International Journal of Advance Industrial Communication and Cvber Securitv Svstems 2023

OPTIMIZING DATA PROTECTION ON CLOUD NETWORK USING PASSWORD BASED IDENTIFICATION AND AUTHENTICATION TECHNIQUES

[1]Nweze Onyekachi M., [2]James Eke

Enugu State University of Science and Technology; Department of Electrical Electronics, Engineering, Enugu State, Nigeria.

[1]Corresponding Author's Tel: +234 8065205191; Email: nwezemarcilinus5191@gmail.com

Manuscript received 4/7/2023; Final submission 26/7/2023; Accepted and published 30/7/2023

ABSTRACT

This paper addresses the crucial issue of data protection in cloud networks through the utilization of password-based identification and authentication techniques. A case study of a secondary school's local area network was conducted, revealing vulnerabilities that allowed unauthorized access to the school server. As the school lacked a central server and relied solely on a network provider for back-end storage, identifying intruders or students accessing the network became challenging. Consequently, the school's ICT personnel faced continuous stress from managing student login issues caused by hackers attempting to gain unauthorized access. To tackle these security challenges, the paper introduces a 4-phase approach consisting of registration, login, authentication, and password agreement phases. An empirical research approach was adopted, involving information gathering, hypothesis formation, data analysis, and conclusion drawing. The proposed methods were designed using a mathematical approach and implemented with SIMULINK. The results demonstrated that the real-time software and IP addresses registered in the database facilitated accurate user identification, leading to an impressive 0.7499% intrusion rate, effectively approaching zero, and an overall authentication accuracy of 98%. By adopting this approach, cloud networks can significantly enhance their data security and safeguard valuable resources from compromise and fraudulent access by unauthorized users.

KEYWORD: Cloud Network, Password authentication, One-time password, Server, Database

1. INTRODUCTION

Loads of data and sensitive information are routinely exchanged over the internet during online activities. While the internet is generally private and secure, it can still pose security risks for information exchange, with social engineering being a common method employed by intruders to obtain users' passwords and account details. Social engineering attacks are external and can occur through phone calls, faxes, emails, or other casual interactions. According to Alexander et al. (2022), raising user awareness and conducting training campaigns against such exploits are essential defensive measures. Internet security holds significant importance for individuals and businesses due to the growing threat of unauthorized access and hacking attempts. While intrusion protection has improved over time, it remains an ongoing process as technological advancements continue to present new challenges and potential vulnerabilities for attackers (Ya and Alibek, 2021). In (Ahmed and Raja, 2010; Devaraju and Ramakrishnan, 2014; Delphin et al., 2021; Fazale et al., 2014), researchers are consistently striving to enhance intrusion prevention effectiveness, but despite their success more work is required to guarantee the element of computer network security which are integrity, availability, and confidentiality. To bolster data protection during internet data exchange, encryption plays a crucial role (Huqquani et al., 2010; Schikuta, 2002). Strong identification protocols, user authentication at all levels, and controlled permissions for profiles within an organization are equally vital measures (Cong and Wang, 2009). Data in use, referring to data currently being updated, processed, accessed, or read by a system, is particularly susceptible to attacks. Thus, implementing encryption during this state becomes even more critical to ensure data security.

2.0 REVIEW OF WORKS

Eljona et al. (2016) conducted a study focusing on machine learning techniques to tackle the growing online threats in 4G networks. By leveraging an unsupervised machine learning algorithm, specifically a neural network, they achieved a commendable detection accuracy of approximately 89%. However, the researchers acknowledged that there is still considerable room for improvement in order to enhance the system's overall effectiveness in countering cyber-attacks.

In a separate effort, Gagnon and Fanadi (2017) explored the application of artificial neural networks for cyber-attack detection in 4G networks. Their findings also demonstrated a detection accuracy of approximately 89.78%, marking significant progress in enhancing network security. Nonetheless, the researchers, like their counterparts, recognized the need to further refine the algorithm to optimize its performance and bolster defense against cyber threats. El-Sayed and Feras (2015) proposed an innovative hybrid approach incorporating artificial intelligence to detect cyber-attacks with an impressive accuracy of 92%. This high success rate showcases the potential of such an approach to significantly improve security measures in 4G networks. The hybrid method, combining a fuzzy classifier and a genetic algorithm, proved to be a promising strategy for identifying and mitigating cyber threats effectively. Sulaiman et al. (2021) employed Support Vector Machine (SVM) in their research to address cyber threats in 4G data communication networks. The study yielded a detection accuracy of 90%, highlighting the capabilities of SVM in detecting and combating cyber-attacks effectively. This result further underscores the potential of SVM as a viable solution in safeguarding 4G networks from malicious activities. On the topic of encryption methods, Ettiane et al. (2018) delved into detecting and preventing Distributed Denial of Service (DDoS) attacks on mobile networks. Their research achieved an accuracy of 85%, which is a promising outcome, but they emphasized the importance of enhancing the adaptability of the encryption techniques to effectively counter the ever-evolving nature of cyber threats. Sulaiman and AlShaikhli (2014) meticulously studied cryptographic algorithms applied in ensuring data transmission security within 4G networks. Through simulations using MATLAB, they evaluated the algorithms and found that the proposed method was particularly favorable for packet security. However, they stressed the need for continuous research and improvements to strengthen overall network security. Finally, Ronaldo et al. (2020) took a comprehensive approach by combining multiple encryption techniques, including Advanced Encryption Standard (AES), Blowfish, and Triple Data Encryption Standard (3DES). Their efforts resulted in an impressive detection accuracy of 92%, signifying the potential of such an approach in enhancing data security. Nevertheless, the researchers acknowledged that further advancements can be made to continuously refine and optimize the combined encryption techniques for even better results.

