events. Initially, Snort is used to identify intrusions when network packets are collected and intrusion events are stored in a database of alerts. Preprocessing non-intrusion packets, using a Bayesian classifier to determine whether they should be classified as intrusions or normal while considering the behaviour base, and finally logging the determined intrusions into an alert database are the subsequent steps in anomaly detection. The NIDS placed on each server can more quickly identify unknown threats by adding alarms to their knowledge base. Because anomaly detection only detects unidentified assaults, this method uses it after signature-based detection to speed up detection. Moreover, the detection rate is raised by sending alerts to other NIDS placed in a cloud environment.

Vieira *et al.* (2010) have proposed an Intrusion Detection System for Grid and Cloud Computing (GCCIDS) that operates at the middleware layer and may identify intrusions by combining knowledge-based and behaviour-based techniques. This system's nodes can detect intrusions and send out alerts to other nodes. As a result, the intrusion detection process develops cooperatively. The node, which contains resources that middleware can access equally, the service, which facilitates communication, and the event auditor, which compiles data from various sources, such as the service, the log system, and node messages, are the other two main components of the proposed architecture, in addition to the IDS service. The fourth element is the storage service, which holds the data that the IDS service will be evaluating. The authors evaluated the behaviour-based system by measuring false positives and false negatives, and they concluded that when the same amount of data is used as input, false negatives are always bigger than false positives. However, they found that if only a few comparison criteria are used, it is possible to monitor traffic in real-time using the knowledge-based system when employing audit data from communication and log systems (Vieira *et al.*, 2010). The authors have not yet released implementation details but intend to in their further work.

Shelke *et al.* (2012) have suggested a multi-threaded NIDS to handle the problem of Cross-Site Scripting (XSS) and

DDoS attacks. Three components make up the proposed NIDS, each of which serves a specific purpose: The UDP, TCP, ICMP, and IP packets are collected by the capture module and sent to a shared queue for processing. To assess the received data packets, the analysis and processing module compares them to a knowledge base and a predetermined set of criteria. The multi-threaded processes of the shared queue speed up NIDS. Good matching and evaluation allow for the identification of malicious packets and the generation of alarms. The reporting module generates alarm reports using data from the shared queue. The third-party service, which is keeping an eye on the entire scenario, alerts the user right away to the nature of the attack and provides the service provider with a consulting report (Shelke *et al.*, 2012). Although being a novel approach, the details of how it would be put into practice are not provided to support the idea.

Cross-site scripting (XSS) and DDoS attacks have been addressed by Shelke *et al.* (2012) using a multi-threaded NIDS. Three components make up the proposed NIDS, each of which serves a specific purpose. The UDP, TCP, ICMP, and IP packets are collected by the capture module and sent to a shared queue for processing. To assess the received data packets, the analysis and processing module compares them to a knowledge base and a predetermined set of criteria. The multi-threaded processes of the shared queue speed up NIDS. Good matching and assessment enable the detection of malicious packets and the warning generation. The reporting module produces alarm reports based on information from the shared queue. The third-party service, which is watching the whole situation, quickly alerts the user to the specifics of the attack and provides the service provider with a consulting report. The details of how it might be put into practice are not provided, even though it is an innovative approach.

According to research by Karande and Bhongade (2017) on hybrid intrusion detection systems for securing cloud-based services, the study makes use of an anomaly-based and signature-based intrusion detection and prevention system (IDS/IPS) together to form a hybrid intrusion detection system that is used to detect known attacks and vulnerabilities by signature-based systems and previously unknown attacks by anomaly-based systems, which are further strengthened by the addition of signatures. The learning of the system is done by conditional random field (CRF) (Karande & Bhongade, 2017). In this model, intrusion detection will be classified as signature-based, which matches the association rule with the packet feature to identify between a normal packet and a forged packet. The features of the Packet or network connection are extracted and compared with the Dataset which is built from a series of network captures of port 80 requests made to service during a period of 7 days. The traffic was captured with Wireshark. This tool is an open-source packet analyser that enables capturing live network packet data. Further characterisation is done by Anomaly-based detection where the trace log for the packet is generated which is in common log format and can be used by all readily available IDSs. The behaviour of a packet is monitored from a log which is labelled by learning with Conditional Random Field (CRF).

Using soft computing methods with conventional IDS in a cloud environment is helpful. Each approach does, however, have specific benefits and restrictions that have an impact on

IDS performance. This is summarised in Table 2.

Table 2. Intrusion detection system techniques

IDS Technique	Characteristics	Limitation
Signature-based detection	High detection reliability for known attacks.	High rate of false alarms for unidentified attackers.
	Matches collected patterns with a pre-configured knowledge base to determine intrusion.	Cannot recognise brand-new or modified assaults.
	Low cost of calculation.	Care should be taken when creating the knowledge base for matching.
Anomaly-based detection	A statistical test is applied to collected behaviour to detect incursion.	Attack detection takes a long time.
	Has the potential to reduce the number of false alarms for unidentified attacks.	The quantity of observed behaviour or features determines the accuracy of detection.
Hybrid detection techniques	It is a successful strategy for precisely classifying rules.	The cost of computation is substantial.

## V. CONCLUSION

Cyberattacks are growing at an exponential rate, and there is no well-known method to stop all these attacks. Security has been a major challenge for cloud computing users because of the open and distributed architecture pattern of the cloud system. One of the most important approaches to reducing or stopping a cyberattack is intrusion detection systems (IDS). The implementation of an intrusion detection system has improved cloud security. It aids in ensuring the network's and data's confidentiality, integrity, and availability. A variety of intrusion detection techniques have been used to detect security threats that have evolved in cloud networks. The paper emphasises existing methods of IDS based on traditional techniques using soft computing. The review is then divided into sections based on the different types of cloud-based IDS, such as network-based IDS, host-based IDS, hypervisor-based IDS, and distributed intrusion detection systems, as well as different approaches for detecting an intrusion. Therefore, despite the advancement of numerous techniques and methods of detecting an intrusion in a cloud-based system, lots of loopholes still exist, making the cloud vulnerable to attacks and intrusion. It is therefore recommended that ensemble techniques be considered, which are used to decrease the variation of predictions and generalisation error when developing an intrusion detection system using any of the soft computing methods; this will therefore help to improve the detection rate and reduce false positives.

## REFERENCES

- Ade, D. (2020). *Cloud computing and everything you need to know*. Trends, Web Design Tutorials and Articles. <https://ictacademy.com.ng/cloud-computing-and-everything-you-need-to-know/>
- Bahram, S., Jiang, X., Wang, Z., Grace, M., Li, J., Srinivasan, D., Rhee, J., & Xu, D. (2010). DKSM: Subverting virtual machine introspection for fun and profit. *29th IEEE Symposium on Reliable Distributed Systems*, 82–91. <https://doi.org/10.1109/SRDS.2010.39>
- Bakshi, A., & Dujodwala, Y. B. (2010). Securing cloud from DDOS attacks using intrusion detection system in virtual machine. *2nd International Conference on Communication Software and Networks (ICCSN)*, 260–264. <https://doi.org/10.1109/ICCSN.2010.56>
- Bharadwaja, S., Sun, W., Niamat, M., & Shen, F. (2011). Collabra: A xen hypervisor based collaborative intrusion detection system. *8th International Conference on Information Technology: New Generations (ITNG)*, 695–700. <https://doi.org/10.1109/ITNG.2011.123>
- Chaudhary, A. (2020). *Cloud security challenges in 2020*. Cloud Security Alliance. <https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020/>
- Chormale, A. A., & Ghatule, A. P. (2020). Cloud intrusion detection system using fuzzy clustering and artificial neural network. *Journal of Physics: Conference Series*, 1478(1), 1–13. <https://doi.org/10.1088/1742-6596/1478/1/012030>
- Chung, C. J., Khatkar, P., Xing, T., Lee, J., & Huang, D. (2013). NICE: Network intrusion detection and countermeasure selection in virtual network systems. *IEEE Transactions on Dependable and Secure Computing*, 10(4), 198–211. <https://doi.org/10.1109/TDSC.2013.8>
- Dinh, H. T., Lee, C., Niyato, D., & Ping, W. (2013). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*, 13(18), 1587–1611. <https://doi.org/10.1002/wcm.1203>
- Doan, K., Lao, Y., Zhao, W., & Li, P. (2021). LIRA: Learnable, imperceptible and robust backdoor attacks. *IEEE/CVF International Conference on Computer Vision (ICCV)*, 11966–11976. <https://doi.org/10.1109/ICCV48922.2021.01175>
- Elmasry, W., Akbulut, A., & Zaim, A. H. (2021). A design of an integrated cloud-based intrusion detection system with third party cloud service. *Open Computer Science*, 11(1), 365–379. <https://doi.org/10.1515/comp-2020-0214>
- Farsole, A. A., Kashikar, A. G., & Zunzunwala, A. (2010). Ethical hacking. *International Journal of Computer Applications*, 1(10), 14–20. <https://doi.org/10.5120/229-380>
- Gao, J. (2022). Network intrusion detection method combining CNN and BiLSTM in cloud computing environment. *Computational Intelligence and Neuroscience*, 2022(7272479), 1–11. <https://doi.org/10.1155/2022/7272479>
- Goyal, P., Ribeiro, V. J., Saran, H., & Kumar, A. (2011). Strap-down Pedestrian Dead-Reckoning system. *2011 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 1–7.

