DYNAMIC KEY GENERATION AND DISTRIBUTION COMPARISON USING MACHINE LEARNING INTEGRATED NODE AUTHENTICATION ROUTING PROTOCOL FOR IMPROVING QOS IN VANET

Parveen Akhther A[1*], A Mary Posonia[2], Prasanth V S[3]

[1,2]Sathyabama Institute of Science & Technology, Sathyabama University, Chennai.
[3]Madanapalle Institute of Technology & Science

Emails: parveena77@gmail.com[1*], maryposonia.cse@sathyabama.ac.in [2], prasanthvydya@gmail.com[3]

ABSTRACT

VANET, or Vehicular Adhoc Network, is widely used in mobile networks that use self-driving, navigation, entertainment, and other emergency applications. It is commonly adopted in the transport system to facilitate communication between the vehicles and crucial points. It is used to control traffic, improve routing efficiency, and better functioning of the transportation systems and controls. It enables communication between the mobile nodes through several base stations. The effectiveness of the VANET is improved through Artificial intelligence techniques. With the wide adoption of VANET networks for better communication, the network is subjected to various security vulnerabilities. This paper proposes a key generation distribution and comparison-based user authentication routing protocol to improve the security of the VANET. The communication metrics of the networks are monitored, and the data obtained are processed through the RNN algorithm. The nodes are authenticated using bilinear mapping, which involves registration, authentication, and verification. The nodes are identified during registration, a private key is assigned for temporary authentication, and the nodes are verified. NS3 is used to simulate the proposed model, where it obtained throughput, PDR, energy efficiency, and packet loss of 99.8, 99.3, 99, and 0.02%, respectively.

Keywords: Machine Learning, VANET, Key Distribution, Authentication, Routing Protocol.

1.0 INTRODUCTION

Security is a crucial impact that must be immediately focused on in various networking applications since data transmission occurs daily. Different malicious activities can easily affect all wireless sensor network applications because they follow multi-path, multi-hop, and multi-channel data transmission. One of our real-time applications used everywhere globally is Vehicular-Adhoc-Network. It is a type of MANET explicitly designed for vehicular communications. The nodes in the VANETs are vehicles that create a network and communicate among cars on the road and roadside units. The main goal of VANETs is to enhance road safety and provide a better driving experience through communication and vehicle coordination. VANETs address several challenges in transportation and vehicular systems, as given in Table-1.

Table. 1: Challenges in The VANET Transportation System

Challenges	**Description**
Road Safety	VANETs can provide current road, traffic, and accident conditions to help drivers make informed decisions and avoid dangerous situations.
Improved Traffic Management	VANETs can help reduce traffic congestion and improve traffic management efficiency by providing real-time information about road conditions and traffic flow.
Driver Assistance	VANETs provide accurate information about the road to make safe driving easier and safer.
Emergency Services	VANETs can provide emergency services with quick and accurate information about road conditions and the location of accidents, helping them respond more quickly and effectively.

Vehicle-to-Vehicle Communication	VANETs enable vehicle communication, allowing them to exchange information about road conditions, traffic flow, and other important information.

VANETs aim to improve road safety, enhance the driving experience, and support efficient and effective traffic management through communication and vehicle coordination. VANETs are vulnerable to malicious activities compromising security and privacy like any other communication network. Some of the main malicious activities in VANETs include:

- Sybil Attack: The attacker creates different false identities to gain control over a large portion of the network and manipulate information being exchanged.
- Privacy Violation: VANETs collect and exchange sensitive information about vehicles and drivers, making it essential to protect their privacy. Privacy violations in VANETs can occur through unauthorized access to personal information, location tracking, and other means.
- Denial of Service Attack: In a DoS attack, an attacker intentionally disrupts the regular network operation, making it unavailable to legitimate users.
- Routing Attack: In a routing attack, an attacker manipulates the routing information in the network to redirect traffic, eavesdrop on communication, or disrupt the regular functionalities of the network.
- Spoofing Attack: In a spoofing attack, an attacker creates false messages and sends them to the network, spreading incorrect information or disrupting its regular operation. To understand how a malicious node is created in VANET, it is illustrated in Figure-1. It shows a real-time sample vehicle Ad-hoc network scenario with malicious nodes presented. It is assumed that all the nodes and the network elements are individual sensors that can communicate with one another. It also communicates and transmits data using a multi-hop -multi-routing model.

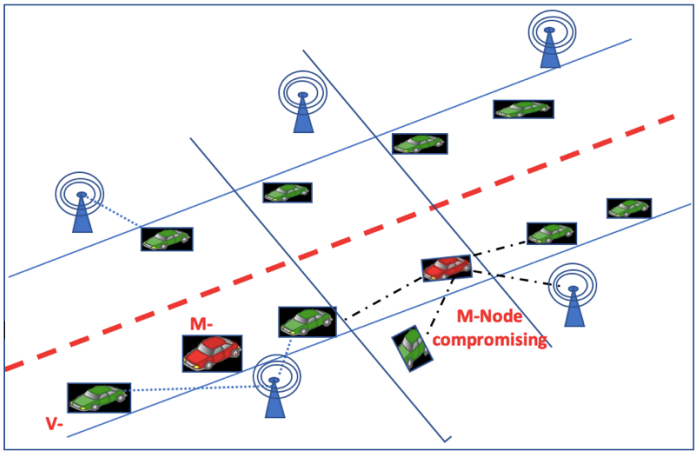

Fig. 1: VANET with Normal and Malicious Nodes

The transport network comprises roads with crossings, roadside units, normal nodes, and malicious nodes. It also has several elements and various kinds of nodes based on the user's requirement. Each node in the road communicates with the other nodes and the RSU, where the RSU can communicate with the base station or the server. VANETs are vulnerable to malicious activities compromising security and privacy like any other communication network. VANETs should implement appropriate security measures to mitigate these threats, such as secure communication protocols, privacy-preserving techniques, and efficient security mechanisms to detect and prevent malicious activities. One of the significant security methods for investigating each node in the network is the Secret Key Sharing Model for VANET, which provides node-level security. Secret key sharing is an essential aspect of ensuring security in VANETs. It refers to distributing secret keys among vehicles and roadside units in the network. Secret keys, such as encryption, message decryption, and authentication, are used for secure communication. There are several methods for secret key sharing in VANETs, including:

- **Key pre-distribution:** In this method, each vehicle or roadside unit is pre-loaded with secret keys, which can be used to establish secure communication with other vehicles and roadside units.