2.1 Research Gap

The gap identified in these studies is the lack of practical validation for the proposed models despite achieving good results and high accuracy in detecting cyber threats. While the studies showcased promising outcomes, there appears to be a disconnect between the theoretical advancements and their real-world implementation and validation. Practical validation is a critical step in assessing the viability and effectiveness of any cybersecurity solution, especially when it comes to safeguarding complex 4G networks against actual cyber-attacks. Real-world scenarios can introduce numerous variables and challenges that may not be fully accounted for during the research phase. Without practical validation, it becomes difficult to ascertain how well these models perform in real-time network environments, where dynamic and unpredictable cyber threats are constantly evolving. Addressing this research gap through practical validation will contribute to building more robust and effective cybersecurity solutions for 4G networks using the proposed encryption method.

3. METHODOLOGY

The development of the new system follows an Empirical research approach, a systematic and data-driven methodology. It starts with gathering relevant information from the school to understand the system's requirements and context. Based on this information, hypotheses are formulated, making educated predictions about the system's expected outcomes using historical data like log tables. To ensure controlled testing and accurate observations, a test environment is prepared. The system's functionalities and features are rigorously tested to validate the initial hypotheses. The collected data is then thoroughly analyzed to interpret the outcomes, identify trends, and draw meaningful conclusions. Based on the findings, a final conclusion is drawn regarding the effectiveness and success of the new system. The Empirical research approach ensures that the system's development is grounded in concrete data and evidence, ultimately leading to a reliable and efficient solution that meets the school's specific data protection needs on the cloud network.

3.1 User and System Requirements for Implementing Cloud-Based Data Encryption

When implementing cloud-based data encryption, the primary concern of the user is to establish a robust and effective network security system that can safeguard against cyber-attacks. The user demands a solution capable of continuous monitoring of incoming and outgoing data within the network. This system must make prompt decisions to either permit or block data based on its nature, ensuring protection from unauthorized access and potential breaches (Ali et al., 2012). Emphasizing the significance of accuracy, the user highlights the need to select essential and discriminative features for the artificial neural network (Mba and Asogwa, 2022). These features should exhibit real-time responsiveness, ensuring no part of the system remains dormant while others are active, thus reducing the occurrence of "False Alarms." Achieving a high level of accuracy in detecting attacks and accurately identifying benign applications is a key goal for the user. Additionally, the user requires a well-designed false alarm system tailored specifically for the client-server environment (Ghanam et al., 2012). The system should categorize incoming requests into three types: almost certainly an attack, uncertain if the packet is an attack or not, and almost certainly not an attack. While recognizing the importance of assuming everything except legitimate traffic as an attack, the user emphasizes the need to strike a balance to avoid overwhelming false alarms for users. Acknowledging that the absence of intrusion detection exposes the network to potential attacks, the user stresses the necessity of an effective intrusion detection system. This system should proactively identify and alert security professionals about potential threats before they can be successfully executed. To meet these requirements, three key aspects must be addressed:

Detection: The network security system should continuously monitor incoming and outgoing data in real-time. Its effectiveness will be measured by the number of correctly detected attacks (TP), inversely proportional to the cumulative number of benign applications mistakenly labeled as assaults (FP), and the number of correctly detected attacks, as indicated by equation 1.

Accuracy: High accuracy in detection relies on feeding the artificial neural network with essential and discriminative features from network data. These features must respond in real-time to prevent any part of the system from being dormant while others are active, thus minimizing "False Alarms." Equation 2 highlights that accuracy is directly proportional to the number of correctly detected attacks and the percentage of applications accurately classified as harmless. Conversely, it is inversely proportional to the cumulative number of correctly detected attacks (TP), the percentage of applications accurately classified as harmless (TN), the number of benign applications mistakenly labeled as assaults (FP), and the number of attacks mistakenly labeled as normal (FN).

False Alarm: For the client-server setup, the system must distinguish among three types of requests: almost certainly an attack, uncertain packets, and almost certainly not an attack. Balancing the assumption of attacks while avoiding excessive false alarms for users is crucial. The absence of intrusion detection exposes the network to potential attacks, while an effective intrusion detection system proactively identifies and alerts security professionals to potential threats, enabling timely responses to prevent successful exploitation. By addressing these user and system requirements, a well-designed cloud-based data encryption system can be developed, providing robust and accurate protection against cyber-attacks while minimizing false alarms and ensuring prompt responses to potential threats.

3.2 DATA COLLECTION

In the context of the discussed password-based authentication technique, certain conditions must be met to ensure its effectiveness:

i. The password lookup table must not be automatically stored inside the computer memory. This measure is implemented to enhance security and prevent unauthorized access to sensitive password information.