- <https://doi.org/10.1109/IPIN.2011.6071935>
- Gupta, S., Kumar, P., Sardana, A., & Abraham, A. (2012). A fingerprinting system calls approach for intrusion detection in a cloud environment. *4th International Conference on Computational Aspects of Social Networks (CASoN)*, 309–314. <https://doi.org/10.1109/CASoN.2012.6412420>
- Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4(5), 1–13. <https://doi.org/10.1186/1869-0238-4-5>
- Hsu, Y. F., He, Z. Y., Tarutani, Y., & Matsuoka, M. (2019). Toward an online network intrusion detection system based on ensemble learning. *IEEE 12th International Conference on Cloud Computing (CLOUD)*, 174–178. <https://doi.org/10.1109/CLOUD.2019.00037>
- Idhammad, M., Afdel, K., & Belouch, M. (2018). Distributed intrusion detection system for cloud environments based on data mining techniques. *Procedia Computer Science*, 127, 35–41. <https://doi.org/10.1016/j.procs.2018.01.095>
- Jang-Jaccard, J., Nepal, S., & Guo, Y. J. (2013). Cybersecurity threats in cloud computing. *Journal of Telecommunications and the Digital Economy*, 1(1), 58–74. <https://doi.org/10.18080/jtde.v1n1.128>
- Jha, J., & Ragha, L. (2013). Intrusion detection system using support vector machine. *International Journal of Applied Information Systems, ICWAC*(3), 25–30. <https://doi.org/10.5120/icwac1342>
- Karande, S. C., & Bhongade, P. S. (2017). Hybrid intrusion detection system for securing cloud based services. *International Conference on Intelligent Computing and Applications*, 1–4.
- Kene, S. G., & Theng, D. P. (2015). A review on intrusion detection techniques for cloud computing and security challenges. *2nd International Conference on Electronics and Communication Systems (ICECS)*, 227–232. <https://doi.org/10.1109/ECS.2015.7124898>
- Khairkar, A. D., Kshirsagar, D. D., & Kumar, S. (2013). Ontology for detection of web attacks. *2013 International Conference on Communication Systems and Network Technologies (CSNT)*, 612–615. <https://doi.org/10.1109/CSNT.2013.131>
- King, S. T., Chen, P. M., Wang, Y. M., Verbowski, C., Wang, H. J., & Lorch, J. R. (2006). SubVirt: Implementing malware with virtual machines. *IEEE Symposium on Security and Privacy*, 1–14. <https://doi.org/10.1109/SP.2006.38>
- Kosamkar, V. B. (2016). Intrusion detection system in cloud computing: An overview. *International Journal on Recent and Innovation Trends in Computing and Communication*, 4(1), 164–167.
- Krishnan, R. (2017). *Security and privacy in cloud computing*. Master Thesis, Western Michigan University.
- Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Garg, S., & Hassan, M. M. (2022). A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. *Journal of Parallel and Distributed Computing*, 164, 55–68. <https://doi.org/10.1016/j.jpdc.2022.01.030>
- Lata, S., & Singh, D. (2022). Intrusion detection system in cloud environment: Literature survey & future research directions. *International Journal of Information Management Data Insights*, 2(2), 1–14. <https://doi.org/10.1016/j.jjime.2022.100134>
- Lee, J.-H., Park, M.-W., Eom, J.-H., & Chung, T.-M. (2011). Multi-level intrusion detection system and log management in cloud computing. *13th International Conference on Advanced Communication Technology (ICACT)*, 552–555.
- Li, Y., Jiang, Y., Li, Z., & Xia, S. T. (2022). Backdoor learning: A survey. *IEEE Transactions on Neural Networks and Learning Systems*, 1–18. <https://doi.org/10.1109/TNNLS.2022.3182979>
- Li, Y., Li, Y., Wu, B., Li, L., He, R., & Lyu, S. (2021). Invisible backdoor attack with sample-specific triggers. *IEEE/CVF International Conference on Computer Vision (ICCV)*, 16463–16472. <https://doi.org/10.1109/ICCV48922.2021.01615>
- Liu, Z., Xu, B., Cheng, B., Hu, X., & Darbandi, M. (2022). Intrusion detection systems in the cloud computing: A comprehensive and deep literature review. *Concurrency and Computation: Practice and Experience*, 34(4), e6646. <https://doi.org/10.1002/cpe.6646>
- Lo, C. C., Huang, C. C., & Ku, J. (2010). A cooperative intrusion detection system framework for cloud computing networks. *39th International Conference on Parallel Processing Workshops*, 280–284. <https://doi.org/10.1109/ICPPW.2010.46>
- Mansouri, N., Ghafari, R., & Zade, B. M. H. (2020). Cloud computing simulators: A comprehensive review. *Simulation Modelling Practice and Theory*, 104, 1–50. <https://doi.org/10.1016/j.simpat.2020.102144>
- Mazzariello, C., Bifulco, R., & Canonico, R. (2010). Integrating a network IDS into an open source cloud computing environment. *Sixth International Conference on Information Assurance and Security*, 265–270. <https://doi.org/10.1109/ISIAS.2010.5604069>
- Mehmood, Y., Shibli, M. A., Habiba, U., & Masood, R. (2013). Intrusion detection system in cloud computing: Challenges and opportunities. *2nd National Conference on Information Assurance (NCIA)*, 59–66. <https://doi.org/10.1109/NCIA.2013.6725325>
- Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. In G. I. Nikolov (Ed.), *Cloud Computing and Government: Background, Benefits, Risks* (pp. 1–7). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-145>
- Mishra, V., Vijay, V. K., & Tazi, S. (2016). Intrusion detection system with snort in cloud computing: Advanced IDS. In S. C. Satapathy, A. Joshi, N. Modi, & N. Pathak (Eds.), *Advances in Intelligent Systems and Computing* (Vol. 408, pp. 457–465). Springer. [https://doi.org/10.1007/978-981-10-0129-1\\_48](https://doi.org/10.1007/978-981-10-0129-1_48)
- Modi, C. N., Patel, D. R., Patel, A., & Muttukrishnan, R. (2012). Bayesian classifier and snort based network intrusion detection system in cloud computing. *3rd International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 1–7. <https://doi.org/10.1109/ICCCNT.2012.6396086>
- Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in Cloud. *Journal of Network and Computer Applications*, 36(1), 42–57. <https://doi.org/10.1016/j.jnca.2012.05.003>
- Mudzingwa, D., & Agrawal, R. (2012). A study of

- methodologies used in intrusion detection and prevention systems (IDPS). *IEEE Southeastcon*, 1–6. <https://doi.org/10.1109/SECon.2012.6197080>
- Mukhopadhyay, R., & Nath, A. (2014). Ethical hacking: Scope and challenges in 21st century. *International Journal of Innovative Research in Advanced Engineering*, 1(11), 30–37.
- Nguyen, T. A., & Tran, T. A. (2020). Input-aware dynamic backdoor attack. In H. Larochelle, M. Ranzato, R. Hadsell, M. F. Balcan, & H. Lin (Eds.), *Advances in Neural Information Processing Systems* (Vol. 33, pp. 3454–3464). NeurIPS.
- Odun-Ayo, I., Ananya, M., Agono, F., & Goddy-Worlu, R. (2018). Cloud computing architecture: A critical analysis. *18th International Conference on Computational Science and Its Applications (ICCSA)*, 1–7. <https://doi.org/10.1109/ICCSA.2018.8439638>
- Patel, A., Qassim, Q., Shukor, Z., Nogueira, J., Júnior, J., & Wills, C. (2010). Autonomic agent-based self-managed intrusion detection and prevention system. In N. Clarke, S. Furnell, & R. von Solms (Eds.), *South African Information Security Multi-Conference (SAISMC)* (pp. 223–234).
- Patil, S., Jangra, A., Bhale, M., Raina, A., & Kulkarni, P. (2018). Ethical hacking: The need for cyber security. *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, 1602–1606. <https://doi.org/10.1109/ICPCSI.2017.8391982>
- Rani, M., & Gagandeep. (2022). An efficient network intrusion detection system based on feature selection using evolutionary algorithm over balanced dataset. In N. Marriwala, C. Tripathi, S. Jain, & D. Kumar (Eds.), *Mobile Radio Communications and 5G Networks. Lecture Notes in Networks and Systems* (Vol. 339, pp. 179–193). Springer. [https://doi.org/10.1007/978-981-16-7018-3\\_15](https://doi.org/10.1007/978-981-16-7018-3_15)
- Sadiku, I. B., Ajayi, W., Sakpere, W., John-Dewole, T., & Badru, R. A. (2022). Effect of traditional and software-defined networking on performance of computer network. *Scientific Journal of Informatics*, 9(2), 111–122. <https://doi.org/10.15294/sji.v9i2.31315>
- Sakr, M. M., Tawfeeq, M. A., & El-Sisi, A. B. (2019). Network intrusion detection system based PSO-SVM for cloud computing. *International Journal of Computer Network and Information Security*, 11(3), 22–29. <https://doi.org/10.5815/ijcnis.2019.03.04>
- Saljoughi, A. S., Mehvarz, M., & Mirvaziri, H. (2017). Attacks and intrusion detection in cloud computing using neural networks and particle swarm optimization algorithms. *Emerging Science Journal*, 1(4), 179–191. <https://doi.org/10.28991/ijse-01120>
- Samreen, A., & Zaidi, F. B. (2012). Design and Development of Credit Scoring Model for the Commercial Banks of Pakistan: Forecasting Creditworthiness of Individual Borrowers. *International Journal of Business and Social Science*, 3(17), 155–166.
- Saraeian, S., & Golchi, M. M. (2020). Application of deep learning technique in an intrusion detection system. *International Journal of Computational Intelligence and Applications*, 19(2), 1–15. <https://doi.org/10.1142/S1469026820500169>
- Shelke, P. K., Sontakke, S., & Gawande, A. D. (2012). Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*, 1(4), 67–71.
- Srilatha, D., & Shyam, G. K. (2021). Cloud-based intrusion detection using kernel fuzzy clustering and optimal type-2 fuzzy neural network. *Cluster Computing*, 24(3), 2657–2672. <https://doi.org/10.1007/s10586-021-03281-9>
- Sunyaev, A. (2020). Cloud Computing. In *Internet Computing* (pp. 195–236). Springer. [https://doi.org/10.1007/978-3-030-34957-8\\_7](https://doi.org/10.1007/978-3-030-34957-8_7)
- Suthar, K. C. (2017). *Data security in cloud computing using encryption and obfuscation techniques*. PhD Thesis, Rai University.
- Thakur, K., Tao, L., Wang, T., & Ali, M. L. (2017). Cloud computing and its security issues. *Application and Theory of Computer Technology*, 2(1), 1–10. <https://doi.org/10.22496/atct20161210>
- Vieira, K., Schulter, A., Westphall, C., & Westphall, C. M. (2010). Intrusion detection for grid and cloud computing. *IT Professional*, 12(4), 38–43. <https://doi.org/10.1109/MITP.2009.89>
- Zhu, Y., Gaba, G. S., Almansour, F. M., Alroobaea, R., & Masud, M. (2021). Application of data mining technology in detecting network intrusion and security maintenance. *Journal of Intelligent Systems*, 30(1), 664–676. <https://doi.org/10.1515/jisys-2020-0146>
- Zouhair, C., Abghour, N., Moussaid, K., El Omri, A., & Rida, M. (2018). A review of intrusion detection systems in cloud computing. In Y. Maleh, A. Ezzati, & M. Belaisaoui (Eds.), *Security and Privacy in Smart Sensor Networks* (pp. 253–283). IGI Global. <https://doi.org/10.4018/978-1-5225-5736-4.ch012>



Editorial

---

# Big Data Concept, Analytics and Hadoop Technology: A Systematic Survey

---

Adelodun Felicia O. and Sakpere Wilson

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Adelodun, F. O., & Sakpere, W. (2023). Big Data Concept, Analytics and Hadoop Technology: A Systematic Survey. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 60-64). Ibadan. <https://doi.org/10.5281/zenodo.8121066>.

# Big Data Concept, Analytics and Hadoop Technology: A Systematic Survey

\*Adelodun Felicia O. and Sakpere Wilson  
Department of Computer Science,  
Lead City University Ibadan, Nigeria  
\*adelodunfelicia@gmail.com

**Abstract:** This paper provides insight into the concept of big data and big data analytic platforms like Spark and Storm to handle a variety of data coming from various sources like the Internet of Things (IoT) which could pose a challenge in production in the industries. The paper discusses the concept of Industry 4.0 and shows how big data in Industry 4.0 can lead to the growth of the economy and the promotion of business in the industry. The paper presents some challenges faced by big data and proffers solutions to these challenges. Hadoop technology is suggested as one of the methods to address some of the challenges of big data. The components of Hadoop technology such as Hadoop distributed file system (HDES), Map reduce, HBASE, HCatalog, Pig and so on, are discussed alongside their functions. The methodology followed to achieve these objectives stated above is a systematic review of current works of literature and related works.

**Key Words:** Big Data, Data Analytics, Industry 4.0, Data Challenges, Hadoop Technology

## I. INTRODUCTION

The importance of Big Data to the industry cannot be overemphasised because of the benefits realised from its analysis. Big Data is the phase that describes the data set with size and type surpassing the capacity of the traditional methods (Komal, 2018; Nagat Mohamed, 2020). Big Data has these attributes: massive volume, great speed, high variety, high accuracy (Komal, 2018) and high complexity. The traditional method differs from data analytics because it is expensive and cannot handle data that are heterogenous and in large volumes (Raheem & Uwanthika, 2019). Data analytics is less expensive and can handle heterogeneous data.