- **Key distribution center (KDC):** A central trusted entity, called a KDC, distributes secret keys to vehicles and roadside units in the network.
- **Public key Infrastructure (PKI):** This method uses cryptography to establish secure communication and distribute secret keys among vehicles and roadside units.
- **Group key management:** This method is used when a group of vehicles or roadside units needs to establish secure communication. In this method, a secret key is shared among the group members and can be used for secure transmission. Finally, secret key sharing is essential to ensuring security in VANETs and should be implemented using appropriate methods and techniques to ensure efficient and secure communication. Regardless of the method used, secret key sharing in VANETs should be efficient, secure, and scalable to accommodate the network's large number of vehicles and roadside units.

The other way to secure the data in VANET is to implement a secured routing protocol. The routing protocol investigates the nodes' location, dynamic behavior, and routing information to provide better security for data transmission in VANET. The public and private keys of the dynamic users are verified to authenticate trustable users and avoid malicious activities. Several earlier methods have focused on key distribution, assignment, and management. This paper contributes a set of tasks to tighten the security level of the VANET applications.

1.1 Contribution of the Paper

The paper aims to design and implement a novel authentication-based routing protocol using a machine-learning algorithm to increase the overall QoS of the VANET. Thus, this paper contributes,

- An application-based vehicular network model is created with a defined number of nodes.
- Dynamic key generation, distribution, management, and comparison model is implemented to examine the nodes and increase trust for secure authentication.
- One popular advanced machine learning algorithm, Recurrent Neural Network, is implemented to verify the entire routing-table data with key comparison to identify and eliminate malicious activities.
- The pair of key verifications is applied for all the nodes' privacy preservation and secured message transmission. One of the central managers and RS can investigate the nodes' data to obtain the normal and abnormal nodes in the network.

2.0 LITERATURE REVIEW

This section reviews various existing protocols and techniques to prove the efficiency of the proposed authenticated protocol for data transmission. The performances of the proposed and existing systems are analyzed through various metric values. The author A. Ahmad et al. (2015) [1] proposed a secured data transmission technique to improve the throughput and security and to reduce the delay time of the transmission between the nodes. At first, the group region in the network is determined from the various sensor nodes. After analyzing the group region, the master head is selected. Then, using the agent node concepts, the swapping technique is established. The final result of the model shows that it increases the throughput value and decreases the delay time during the data transmission with high security. D. Yang et al. (2015) [2] presented a review to define various electromagnetic coupling techniques, wireless ultrasonic data transmission methods, ultrasonic through-metal-wall system features, and challenges and issues in various electromagnetic systems are discussed in detail. Finally, the review concluded by suggesting that the electromagnetic coupling method is more suitable for data transmission. R. Bhandari and V.B. Kirubanand (2019) [3] proposed an enhanced cryptography technique; that is, the new model is designed by combining the features of the public key server and symmetric and asymmetric algorithms. A unique address and key are generated using the Elliptic curve equation. The final result of the model defines that the proposed mechanism securely transfers the data without any interruption. S. Oh et al. (2016) [4] developed a new data transmission scheme for the narrow band-based IoT system. The main purpose of the scheme is to handle the radio resource issues in the NB-IoT system.

The result of the proposed scheme shows that compared to other conventional methods, the proposed model effectively handles the devices in the network with more than 60% efficiency. J.F. Dynes (2016) [5] discussed the efficiency of the quantum key distribution (QKD) to establish a secure path in the optical fiber network. The proposed QKD technique is more suitable for combining with 10 Tb/s data. The simulation result of the model indicates that the proposed QKD is more feasible to combine with other quantum technology to establish a secured data transmission in the optical fiber network. P. Mohanty and M.R. Kabat (2016) [6] proposed effective data transmission techniques to avoid issues in sending patients' health reports to their respective physicians. Due to

less security, data loss and malware attacks may occur. The result of the proposed model is evaluated through various simulations. The result illustrated that the proposed model performs better than the existing model and provides a secure path for data transmission in healthcare sectors.

A.A. Yazdeen et al. (2021) [7] Proposed an Advanced Encryption Standard (AES) and Data Encryption Standard (DES) technique for secured data transmission. When compared to another model, the FPGA-based techniques provide better results. C, J, Ezeofor, and A.G. Ulasi (2014) [8] conducted research work to define various algorithms to perform data encryption and decryption processes for secured data transmission. The model's visualization result indicates that, compared to other methods, the DES algorithm is more efficient in establishing the secured data transmission path between the nodes. N. Manohar and P.V. Kumar (2020) [9] discussed various secure steganography methods such as LSB, neural networks, and fuzzy logic. The research results indicate that, compared to other traditional methods, the methods discussed in this work have achieved high accuracy results and transmitted the data with high security. E.Y. Baagyere et al.(2020) [10] developed a genetic algorithm (GA) based on a new method is implemented. It is a combination of cryptographic and steganographic techniques. The model's efficiency is analyzed through the PSNR and MSE values. The result is evaluated by experimenting with it using MATLAB software. The model's result showed that compared with other methods, this model reduces the delay time and improves efficiency. A.V. Mota et al. (2017) [11] presented a study to define the efficient data encryption technique. Various encryption algorithms such as AES, DES, 3DES, and blowfish are analyzed for this. These blowfish algorithms efficiently encrypted the data. Further, various asymmetric algorithms like RSA, Elgamal, and ECC are compared to project the best one. The result shows that the ECC algorithm provides better results than other algorithms. Then, various hash functions are compared; the result defines that SHA256 is the best.