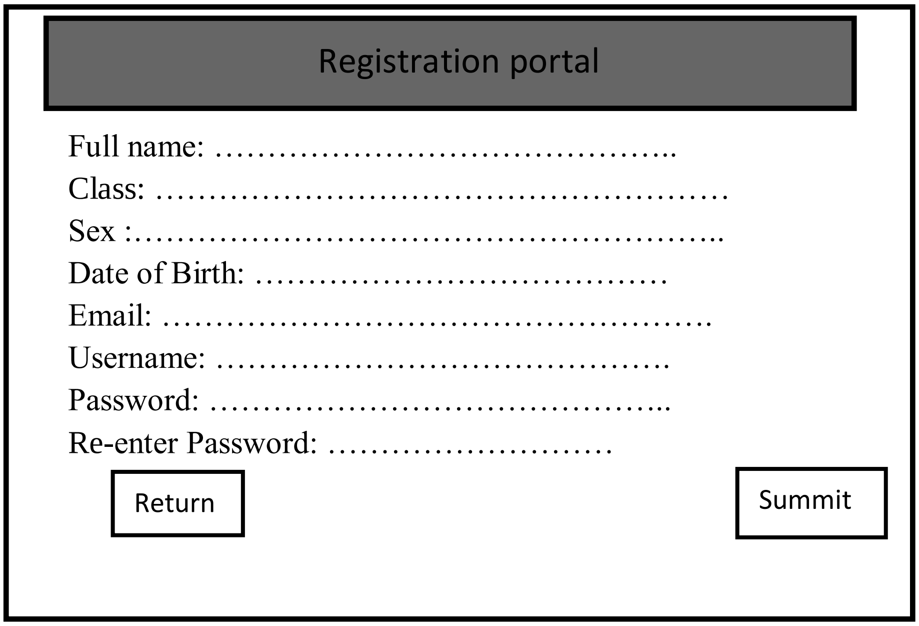
ii. Passwords should be easily chosen by users and be subject to change when necessary. This flexibility allows users to create strong and memorable passwords while adapting to evolving security requirements.

iii. Passwords must be encrypted during transmission, especially when third-party involvement is present. Encrypting passwords adds an additional layer of protection against potential interception and unauthorized access.

iv. The authentication system must be resistant to guessing attacks and stolen modification attacks. Robust security measures must be in place to prevent malicious actors from successfully compromising user passwords.

v. Passwords must adhere to certain complexity requirements, such as containing alphanumeric characters, and their length should be sufficient for easy memorization.

To gather the necessary data, the ICT department of the school collected the following information from the students: Name, Class, Age, and computer IP address. Using this information, a log table was created in the database for each student, with each student being assigned a unique identity consisting of a username and password as in figure 3.1. This log table and unique identity allow for the implementation of the password-based authentication technique, ensuring secure access to the system's resources.



Registration portal

Full name: ……………………………………..
Class: ……………………………………………
Sex :……………………………………………..
Date of Birth: …………………………………
Email: ………………………………………….
Username: …………………………………….
Password: ……………………………………..
Re-enter Password: ………………………

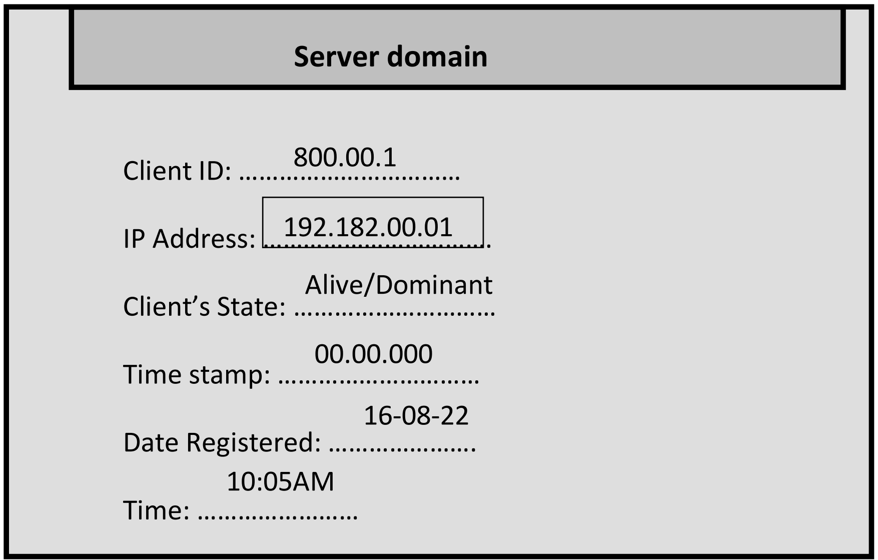
Fig 3.1: Registration interface

During the registration process in this type of domainMySQL (with PHP) enables users and administrators to interact with a database through internet pages; then, the data management systems automatically insert the user's input into the administrator's table, reducing the administrator's burden. As a result, the website's registration page is designed to filter and validate the user's data entry.Users (students) may therefore be permitted to update and change their own entries in a database from the interactive website.