Data analytics is the use of advanced analytical techniques on big data to extract hidden patterns and information to help business organisations to study their business trends, make quick decisions and discharge their duties at a fast rate when compared to the traditional method (Raheem & Uwanthika, 2019). The traditional method can only process data that is in structured form whereas, Big Data analytics can process any form of data. It can be applied to semi-structured, unstructured or no form of data.

Data analytics is a combination of big data and data analysis (Russom, 2011). Big data and data analytics remarkably affect research and technology because decision-makers use the information gained from accumulated data for competitive advantage (Cuzzocrea et al., 2011).

The following sections of the paper will discuss related works, the importance of big data analytics in the industry,

industry 4.0 and its expectations for business organisations, Hadoop and its components, challenges of big data and solutions to big data challenges. The methodology used in this paper was the systematic review of the literature.

## II. RELATED WORKS

To meet up with challenges and avoid disruptions in production, Gokalp et al. (2016) built a conceptual framework that supported multiple big data platforms such as Spark, Storm and Flink. Their framework was to handle the variety of data coming from various sources like Internet of Things (IoT) devices which could pose challenges to the acceptance of Big Data analytics in Industry 4.0 (Mishra & Misra, 2017; Shi-Nash & Hardoon, 2017).

Tsai et al. (2015) in their study suggested sampling, data condensation, divide and conquer as methods to reduce the complexity and improve the performance of data analytics. They stated that sampling could be used to accelerate the computational time of data analytics. It should be noted that though sampling speeds up the computational time of data analytics, by it reducing the volume of information, it avoids dreariness in work and the limitation of information may mislead the results. Data condensation is when a small data set replaces a large data set. In this case, one will not have true knowledge of what is happening so one cannot be depended upon to make true decisions concerning customers, production or business trends.

In the review paper and comparative assessment of big data analytics, Komal (2018) identified some of the challenges associated with big data, like data storage issues, data inconsistency, data insecurity and untimeliness, but did not provide solutions that will correct these challenges. The review paper by Elgendy and Elragal (2014) on data analytics discussed some challenges and solutions to big data and data analytics problems. The solutions they provided to solve these challenges were narrowed only to data storage and its management. They developed a non-relational database, not only SQL (NoSQL), for data management and data storage.

## III. BIG DATA ANALYTICS IN THE INDUSTRY

Big data analytics is very important and needful in this age where business worlds are in a high competition requiring smart manufacturing, meeting targets, operating at high speed and maintaining high production quality and efficiency (Ajah & Nweke, 2019; Tawalbeh & Saldamli, 2021; Wang et al., 2022).

1. Big data or huge amounts of data are generated in real-time over infrastructures because of advancements in sensor technology and the traditional methods of analysing data cannot manage or handle these data

because of their size.

2. Big data comes in a variety of forms such as structures, semi-structured and unstructured forms and from different sources and sizes that could pose challenges that can prevent the adoption of analytic tools in Industry 4.0. The larger the data the more difficult it is to analyse. Big data analytic tools play an important role in the analysis and mining of a variety of data generated over the internet.
3. Big Data analytic tools perform analysis and mining on huge amounts of data collected from smart sensors to discover patterns and trends to improve business decisions.
4. Big data analytic tools can identify the source(s) of problem production and help the manufacturer to improve productivity while eliminating waste and reducing cost.
5. Control software connected to robots can take inferences made from big data analytic tools to alter settings on equipment and machine without any human intervention.
6. Big data analytics help industries study business trends, make quick decisions and work at a faster rate when compared to the traditional method (Raheem & Uwanthika, 2019).

Elgendy and Elragal (2014) presented the following benefits to be realised in the application of Data analytics on big data.

1. Data analytics enhances Advanced Data Visualisation (ADV) (Russom, 2011), so that information can be consumed effectively to enable decision-makers to analyse data properly (Manyika et al., 2011).
2. Data analytics can enable organisations to invent new products and services, new business ideas and models.
3. Benefits can be realised from big data analytics in customer preference, supply chain intelligence, fraud detection and risk management (Manyika et al., 2011).
4. Big data analytics creates clarity and ensures that appropriate data are easily accessible to the stakeholders on time (Manyika et al., 2011). The main stakeholders that benefit from data analytics are the manufacturers, retailers, government, healthcare system, telecommunication and banking industries.
5. Big data analytics help industries to make more knowledgeable decisions and alert them on time when customers are moving to different products so that prompt actions can be taken before it is too late (The Economist Intelligence Unit, 2012).
6. Information obtained from data analytics helps organisations segment customers based on their socioeconomic status as well as increase their levels of satisfaction.

#### IV. INDUSTRY 4.0 AND ITS EXPECTATIONS FOR ORGANISATIONS

Industrial development has evolved into four stages of the industrial revolution. The mechanical revolution involved doing work with machines instead of working with hands or animals. The second revolution is the stage of the mass production era. It was the application of technology to increase the production of large amounts of similar products with little human effort. The third stage of the industrial revolution was the development of digital computers to enhance connectivity and access to trade and public services.

The fourth industrial revolution is the emergence of Industry 4.0. It uses technologies such as data analytics and the Internet of Things to monitor the production process (Singhal, 2021). Industry 4.0, also called a smart factory, is the act of using computers in the manufacturing process (computer-aided manufacturing) to take charge of the whole production process in the industry (Rai et al., 2021; Sadiku et al., 2022). Industry 4.0 focuses on connectivity, intelligence and flexible automation (Machado et al., 2020; Rai et al., 2021; Xu et al., 2021). Manufacturing was defined as the coupling of components into finished products on a large scale to produce high-quality products at minimised cost (The Editors of Encyclopaedia Britannica, 2023).

Industry 4.0 is based on intelligent systems with Internet of Things and Internet of Services (Haller et al., 2009; Hogan et al., 2016; Wang et al., 2022) and big data mining (Oks et al., 2017; Oliff & Liu, 2017). Industry 4.0 offers industries the possibilities of digital transformation and data-driven solutions through the application of big data analytics and data analysis tools (Elgendy & Elragal, 2014; Komal, 2018). Manufacturers can gain insights to optimise productivity through the application of data analysis.

The goal of Industry 4.0 is to use digital technology to automate the processes involved in manufacturing to maximise efficiency and identify barriers before they occur (Rai et al., 2021) and lowering production costs of existing industries and increasing product quality and innovation (Oliff & Liu, 2017; Xu et al., 2021). Industry 4.0 helps to address workforce insufficiency and promotes competence in performance (Machado et al., 2020). Industry 4.0 implies manufacturing in the industry.

Industry 4.0 connects the digital world to the physical world using computer-based algorithms, sensors and devices to link and exchange data with systems and other devices over the Internet (Gokalp et al., 2016; Rai et al., 2021; Xu et al., 2021). Industry 4.0 aims at increasing individualised customer requirements (Machado et al., 2020). It is the technological evolution from embedded systems to cyber-physical systems (Gröger, 2018; Oks et al., 2017). A Cyber-physical system is the physical production steps accompanied by computer-based processes (Oks et al., 2017). Industry 4.0 is the digitalisation of the manufacturing sector and the analysis of all relevant data (Manyika et al., 2011).

#### V. HADOOP AND ITS COMPONENTS

Hadoop is an open-source software framework that supports the processing and storage of large amounts of data sets with high processing power and the ability to handle concurrent tasks. Hadoop provides two fundamental functions for data processing; Map and Reduce (Rajput & Mehta, 2017). Map combines and transforms the data supplied by the user while Reduce groups the output obtained from Map. Hadoop is best for handling big data processing. Hadoop processes big data in a distributed computing environment (Rajput & Mehta, 2017). Hadoop Technology process massive data in an efficient, cost-effective and timely manner (Khan et al., 2014).

Hadoop, MapReduce and Big Table are some of the most commonly used tools used for the organisation and

examination of big data. Hadoop comprises of Hadoop Distributed File System (HDFS), MapReduce, HBase, Hcatalog, Pig, Hive, Oozie, Zookeeper Mahout, and Kafka. HDFS and MapReduce are the most well-known component

of Hadoop (Khan et al., 2014).

Figure 1 shows the Hadoop ecosystem. Table 1 depicts the components of Hadoop and their functions.

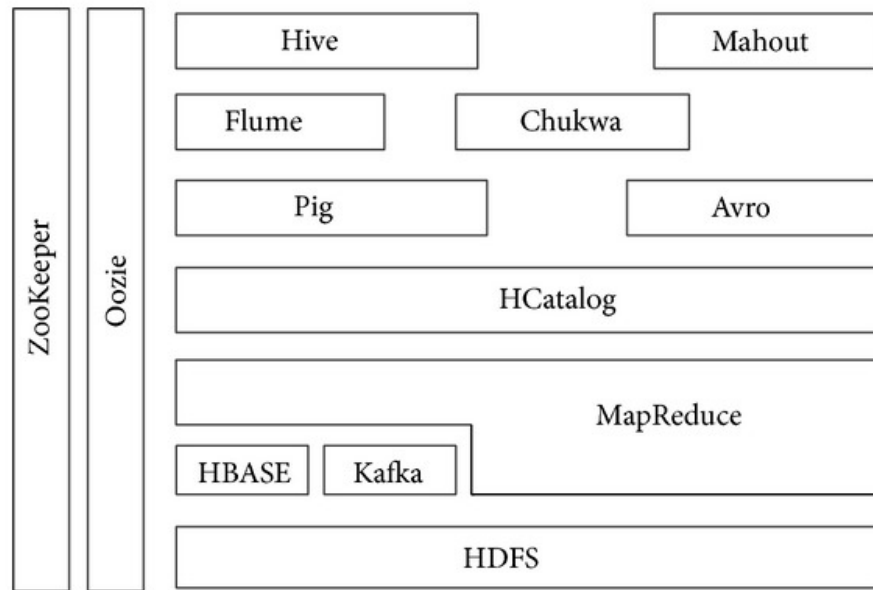


Figure 1: Hadoop Ecosystem (Khan et al., 2014)

Table 1: Hadoop components and their functions

Hadoop Component	Functions
HDFS	Stores large volumes of data and its fault tolerance is high.
MapReduce	Analyses complex big data.
HBASE	Increases the performance of similar data in big data.
HCatalog	Enables users with diverse processing tools into a grid with little effort.
Pig	Enables users to execute jobs in MapReduce.
Mahout	It is a collection of machine learning and data mining tools.
Oozie	Scheduling and executing workflow in Hadoop.
ZooKeeper	Maintains and coordinates large volumes of data.
Kafka	Massive message streams and data integration for data analysis
Hive	Facilities for storing data.

HDFS is used for handling big data beyond the capacity of one machine. HDFS facilitates the concurrent processing of massive data. HDFS stores a very large volume of data and its fault tolerance is very high (Rajput & Mehta, 2017). HDFS architecture is made up of three nodes which include the Name, Data and Edge nodes. The name Node plays the role of the master node, Data Node plays the role of the Slave Node and the Edge Node acts as a link between the Data node and Name node. The Name nodes receive requests from the Edge node and transfer these requests to Data nodes where successful requests will reside.

HBase: Relies entirely on the zookeeper instance to increase the performance of operations over similar values across large data sets.

