Multidisciplinary Journal of Engineering, Technology and Sciences, Volume 1 Number 1, 2024
Online publication with Google Scholar indexing, Email: mjets85@gmail.com
Title: Mitigation of Packet Drop in Wireless Network Using Hybrid Authentication
Authors: Agbo Esther U[1] Alumona Theophiliphus[2] Alagbu Ekene[3] Onyeyili Toochukwu[4]

Mitigation of Packet Drop in Wireless Network Using Hybrid Authentication

Agbo Esther U[1] Alumona Theophiliphus[2] Alagbu Ekene[3] Onyeyili Toochukwu[4]
Email:divineangel21@gmail.com
Department of Electronic and Computer Faculty of Engineering Nnamdi Azikiwe University

Abstract
The wireless network interface is open and accessible to both authorized and unauthorized users due to the broadcast nature of radio propagation. Wireless transmission is more vulnerable to malicious assaults than wired transmission due to the open communication environment, which includes both passive and active attackers for disrupting valid signals. This research work aimed at developing a model that will mitigate packet drop in a wireless network using hybrid authentication i.e User identification code (UIC) and One time password (OTP). After the evaluation parameters taken into consideration such as the false alarm rate= 8.2% the detection rate= 4.22% and the Accuracy = 92%. It can be said that the model developed actualized its aim of mitigating packet drop in a wireless network to the lowest minimum.

Introduction
The advancement in information and communication technology has given rise to ubiquitous connectivity across the globe. This enables computers and electronic devices to be linked-up via internet connections. Internet connectivity is made possible through wireless networks. Wireless network can be described as a network established using any wireless data connections. Wireless communication takes place with the help of radio waves. There are different types of wireless networks such as Personal area network, Local area network, mesh network, Metropolitan area network, Space network, Cellular network.

Network security is a set of policies and practices implemented to prevent unauthorized access, modification, misuse, denial of network service and resources. Achu et al, (2019) stated that the availability of networks makes it possible for one to send and receive any form of data like e-mails, audio, videos, texts, and images around the world. These data are transmitted real-time every second and this makes the data network traffic to be of a major concern in terms of security and availability.

The major limitations in the mobile ad-hoc network. As one node moves away from the network, the connection gets lost and the packet drop may happen and also because of congestion packet loss happens. Congestion happens when many demand request gathers and when there is a shared medium, Packet loss is caused due to poor signal strength at destination, natural or human-made interference, system noise, hardware failure and software corruption and many more. Packets may also be lost when a particular router receives it and the router decides not to send the packet to the next hop. This way of packet loss is called “packet dropping”. There are many reasons for packet dropping for example, if the router is overloaded, or if router believes packet as a part of denial-of-service attack.

Literature Review
U. Srilakshmi et al, 2021 stated in their work, "An Improved Hybrid Secure Multipath Routing Protocol for MANET," that Mobile ad hoc networks (MANETs) are self-organizing nodes in a mobile network that collaborate to form dynamic network architecture to establish connections. In MANET, data must traverse several intermediary nodes before reaching its destination. There must be security in place to prevent hostile nodes from accessing this data. Multiple methods were suggested in literature for securing routing; these techniques tackle different aspects of security. In order to enhance fault tolerance, wireless network multipath routing is typically used instead of the original single path routing. The routing protocol Genetic Algorithm with Hill climbing (GAHC) described in this article shows a hybrid GA-Hill Climbing algorithm that picks the optimal route in multipath. Prior to this in the beginning, the Improved fuzzy C-means algorithm method was built on density peak, and cluster heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust. The computation is based worth nodes are at the trust threshold found in addition. Even CHs take part in the alternate paths, the blend of all the many paths from these Cluster Heads that chooses the optimal route, which is based on the predicted hybrid protocol, as well as the optimum route’s aggregate features such as throughput, latency, and connection. This suggested technique requires a minimum amount of energy of 0.10 m joules and a small amount of delay time of 0.004 msec, which also yields a maximum

throughput of 0.85 bits per second, a maximum detection rate of 91 percent and maximum packet delivery ratio of 89percent. The suggested approach was put through the paces with the selective packet dropping attack.

Aniekwe, et al (2021) stated in a research work that the widespread proliferation of computer networks has resulted in the increase of attacks on information systems. These attacks are used for illegally gaining access to unauthorized information, misuse of information or to reduce the availability of the information to authorized users. This results in huge financial losses to companies and can also result in losing their goodwill to customers and services are severally disrupted. So, the research work designed a system to improve the data transmission security in wireless network. The packet loss was evaluated and a modified digital signature algorithm was developed. The thesis also simulates the Network Activity Tracking using digital Signature using php-mysql model. With the modified digital signature algorithm, the network security was improved resulting to less packet delivery response time on the data network as the minimum packet delivery time recorded was 1.2 seconds in different simulations time which is less when compared to the earlier measurement when digital signature was not used and we obtained minimum packet delivery time recorded of 20 seconds. This shows a reduction in minimum packet delivery time of 18.8 seconds which is a great improvement in data delivery rate in network. The improvement can reduce data loss due to network delay and improve the security in the network.

P.Zhao et al, 2022 stated in their work "Federated Learning-Based Collaborative Authentication Protocol for Shared Data in Social IoV," that In the Social Internet of Vehicles (SIoV), federated learning is able to significantly protect the private data of the vehicle's client, while reducing the transmission load between entities. Nevertheless, data can still be stolen by an adversary who analyzes the parameters uploaded by the client to steal it. In this paper, to effectively prevent data leakage and reduce the propagation delay of data, we design a federated learning collaborative authentication protocol for shared data. The parameters of the vehicle client model are encrypted by the protocol in the federated learning. The vehicle and other entities of the protocol realize efficient anonymous mutual authentication and key agreement. The security of the proposed protocol is proved in the stochastic predictive machine model. The simulation results on the SUMO and OMNeT++ platforms show that the authentication delay is the lowest compared to other protocols and the packet loss rate is reduced to 4.68%. Moreover, the overfitting of the globally aggregated model is effectively resolved.