3.3 THE SERVER

In Figure 3.2, the server plays a crucial role in providing services to the database. To effectively serve its purpose, the database requires a server that can handle various tasks. An all-in-one Database Management System (DBMS) is the system that was used to fulfill this role. Additionally, the presence of a PHP processor further enhances the capabilities of the server in managing and processing data. The DBMS serves as the central component responsible for organizing, storing, and retrieving data from the database. It manages data integrity, security, and ensures efficient data access and manipulation. With an all-in-one DBMS, multiple functionalities related to database management are integrated, simplifying the setup and maintenance of the database system.

The PHP processor, in conjunction with the server and DBMS, enables the execution of dynamic web applications. PHP is a widely used server-side scripting language, adept at processing data and generating dynamic content based on user interactions and data retrieval from the database. By combining the server, all-in-one DBMS, and PHP processor, the database system gains the ability to deliver a seamless user experience through responsive and dynamic web applications. The server acts as the foundation, handling client requests and serving database-related content efficiently. The all-in-one DBMS ensures data integrity and effective data management, while the PHP processor facilitates dynamic data processing and content generation, ultimately contributing to a fully functional and reliable database serving its intended purpose.



Server domain

Client ID: 800.00.1

IP Address: 192.182.00.01

Client's State: Alive/Dominant

Time stamp: 00.00.000

Date Registered: 16-08-22

Time: 10:05AM

Fig 3.2 Server domain

3.4 DATABASE

This is similar to one or more files on a computer and enables the linking of data from several sources into a single entity. While spreadsheets can be valuable tools for examining data held in a database, they are not ideal for replacing databases entirely. Spreadsheets may serve well for simple data analysis and presentation, but they lack the robustness and efficiency required for handling more intricate data structures and relationships.

In this case, relying on a dedicated database system, such as one powered by Apache Server, proves to be a superior solution. Apache Server offers a powerful platform for managing databases, providing features like data integrity, security, and optimized data retrieval and storage. Unlike spreadsheets, databases excel in handling diverse data types and complex relationships between entities. By leveraging Apache Server as the backend, databases can efficiently store and manage vast amounts of data, ensuring data integrity and consistent performance even under heavy loads. Additionally, databases offer advanced querying capabilities, enabling users to extract valuable insights from the stored data efficiently. The figure 3.3 presented the mode model of the data and web server, while the flow chart in figure 4.4 presented the transmitted packet work flow.

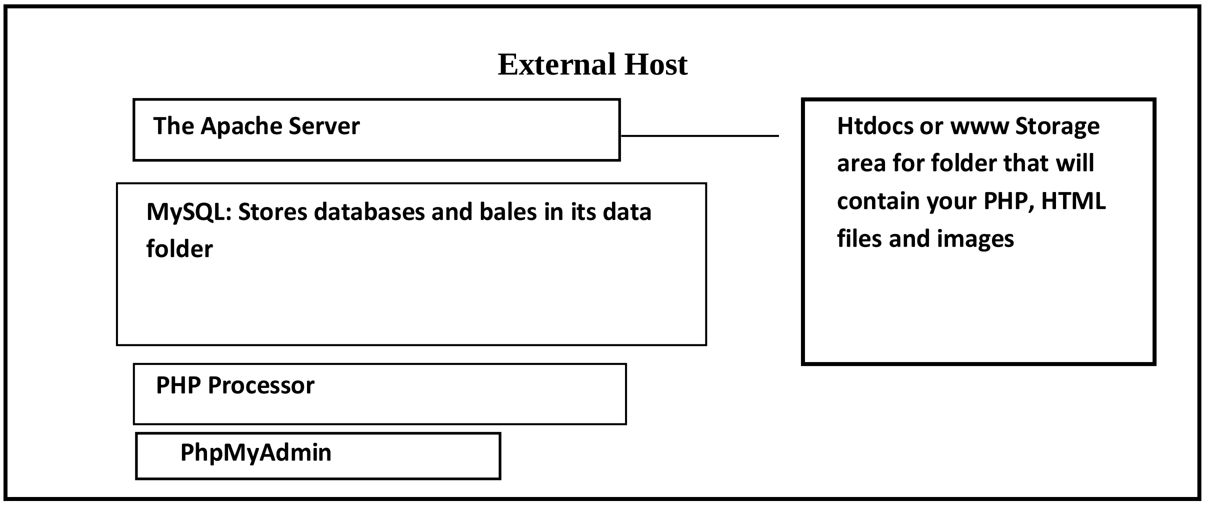

External Host
The Apache Server
MySQL: Stores databases and bales in its data folder
PHP Processor
PhpMyAdmin
Htdocs or www Storage area for folder that will contain your PHP, HTML files and images