HCatalog: It stores metadata and generates tabular data of HIVE metastore to enhance users with diverse data processing tools to write data into a grid without difficulty.

Pig: generates a high-level platform that creates programs (Pig latin) that enables users to execute jobs in MapReduce.

Mahout: This is a collection of machine learning and data mining tools.

Oozie: organises, executes and schedules job flow.

Avro: A data serialisation framework that provides data exchange services, between big data in any programming language. It performs remote procedure calls.

Zookeeper: provides the services of maintenance, configuration and naming of large amounts of data.

#### A. Advantages of the Components of Hadoop (Suguna, 2016)

1. Hadoop Distributed File System (HDFS) is not expensive, and the fault tolerance is high.
2. HBase is consistent and its flexibility is high.
3. Hive has infrastructure for storing data.
4. Pig saves development time and reduces duplication of data.
5. Zookeeper produces reliable data, it is simple and fast to use.
6. Mahout analyses and mines large volumes of data. It is used for data mining to find hidden patterns.
7. Oozie allows jobs to be controlled from anywhere.

## VI. CHALLENGES OF BIG DATA

Despite the benefits of big data and data analytics, they face a lot of problems and challenges. A few of these challenges are discussed below.

1. Representation of data, which can result in the reduction of data validity and originality and eventually cause ineffective data analysis. A well-represented data will show data structure, class, type and integrated technologies, which will assist in efficient operations

- on the various data set and reduce redundancy and cost.
2. Data contradiction and deficiency, untimeliness and scalability (Ajah & Nweke, 2019; Prarthana & Jayakumar, 2017; Raheem & Uwanthika, 2019).
3. Traditional methods cannot process massive heterogeneous data within a given period.
4. Data security. The major risk in big data is data insecurity (Khan et al., 2014). A situation where data is constantly being attacked by unauthorised persons and data confidentiality is not guaranteed.
5. Lack of supervision of electrical energy consumed during the Processing, transmission and storage of big data.

#### A. Solutions to Big Data Challenges

Some of the solutions to these challenges stated above can be handled by cloud computing since it can accommodate large data computing and data storage.

1. Hadoop manages big data by effectively processing large amounts of data at an effectively reduced cost promptly (Khan et al., 2014).
2. Distributed storage systems that are consistent, available and partitioned tolerance, and have the ability of tolerating problems caused by network failure should be used for big data storage (Khan et al., 2014).
3. Ensure data integrity by preventing illegal and unauthorised tampering of data and data usage. It has to do with the quality and reliability of data.
4. Encryption of large amounts can also be a form of preservation of privacy and security.
5. Data security policies should be put in place to checkmate people and security agents from using data generated by people without permission.
6. Expandability and scalability. The system that is developed for data analytics should support both the present and future data sets. Also, the algorithms must be able to analyse ever more large and complex data sets.
7. The establishment of a comprehensive big data network architecture may be necessary to provide access to scientists from various fields so that the analytical objectives could be achieved.

## VII. CONCLUSION

This paper discussed big data and the benefits that are realised from the analysis of big data using data analytics. Data analytics are advanced analytical techniques applied to big data to extract patterns and information to help business organisations understand their business trends and make quick decisions. Further, the paper discussed Industry 4.0, also called the smart factory, whose goal is to use digital technology to connect to the physical world to maximise efficiency, lower production costs and increase product quality in the industry. Industry 4.0 is the digitalisation of the manufacturing sector and the analysis of relevant data. It also discussed big data challenges and proffered some solutions to these challenges. Hadoop and its components cannot address all the problems of big data, and SAS, R and MATLAB are not suitable. Proper tools for analysis are still lacking.

## REFERENCES

- Ajah, I. A., & Nweke, H. F. (2019). Big data and business analytics: Trends, platforms, success factors and applications. *Big Data and Cognitive Computing*, 3(2), 1–30. <https://doi.org/10.3390/bdcc3020032>
- Cuzzocrea, A., Song, I.-Y., & Davis, K. C. (2011). Analytics over large-scale multidimensional data: The big data revolution! *14th International Workshop on Data Warehousing and OLAP*, 101–104. <https://doi.org/10.1145/2064676.2064695>
- Elgendy, N., & Elragal, A. (2014). Big data analytics: A literature review paper. In P. Perner (Ed.), *Advances in Data Mining: Applications and Theoretical Aspects. ICDM 2014. Lecture Notes in Computer Science*, vol 8557 (pp. 214–227). Springer. [https://doi.org/10.1007/978-3-319-08976-8\\_16](https://doi.org/10.1007/978-3-319-08976-8_16)
- Gokalp, M. O., Kayabay, K., Akyol, M. A., Eren, P. E., & Kocyigit, A. (2016). Big data for Industry 4.0: A conceptual framework. *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, 431–434. <https://doi.org/10.1109/CSCI.2016.0088>
- Gröger, C. (2018). Building an industry 4.0 analytics platform: Practical challenges, approaches and future research directions. *Datenbank Spektrum*, 18(1), 5–14. <https://doi.org/10.1007/s13222-018-0273-1>
- Haller, S., Karnouskos, S., & Schroth, C. (2009). The Internet of things in an enterprise context. In J. Domingue, D. Fensel, & P. Traverso (Eds.), *Future Internet Symposium. FIS 2008. Lecture Notes in Computer Science*, vol 5468 (pp. 14–28). Springer. [https://doi.org/10.1007/978-3-642-00985-3\\_2](https://doi.org/10.1007/978-3-642-00985-3_2)
- Hogan, O., Holdgate, L., & Jayasuriya, R. (2016). The value of big data and the Internet of Things to the UK economy. In *Report for SAS*. [https://www.sas.com/content/dam/SAS/en\\_gb/doc/analytystreport/cebr-value-of-big-data.pdf](https://www.sas.com/content/dam/SAS/en_gb/doc/analytystreport/cebr-value-of-big-data.pdf)
- Khan, N., Yaqoob, I., Hashem, I. A. T., Inayat, Z., Mahmoud Ali, W. K., Alam, M., Shiraz, M., & Gani, A. (2014). Big data: Survey, technologies, opportunities, and challenges. *Scientific World Journal*, 2014, 1–18. <https://doi.org/10.1155/2014/712826>
- Komal, M. (2018). A review paper on big data analytic tools. *International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES)*, 4(5), 1012–1017.
- Machado, C. G., Winroth, M. P., & Ribeiro da Silva, E. H. D. (2020). Sustainable manufacturing in Industry 4.0: An emerging research agenda. *International Journal of Production Research*, 58(5), 1462–1484. <https://doi.org/10.1080/00207543.2019.1652777>
- Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition, and productivity. In *McKinsey Digital*. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/big-data-the-next-frontier-for-innovation>
- Mishra, S., & Misra, A. (2017). Structured and Unstructured Big Data Analytics. *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, 740–746. <https://doi.org/10.1109/CTCEEC.2017.8454999>
- Nagat Mohamed, M. Y. (2020). Big data and the future of the accounting profession. *Indian Journal of Science and Technology*, 13(8), 883 – 892. <https://doi.org/10.17485/ijst/2020/v13i08/149808>
- Oks, S. J., Fritzsche, A., & Möslin, K. M. (2017). An

- application map for industrial cyber-physical systems. In S. Jeschke, C. Brecher, H. Song, & D. B. Rawat (Eds.), *Industrial Internet of Things* (pp. 21–46). Springer. [https://doi.org/10.1007/978-3-319-42559-7\\_2](https://doi.org/10.1007/978-3-319-42559-7_2)
- Oliff, H., & Liu, Y. (2017). Towards Industry 4.0 utilizing data-mining techniques: A case study on quality improvement. *Procedia CIRP*, 63, 167–172. <https://doi.org/10.1016/j.procir.2017.03.311>
- Prarthana, T. V., & Jayakumar, J. (2017). Challenges and opportunities with big data. *International Journal of Engineering Research & Technology*, 6(7), 240–244. <https://doi.org/10.17577/ijertv6is070139>
- Raheem, F., & Uwanthika, I. (2019). Big data analytics: Challenges, technologies and key applications. *8th Annual International Research Conference on Sustainability through Business, Humanities and Technologies*, 157–164.
- Rai, R., Tiwari, M. K., Ivanov, D., & Dolgui, A. (2021). Machine learning in manufacturing and Industry 4.0 applications. *International Journal of Production Research*, 59(16), 4773–4778. <https://doi.org/10.1080/00207543.2021.1956675>
- Rajput, K., & Mehta, V. (2017). An analytical study of Hadoop and its components. *International Journal for Scientific Research and Development*, 5(8), 539–542.
- Russom, P. (2011). Big data analytics. In *TDWI Best Practices Report, Fourth Quarter*. [http://download.101com.com/pub/tdwi/Files/TDWI\\_BReport\\_Q411\\_Big\\_Data\\_Analytics\\_Web.pdf](http://download.101com.com/pub/tdwi/Files/TDWI_BReport_Q411_Big_Data_Analytics_Web.pdf)
- Sadiku, I. B., Ajayi, W., Sakpere, W., John-Dewole, T., & Badru, R. A. (2022). Effect of traditional and software-defined networking on performance of computer network. *Scientific Journal of Informatics*, 9(2), 111–122. <https://doi.org/10.15294/sji.v9i2.31315>
- Shi-Nash, A., & Hardoon, D. R. (2017). Data Analytics and Predictive Analytics in the Era of Big Data. In H. Geng (Ed.), *Internet of Things and Data Analytics Handbook* (pp. 329–345). John Wiley & Sons, Inc. <https://doi.org/10.1002/9781119173601.ch19>
- Singhal, N. (2021). An empirical investigation of Industry 4.0 preparedness in India. *Vision*, 25(3), 300–311. <https://doi.org/10.1177/0972262920950066>
- Suguna, S. (2016). Improvement of HADOOP ecosystem and their pros and cons in big data. *International Journal Of Engineering And Computer Science*, 5(5), 16680–16685. <https://doi.org/10.18535/ijecs/v5i5.57>
- Tawalbeh, L. A., & Saldamli, G. (2021). Reconsidering big data security and privacy in cloud and mobile cloud systems. *Journal of King Saud University - Computer and Information Sciences*, 33(7), 810–819. <https://doi.org/10.1016/j.jksuci.2019.05.007>
- The Economist Intelligence Unit. (2012). The deciding factor: Big data & decision making. In *Business Analytics*. [https://www.capgemini.com/wp-content/uploads/2017/07/The\\_Deciding\\_Factor\\_\\_Big\\_Data\\_\\_Decision\\_Making.pdf](https://www.capgemini.com/wp-content/uploads/2017/07/The_Deciding_Factor__Big_Data__Decision_Making.pdf)
- The Editors of Encyclopaedia Britannica. (2023). *Manufacturing*. Encyclopaedia Britannica. <https://www.britannica.com/technology/manufacturing>
- Tsai, C.-W., Lai, C.-F., Chao, H.-C., & Vasilakos, A. V. (2015). Big data analytics: A survey. *Journal of Big Data*, 2(1), 1–32. <https://doi.org/10.1186/s40537-015-0030-3>
- Wang, J., Xu, C., Zhang, J., & Zhong, R. (2022). Big data analytics for intelligent manufacturing systems: A review. *Journal of Manufacturing Systems*, 62, 738–752. <https://doi.org/10.1016/j.jmsy.2021.03.005>
- Xu, X., Lu, Y., Vogel-Heuser, B., & Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. *Journal of Manufacturing Systems*, 61(2021), 530–535. <https://doi.org/10.1016/j.jmsy.2021.10.006>



Editorial

---

# Haptoglobin Phenotype, Serum Iron Levels and Severity in Multi-Drug Resistant Mycobacterium Tuberculosis Patients in Ibadan

---

Ojikah Obianuju Ibifuro, Muhammed Jamiu Aasia, Ochayi Okwute Michael and Nze Okechukwu

FASCON 2022 Proceedings

Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era

Edited by

Wilson Sakpere, *PhD*

Cite:

Ojikah, O. I., Muhammed, J. A., Ochayi, O. M., & Nze, O. (2023). Haptoglobin Phenotype, Serum Iron Levels and Severity in Multi-Drug Resistant Mycobacterium Tuberculosis Patients in Ibadan. In W. Sakpere (Ed) *3rd International Conference, Faculty of Natural and Applied Sciences (FASCON) 2022: Translational Research in Science and Technology for Sustainable Development Circa COVID-19 Era, 2-4 November 2022* (pp. 66-73). Ibadan. <https://doi.org/10.5281/zenodo.8121068>.