P. Dinesh Kumar et al, (2023), stated that nodes are deployed randomly in the network area of the WSN. data transmission from source to destination via intermediate nodes should be done in a secure fashion. Due to the large size of packet loss and energy consumption of sensor nodes, a secure and energy-efficient path must be required. The main objective of this research was to provide secure data transmission among node-to-node for efficient delivery of data packets to the destination. The system uses a novel hybrid firefly and BAT algorithm for path selection, an innovative trust value generation, and optimal neighborhood selection using fuzzy logic. The research employs Elliptic Curve Cryptography (ECC) combined with Diffie-Hellman exchange for key generation and key exchange. Path selection is done by fuzzy logic and optimization of selection has been carried out by hybrid BAT and Firefly algorithms. Key generation includes a time-based randomness factor that increases the complexity of cryptanalysis, thereby providing the most security. The performance of the simulation is analyzed and depicted in terms of delay, throughput, energy, and processing time. The research has been carried out using a network simulator with nodes deployed randomly in the network area with mobility as the primary concern that requires dynamic path selection.

Analysis of the Proposed System

To improve the security of the Wi-Fi data network, every user must be registered on the data network server and during the registration, the user obtains user identification code (UIC). To use the data network, first the user will detect access points either by sending a probe request and receiving a probe response, or purely by looking at the beacon frames frequently transmitted by an access point. Upon discovery, the user may try to authenticate to the access point. This authentication is done by providing the user identification code (UIC). If successfully authenticated, the system will go further to identify the user by sending a onetime password (OTP) to the users' phone via SMS. The user is expected to enter the OTP received for the second authentication. If the OTP is valid, the user may try to associate with the access point by sending an association request.

Multidisciplinary Journal of Engineering, Technology and Sciences, Volume 1 Number 1, 2024
Online publication with Google Scholar indexing, Email: mjets85@gmail.com
Title: Mitigation of Packet Drop in Wireless Network Using Hybrid Authentication
Authors: Agbo Esther U[1] Alumona Theophiliphus[2] Alagbu Ekene[3] Onyeyili Toochukwu[4]

Use Case Diagram of the New System.

The system designed in this research work is divided into several modules that needs access restrictions. Different use cases were described in the way they were applicable in the software designed. The researcher identified total of two roles that functions as access levels in our diagrams. A use case is a function to be performed by the system from the user's perspective.

Figure 1 below is the use case boundary diagram of the system**.** This shows the various processes that lead to securing data in the data network. It starts with verifying the user identification code (UIC), and confirming the OTP entered. Once this is done, the user can upload / download data from the data network.

Sequence Diagram. The sequence diagram in figure 3 and 4 shows how objects interact with one another and in what order. It depicts the objects and classes involved in the scenario.

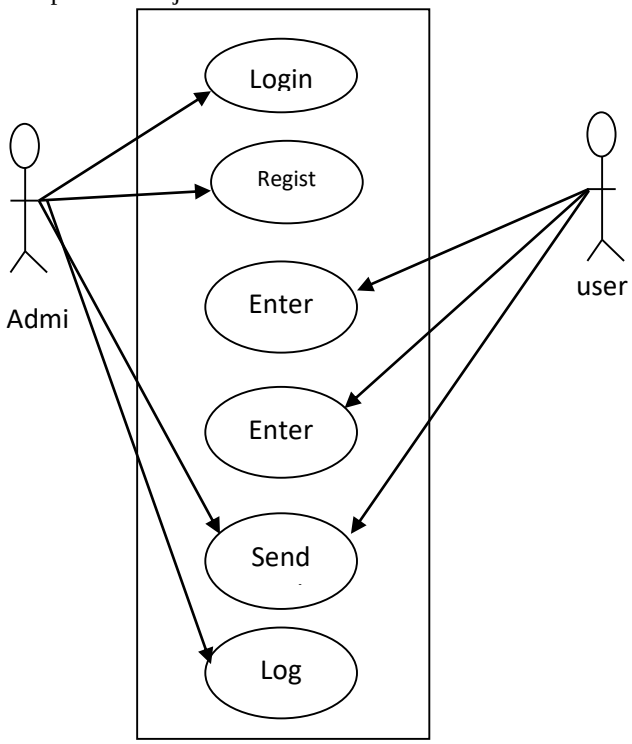

Fig. 1: Use Case Diagram of the System

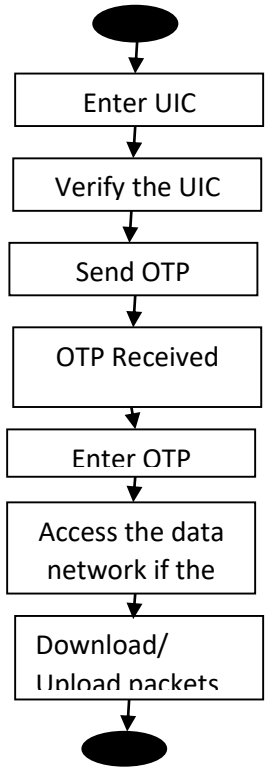

Fig. 2 Activity Diagram of the New System

Sequence Diagram (User)