Fig 3.3: Main components of Data, Webserver and packet transmission

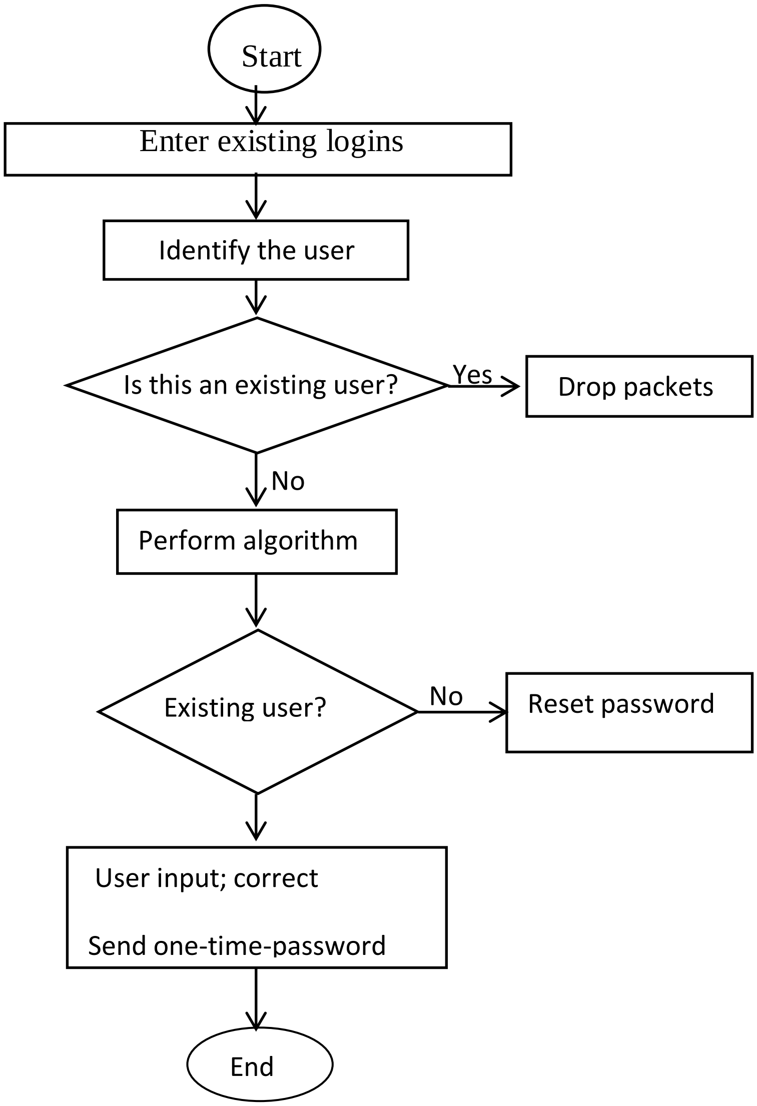


Fig 3.4 flow-chat for data in the network

The functionality of this flow chat is based on the already existing lookup table or log table existing on the database, whenever an input (username and password) is keyed in, the server will redirect and make a quick search to the database to check if the username is registered and stored in the data base, if this user is found then it checks whether the username and password been inputted corresponds with the one found in the table stored in database, this process helps the application in decision making.

3.5 The PROPOSE SCHEME

Password Based Identification and Authentication technique Authentication ensures that system's resources are not obtained fraudulently by illegal users. Authentication scheme includes three major phases: registration, login and authorization. Using Hopfied Neural Network (HPNN) of password authentication which basically works upon recalling the stored pattern, this recalling is the matching of giving input pattern with the already stored pattern.

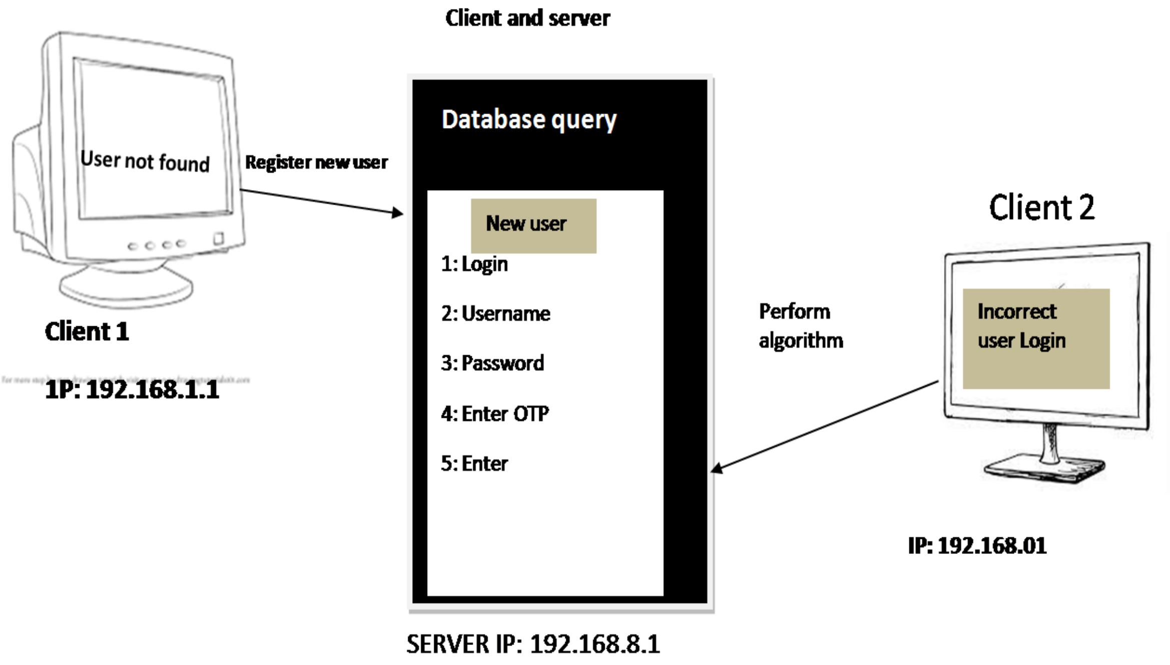


Figure 3.5: The authentication system architecture

In Fig 3.5, client 1 logins were not recognized or found on database which means that the user had not been a registered student automatically will be redirected to creating new account on the school portal. Client 2 identities matched an already existing account but the user input does not match with the registered user login, it then means that the user could have made an error while inputting the username or password, the user is given a 3 attempt trials which after which failed the 3 attempts the system will redirect for authentication process, an algorithm for this process is seen in Fig 3.6