# Haptoglobin Phenotype, Serum Iron Levels and Severity in Multi-Drug Resistant Mycobacterium Tuberculosis Patients in Ibadan

\*<sup>1</sup>Ojika Obianuju Ibifuro, <sup>2</sup>Muhammed Jamiu Aasia, <sup>3</sup>Ochayi Okwute Michael and <sup>4</sup>Nze Okechukwu

<sup>1,2</sup>Department of Biotechnology, Baze University, Abuja, Nigeria

<sup>3</sup>Department of Physiology, Baze University, Abuja, Nigeria

<sup>4</sup>Department of Chemistry, Baze University, Abuja, Nigeria

\*obianujuojika@gmail.com

**Abstract:** Haptoglobin (Hp) phenotypes possess biochemical and functional efficiencies accounting for distinct antioxidant and immuno-modulatory capacities. Hp 2.2 phenotype has been observed as a genetic risk factor for several infectious diseases, including Mycobacterium tuberculosis (MTB). Nigeria is ranked 4th globally, with 590,000 cases, the increase in antibiotic resistance worldwide, has called for better personalized treatment on a genetic level, as patients with multi-drug-resistant tuberculosis (MDR-TB) need to undergo extended, expensive, and hazardous second-line therapy. Given that iron homeostasis is crucial for the microbiological growth of MTB, the objective of this work was to observe the relationship and investigate possible associations with the Hp phenotypes as well as CRP concentrations measuring severity in TB patients. Fifty (50) clinically and Laboratory diagnosed tuberculosis patients were classified by the Gene-Xpert system into MDR-TB (25) and DS-TB (25) and 25 health control were recruited for the study after ethical clearance. Haptoglobin phenotypes were determined using electrophoresis while plasma iron and CRP levels were determined through spectrophotometry using kits obtainable from My BioSource Inc. The Haptoglobin phenotype distribution (Hp 1.1, Hp 2.1, and Hp 2.2) showed the following: MDR-TB population, 5(20%), 7 (28%), and 13 (52%). Overall, MDR-TB represents a severe spectrum of the disease compared to control due to increased levels of inflammation and increased serum iron, influenced by haptoglobin 2-2 phenotype. Hp 2-2 positively correlated with increased Fe and CRP levels (0.014) and (p=0.009) respectively but not with Hp 1-1 and Hp 2-2 phenotypes. The Hp 2.2 phenotype prevalence in the MDR-TB population can be used as a predictive/predisposing factor to determine the trend for individuals who contract TB. The Hp 2-2 gene polymorph is almost exclusive to the African race explaining the high cases of TB. It is therefore important to know all risk factors, especially on a genetic level, to better understand and manage the disease.

**Key Words:** Haptoglobin, Genetics, Tuberculosis, Iron, Gene-Xpert, SSS

## I. INTRODUCTION

Currently, it is estimated that TB infects one in every four people in the world (World Health Organization, 2022). Each year, 1% of the population develops new infections. Over 10 million cases of active TB were reported in 2017, leading to 1.6 million deaths worldwide (World Health Organization, 2013). Of these deaths, 95% happened in developing nations (World Health Organization, 2008). Humans have been

infected with tuberculosis since antiquity, and the origin of transmission is unknown (Gan *et al.*, 2004; World Health Organization, 2013). Tubercular degradation was discovered in the spines of Egyptian mummies and cattle. Nigeria is ranked second in Africa and seventh worldwide as having the highest TB burden. In Nigeria, the incidence rate of TB is estimated to be 322 cases per 100,000 people, with only 15% of the overall burden being reported (Khazaei *et al.*, 2013).

Mycobacterium tuberculosis (MTB) bacteria are the source of the infectious illness tuberculosis (TB). The majority of infections do not manifest any symptoms; this is known as latent tuberculosis. Tuberculosis often affects the lungs, but it can also affect other body regions or organs (Barnes, 2000). 10% of these dormant infections will become active diseases if untreated, killing 50% of those who are infected. Traditional signs of active tuberculosis include persistent coughing that produces sputum that contains blood, night sweats, fevers, and weight loss. Historically, it was referred to as "consumption" because of weight loss (Arredouani *et al.*, 2005). Extra-pulmonary tuberculosis patients can present with a variety of symptoms (Khazaei *et al.*, 2013). When individuals with active TB in their lungs cough, spit, speak, or sneeze, it spreads via the air (World Health Organization, 2022). Latent TB carriers do not spread the illness (World Health Organization, 2013). People with HIV/AIDS and smokers are more likely to have an active infection. Chest X-rays, microscopic inspection, and body fluid culture are used to diagnose active TB. 6. Blood tests or the tuberculin skin test (TST) are used to diagnose latent TB (Khazaei *et al.*, 2013).

Screening those at high risk for early detection, treatment, and immunization with the bacillus Calmette-Guérin (BCG) vaccine is all part of the prevention of tuberculosis (TB). People at the home, place of employment, and social contacts of those with active TB are at a high risk. Treatment involves using numerous antibiotics over an extended period. As antibiotic resistance increases globally, more cases of extensively drug-resistant tuberculosis (XDR-TB) and multiple drug-resistant tuberculosis (MDR-TB) are being recorded. Gene-Xpert System is used to identify the MDR gene in TB disease early diagnosis. HIV, overcrowding, subpar housing systems, hunger and smoking are risk factors for TB (World Health Organization, 2013).

Haptoglobin is produced in the liver, a plasma alpha-2 sialoglycoprotein, which is composed of two distinct polypeptide chains. All individuals have the same chains, which are polymorphic and have two dominant alleles, Hp 1

and Hp 2, which have partial dominance. Haptoglobin has three main phenotypes: Hp 1-1, Hp 2-1, and Hp 2-2 (Arredouani *et al.*, 2005). By binding, this protein stops iron from leaving the body through the kidneys, keeping it for erythropoiesis and other uses. Haptoglobin in humans is polymorphic, with the three main phenotypes being Hp 1-1, Hp 2-1, and Hp 2-2, which may be identified by gel electrophoresis. On chromosome 16, there is a gene for haptoglobin (16q22.2 which is between 72,054,505 bp to 72,061,055 bp). Polymorphic distribution can vary between ethnic and geographical locations, however, Hp 2-1 is the most prevalent phenotype (Arredouani *et al.*, 2005). Individuals with Hp 1-1 have the highest haptoglobin concentration, followed by those with Hp 2-1 and Hp 2-2, respectively. Increased vulnerability to various illnesses, such as TB, has been associated with those who have the Hp 2-2 phenotype TB (Khazaei *et al.*, 2013).

People who are iron deficient are typically more susceptible to TB (World Health Organization, 2013). The protein shields the lungs from inflammatory substances and prevents lung damage. Emphysema and COPD begin when a deficiency causes the natural bacteriostatic neutrophil activity in the body to destroy lung tissue (Fedoseeva *et al.*, 1993). Controlling microorganisms, sporadic epidemics caused by drug-resistant microorganisms and unidentified pathogenic microbial species pose a critical threat to public health (Eckersall, 2000). Infectious diseases significantly contribute to morbidity and mortality worldwide, accounting for roughly 50% of all deaths in tropical countries.

According to Kasvosve *et al.* (2000), people with the Hp 2-2 phenotype had 6.1 times greater mortality rates from tuberculosis than those with the Hp 1-1 phenotype. Additionally, in individuals with extensive cavities due to tissue loss, Hp 2-2 phenotype was overrepresented in patients with more advanced dissemination and nephrotic TB (Eckersall, 2000; Ubaïdullaev *et al.*, 2002). These unfavourable health trends necessitate an international effort to create fresh approaches to the prevention and treatment of infectious diseases. Realizing the urgent need to evaluate every possible risk factor, particularly on a genetic level, to better understand and manage the disease given the epidemic of antibiotic resistance and to promote a better future for humanity on Earth. Given that the Hp 2:2 phenotype was found to increase the risk of dying from TB (a result observed in multiple research works). Therefore, it is crucial to look at how the Hp phenotype and drug-sensitive TB and multidrug-resistant TB are related in Nigerian populations.

#### A. Objectives of the Study

To achieve the aim of this study, the following tasks were placed:

- To observe the distribution of haptoglobin phenotype.
- To investigate any possible associations between Hp phenotypes, serum iron and CRP concentrations that measured severity in Tb patients.
- To observe Hp phenotypes as possible genetic predisposing factors.

## II. LITERATURE REVIEW

Haptoglobin locus is located on the long arm of chromosome 16 (16q22). Because the loci for the chains are linked to one another, a single mRNA creates a long polypeptide chain that

is cleaved to produce the two Hp chains (Soejima *et al.*, 2007).

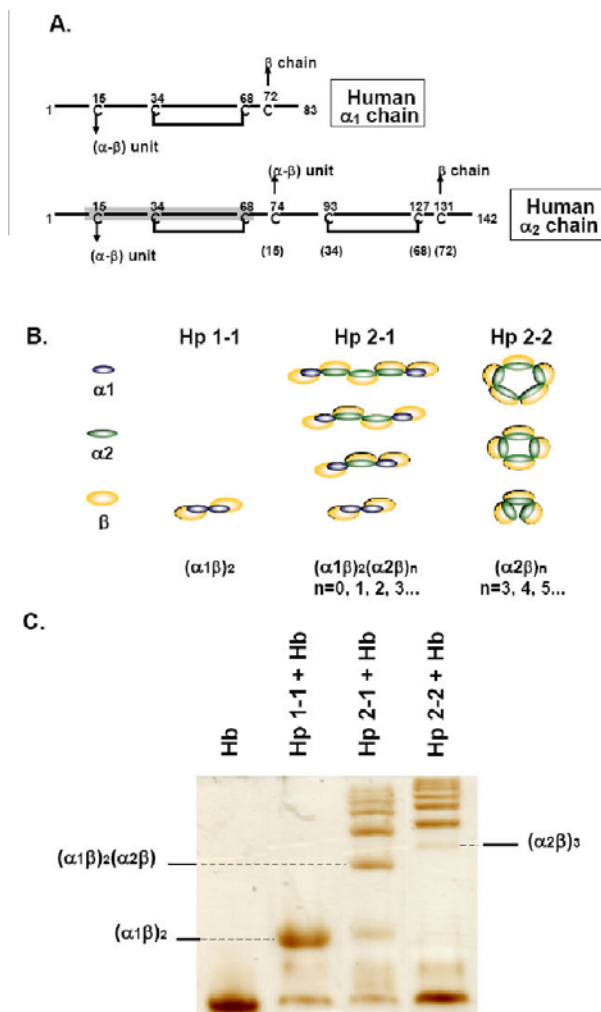


Figure 1: Polymeric Hp 1-1, 2-1, and 2-2 structures.