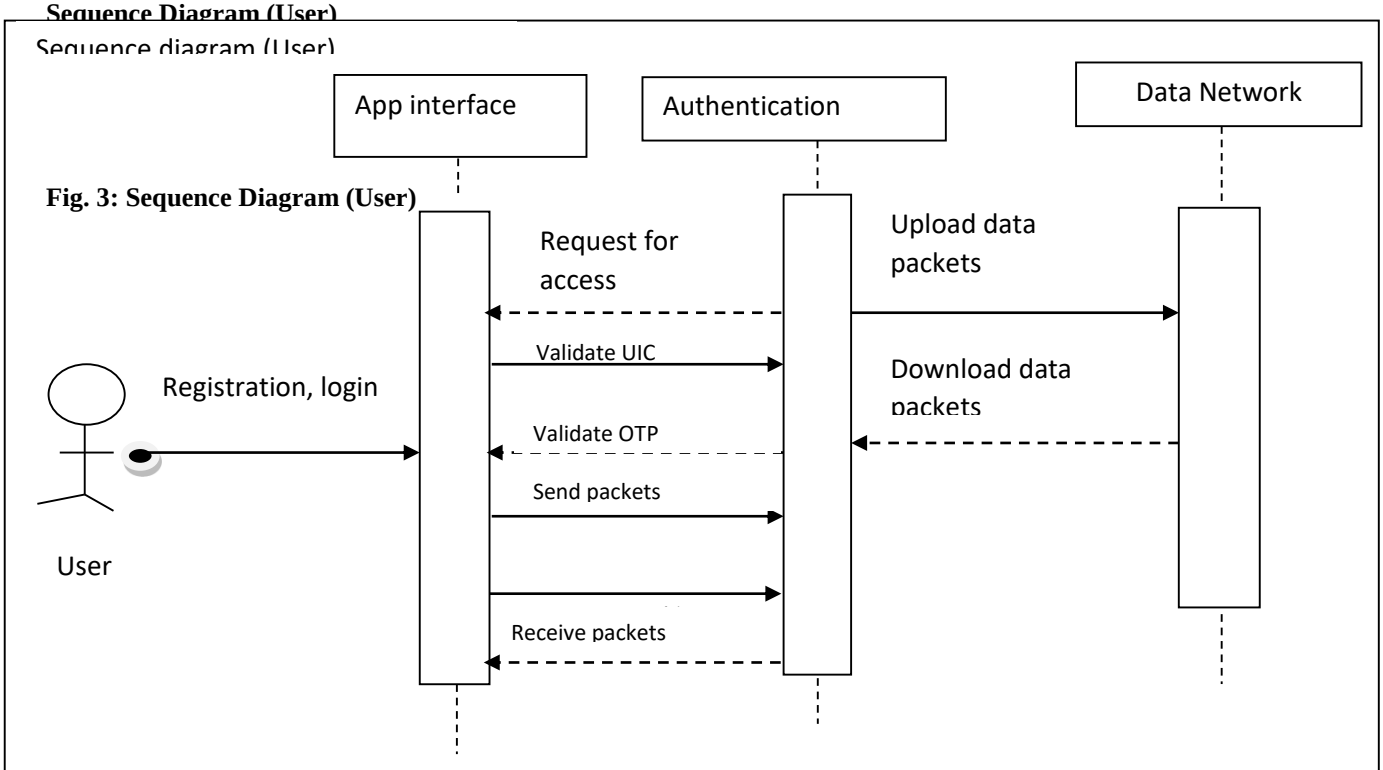

Fig. 3: Sequence Diagram (User)

As can be seen in figure 3, the user can do the following things.

1. Request for access to data network
2. Validate the UIC and OTP
3. Download and upload data packets

Sequence Diagram (Admin)

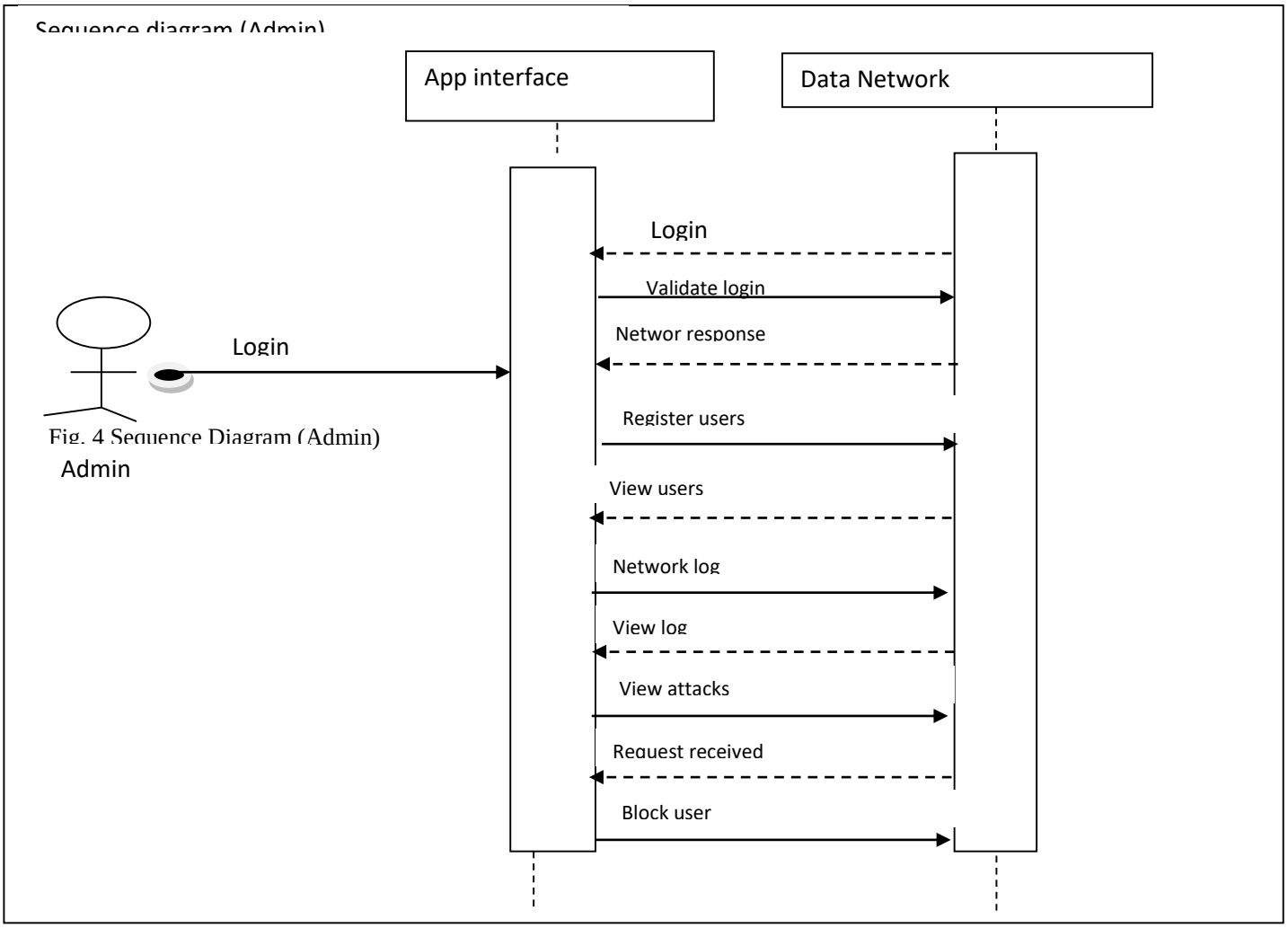

Fig. 4 Sequence Diagram (Admin)

As can be seen in figure 4, the admin can do the following things.

1. Login
2. Validate the login details
3. Register users
4. View users
5. View network log
6. View network attacks

Figure 4 Sequence Diagram (Admin), This section presents the design of the proposed model and how it was used to actualize the aim of the research.