A.A. Ahmed et al. (2020) [12] discussed the dynamic reciprocal authentication to secure data transactions in mobile cloud computing. The proposed model utilized different authentication factors, such as OTP, username, and password, to establish a secure platform. The efficiency of the proposed model is tested using the JAVA. The simulation result shows that the proposed model produces a more secure protocol with computational time and cost compared to existing methods. A.A. Ostad-Sharif (2019) [13] introduced a secured data transmission protocol with lightweight and key agreement protocols. The proposed model provides automatic validation security protocol and application tools. The proposed model has high security and performance compared to the existing model. D. Mishtra et al. (2018) [14] proposed an efficient authentication protocol for secure data communication in IoT-based WSN systems. It is more efficient in creating the secured platform for the IoT-WSN system. V.O. Nyangaresi et al. (2021) [15] proposed a mutual authentication protocol for secure data transactions in the VANET system. The simulation result of this model illustrated that this mode is more secure and efficient for data sharing in the VANET system.

Some of the recent research work has focused on secured authentication for vehicular ad-hoc networks. Different security algorithms, like the Diffie-hellman ephemeral algorithm, are proposed utilizing an elliptic curve, which provides a space for sharing the key between the nodes. It was implemented in a fog gateway sharing the key between the nodes present in the network. The network also used various IoT devices to improve the model's security. Different types of neural networks like CNN, Graph-CNN, and RNN algorithms were used to enhance the security of the model. The networks are fine-tuned using hyperparameters selected through the Branch-and-Bound method. Cryptography was also used to generate security keys and authenticate network users. It provided better efficiency and reduced communication costs, with better security. The EBAKE-SE model provided a trustworthy network with a highly reliable and efficient model for the prediction process and inter-device authentication. The security of the model was improved with the MQTT protocol. [16] [17]

The data security plays an important role in evaluating the model's reliability. Instead of depending on a single owner, multi-owner authentication can significantly improve the model's performance. The Merkle hash tree method was used to check the data's integrity to improve the model's cloud storage security. The Merkle hash tree consists of the details of the client and the parent nodes. TPA public key is used to authenticate the request for encrypting the data. Once the user is authorized, the decryption key is given to the user. Biometric-based security schemes using the RUA scheme are also adopted in a multi-server environment. The authentication performance of the RUA is compared with Chen, where the RUA provides better security. It is also adopted in other methods like random oracle. Blockchain models are also used to improve the data security in the VANET networks. It uses distributed ledger technology to protect the network. Some protocols focused on mobile communication between the nodes called the Internet of Vehicles are proposed. [18] These models adopt the CNN algorithm along with Blockchain for improved security and performance efficiency during data transmission.

2.1 Limitation and Motivation

Rapid urbanization and industrialization have increased the usage of vehicles worldwide, with more cars and bikes on the road. In order to reduce and streamline the data flow of vehicles on the road, it is essential to deploy a systematic process. Each vehicle on the roads was considered as nodes, and these nodes are connected within a network. It is controlled from the network, and the controls are passed on to them. However, in most networks, the nodes are static, which makes it easy for the network to communicate with the other nodes. But, to control mobile nodes in the case of moving cars and bikes, a flexible network providing a better connection to mobile nodes needs to be considered. VANET is one such network, also known as the Vehicular ad Hoc Network, that connects mobile nodes and vehicles. Various research works are being done to intelligently control the flow of vehicles through the roads. These researchers considered ML and DL models for their optimization. Though the VANET provides better optimization, it faces various security issues while scaling for larger applications. In order to overcome this, various security measures are proposed, and different architectures are considered for secured communication between the nodes. Though there are different kinds of networks, they can be classified into two types: centralized and distributed. The centralized network consists of a single control, while the distributed consists of distributed control over the nodes. The distributed network is the most preferred among them as it is cheap and scalable for bigger networks. Though they are scalable, they are vulnerable to various attacks easily as it has multiple controls in a single network. Hence, a security mechanism must proposed to overcome the issues faced in a distributed network through the various encoding and decoding schemes and other security enhancements.

3.0 EXISTING APPROACH

The existing FDMS model collects information about the nodes from the VANET network. It uses different classification algorithms and routing protocols to control the network dynamically. These algorithms optimize the energy usage of the network but fail to provide the necessary security. Most of these networks follow a multi-hop communication model, with more intermediate nodes, and the algorithm clusters these nodes, and the optimal routing path is found. This network functions in an IoT-based VANET environment. These networks may show more security issues while scaling to larger networks, even while providing better quality of service.

3.1 Preliminaries

The elliptic function **E(**F_p represents all the points on an elliptic curve expressed as $y^2 = x^3 + ax + pmodp, \forall a, b \in F_p$, where p is the large-prime number. **E(**F_p includes all the points with $\odot$ an infinite point from G_1, its generator P order of q. The security analytics involved two random-hash functions $R_1$and R_2, where,

$$R_1: \{0,1\} \rightarrow G_1$$
$$R_2: \{0,1\} \rightarrow Z_q$$

Considering $G_1$is a multiplicative group, then it is defined by mapping, as

$$e: G_1 \times G_1 \rightarrow G_2$$

Since e is a bi-linear mapping model, then it should satisfy the following:

- Bilinearity: $e(aP, bP) = e(P, P)^{ab} \forall a, b \in Z_q$
- Non-Degeneracy:$\exists P \in G_1 \ni e(P, P) \neq 1$
- Computability: The computation of $e(P, Q)$is efficient$\forall P, Q \in G_1$

3.2 Security Analysis

In this paper, the security provision is proved by assuming two random numbers as $R_1$and R_2, and adversary **A1** attempted to forge the data in the environment.