Source: [https://www.researchgate.net/figure/Polymeric-structures-of-Hp-1-1-2-1-and-2-2-Haptoglobin-polymers-are-made-up-of-ab\\_fig1\\_300390198](https://www.researchgate.net/figure/Polymeric-structures-of-Hp-1-1-2-1-and-2-2-Haptoglobin-polymers-are-made-up-of-ab_fig1_300390198)

Haptoglobin polymers are composed of  $(\alpha\beta)$  units with various numbers of -thiol groups in position  $\alpha1\beta$  and position  $\alpha2\beta$ . From Figure 1:

A) A diagram showing the  $\alpha1$  and  $2\beta$  chains, respectively, that are encoded by the Hp 1 and Hp 2 alleles. A basic unit that forms a chain is always linked to by Cys-72's -COOH terminal in position 1 $\alpha$ . While 2 has a tandem repeat of residues 12-70, 2 is "trivalent" because Cys-15 and -74 link to other units.

B) A diagrammatic representation of how the repeat unit (n) is arranged in each Hp phenotype.

C) 7% Native-PAGE of Hp-hemoglobin complexes displaying each phenotype's distinctive polymeric pattern. For HP phenotyping, these complexes are employed. It should be noted that there is a relatively little quantity of cyclic Hp 2-2 trimer, or  $(\alpha2\beta)_3$ .

#### A. Association between Haptoglobin Phenotypes and Diseases

Relationships between Hp phenotypes and heart disease have been a subject of interest for many years (Ubaïdullaev *et al.*, 2002). The Hp 2-2 phenotype correlating to high-risk cardiac patients reported a significant increase in the incidence

compared to healthy control groups. Myocardial infarction followed by extensive damage was understood to be more problematic with Hp 2-2 than in other phenotypes (Van Vlierberghe *et al.*, 2004). The Hp 2-2 phenotype is an additional genetic risk factor for coronary atherosclerosis, independent of established risk factors like smoking, high cholesterol, hypertension, and diabetes mellitus. In atherosclerotic plaques, this phenotype is also known to offer less protection against oxidative stress, which may result in the development of refractory hypertension. Better blood pressure management requires patients with this phenotype to undergo complex anti-hypertensive drug combinations. Hp may be used to forecast a patient's prognosis and cardiovascular disease due to its diverse biological roles and functions (S. E. Yang *et al.*, 2000). This polymorphism may be involved in several infectious diseases, according to studies. Haptoglobin can function as a natural bacteriostat by restricting the consumption of iron necessary for the growth of various dangerous bacteria, including *Neisseria meningitidis*, *Campylobacter jejuni*, and *Bacteroides fragilis* (Van Vlierberghe *et al.*, 2004).

Hp was discovered to be a substitute CD11b/CD18 ligand in HIV, indicating that this protein is crucial to the infection (Ubaïdullaev *et al.*, 2002). Additionally, Hp 2-2 patients had a greater mortality and even worse prognosis due to Hb-driven oxidative stress, which could be exacerbated by residual iron circulating in HIV-seropositive patients' plasma and encouraging viral proliferation and transmission. According to a documented relationship between hepatitis C and Hp polymorphism (Hp 1-1 was overrepresented), the Hp phenotype may have an impact on how hepatitis C develops clinically. It's interesting to note that people with the Hp 2-2 phenotype produce less hepatitis B antibody response after vaccination than people with other phenotypes.

In a different study, Sudanese patients with both simple and severe (cerebral) falciparum malaria had a significantly higher incidence of Hp 1-1 individuals. Among patients, the phenotypic frequency distribution for Hp 1-1, Hp 2-1, and Hp 2-2 was 60.8%, 29.7% and 9.5% respectively, while in healthy (control) persons, it was 26.0%, 55.8% and 18.3% (Ubaïdullaev *et al.*, 2002). A different study, one which involves malaria, revealed a comparable link. Hp 1-1 infection and severe *P. falciparum* malaria in patients from Ghana's coastal region.

#### B. Role of Iron in Immune Response

Almost all known species depend heavily on iron for growth and survival. Depriving pathogens of this crucial nutrient is a key tactic in the antimicrobial defence of mammalian species (Quaye *et al.*, 2000). The transporter responsible for pumping iron out of the phagosome, NRAMP1, is one of the most well-studied examples of this technique. Numerous studies using mouse models and tissue culture have demonstrated that the ability of NRAMP1 to reduce phagosomal iron content is essential for the survival and proliferation of several intracellular infections. These pathogens include *Leishmania donovani*, *Salmonella typhimurium*, and *Mycobacterium bovis* BCG. Polymorphisms in the NRAMP1 gene have been associated with leprosy and tuberculosis susceptibility (Delanghe *et al.*, 1999).

It was shown that upregulating FPN expression in response

to hepcidin had the opposite effect of significantly inhibiting intracellular *Salmonella* growth in either HeLa cells or J774 murine macrophages (Willemetz *et al.*, 2017). A gene in bacteria that is expressed more when there is low iron concentration was shown to be connected with elevated FPN levels, leading researchers to conclude that FPN-mediated iron efflux ultimately caused the element to be depleted in the pathogen's immediate microenvironment. With the use of iron-regulated transcriptional reporters, *Salmonella* strains were altered. Based on these first-hand accounts, multiple other teams have replicated related findings using *Salmonella* and other intracellular bacterial infections including *Legionella pneumophila*, *Chlamydia psittaci*, *C. trachomatis*, and *M. tuberculosis* (Van Vlierberghe *et al.*, 2004). According to research demonstrating that activation of macrophages, whether by bacterial infection or by interferon, is connected with transcriptional up-regulation of FPN, it may be a fundamental component of the phagocyte antimicrobial reserve. It is important to note that a variety of increased FPN gene transcription effects 3; 2 may reduce lipopolysaccharide (LPS)-induced hepcidin synthesis in macrophages.

#### C. Iron and Virulence of *M. Tuberculosis*

Siderocalin can bind to a separate class of siderophores known as the carboxymycobactins that are produced by *M. tuberculosis* and other mycobacteria in addition to its capacity to isolate enterobactin-like siderophores. In opposition to this finding, Kasvosve *et al.* (2000) showed that siderocalin is involved in preventing the growth of *M. tuberculosis* both in vitro and in vivo. Similar investigations found that the addition of recombinant siderocalin significantly reduced *M. tuberculosis* growth in both bacterial media and mice macrophages (Johnson *et al.*, 2010). Research on the contacts of people with active pulmonary tuberculosis patients revealed that siderocalin also has a function in human defence against the disease (Cherayil, 2011). The majority of cases of this infection were observed in people of African heritage; this finding was associated with decreased serum siderocalin concentrations and circulating neutrophil counts. Combinatorially, serum siderocalin levels were shown to be low in HIV-infected people, which may contribute to both pathways of immunity being disrupted and lower resistance to *M. tuberculosis* (Ferri, 2011).

#### D. Serum Iron in Relation to Drug Sensitivity and Multiple-Drug Sensitivity

It is urgently necessary to conduct research into new targets and processes because *Mycobacterium tuberculosis* (MTB) acquired multidrug resistance (MDR) by repeated use of antitubercular medications. MTB's capacity to detect and adapt to a variety of alterations in the host is crucial for survival and is the basis of infection (World Health Organization, 2013). Iron deficiency is a critical issue that *M. tuberculosis* must overcome at the beginning of the infection since both bacteria and human systems need iron. A study examined the effects of iron deficiency on the susceptibilities of *Mycobacterium smegmatis*, a "surrogate of MTB," to recognise anti-TB medications. Results revealed that iron deficiency increased the potency of the majority of first-line anti-TB medicines, which may be reduced by taking an iron supplement. Additionally, iron appears to be necessary to maintain genotoxicity, indicating the potential involvement of iron in the DNA repair system. When these parameters

were considered, for the first time a connection between cellular iron and mycobacteria's drug sensitivity was discovered, proposing iron as a new determinant to fight MDR in tuberculosis infection (Ferri, 2011).

**E. Haptoglobin Polymorphism and Iron Homeostasis**  
Haptoglobin collects haemoglobin that has escaped into the plasma and transports it to the parenchymal cells of the liver and ultimately to macrophages. There is no evidence to support the idea that the haptoglobin pathway is a significant barrier to iron homeostasis (Jacob *et al.*, 2009). However, it was revealed that those who were homozygous for the Hp 2 gene had higher levels of serum iron, transferrin saturation, and ferritin in their bodies for unknown reasons (in read literature) (Beutler *et al.*, 2002).

#### **F. C-Reactive Protein in Relation to Drug Sensitivity and Multiple-Drug Sensitivity.**

CRP levels increase quickly during infectious or inflammatory illness states within the first 6 to 8 hours and after 48 hours (Bento *et al.*, 2011). The levels of fibrinogen and CRP may therefore help predict the progression of TB and the success of the anti-tubercular treatment since pulmonary-reactive protein (CRP) is an acute-phase protein that serves as an early marker of tuberculosis, an inflammatory disease. In earlier research, patients with TB had significantly elevated CRP levels between 10 and 100 mg/L (Chandrashekar, 2014). The study measured CRP levels in patients with TB of various severity levels (drug-sensitive and drug-resistant) as well as in multi-drug-resistant TB patients undergoing therapy. To distinguish between the two types of TB patients and track therapy response in MDR-TB, it is necessary to determine the utility of these acute phase proteins (Bento *et al.*, 2011; Chandrashekar, 2014).

### **III. MATERIALS AND METHODS**

#### **A. Ethical Clearance**

Ethical Clearance from Oyo State Human Research Ethical Committee Ministry of Health, Oyo State.

#### **1. Recruitment of Patients**

Seventy-five (75) human samples were collected, and 10 ml of blood was collected once. 50 diagnosed TB patients, from Oyo State Chest Clinic, Jericho, Ibadan. 25 Tb free individuals as control from the blood bank of UCH. Exemption of Patients on iron supplements. (The sampling carried out in the course of this work was not random but purposive sampling).

#### **B. Materials**

- Plain bottles were used in the collection of whole blood samples.
- Needles and 10 ml syringes.

#### **1. Equipment**

Gel electrophoresis; power pack and tank

#### **2. Reagents**

Haptoglobin Phenotype (Hp) Standard: 2.1, 2.2 and 1.1 obtainable from MyBioSource INC

#### **C. Methods of Research**

Laboratory analyses were done using the following methods:

- a. Human C-Reactive Protein

- b. Serum Iron

- c. Haptoglobin Phenotype (Hp) Standard: 2.1, 2.2 and 1.1

#### **D. Methodology**

Preparation of Blood Samples: Blood was collected via venipuncture. The serum was then separated from the cells after clotting by centrifugation. For plasma samples, blood was collected into a container in a plain bottle and then centrifuged. Care was taken to minimize hemolysis.

#### **E. Methods**

##### **1. Human C-Reactive Protein Test.**

##### **Reagent Preparation**

Before usage, reagents should be at room temperature (18–25 °C). The patient's serum was 100 times diluted before usage. Several tiny tubes (i.e., 1.5 ml microcentrifuge tubes) were made, and 5 ml of serum was mixed with 495 ml (0.495 ml).