Control Center/Main Menu

Figure 5 represents the main menu of the proposed mitigation of packet drop using hybrid authentication. It shows the various modules that were designed in the program. Each module performs a specific task and is accessible through the main menu. It controls access to other sub systems in the program design. In the main menu, the server side controls network administrator operations while the client side controls the network users' operations.

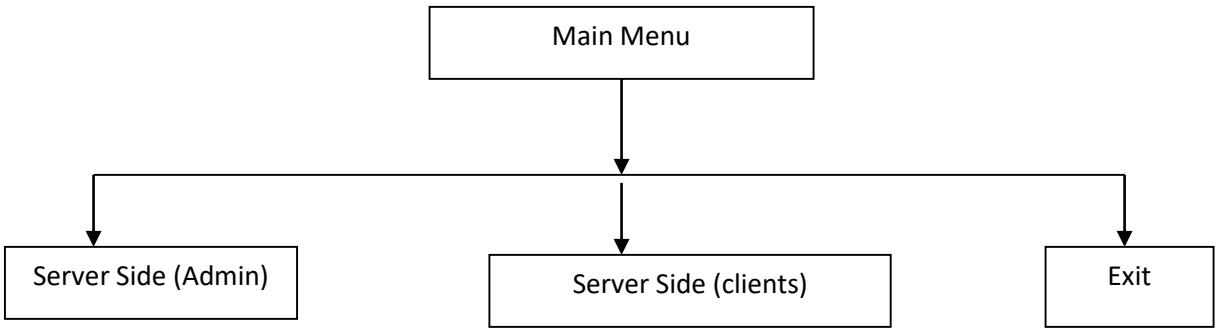

Fig 5: The Main menu

The Submenus/Subsystems

The support system developed in this project has some sub systems that makes up the proposed system. The sections below present the sub systems as contained in the new system.

` **Admin Sub System**

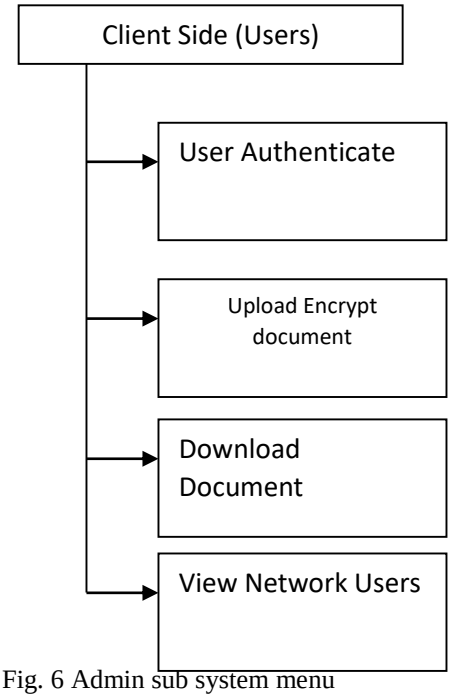

Fig. 6 Admin sub system menu

Users Sub System

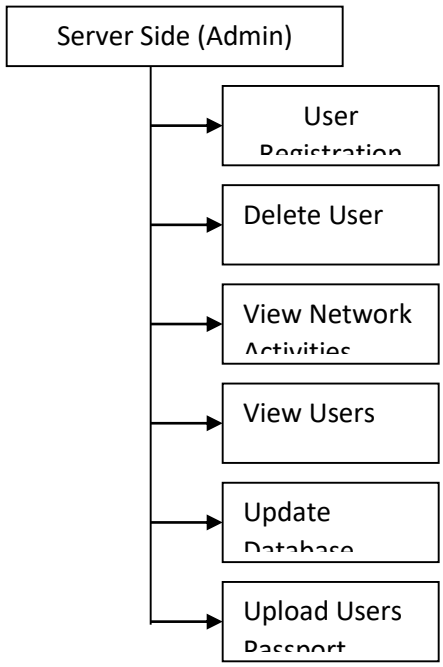

Fig 7 Users sub system menu

Figure 6 represents the admin sub system and is accessible to system administrators. Figure 7 represents the user's module. They use this module to send and receive packets.

Admin can use the module to register users on the platform for the purpose of obtaining password for login into the support system. It basically contains the administrative setup functions of the system networks and users on the network. The admin can also monitor the network log information.

Math Specification

AES algorithm is based on AES key expansion to encrypt and decrypt data. It is another most important steps in AES structure. Each round has a new key. The key expansion routine creates round keys word by word, where a word is an array of four bytes. The routine creates 4x (Nr+1) words. Where Nr is the number of rounds. The process is as follows: The cipher key (initial key) is used to create the first four words. The size of key consists of 16 bytes (k0 to k15) that represents in an array. The first four bytes (k0 to k3) represents as w0, the next four bytes (k4 to k7) in first column represents as w1, and so on.

Program Module Specification

Below are some of the modules designed and their specifications.

Login Module

The Login module presents users with a form with username and password fields. If the user enters a valid username/password combination they will be granted access to the network otherwise access will be denied the user.

Password creation Module

The administrators use this form to create name, address, phone, email, user name and password with access level.

OTP Module

A one-time password is generated and sent automatically to the user's phone. The user is expected to enter the one-time password for further authentication. If the validation was successful, the system will launch the user to the cloud platform having completed all authentication modules.

SMS Module

This module is used to send OTP to user's phone.

Network Log Module

This module is used to display the activities on a network. All the alerts triggered by the attack detection system are registered on the log.

Packet: This module is used by network users to transmit packets from the source to the designation.

Input / Output Format Specification

The input / output implementation in the new system are structured to allow users to fill forms and submit the data to the database. Below are some of the inputs / output forms.