Lemma-1: Let us assume if the A forging the authentication signature of a genuine node within interval t by the probability $\varepsilon > 10_{qR1}(q_S + 1)\left(q_{R_2} + q_S\right)/q$, then queries raised to R_1, R_2, extract, and send, denoted as $qR1$, q_{R_2}, q_{R_2}, and q_S, respectively. This CDH problem in Group-1 with all the nodes is solved using a solution **S** within the time $110286 \cdot q_{R_1} \frac{t}{\varepsilon}$

4.0 PROPOSED MODEL

In this paper, a secured, authenticated protocol is developed to securely and efficiently transfer the data between the nodes. In this proposed approach, an authorization server is implemented to manage the path between the nodes effectively. Data transmitting through the trusted authorization server protects the data with high security and improves the computing speed and authentication process. The following sections elaborately explain the proposed authenticated protocol's step-by-step process. The overall architecture is constructed based on four different components: service provider, server provider (SP), server manager (SM), sensor units (SU), and object detector (OD). The service provider's main function (SP) is to manage the entire network based on pre-defined rules. In addition to this, the major responsibility of the SP is to handle the SU and SM. As mentioned above, SU and SM are also components of the VANET model, where SU collects data from various sensing units fixed in different locations. It is the major component for transferring messages within the network. The SM is utilized to manage the requests received from the authorized and unauthorized nodes within the network region. The object unit is fixed within the nodes to establish tamper-proof communication between the devices in the network. The general steps to create an authenticated protocol are key generation, node registration, signature verification, and transmission.

4.1 Key Generation

Initially, the SP allocates SM on various locations based on the system server configuration. The SM generates various Token T values for the various entities in the network. Then, using the elliptic curve algorithm (ECA), the public P_b and private P_r key and unique authentication ID is generated. Using the following equation 1, the ECA is performed.

$$X^2 = a^3 + ba + ymodm \quad \textbf{(1)}$$

The equation -1 is performed using the parameters such as (m, n, a, b, y, G, q). Where m and n are the two large prime numbers, b and y indicate the coefficient value of the elliptic curve; using this parameter, a unique ID is randomly generated to the SU and deployed into various locations to gather the data. Then, the SP shards the P_r and ID value of the SU to get a T value.

4.2 Node Registration

Before transferring the data, the SP has to verify the requested node based on the node identity (N_{ID} and generated unique SU identity (SID) to the node ($(N|SID)$. Now the SP rregisters all the details received from the node in the serve DB. Along with this public key value of the node is open paren cap N vertical bar cap P sub b , close paren also stored intohe DB. Then suing the TLS protocol the details of the node is shared to the SM to register the node details. Further the SP ordered the SM to continue the registration process, then the SM send message ms_1 =n‖ $a \parallel b \parallel y \parallel g \parallel qh_1(N|ID)$to the SU to find the authorized nodes in the network. It is performed using the elliptic curve parameters. Here, the requested node randomly selected the private keyN_{P_r}. Once the node private key N_{P_r}value is generated again the SU generated the specific public key value to the node N_{P_b} and message $ms_2 = (N|P_b \parallel N_{ID})$ is send to the SM to extract the constant public key value. It is generated based on the identities provide by the requested node in the network. Now the SM can easily extracted the N_{P_b} from thems_2. Then the SM verified the authenticated key value of the node and stored in to the DB. Then again message $ms_3 = N_{TID}h_1(N|ID)$is send to the SU to generate the node token ID or key value (N_{TID}. After generating the token value from ms_3, the SU registered the node token ID to the main server database. Before entering into the data transmission process, every node has to share their registered node identity (N_{ID}) to the SM to store in the database DB. At the every time of data transmission the SP has verified the $N_{P_r}$and N_{ID} with the registered details by sending the signature (S) to the SP to perform the further tasks. It is performed based on the following equations.

$$S_0 = H_1(N_{ID}) \quad \textbf{(2)}$$

$$S_1 = (\upsilon + S_0)N_{P_r} \quad \textbf{(3)}$$

$$S_2 = \upsilon P_b \quad \textbf{(4)}$$

The signature S = $\{N_{ID}, S_0, S_1, S_2\}$received from the node is verified with the registered values. If the requested S is valid one, then the equation (5) and (6) is computed.

$$e(S_1.p) = e(H_1(N_{ID}), S_0 + S_2.P_b) \quad \textbf{(5)}$$

$$e(S_1.p) = e \quad \textbf{(6)}$$

After computing the equation (5) and (6), the SP produces the Signature G = $\{G_0, G_1, G_2\}$ and again verified using the equation 5 and 6. After confirmed the request received from the nodes in the network. The SP encrypted the data received from the node-1.

4.3 Data Encryption

In this stage the SP verified the various details of the node and randomly generated the symmetric key (SK) value to encrypt the data transferred by the node-1 and transferred to the SU. It is performed using the following equation (8).

$$E_0 = sk.e(H_1(N_{ID})Pb)^r \quad (7)$$

$$E_1 = rp \quad (8)$$

4.4 Data Transmission

Now the encrypted data are transferred to the destination node in the network with high security. The node-2 verifies the details of the source node in terms of node ID, token address, private and public key. If all t hese entities are valid the node-2 (i,e., destination node) accepted the data send from the node-1 and the SU of the node-2 decoded the encrypted data (E_0, E_1 received from the SP using the sk values, which is illustrated in the following equation (9).

$$sk = \frac{E_0}{sk(N_{P_{r'}}, E_1)} \quad (9)$$

If any source node entity shows an error, the SU in the destination node rejected the data or request received from the node-1 and discards the data from the network region by sending the error message to the unauthenticated node.

4.5 Node Analysis With Rnn

Recurrent Neural Network (RNN) processes both static and dynamic data obtained from node and network. RNN helps in the reinforced learning that helps in optimizing the network and comparison of previous values from VANET. The nodes in the network can be graphically plotted using $G(V, E, X)$**,** were

$$V = \{V_1, V_2, \dots V_i, \dots, V_n\}, \forall i = 1n$$

the above equation represent the data collected from VANET nodes at different time frames,

$$TD = \{TD_1, TD_2, \dots TD_i, \dots, TD_m\}, \forall i = 1m$$

(V_i**)** is the unique network element, and G represent the graph in the VANET. An index Δ is used by the network element V.

$$\Delta = V \times V$$

V is authenticated through the weight function w and the respective output obtained is

$$w = \Delta \rightarrow \{0,1\}$$

A binary validation is carried out for the nodes. The RNN algorithm is a reinforcement learning based model that adopts three different gates: input, hidden and output. A feature of the RNN algorithm is that it is similar to LSTM; hence, a forget gate is introduced in the proposed model. The data is fed to the input layer which classifies the data and looks whether the data needs to be considered or not. Then, when the data is considered, it is passed to the hidden layer. The hidden layers can be increased based on the computational complexity of the model. With the increasing number of hidden layers, the accuracy of the model can be further improved. The hidden layer consists of a memory, that compares the values with the previous layers and adjusts its weights. The forget gate mentioned

before is similar to that. This helps in achieving the maximum accuracy possible. Finally, based on the number of outputs, the output neurons are fixed and the following prediction is made. The machine learning based authentication model proposed in the following paper can be classified into three types, they are routing route prediction, traffic evaluation and data organization, encryption and decryption. The stochasttic concepts are considered while routing the nodes through RNNRP. Some of the important criteria considered while routing are gathering data, feature extraction and RNN implementation. The turmoil logistic maps are used to better data transmission between the nodes. The architecture of the proposed model can be seen in Figure-1.