##### **Sample Preparation**

- a. For this test, serum samples were used.
- b. Standard venipuncture procedures were used to obtain the specimens. Within 60 minutes of the serum being collected, it was extracted from the packed or coagulate cells.
- c. Specimens were frozen at -20°C or below if they weren't analyzed within 24 hours of collection.
- d. Avoid samples that are grossly lipemic (milky), grossly hemolytic (bright red), or cloudy (after centrifugation).

C-reactive protein (CRP) is measured using this technique's latex-enhanced nephelometry. A soluble analyte and the matching antigen or antibody attached to polystyrene particles react in particle-enhanced tests. Anti-CRP antibodies are covalently linked to particles with a polystyrene core and a hydrophilic shell to quantify CRP. Latex particles coated with mouse monoclonal anti-CRP antibodies are combined with a diluted solution of the test sample. The test sample's CRP will combine with the latex particles to form an antigen-antibody combination. After six minutes, the amount of light scattering, as determined by a nephelometric method, is inversely proportional to the amount of analyte in the sample. There is an automated blank subtraction. A calibration curve is used to calculate CRP concentrations.

##### **2. Serum Iron Procedure**

##### **Reagent Preparation**

- a. Combining 3 g/dL sodium chloride and 0.2 mol/L hydrochloric acid: A 2-L flask containing 250 mL of deionized water was filled with 34 mL of concentrated HCl and 60 g of NaCl. Mixed thoroughly and diluted with deionized water to volume. (This solution was made as needed to be utilized as a component of the working solution; it remained stable at 20 to 25°C.)
- b. A working solution of HCl, NaCl, and Brj: 20 drops of Brij were added to 200 mL of 0.2 mol/L HCl and 3 g/dL NaCl and thoroughly mixed for every 150 samples that needed to be tested.
- c. Using HCl, NaCl, and ascorbic acid as a solution: Add 1 g of L-ascorbic acid and 10 drops of Brij to 100 mL of 0.2 mol/L HCl with 3 g/dL NaCl for every 150 samples that need to be tested. Mix thoroughly.
- d. Buffer with 0.75 mol/L acetate: Then, in a 4-L flask containing 2 L of deionized water, 408.1 g of sodium

acetate was added. This needs to be made once a week; the solution is stable between 20 and 25 degrees Celsius.

- e. Ferrozine 0.07 g/dL with 1% (w/v) thiourea: To 1 L of the acetate buffer-thiourea solution, 0.7 g of ferrozine and 10 g of thiourea were added and thoroughly mixed. Removed after filtering through a 0.45-µm Millipore. Additionally, any undissolved particles. (Weekly preparation; solution stable at 20–25 °C.)
- f. Brij-35 wash solution, 0.5 mL/L (v/v): 2 L of deionized water was combined with 1 mL of Brij-35, 30% solution.
- g. Hydrochloric acid, 0.1 mol/L (for standard preparation): In a 1-L volumetric flask, 8.3 mL of concentrated HCl was added to 500 mL of deionized water. Combined thoroughly and diluted to volume with more water. Brij-35 was left out. To prepare intermediate and working standards, approximately 5 L of this solution are needed.
- h. Iron-saturating solution for TIBC at 400 L/dL: A 500 mL flask containing deionized water was filled with 2.0 mL of the 1.0 g/L stock iron standard. (Moved to a plastic storage bottle and given a week to settle before use. At 20 to 25 °C, the solution is stable.)

#### Standards Development (allow standards to equilibrate for 24–72 hours)

- a. g/L standard solution for stock iron: One volumetric litre was filled with one kilogram of iron wire. With a little heat, 12 mL of strong HCl was added, dissolving the wire. The flask was allowed to cool to ambient temperature when the wire had completely disintegrated, and the contents were then diluted to volume with deionized water. (The solution is stable when kept at 20 to 25 °C in a polypropylene container.
- b. iron intermediate stock solution at 50.0 mg/L: With 0.1 mol/L of HCl, 25 mL of the 1.0 g/L stock iron solution is diluted to make 500 mL.
- c. Iron standards in use: Prepare dilutions from the intermediate standard as shown below in a series of 500 mL volumetric flasks. Mix well after dilution to 500 mL with 0.1 mol/L HCl. (As needed; the solution is stable between 20 and 25 °C.) Standard reference material can be diluted at concentrations between 1 and 1000 L/dL to check the correctness of the working standard dilutions. It has a concentration of 1.0001 mg/mL.

#### Reportable Normal Ranges

Males >18 years old: 60-190 µL/dL iron; Females >18 years old: 40-175 µL/dL iron and Children 3-17 years old: 32-175 µL/dL iron.

#### 3. Haptoglobin Typing

- a. Standards: In 1mL of double-distilled water (final concentration 1g/L), purified haptoglobin phenotypic standards (My Biosource, Inc.) were dissolved, aliquoted, and kept at -30°C.
- b. Free haemoglobin: After being cleansed twice with 0.9% (v/v) saline, whole blood was diluted with double-distilled water to a concentration of around 10% haemoglobin, which was then measured by a Coulter counter using the cyanomethaemoglobin method. At 4°C, this solution was kept.
- c. Electrophoresis: Electrophoresis was completed in its entirety. The kits came with the citratemaleate electrophoresis buffer (pH 6.2).
- d. Stain: Just before use, the stain was prepared. It comprised 1mL of 1% (w/v) potassium ferricyanide,

150J.L of 30% (w/v) hydrogen peroxide, 5mL of 0.22% (w/v) 3,3',5,5'-tetramethylbenzidine in methanol, 5mL of dimethylsulphoxide, and 1mL each of glacial acetic acid and 1% (w/v) potassium ferricyanide.

- e. Fixative/destain: Glacial acetic acid was combined with methanol and double-distilled water in a 2:1:1 ratio.

#### Electrophoresis

Free haemoglobin (5 J.L) was added to 95 J.L of serum samples from patients or haptoglobin standards. The samples were vortexed for five minutes and then permitted to stand for the formation of the haptoglobin-haemoglobin complex. Aliquots (3 J.L) of each sample were loaded onto the gel using a template, and electrophoretic separation was carried out for 35 min at 50 V and 20 mA (or by the manufacturer's instructions). Gels were destained for two 5-minute washes in gel fixative after staining for 10 minutes at the end of each run. Gels were rinsed with tap water and dried in the sun to avoid fading, in an oven at 65°C for 30 min., and then stored at room temperature without exposure to light.

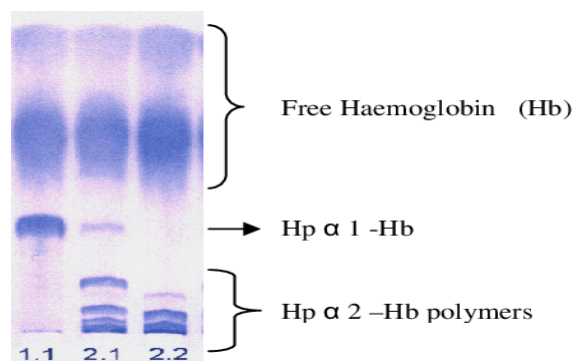


Figure 2: Electrophoresis

**Note:** samples were already differentiated and characterised by the Gene-Xpert machine upon collection. and then subjected to the test procedures listed above.

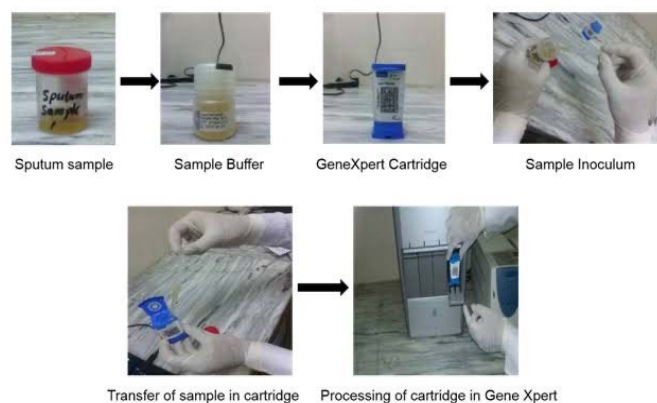


Figure 3: Layout of GeneXpert Assay

#### F. Data Analysis

Hardy Weinberg Equilibrium was used to check for genotypic predisposition, allelic frequency and phenotypic distribution. Data obtained were analysed using SPSS. Analysis for Homogeneity of the groups. Student's t-test and Chi-square were used to check the differences between the two groups. ANOVA was used to find significance between the mean and standard deviation of study groups. Kruskal Wallis was used to test the differences between study groups. Pearson's correlation was used to find the correlation

between groups. Statistical significance (p) will be at  $< 0.05$  and 95% confidence interval.

#### IV. RESULTS

The results of the between haptoglobin phenotype, serum iron, the severity of MDR and DS Tubercle bacilli are displayed below:

Table 1: Haptoglobin Phenotype Distribution and Allele Frequency in MDR-TB Population

Haptoglobin Phenotypes Distribution				Hp Allele Frequency	
Groups	Hp 1-1	Hp 2-1	Hp 2-2	Hp 1	Hp 2
MDR-TB	5 (20%)	7 (28%)	13 (52%)	0.34	0.66
Control	10 (40%)	10 (40%)	5 (20%)	0.6	0.4

P-value is significant at  $\leq 0.05$

Table 2: Plasma iron and CRP Concentrations in MDR-TB and Control Population

Parameters	MDR-TB	Control	P-value
Fe	85.60 $\pm$ 27.82	84.68 $\pm$ 36.77	0.921
CRP	24.37 $\pm$ 23.63	2.6 $\pm$ 1.72	0.001*

P-value is significant at  $\leq 0.05$

Table 3: Correlation between Haptoglobin Phenotypes, Serum Iron and CRP in MDR-TB Population

Parameters	Fe r(p)	CRP r(p)
Hp 1-1	-0.017 (0.935)	0.000 (0.998)
Hp 2-1	0.025 (0.905)	-0.134 (0.525)
Hp 2-2	1.01 (0.014)*	1.297 (0.009)*

P-value is significant at  $\leq 0.05$

#### V. DISCUSSION

In this study, the MDR-TB population, 5 (20%) had the Hp 1-1 phenotype, 7 (28 %) had the Hp 2-1 phenotype, and 13 (52%) had the Hp 2-2 phenotype. While in the control group, 10 (40%) samples had the Hp 1-1 phenotype, 10 (40%) had the Hp 2-1 phenotype, and 5 (20%) had the Hp 2-2 phenotype. Using Hardy Weinberg equilibrium principle allelic frequency, MDR-TB had a distribution of 0.34 for Hp 1 and 0.66 for Hp 2 while Control had a distribution of 0.6 for Hp 1 and 0.4 for Hp 2 showing that it could be a genetic predictive biomarker but not predisposing factor to this infection. It was also observed that there were more individuals with the Hp 2-2 phenotype than any of the three phenotypes with Hp 1-1 having the lowest frequency. However, this result could be better validated with a larger sample size associated with genetic studies.

Studies have linked the Hp 2-2 phenotype to higher rates of morbidity from illnesses like diabetes, HIV infection, and cardiovascular disease. The highest levels of haptoglobin are found in those with Hp 1-1 > Hp 2.1 > Hp 2-2 (Arredouani *et al.*, 2005). Hp 2-2 has also been linked to higher serum ferritin levels, increased susceptibility to infections including

TB, and increased macrophage iron buildup (Fedoseeva *et al.*, 1993).