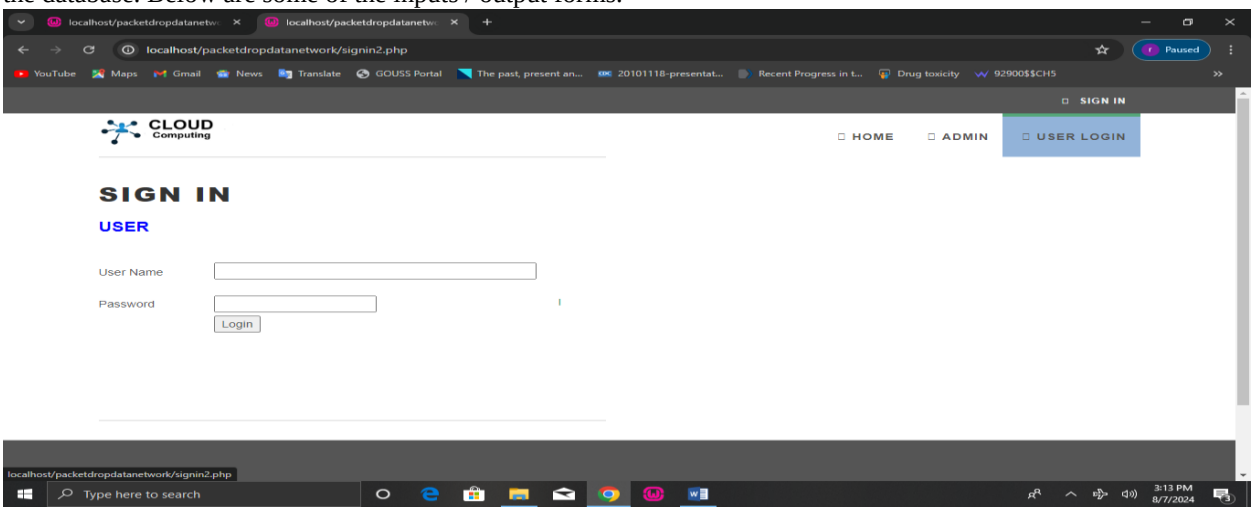

Fig. 8 User Login form, this shows the user login form which is the first authentication. The user provides the user's name and password to access the cloud computing platform. Once the user identity is established to be correct the second authentication form displays as shown in figure 10.

Title: Mitigation of Packet Drop in Wireless Network Using Hybrid Authentication
Authors: Agbo Esther U[1] Alumona Theophiliphus[2] Alagbu Ekene[3] Onyeyili Toochukwu[4]

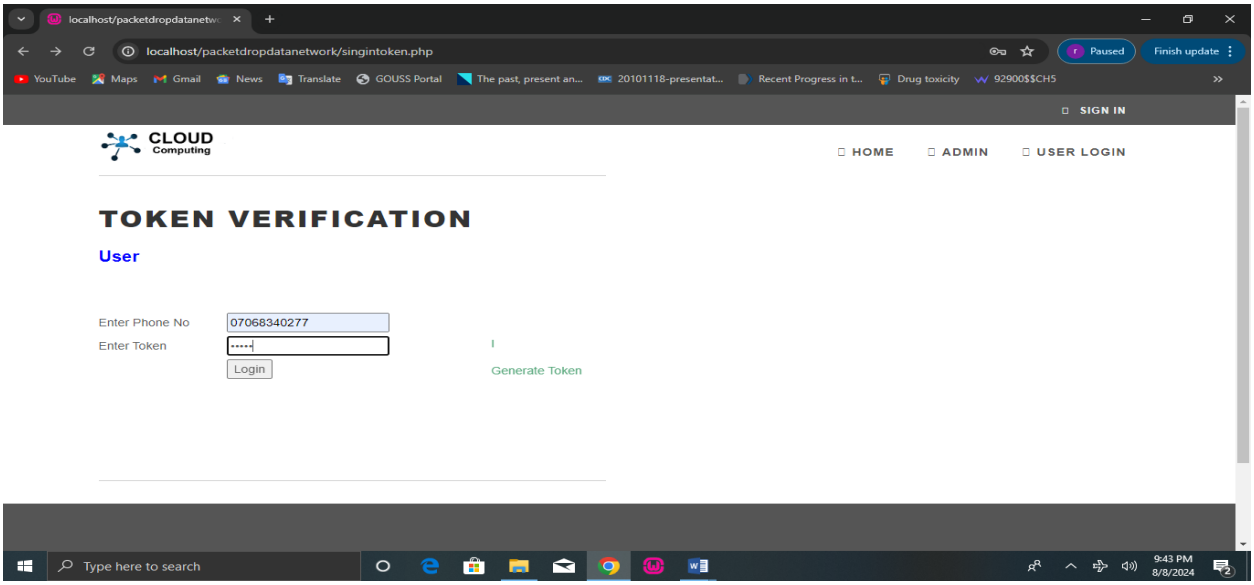

Fig. 9: OTP verification form for Cloud Users – second authentication. A one-time password is generated and sent automatically to the user's phone. The user is expected to enter the one-time password for further authentication. If the validation was successful, the system will launch the user to the cloud platform having completed all authentication modules.

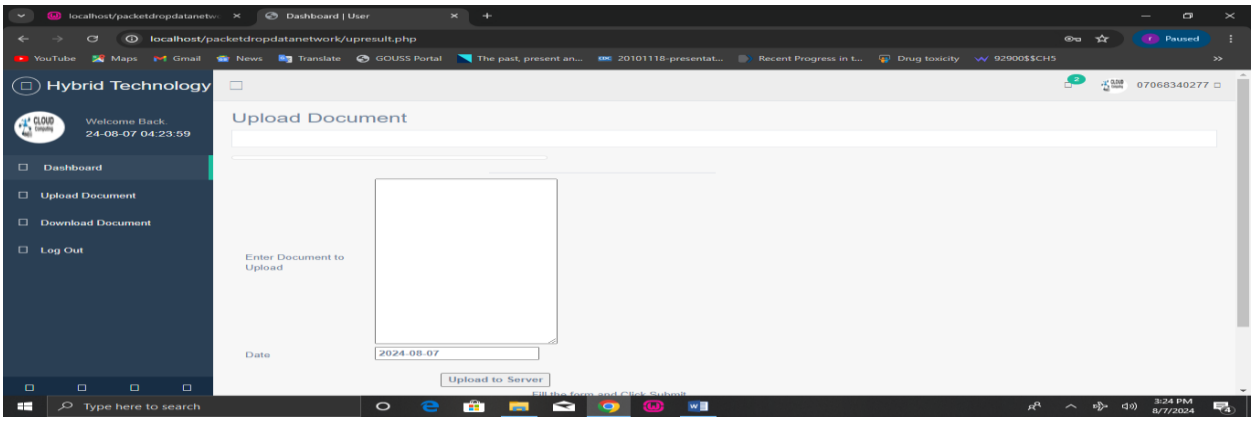

Fig. 10: Document Upload Form. allows the user to upload documents to the server in the cloud. The document is encrypted using the AES algorithm.