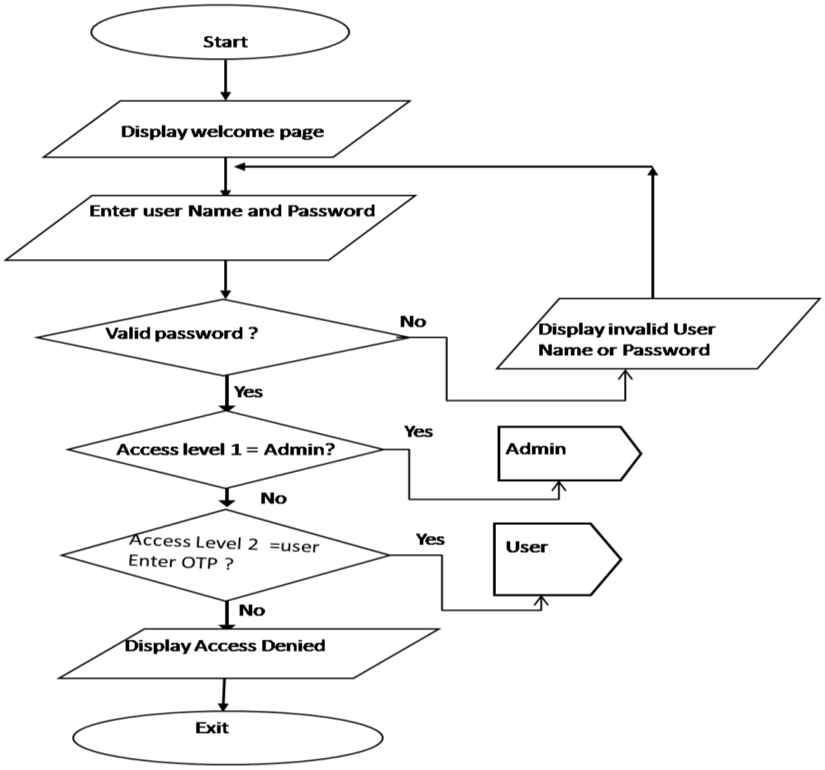


Fig 3.6: Login attempt and authentication flow chat

Performance Evaluation intrusion prevention when compared to already existing system using Matlab tools. The following conditions were satisfied as corresponding features were considered important.

1. Reduced accuracy and decreased FP
2. Reduced accuracy and increased FP
3. Increase in FP without a change in accuracy
4. Accuracy and FP will rise.

As evaluation parameters, some assessment metrics that are computed using the confusion matrix were used, including accuracy, detection rate, and false alarm rate.

TP: The number of correctly detected attacks.

TN: The percentage of applications that were accurately classified as harmless.

FP: The amount of benign applications that were mistakenly labeled as assaults

FN: The number of attacks that were mistakenly labeled as normal.

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FN+FP} \tag{1}$$

$$\text{Detection}= \frac{TP}{TP+FP} \tag{2}$$

$$\text{False Alarm}\frac{FP}{FP+TN} \tag{3}$$

4.0 Simulation Performance Measurement and Result

Illegal network access reduces system effectiveness because it increases processing times. Based on the two metrics of accuracy and false positive rate, the presence and relevance of each characteristic are assessed. The criteria mentioned above must be met in order for the feature to remain in the dataset, along with satisfying them. Table 4.1 shows the complete table of login attempts also called register; this table is found in Data base to keep record of the entire login attempts which also is in reference to the algorithm developed. From the table "Alert ID" 85 authentication was successful hence the user's inputs (password and username) were correctly inputted which and as such the system allowed access to the user. ID 86 was record as threat; this user's detail was not found in the database, the safest rule is to assume that everything except legitimate traffic is an attack so this user was considered an attack and the packet was dropped.

Table 4.1: Results of Intrusion Detection System

Host ID	Alert ID	Time Stamp	Rule ID	Respond message	Action
800	85	2022-07-15 10:43:30	1002	Authentication successful	Allow access
0	86	0000.00.00 00.00.00	1005	Threat	Block
0	87	2022-07-16 11:30:15	1008	Attempted Admin Login	ignore
0	88	2022-07-16 12:14:05	1009	Attempted User Login	Ignore
800	89	2022-07-16 12:16:30	1002	Authentication successful	Allow access
0	90	2022-07-16 12:17:15	1002	Authentication successful	Allow access
0	91	2022-07-16 12:27:14	1002	Authentication successful	Allow access
0	92	2022-07-16 12:27:16	1002	Authentication successful	Allow access
0	93	2022-07-16 12:27:18	1002	Authentication successful	Allow access
0	94	2022-07-16 12:27:20	1005	Threat	Block
800	95	2022-07-16 12:30:11	1002	Authentication successful	Allow access
0	96	0000-00-00 00:00:00	1007	Buffer overflow	ignore
0	97	2022-07-16 12:30:28	1002	Authentication successful	Allow access
0	98	2022-07-16 12:30:30	1002	Authentication successful	Allow access
0	99	2022-07-16 12:30:51	1007	Buffer overflow	Ignore
0	100	2022-07-16 12:35:27	1008	Attempted Admin Login	Ignore
800	101	2022-07-16 12:35:37	1002	Authentication successful	Allow access