Lack of haptoglobin in tuberculosis can cause lung tissue to be destroyed by bacteriostatic neutrophil action, which can result in the start of emphysema and COPD (F. Yang *et al.*, 2000). Additionally, patients with extensive cavities caused by tissue damage, more advanced dissemination, and the presence of nephritic TB were overrepresented in the Hp 2-2 phenotype (Fedoseeva *et al.*, 1993; Ubaïdullaev *et al.*, 2002). The lungs are more vulnerable to metal-induced oxidative stress than any other organ in the body because of their special anatomical function in high-volume oxygen exchange and big blood supply.

Due to an elevated amount of inflammation, MDR-TB generally indicates a severe spectrum of the disease in comparison to control. Increased blood iron levels and a p-value of 0.001\* were found to indicate a correlation between the MDR-TB and control groups. Additionally, a worse prognosis and more severe tuberculosis TB have been linked to higher CRP values.

According to reports, individuals with more severe lung dysfunction, as shown by lung cavitation, had CRP levels that were noticeably greater than those of patients without cavitation. It has been demonstrated that Mycobacterium tuberculosis and its components induce the release of IL-6 from mononuclear phagocytes in vitro, which is regarded as an inflammatory mediator. There is evidence that IL-6 causes liver acute phase reactants (including CRP).

Numerous clinical and laboratory research have supported the significant correlation between IL-6 and CRP. Bekker and Wood (2010) speculate that the decrease in serum CRP levels that occur during pulmonary tuberculosis treatment may be connected to the resolution of the systemic inflammatory process. This is because the plasma levels of cytokines, such as IL-6, are the principal cytokine that triggers CRP synthesis, which is accompanied by a fall in CRP concentration in patients treated for pulmonary tuberculosis (Bekker & Wood, 2010).

Additionally, it was shown that there was a connection between elevated levels of inflammation and potential bacterial growth and serum iron. Overall, compared to DS, MDR-TB indicates a more severe spectrum of the illness because of higher levels of inflammation and serum iron, both of which are regulated by the haptoglobin 2-2 phenotype. Hp 2-2 and serum iron were positively linked, although Hp 1-1 and Hp 2-1 did not (Table 3). Therefore, regardless of their haptoglobin phenotypes, MTB patients should be advised to avoid drinking alcohol, which has been shown to increase iron stores in the body even at low levels of consumption, and taking iron supplements, both of which have the potential to increase oxidative stress in the body and encourage the growth of co-infecting organisms like MTB and other organisms.

#### VI. CONCLUSION

All objectives of this study were met. There is little or no work done in this dynamic of using all these parameters and variables such as the haptoglobin phenotype as a severity factor of TB, in relationship to serum iron as well as C-

reactive protein as biomarkers and measures of severity in drug-resistant and sensitive TB in this region of the world. It is important to know all the risk factors, especially on a genetic level, to better understand and manage the disease. The Hp 2-2 gene polymorph is almost exclusive to the African race which would explain the high cases of TB. This Hp 2-2 gene polymorph is associated with raised serum iron levels and is most prevalent in the severity of the MDR-TB patients (but does not predispose to MDR-TB) in TB predictive biomarkers to determine the trend for individuals who contract TB.

#### ACKNOWLEDGEMENT

This poster was made possible by the team at Bioinformatics Services, Mokola, Public Private Partnership Lab UCH and Oyo State Chest Clinic, Jericho, Ibadan. Dr. Ighodaro and Mr Adeosun whose assistance was instrumental to the compilation of this work.

#### REFERENCES

- Arredouani, M. S., Kasran, A., Vanoirbeek, J. A., Berger, F. G., Baumann, H., & Ceuppens, J. L. (2005). Haptoglobin dampens endotoxin-induced inflammatory effects both in vitro and in vivo. *Immunology*, 114(2), 263–271. <https://doi.org/10.1111/j.1365-2567.2004.02071.x>
- Barnes, P. J. (2000). Chronic obstructive pulmonary disease. *The New England Journal of Medicine*, 343(4), 269–280. <https://doi.org/10.1056/NEJM200007273430407>
- Bekker, L. G., & Wood, R. (2010). The changing natural history of tuberculosis and HIV coinfection in an urban area of hyperendemicity. *Clinical Infectious Diseases*, 50(Supplement\_3), S208–S214. <https://doi.org/10.1086/651493>
- Bento, J., Silva, A. S., Rodrigues, F., & Duarte, R. (2011). Métodos diagnósticos em tuberculose [Diagnostic tools in tuberculosis]. *Acta Medica Portuguesa*, 24(1), 145–154. Portuguese. <https://doi.org/10.20344/amp.333>
- Beutler, E., Gelbart, T., & Lee, P. (2002). Haptoglobin polymorphism and iron homeostasis. *Clinical Chemistry*, 48(12), 2232–2235. <https://doi.org/10.1093/clinchem/48.12.2232>
- Chandrashekhara, S. (2014). C-reactive protein: An inflammatory marker with specific role in physiology, pathology, and diagnosis. *Internet Journal of Rheumatology and Clinical Immunology*, 2(S1), 1–23. <https://doi.org/10.15305/ijrci/v2is1/117>
- Cherayil, B. J. (2011). The role of iron in the immune response to bacterial infection. *Immunologic Research*, 50(1), 1–9. <https://doi.org/10.1007/s12026-010-8199-1>
- Delanghe, J., Langlois, M., Duprez, D., De Buyzere, M., & Clement, D. (1999). Haptoglobin polymorphism and peripheral arterial occlusive disease. *Atherosclerosis*, 145(2), 287–292. [https://doi.org/10.1016/S0021-9150\(99\)00079-9](https://doi.org/10.1016/S0021-9150(99)00079-9)
- Eckersall, P. D. (2000). Recent advances and future prospects for the use of acute phase proteins as markers of disease in animals. *Revue de Médecine Vétérinaire*, 7(151), 577–584.
- Fedoseeva, S. V., Iusopova, M. M., Chukanova, V. P., & Pospelov, L. E. (1993). Techenie infil'trativnogo tuberkuleza legkikh v zavisimosti ot genotipa bol'nogo [Course of infiltrating pulmonary tuberculosis depending on the patient's genotype]. *Problemy Tuberkuleza*, 2, 8–10. Russian.
- Ferri, F. F. (2011). *Ferri's differential diagnosis: A practical guide to the differential diagnosis of symptoms, signs, and clinical disorders* (2nd ed.). Mosby Inc. Elsevier.
- Gan, W. Q., Man, S. F. P., Senthilselvan, A., & Sin, D. D. (2004). Association between chronic obstructive pulmonary disease and systemic inflammation: A systematic review and a meta-analysis. *Thorax*, 59(7), 574–580. <https://doi.org/10.1136/thx.2003.019588>
- Jacob, J. T., Mehta, A. K., & Leonard, M. K. (2009). Acute forms of tuberculosis in adults. *The American Journal of Medicine*, 122(1), 12–17. <https://doi.org/10.1016/j.amjmed.2008.09.018>
- Johnson, E. E., Srikanth, C. V., Sandgren, A., Harrington, L., Trebicka, E., Wang, L., Borregaard, N., Murray, M., & Cherayil, B. J. (2010). Siderocalin inhibits the intracellular replication of Mycobacterium tuberculosis in macrophages. *FEMS Immunology and Medical Microbiology*, 58(1), 138–145. <https://doi.org/10.1111/j.1574-695X.2009.00622.x>
- Kasvosve, I., Gomo, Z. A. R., Mvundura, E., Moyo, V. M., Saungweme, T., Khumalo, H., Gordeuk, V. R., Boelaert, J. R., Delanghe, J. R., De Bacquer, D., & Gangaidzo, I. T. (2000). Haptoglobin polymorphism and mortality in patients with tuberculosis. *International Journal of Tuberculosis and Lung Disease*, 4(8), 771–775. [https://doi.org/10.1007/978-3-642-18480-2\\_7](https://doi.org/10.1007/978-3-642-18480-2_7)
- Khazaei, H. A., Teymuri, B., Nakhaei, A., Mohammadi, M., Noura, M., Khazaei, A., Tofiqh, N., & Rezaei, N. (2013). Association of haptoglobin phenotypes with clinical features of preterm labor disease. *Acta Medica Iranica*, 51(8), 554–559.
- Quaye, I. K. E., Ekuban, F. A., Goka, B. Q., Adabayeri, V., Kurtzhals, J. A. L., Gyan, B., Ankrah, N. A., Hviid, L., & Akanmori, B. D. (2000). Haptoglobin 1-1 is associated with susceptibility to severe Plasmodium falciparum malaria. *Transactions of the Royal Society of Tropical Medicine and Hygiene*, 94(2), 216–219. [https://doi.org/10.1016/S0035-9203\(00\)90281-5](https://doi.org/10.1016/S0035-9203(00)90281-5)
- Soejima, M., Koda, Y., Fujihara, J., & Takeshita, H. (2007). The distribution of haptoglobin-gene deletion (Hpdel) is restricted to East Asians. *Transfusion*, 47(10), 1948–1950. <https://doi.org/10.1111/j.1537-2995.2007.01467.x>
- Ubaïdullaev, A. M., Kazakov, K. S., & Khakimov, M. A. (2002). Geneticheskie varianty gaptoglobina u bol'nykh nefrotuberkulezom [Genetic variants of haptoglobin in patients with nephrotuberculosis]. *Problemy Tuberkuleza*, 7, 42–43. Russian.
- Van Vlierberghe, H., Langlois, M., & Delanghe, J. (2004). Haptoglobin polymorphisms and iron homeostasis in health and in disease. *Clinica Chimica Acta*, 345(1–2), 35–42. <https://doi.org/10.1016/j.cccn.2004.03.016>
- Willemetz, A., Beatty, S., Richer, E., Rubio, A., Auriac, A., Milkereit, R. J., Thibaudeau, O., Vaulont, S., Malo, D., & Canonne-Hergaux, F. (2017). Iron- and hepcidin-independent downregulation of the iron exporter ferroportin in macrophages during Salmonella infection. *Frontiers in Immunology*, 8, 1–11. <https://doi.org/10.3389/fimmu.2017.00498>
- World Health Organization. (2008). *Implementing the WHO stop TB strategy: A handbook for national*

- tuberculosis control programmes*. WHO Press.  
<https://apps.who.int/iris/handle/10665/43792>
- World Health Organization. (2013). *Tuberculosis*. Fact Sheets. <https://www.who.int/news-room/fact-sheets/detail/tuberculosis>
- World Health Organization. (2022). *Global tuberculosis report 2022*.  
<https://www.who.int/publications/i/item/9789240061729>
- Yang, F., Ghio, A. J., Herbert, D. C., Weaker, F. J., Walter, C. A., & Coalson, J. J. (2000). Pulmonary expression of the human haptoglobin gene. *American Journal of Respiratory Cell and Molecular Biology*, 23(3), 277–282. <https://doi.org/10.1165/ajrcmb.23.3.4069>
- Yang, S. E., Min, W. K., Park, H., Chun, S., Nah, J., & Kim, J. Q. (2000). Distribution of haptoglobin phenotypes in a Korean population, using the semi-automated PhastSystem. *Annals of Clinical Biochemistry*, 37(2), 205–209.  
<https://doi.org/10.1258/0004563001899014>