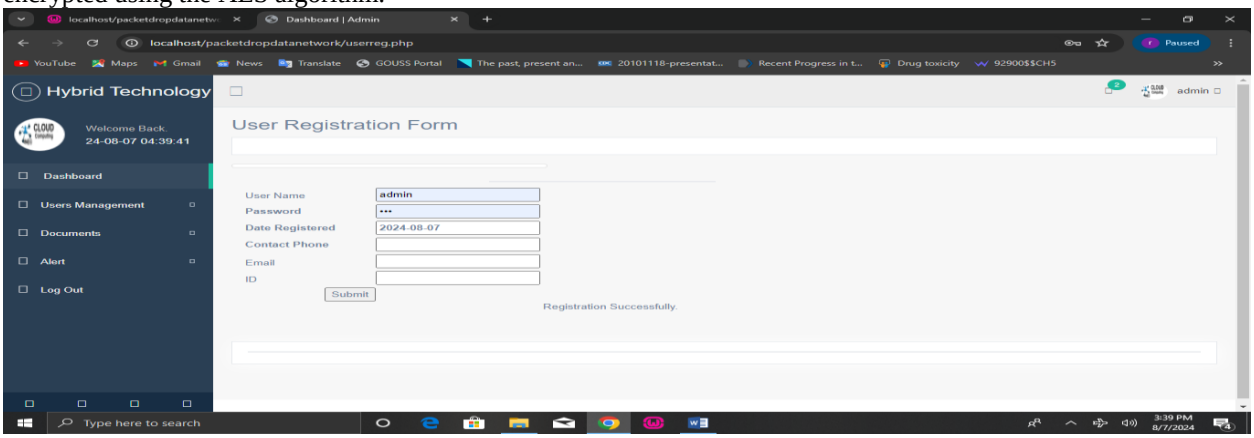

Fig 11: User Registration Form. This sub system is implemented to capture network user's data. The capture includes the personal details, passport, etc.

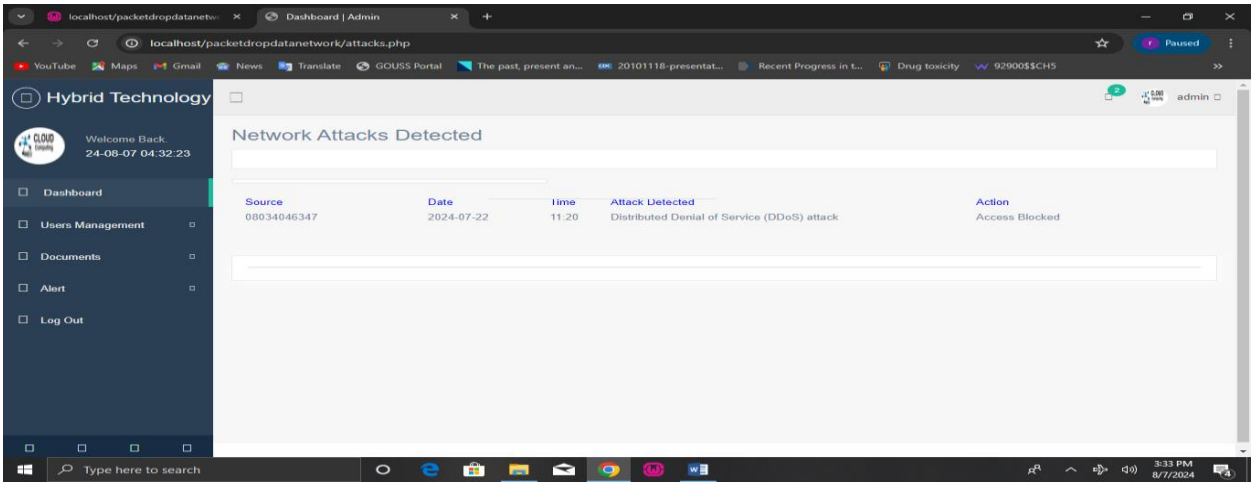

Fig. 12: Service attack report, shows the attacks detected on the network.

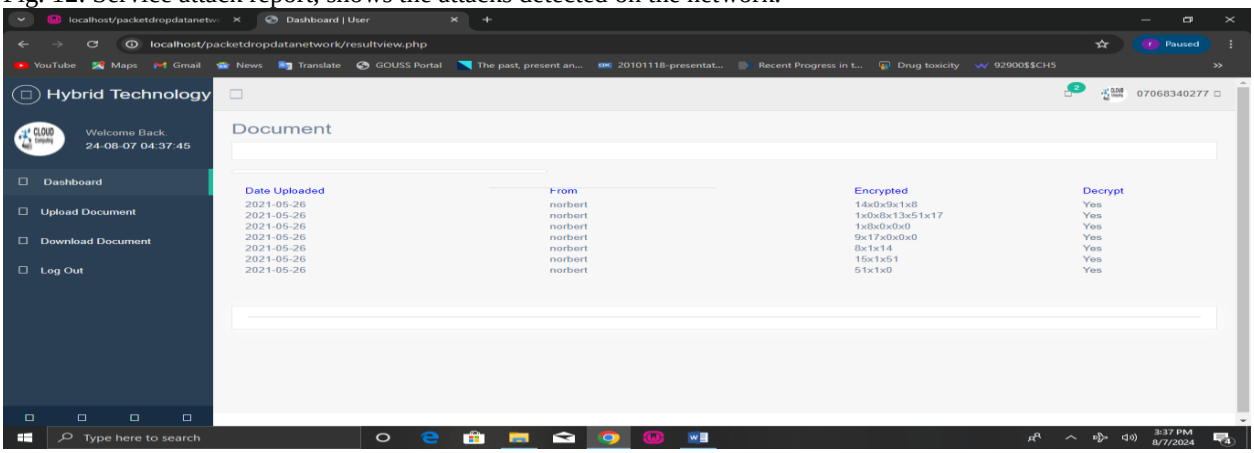

Fig. 13: Data encryption Report, shows data encrypted using AES algorithm. The result column is encoded before transmission on the cloud environment.