0	102	2022-07-16 12:41:39	1002	Authentication successful	Allow access
0	103	2022-07-16 12:46:41	1002	Authentication successful	Allow access
0	104	2022-07-16 12:59:58	1002	Authentication successful	Allow access
0	105	2022-08-13 11:46:31	1008	Attempted Admin Login	Ignore
0	106	2022-08-13 11:46:41	1008	Attempted Admin Login	Ignore
0	107	2022-08-13 11:46:44	1009	Attempted Admin Login	Ignore
0	108	2022-08-13 11:46:46	1008	Attempted Admin Login	Ignore
0	109	2022-08-13 11:46:49	1009	Attempted Admin Login	Ignore
0	110	2022-08-13 11:46:51	1008	Attempted Admin Login	Ignore
800	111	2022-08-16 09:11:20	1001	Changed to un-authenticate	Block
800	112	2022-08-16 09:11:30	1001	Changed to un-authenticate	Block
800	113	2022-08-16 09:12:40	1002	Authentication successful	Allow access

The simulation results in table 4.1 reveal several key findings about the intrusion detection system's performance. Firstly, the system demonstrated high efficiency in handling successful authentications (Alert ID 85, 89-94, 95, 97, 98, 101, 102, 103, 104, and 113), appropriately allowing legitimate user logins. This showcases the system's reliability in providing seamless access to authorized users. Secondly, the system effectively identified and blocked detected threats (Alert ID 86 and 94), demonstrating its ability to protect against specific types of attacks. This highlights the system's capability to respond promptly to potential security risks and mitigate them. However, a concerning aspect arises from the ignored threats, particularly attempted admin logins and buffer overflow incidents (Alert ID 87, 88, 96, 99, 100, 105-110). Ignoring such events poses significant risks to the network's security, potentially leaving it vulnerable to unauthorized access and data breaches. This indicates a critical area for improvement in the system's response and handling of these types of threats. On a positive note, the system's response to unauthenticated changes (Alert ID 111 and 112) was effective, correctly blocking access. This demonstrates the system's ability to safeguard against unauthorized alterations and maintain the integrity of security settings. In conclusion, the intrusion detection system shows promise in detecting successful authentications and blocking specific threats, contributing to a robust security framework. However, the identified issues with handling attempted admin logins and buffer overflow incidents demand immediate attention to prevent potential security vulnerabilities. Fine-tuning the system's response mechanisms and implementing advanced anomaly detection techniques could enhance its overall effectiveness in safeguarding the network from cyber threats.

5.0 Conclusions

Intrusion detection became quite difficult when the volume of data in the network began to increase. Therefore, it was necessary to manage these enormous databases. Many IDS still lacks the ability to detect all kinds of new attacks in the network so researchers are inclined towards modeling the normal instances to increase their system effectiveness. Real-time anomaly identification has always been difficult since it relies on outliers. By using cluster-based and distributed data, I infer that authentication and identification boost high detection rates, minimal false alarm rates, memory utilization, and time responses, as well as lower the stress associated with using a manual spreadsheet database type. The proposed point out algorithms may provide a better solution even though the reduction has not been very significant because they are made to function in a distributed environment by carefully considering the computing and communication resources, such as IP addresses, databases, domain servers, and network providers. After achieving data privacy in a distributed data setting, the clustering technique allows for a large data processing optimization. Due to the expense of the computation, there is a trade-off between clustering accuracy and performance. From the simulation result, there is a better performance in terms of intrusion detection and threat blocking response time, memory utilization and processing distribution comparing with genetic algorithm, Authentication & Identification technique. When putting the entire project into perspective, this approach largely concentrated on feature reduction, clustering analysis, and modeling the typical cases in the presence of attack information. The strategy is effective and overcomes one of the problems with rule-based strategies. Having talked about the efficiency of this work based on performance indicators, accuracy, and failed and successful login attempt. Thus, our work provides a practical solution for construction of better IDS based on data mining technique. Thus, with the of 0.7499% intrusion rate achievement in this work; which is also very good as it is approximately zero, the TCP header information that allows deal with anomaly detection in fast incoming traffic in real time with lower false positive detection rate.

5.1 Contribution to Knowledge

This research work has examined different intrusion prevention algorithm, and as such provides;

(i) A systematic approach of User, Database and Server information sharing (System)

(ii) A novel of strategy for Authentication and Identification (Application)

(iii) Novel to detect illegal intrusion after 3 unsuccessful login attempt (Algorithm). In addition, this work also provides material for further research in the field of intrusion prevention, data mining and authentication techniques

6. REFERENCES

Ahmed, S., & Raja, M. (2010). Tackling cloud security concerns and forensics methodology. In High-Capacity Optical Networks and Enabling Technologies (HONET) (pp. 1-5). DOI:10.1109/HONET.2010.5715771

Alexander Salomatin, A. Y. Iskhakov, & R. Meshcheryakov (2022). Proactive Detection of Attacks on APCS Accounts Based on Analysis of User Identification Graphical Attributes. In Frontiers in Robotics and Electromechanics (pp. 163-177).