The H_{t-1} is used to process the data TD given to C_{t-1} in the RNN algorithm. After the data being processed, C_t and H_t is sent to the next layers. The forget gate stores the information if required, which can be seen in the following formula,

$$f_t = \sigma\left(X_t * U_f + H_{t-1} * W_f\right)$$

The current time-stamp is represented as X_t and the U_f the input weights. H_{t-1} represent the hidden state's previous time stamps and W_f its corresponding weight matrix. The sigmoid function is used to process the output, which gives binary output f_t. By multiplying f_t and the previous cell state obtained through previous time-stamps, the output is obtained, which is shown,

$$C_{t-1} * f_t = 0 \ldots if f_t = 0$$

$$C_{t-1} * f_t = 0 \ldots if f_t = 1$$

4.6 RNN For Node And Data Processing

By improving the accuracy of the prediction obtained from the RNN model, the traffic flow can be controlled better. It is improved by training the RNN with the training dataset, used in [19], and its architecture is shown in figure-3, and over very cycle k, the traffic data is $D(k)$, where the initial data is considered as $D(i)$, where , w$D1(i) = 1/n$here network model finds the smallest value of the RNN predictor, and the output altered accordingly is shown below,

$$T_k = \sum_{k=0}^{n}[0(G_k^0.O_k + G_k^0.e_{k-1} + s_k)] \quad (1)$$

A user-definite error function is used for estimating the boosting results,

$$e_k = (T_{actual} - T_k) \quad (2)$$

α_k is used to compute the network parameters, shown below:

$$\alpha_k = 0.5\{ln\,(1 - e_k)/e_k\} \quad (3)$$

In each iteration e_k and when the error value becomes zero, the outcome of the ensemble boosted model is calculated which is shown as,

$$Yk = \sum_{k=0}^{n} 1/\alpha k\{\alpha k.T_k\} \quad (4)$$

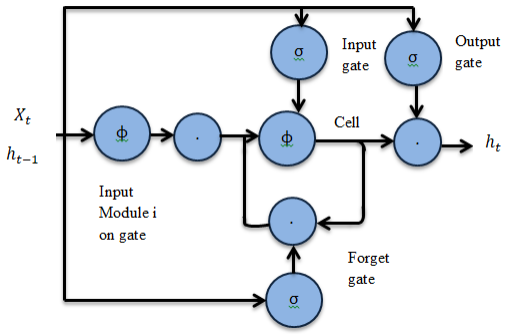

Fig. 2: RNN architectural diagram

When the RNN is completely trained, a number of weak RNN predictors is estimated, and K-RNN models are combined to form a single model which predicts the traffic in the network.

4.7 Proposed Blm Authentication Scheme

The VANET network is secured through Bilinear pairing method for authenticating the vehicles in the network. It is classified into different phases, they are register, retrieval, initialize, verify and message creation and verification. Different symbols and its explanations regarding the proposed model is shown in table-1.

4.8 System Initialization

A third party authority is set to obtain the required tasks, and parameters, thus,

- The TPA considers the following things, P the prime member is selected, and E and GF are the elliptic curve and finite field, corresponding to the base point P, and q represent the order of P. Here G represent the cyclic additive group for the point P, and the cyclic multiplicative group is represented as G_T. Two different group G_1 and G_2 is compared and mapped through bilinear mapping.

- Two hash functioning $h(.)$ and $H_1(.)$ are used for securing the network. The secure hash function is given as$h(.)h: 0,1 \rightarrow Z_q$where the map-to-point has function is represented as $H_1: 0,1 \rightarrow G$.

$$H(\cdot)H: E_p(a, b) \rightarrow \{0,1\}^l$$

  The string length is represented as l.

- $s \in Z_q$ is the private key obtained from the hash functions, TPA assigns a public key of $x, y \in Z_q$**.** The TPA takes care of the key generation and storage securely.

- The parameters are initialized after carrying out the steps discussed, and thus, the following equation represent the parameters generated by TPA.

$\{E, q, P, G, G_T, h(\cdot), H(\cdot), P_{pub}\}$

Registration:
The registration process can be classified into two types, they are RLS and CBU,

4.9 Central Board Unit (CBU) registration phase

V_j represent the vehicle details registered by TPA, before allowing for access in the VANET, and the following steps are carried out by TPA

- For each vehicle a unique ID_{V_j} and password PW_{V_j} and then a random number between $P_{v_j} \in Z_q$ is selected, and $B_{V_j} = h\left(b_{V_j} | PW_{V_j}\right)$. Once the pair $\left\{ID_{V_j}, PW_{V_j}\right\}$ is computed, the details are sent to TPA through a secure channel.

- Once the vehicle details are received at the TPA end, a random number r_{V_j} is created and computed as follows,

$$A_{V_j} = h\left(x \vee r_{V_j}\right)$$

$$C_{V_j} = A_{V_j} \oplus B_{V_j}$$

$$D_{V_j} = h\left(ID_{V_j} \vee B_{V_j} \vee A_{V_j}\right)$$

TPA considers the selected random number $uprk_j \in Z_q$ as the private key and computed it with a public key $upuk_j = uprk_j.P$.

- The following information $\{C_{V_j}, D_{V_j}, r_{V_j}, h(\cdot), H(\cdot), q, uprk_j, upuk_j\}$ is fed into the vehicle V_j'tamper proof device (TPD), where $\left(ID_{V_j}, upuk_j\right)$ is the information maintained by the tracking list.