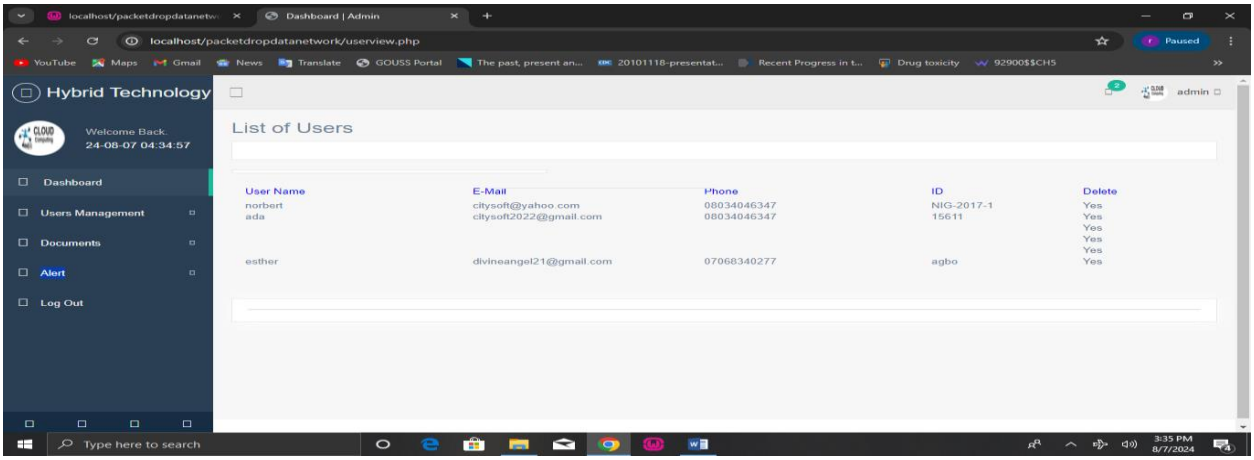

Fig 14: Network Users Report, shows the list of registered network users in the system. The administrator has the access to this report and can delete any of the users from this interface.

Algorithm / Pseudocode

If the packets are considered to be suspicious, the verifier node verifies the packets using various models and finally, the suspicious packets are added to the suspicious list which is moved to blacklist later and the legitimate requests are forwarded to the cloud. The cloud server sends the requested service to the user.

System Flowchart

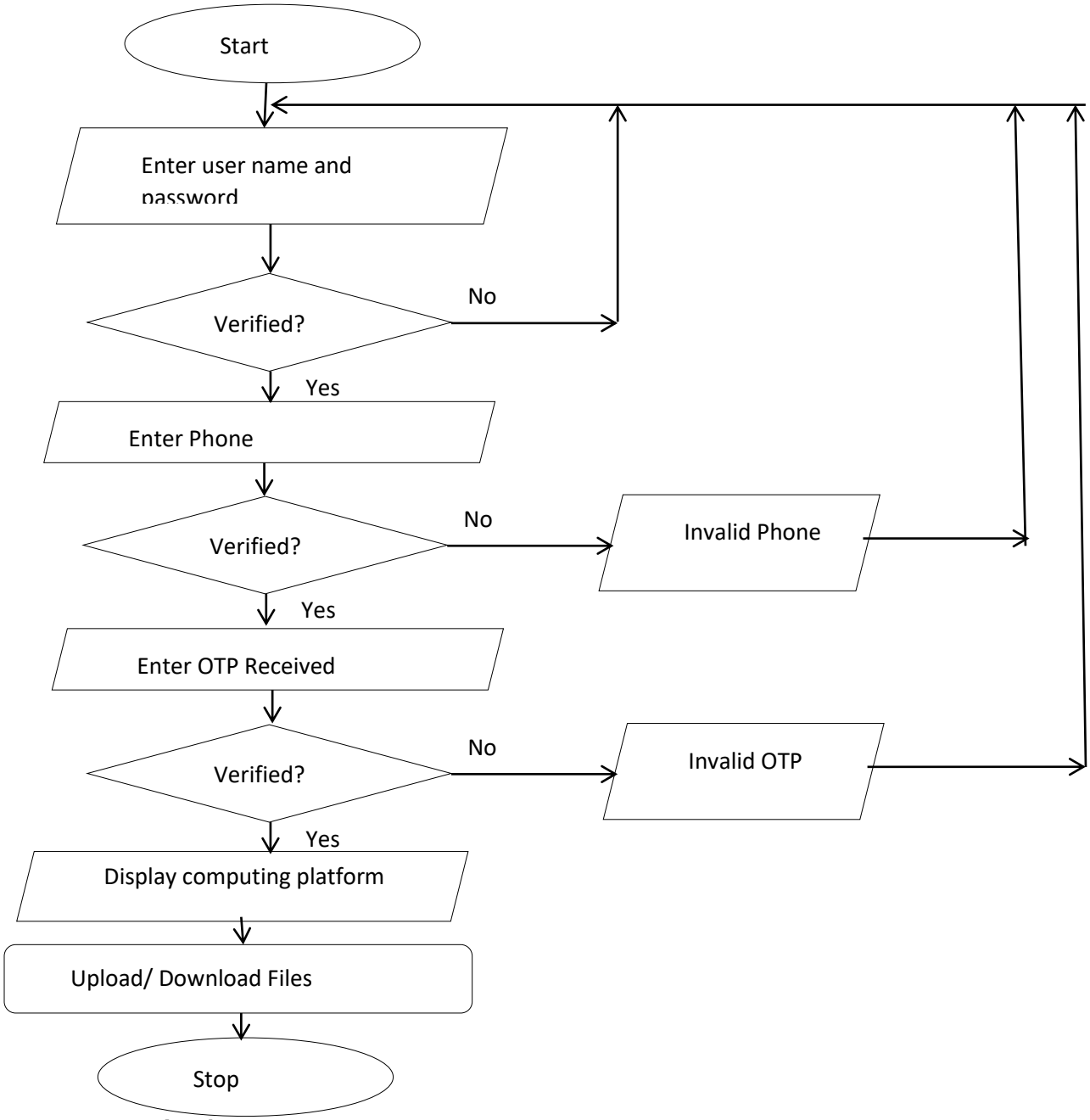

Fig. 15: System Flowchart

As shown in figure 16, if the username and password provided by the user to the network server is correct, then the cloud server sends the reply of validation at the user side and sends OTP to the user's phone for verification. Once the user enters the OTP, the application program gets this validation reply at the user side and launches the application environment.