Ali, A. S., Wasimi, S. A., & Khorshed, M. T. (2012). A study of the gaps, difficulties in threat remediation, and ideas for proactive attack detection in cloud computing. Computer Systems of the Future, 28(6), 833–851.

Ana, C. O., Henryson Chagas, & Marco Spohn (2014). IEEE Symposium on Computers and Communication (ISCC). Proceedings - International Symposium on Computers and Communications. DOI:10.1109/ISCC.2014.6912551

Bachar A. EIHassan, Abdallah M'Hamed, & Pierre E. Abi-Char (2007). A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography. In Information Assurance and Security, IAS 2007. Third International Symposium. DOI:10.1109/IAS.2007.57

Boutaba R, Cheng L, & Zhang Q (2010). Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1(1), 7-18.

Chia-Ming Wu & Ruay-Shiung Chang (2010). Green Virtual Networks for cloud Computing. Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on, pp. 1, 7.

Cong Wang & Qian Wang (2009). Ensuring data storage security in cloud computing. International Workshop on Quality of Service, 2009, pp. 1–9.

Delphin Raj Kesari Mary, Eunbi Ko, Seung-Geun Kim, Sun-Ho Yum, Soo-Young Shin, & Soo-Hyun Park (2021). A Systematic Review on Recent Trends, Challenges, Privacy and Security Issues of Underwater Internet of Things. PMID: 34960366 PMCID: PMC8706400 DOI: 10.3390/s21248262

Devaraju S. & Ramakrishnan, S. (2014). Performance Comparison for Intrusion Detection System using Neural Network with KDD dataset. ICTACT Journal on Soft Computing, 4, DOI:10.1016/j.ieri.2014.09.099. LicenseCC BY-NC-ND 3.0

Fazal-e-Amin, M. Irfan Khan, & Soofi Aized Amin (2014). A Review on Data Security in Cloud Computing. International Journal of Computer Applications, 94(5), 975-8887. DOI:10.5120/16338-5625

Ghanam Y., Jennifer Ferreira, & Frank Maurer (2012). Emerging Issues & Challenges in Cloud Computing—A Hybrid Approach. Journal of Software Engineering and Applications, 5(11), 923-937.

Huqqani, A. A., Beran, P. P., Schikuta, E., & Xin, L. (2010). Cloud-based Neural Network Simulation Application. In International Joint Conference on Neural Networks (IJCNN). DOI:10.1109/IJCNN.2010.5596747

Rules (2004). Published in CNNA '04: Proceedings of the 8th IEEE International Bi-annual Workshop on Cellular Neural Networks and their Applications, Los Alamitos, California, USA, IEEE Computer Society.

Schikuta, E. W. (2002). NeuroWeb as an online neural network simulator. In the 14th International Conference on Tools with Artificial Intelligence (ICTAI'02) of the IEEE. DOI:10.1109/TAI.2002.1180832

Ya, L., Seyed M. G., & Alibek, I. (2021). Improving the Accuracy of Network Intrusion Detection System in Medical IoT Systems through Butterfly Optimization Algorithm. Wireless Personal Communications International Journal.

Mba J. & Asogwa T. (2022). Modeling of Neuro-based Strategy for Mitigation of Cyber Threat on 4G Wireless Network using Artificial Intelligence Technique. In International Journal of Advance Industrial Communication and Cyber Security Systems, 1(6), 85-97.

Ronaldo, F., Pramadihanto, D., & Sudarsono, A. (2020). Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE Network. In 2020 International Electronics Symposium (IES) (pp. 116-122). IEEE.

Eljona Proko, Alketa Hyso, & Dezdemona Gjylapi (2016). Machine Learning Algorithms in Cyber Security. In CEUR Workshop Proceedings, Vol. 2280, pp. 507-522.

Gagnon, F., & Esfandiari, B. (2017). Using Artificial Intelligence for Intrusion Detection. In Proceedings of the Conference on Emerging Artificial Intelligence Applications in Computer Engineering, Amsterdam, Netherlands, pp. 295-306.

Sulaiman, A. G., & Al Shaikhli, I. F. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. International Journal of Computer Science and Telecommunications, 5(7), 7-10.

El-Sayed M. El-Alfy & Feras N. AlObeidat (2015). Detecting Cyber-Attacks on Wireless Mobile Networks Using Multicriterion Fuzzy Classifier with Genetic Attribute Selection. In Mobile Information Systems, Volume 2015, Article ID 585432, 13 pages. DOI:10.1155/2015/58543

Ettiane, R., Chaoub, A., & Elkouch, R. (2018). Robust detection of signaling DDoS threats for more secure machine type communications in next-generation mobile networks. In Electrotechnical Conference (MELECON), 2018 19th IEEE Mediterranean, pp. 62-67. IEEE.

Sulaiman, A. G., & Al Shaikhli, I. F. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. International Journal of Computer Science and Telecommunications, 5(7), 7-10.