4.10 Relay Station (Rls) Registration Phase

Here the i represent the vehicles $R_i, i \in \{1,2,3, \dots, n\}$ and registration of each vehicle for RLS is explained in detail.

- R_i is the RSU that transfers the vehicle details to TPA.

- The random value between $rprk_i \in Z_q$ is assigned by TPA as R_i's which acts as a private key that is used with public key$rpuk_i = rprk_i \cdot P$.

- A signature $Sign_{ri} = h(y \vee RID_i)$ is generated with the computed key value, that is, $R_i's$which is used to identify the vehicles, and the details about the vehicle $\{RID_i, Sign_{ri}, rprk_i, rpuk_i\}$ is stored in RLS and transferred with a secured channel.

4.11 Key Retrieval Phase

The vehicles under the RLS range receive the temporary private key sent by RSU, where the R_i represents the random generated value between $\delta_i \in Z_q$, and the temporary master key is MK_i=$h(rprk_i \oplus \delta_i)$ value, which is stored in TPD. The RLS is used to verify the $RPK_i = MK_iP$ value, which is the temporary public key. RPK_i public key is periodically generated by RLS using the random number %delta_i, which lies within the coverage area.

4.12 Vehicle Authentication Phase

The vehicles entering the coverage area are verified with its random value R_i which corresponds to the vehicle V_j, that is present within the tracking list RLS. Thus, RLS verifies the reliability of the vehicle, whether a old or a new one entering the coverage area. In case of a registered vehicle, a temporary master key is generated by the RLS, and the vehicle is allowed to access the identity through R_i^'s through the temporary master key.

The generation of anonymous identity value is followed by the message verification code generated by the vehicle V_j. The legality of the vehicle is also verified, and the authentication process continues as follows,

- A vehicle V_j can be accessed by the user only through identity ID_{vj} and password PW_{vj} to theCBU_j. The details of the vehicles $D_{vj} = D_{vj}$ obtained from the user is verified with the tracking list, and if equal, a request message is sent to the user by CBU_j to use the vehicle. After logging in to the vehicle with the details, a time stamp T_{vj} is given and $TID_{vj} = ID_{vj} \oplus h\left(A_{vj} \parallel T_{vj}\right)$ and $Cert_{vj} = h\left(A_{vj} \parallel ID_{vj} \parallel T_{vj}\right)$ are computed,

$$B_{V_j} = h\left(b_{V_j} \vee PW_{V_j}\right)$$

$$A_{V_j} = B_{V_j} \oplus C_{V_j}$$

$$D_{V_j} = h\left(ID_{V_j} \vee B_{V_j} \vee A_{V_j}\right)$$

- the message $M_1 = \{TID_{vj}, r_{vj}, upuk, Cert_{vj}\}$ is sent to RLS by CBU through a public channel.

- The RLS verifies the message by checking the time-stamp, and authenticates the request, and a certificate value is calculated and a pass message is sent to TPA via public channel.

$$Cert_{ri} = H\left(rprk_i . P_{Pub} \oplus \left(TID_{vj} || Cert_{ri} || \vee Sign_{ri} \vee T_{C1}\right)\right)$$

$$M_1, Cert_{ri}, RID_i, rprk_i, T_{c1}$$

4.13 Vehicle Verification Phase

- The RLS sends the message $\{M_1, Cert_{ri}, RID_i, rprk_i, T_{c1}\}$ to TPA, which checks the time-stampT_{C1} , and if the value holds, then, the following steps are computed,

$$\Theta_j = SK_j^1 + h(M_s).SK_j^2$$

After computation, the signature is verified as $Sign_{ri} = Sign_{ri}$ by TPA, and if it proves to be legitimate, then TPA approves the RLS.

- The message M_1 is extracted by TPA computed as follows,

$$A_{vj} = h(x \parallel r_{vj})$$

$$ID_{vj} = TID_{vj} \oplus h(A_{vj} \parallel T_{vj})$$

$$Cert_{vj} = \mathbf{h}\ (A_{vj} \parallel ID_{vj} \parallel T_{vj})$$

And then TPA verified whether the $Cert_{vj} = Cert_{vj}$ are similar, to approve the V_j as a legitimate vehicle.

- Then, TPA computes the certificate

$$Cert_{TA} = H(S.rpuk_i) \oplus \left(TID_{vj} \middle|\middle| h(y \parallel RID_i) \middle|\middle| T_{c1} \vee T_{c2}\right)$$

and sends as a message $\{Cert_{TA}, T_{C2}\}$ to R_i. In the registration phase, ifR_i entered to a vehicle V_j then V_j should be the legitimate vehicle. After the verification process, the R_i calculates

$$C_1 = H(rprk_i.upuk_i) \oplus \left(TID_{vj} \parallel MK_i \parallel T_{C1} \parallel T_{C2}\right)$$

and sends C_1 to the vehicle V_j available in the coverage area.

- The vehicle computes the MK value after verifying the message fromR_i, and the V_j computes the master key, and gets to the signing phase and authentication phase shown in figure-2.

$$C_1 \oplus H(uprk_j.rpuk_i) =$$

4.14 Message Signing Phase

The vehicles need to verify themselves with RLS through messages periodically. The authenticity of the vehicles are checked over each message and the details are compared with the list for privacy and security. This is one of the crucial process for the VANET as it is difficult to detect the intruder at different time stamps. The signature also improves the security of the system, and the following process is given in detail:

- The V_j selects the random id $\sigma_i \in Z_q$ and a pseudo-identity ID $pID_j = \{pID_j^1, pID_j^2\}$ is generated and private key $SK_j = SK_j^1, SK_j^2$ value.

$$pID_j^1 = \sigma.P,$$

$$pID_j^2 = ID_{vj} \oplus h(\sigma \parallel MK_i)$$

$$SK_j^1 = MK_i.pID_j^1$$

$$SK_j^2 = MK_i.H_1(pID_j^1 \parallel pID_j^2 \parallel)$$

- The vehicles update the TPA about the traffic with time-stamps, and also the sign in message for signing in shown in equation 9.

$$\theta_j = SK_j^1 + h(M_s) \cdot SK_j^2. \qquad (9)$$

- Message about the traffic $\{pID_j, \theta_j, M_s, RID_i\}$ is generated, and the RID_i represent the id of the RLS is identified with that id, and the traffic related information is also verified with that using the temporary master key value R_i.