Result Evaluation and Discussion

Test Plan

The new system will be tested in three stages; Unit Testing, Integrated testing and System Testing. This is to find out if there is still burgs in the program developed.

Unit/Module Testing: Unit/Module testing is the testing of the individual unit or group of related units. It is often done to test that the unit is producing expected output against given input. This method shall ensure and confirm the efficiency and reliability of the system. So far, the various units/modules have been tested and each has proved efficient as an entity.

Integration Testing: Integration testing is the testing in which a group of components are combined to produce output and the interaction between software and hardware is also tested. The essence of this integrations is to check how these modules when they are integrated into subsystem stand as main system. Therefore, the test carried out here is to ascertain that those modules do not lose their efficiency and reliability (which has been proved in the module testing above) due to the integration into subsystem and system. The coordination and linking relationship existing between the form and procedure retained and performed the primary function for which they were designed.

System Testing: System testing is the testing to ensure that by putting the software in different environments (e.g., Operating Systems) it still works. System testing is done with full system implementation and environment. In this system testing, test has been done in both windows 7, 8 & 10 operating system and it still function effectively.

Performance Evaluation

The importance measure of each feature is evaluated based on the two parameters of accuracy and false positive rate. More specifically, the classification algorithm is executed with and without each feature. This study uses some assessment metrics such as accuracy, detection rate, and false alarm rate as evaluation parameters, which are computed based on the confusion matrix.

Table 1: Confusion Matrix

		Actual Class (Observation)	
		Anomaly	**Normal**
Predicted Class (Expectation)	**Anomaly**	True Positive (Correctly classified as Anomaly)	False Positive (Incorrect classified as Anomaly)
	Normal	False Negative (Incorrectly classified as Normal)	True Negative (Correctly classified as Normal)

TP: The number of correctly detected network attacks
TN: The number of harmless applications correctly recognized as harmless
FP: The number of harmless applications falsely recognized as attacks
FN: The number of attacks falsely recognized as normal.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \text{ x } 100\% \qquad 4.1$$

$$Detection\ Rate = \frac{TP}{TP + FP} \text{ x } 100\% \qquad 4.2$$

$$False\ Alarm = \frac{FP}{FP + TN} \text{ x } 100\% \qquad 4.3$$

Table 2**:** Network attacks detection using hybrid authentication

True Positive (TP)	2304
False Positive (FP)	52293
False negative (FN)	0
True negative (FN)	587033
Total No of cluster	641630

Detection rate = 2304 /2304+52293 =0.0422*100 =4.22%
False alarm rate= 52293 /52293+587033 =0.082* 100 =8.2%
The lower the detection rate and the false alarm rate, the higher the accuracy of the system.
Accuracy = (2304 + 587033) / 641630 = 0.9185
The accuracy of the network attacks detection using hybrid authentication is 92%

Conclusion

Wireless network faces a lot of security concerns which centers on the packet drops, privacy and validity of their data. This calls for more secured authentication system for wireless networks so as to mitigate the packet drop on the network. In this research work, multi-level authentication scheme was introduced. For getting the access of the requested service, the attacker has to break all the authentication layers. At the first tier, the username and password of the user is verified. At the second tier, OTP is sent to the user's phone number and the user is expected to enter the OTP for final identification

References

Achu Anna Anthony and Bino Thomas (2019). *A study on packet loss reduction methods and node registration methods in AODV for MANET*. IOP Conf. Series: Materials Science and Engineering 396 (2019) 012032 doi:10.1088/1757-899X/396/1/012032.

IR Team (2022) retrieved from info@ir.com.

Global threat landscape report 2H (2023) retrieved from https://www.fortinet.com.

Ruchir Bhatnagar and Vineet Kumar Birla, (2019). *A literature review of security in wireless network.* : International Journal of Research in Engineering & Technology (IMPACT: IJRET).

Preeti Sinha, Vijay Kumar Jha, B. Bhushan, (2020) *Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model* Published in IEEE Conference on Systems Computer Science, Engineering, Environmental 2020.

Ahmed Najah Kadim, Sattar B. Sadkhan (2021) *Security threats in wireless network communication status, challenges and future trends* published in 202 international conference on advanced computer application ACA

Amrita Ghosal and Linda Bushnell, (2021) *Truck platoon security: State-of-the-art and road ahead* published in journal of Computer Networks, 2021.

Chirag Modi, and Muttukrishnan Rajarajan, (2023). *A survey of intrusion detection techniques in Cloud* published in Journal of Network and Computer Applications, 2023.

Global threat landscape report, 2023. *What Is A Keylogger? Definition and Types* retrieved from https://www.fortinet.com.

P.S Seemma, S.Nandhini and M. Sowmiya,, 2019. *Overview of cyber security*. Published in international journal of advanced research in computer and communication engineering vol 7,issue 11.

Tim Callan, 2020. *SSH keys generation, authentication, key pair info and more* published in blog post online library.

Ume L.E and Ibebuogu C.C, 2019. *The relevance of firewall technology in combating internet insecurity* published by international journal of basic applied and innovative research.

Eric Conrad and Joshua Feldman, 2019. *Authentication systems* published in eleventh hour.

Rajeev Kumar and Alka Agrawal, 2024. *Using blockchain to secure biometric healthcare apps* published by Biometric technology today online library.

Dongzhi Xu and Wenjuan Zheng, 2022. *Application of data encryption technology in network information security sharing* published in security and communication networks.

Veeraiah Akunta, 2021. "*Trust Aware Secure Energy Efficient Hybrid Protocol for MANET"* Published in international journal of Scientific and Engineering research.

Aniekwe V. N., Ufoaroh S.U., and Alumona T.L ,2021. *Improving Data Transmission Security in a Wireless Network Using Digital Signature*. International Journal of Scientific & Engineering Research Volume 12, Issue 7, 283 ISSN 2229-5518.

U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf and B. V. Subbayamma, 2021. *"An Improved Hybrid Secure Multipath Routing Protocol for MANET,"* in IEEE Access, vol. 9, pp. 163043-163053, doi: 10.1109/ACCESS.2021.3133882.

P. Zhao, Y. Huang, J. Gao, L. Xing, H. Wu and H. Ma, 2022.*Federated Learning-Based Collaborative Authentication Protocol for Shared Data in Social IoV*, in IEEE Sensors Journal, vol. 22, no. 7, pp. 7385-7398, 1 April1, 2022,doi: 10.1109/JSEN.2022.3153338.