4.15 Message Verification Process

The message $\{pID_j, \theta_j, M_s, RID_i\}$ giving the traffic details is received from the recipients and validated. The validations process is shown in equation 10.

$$\hat{e}(\theta_j, P) = e(pID_j^1, RPK_i) \times \hat{e}(h(M_s) \cdot H_1(pID_j^1 \parallel pID_j^2 \parallel \delta_i), RPK_i) \quad (10)$$

$$L.H.S = \hat{e}(\theta_j, P) = \hat{e}(SK_j^1 + h(M_s) \cdot SK_j^2, P)$$

$$= \hat{e}(SK_j^1, P) \times \hat{e}(h(M_s) \cdot SK_j^2, P)$$

$$= \hat{e}(MK_i \cdot pID_j^1, P) \times \hat{e}(h(M_s).H_1(pID_j^1 \parallel ID_j^2 \parallel \delta_i), P)$$

$$\hat{e}(pID_j^1, MK_i \cdot P) \times \hat{e}(h(M_s) \cdot H_1(pID_j^1 \parallel pID_j^2 \parallel \delta_i), RPK_i) = R.H.S$$

The above formulation helps in verifying the data obtained from recipients on the traffic. This also validates the messager, and the message. If more messages are received, batch verification technique is adopted to verify it and a responses such as $\{\{pID_1, \theta_1, M_{s1}, RID_i\}, \{pID_2, \theta_2, M_{s2}, RID_i\}, \ldots, \{pID_n, \theta_n, M_{sn}, RID_i\}$ is shown in the following formulation,

$$\hat{e}(\sum_{j=1}^{n} \theta_j, P) = \hat{e}(\sum_{j=1}^{n} pID_j^1, RPK_i) X \hat{e}(\sum_{j=1}^{n} h(zM_{sj}).H_1(pID_j^1 \parallel pID_j^2 \parallel \delta_i), RPK_i)$$

Verifying the signature is also accelerated through batch verification, which consumes less time and computes more data.

4.16 Message Verification

In this section, a message verification process is performed to improve the security system of the authenticated vehicles in the network. Based on the messages generated by the CB units, the TP and RS verify the node authentication. The main process of the TP in the proposed approach is to verify the fake messages generated by the nodes and revoke it. Based on the RID_i, the TP identify the authenticated vehicles within the network coverage. The following equation-13 is used to identify the real authenticated vehicle in the network.

$$pID_j^2 \oplus h(\sigma \parallel MK_i) = ID_{vj} \quad (13)$$

Once the above equation-13 is performed, the TP generated the specific ID to the requested vehicles in the network. Based on this ID, the vehicle is added to the authenticated vehicle list. Then, the information of the vehicle is shared to the all RS within the network. If the requested node is registered in the authenticated vehicle list, then the RS allowed it transfer the data. else, it revokes the nodes to share the data within the network. Based on the private and public key value of the vehicles, the RS can easily detect and classify the original and fake traffic related messages passed by both authorized and unauthorized vehicles.

5.0 ROUTING PROTOCOL

In this, the discussion is about the KGDC-RNN model and its routing logic for vehicle-to-vehicle communication. In this model, there is a presence of proposed analysis information of energy, distance, signal strength, and other node parameters to authorize them in the network. The network process with the data by RNN model and the node analysis proceeds with the BLM algorithm. Once authorized, the nodes can communicate with each other. The sending data between nodes is involved with several intermediate nodes in the routing process. The routing logic is focused on the vehicle-to-vehicle communication and networking algorithm shown in Algorithm 1. Thus, vehicle-to-vehicle communication reduces the workload of RS. Based on certain criteria the clustering head is chosen, and it is the same as the method used [20]. There is the presence of several elements such as RSSI and CC. Both elements achieve the stochastic time interval.

To elect the grouping head, consider the transmission area of all the vehicles as D_t, and the inter-vehicle gap is illustrated as S_i, where the values of i=1, 2, 3…. The range among the values of S_i is i and i+1, this range is not beyond the value of D_t, then rapid communication gets enabled. If the transmission in the vehicle fails, then the value of S_i is more than D_t. In this paper, RSU is used to elect the grouping head between vehicles by estimating the received signal strength indicator. Thus, the moment of RSU and node distance can be written as:

$$D_{(N_s,BS)} = 10\left[\frac{(P_0 - F_m - P_r - 10nlog(f) + 30n - 32.44)}{10n}\right] \quad (14)$$

In the above equation, P_0 indicates the power of the signal lies in zero distance, D indicate the distance between Node and RSU, F_m indicates the fade margin, F indicates the signal frequency, P_r indicates the power line distance d, and n represents the pass-loss. Based on the distance d the dynamic group head is selected, which lies in the transmission capacity (CC), where RNN provides the information.

6.0 RESULT AND DISCUSSION

In this section, the simulation result of the proposed approach on various experiments is discussed in detail. The performance of the model is evaluated using the network simulator software. The performance of the proposed approach to detecting intruders is evaluated using different nodes from 500 to 2000. The result of the analysis shows that the proposed model detects the intruders without affecting the network quality. At each time of node communication, the proposed approach verifies the information nodes communicate. Based on this intrusion detection ratio, the detection rate of the proposed model is detected. The number of intruders detected by the proposed among 500 nodes is 24, 1000 node is 37, 1500 node is 40, and 2000 node is 56.5.

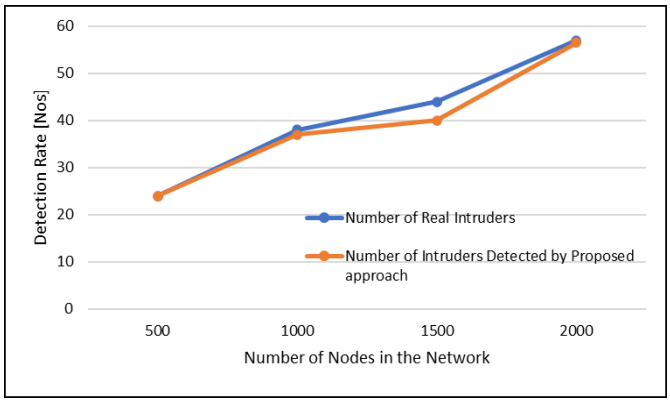

Fig. 3: Intrusion detection ratio

Each node requires a certain amount of energy to perform the tasks during communication. After performing the task, the remaining energy consumed in the network is evaluated and depicted in figure-4. The result shows that after completing each round, the proposed approach has remained for 500, 1000, 1500, and 2000 nodes at 99.86%, 98%, 88%, and 83%, respectively. Each node's total energy is consumed more efficiently based on this remaining energy.

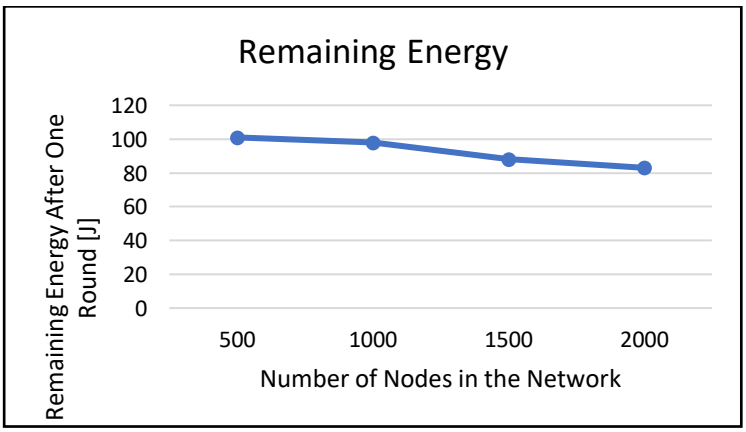

Fig. 4: Remaining energy

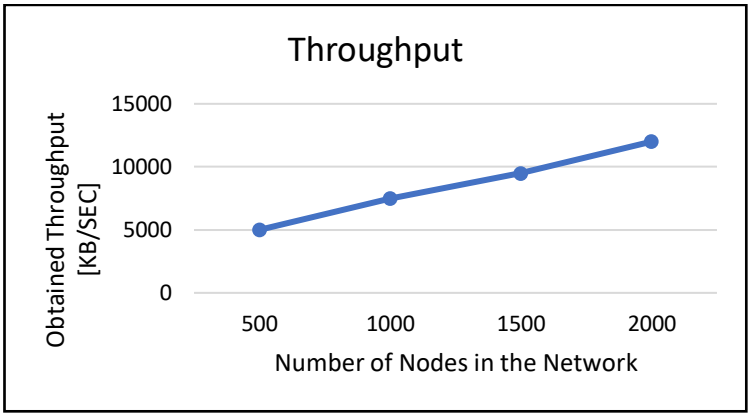

Fig. 5: Throughput

After evaluating the remaining energy level of each node in the network, the throughput value of the proposed approach is calculated. For this, the model's efficiency on different nodes is experimented with and depicted in figure-5. The analysis shows that the proposed model has performed the communication task with a high throughput ratio. That is, 500, 1000, 1500, and 2000 nodes transfer the vehicle information with 5000, 7500, 9500, and 12000 KB\Sec, respectively. From the result, the proposed model is more suitable for heterogeneous network-based communication. The time taken by the proposed approach to communicate the information is now examined. It is denoted as delay time; it represents the time taken to transfer the data between the nodes in a single path. The delay time analysis result of the proposed model is shown in Figure 6. That is, the 500 nodes took 22 ms, 1000 nodes took 30 ms, 1500 took 40 ms, and 2000 nodes took ms delay time to transfer the data.

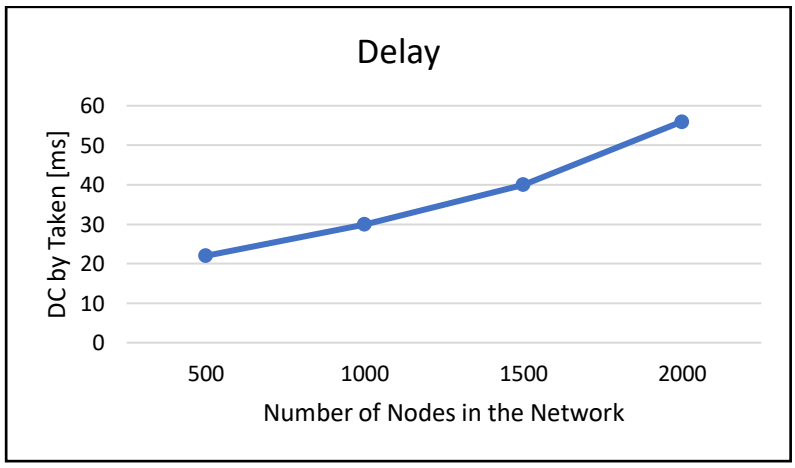

Fig. 6: Delay time

The overall analysis of the proposed approach defines that, based on the figure-3 result, the proposed approach is more efficient in detecting intruders in both large and smaller nodes. As per the Figure-4 result, performing the input task consumes much less energy. It is verified with various nodes to demonstrate the energy consumption ratio. In figure-5, the number of nodes increases, and the throughput value of the proposed model also increases. This will show the model's efficiency in processing the communication task in the VANET system. According to figure-6, the proposed approach utilized very little time to communicate the information between the nodes in the VANET network.

Table-2 depicts the performance evaluation result of the proposed approach to transferring the data between the nodes in the network. The model's performance is evaluated by experimenting with 50 to 500 nodes. At first, the throughput ratio of the model is examined, and the result shows that the proposed model transfers the data with high throughput ratio and is more efficient to handle the available bandwidth in the network. Second, the Packet delivery ratio of the model is analyzed. The result indicates that the proposed model more efficiently and accurately delivers the data between the nodes. Third, the remaining energy consumed by each node is examined. The result shows that the proposed model transfers the data with less energy, as mentioned in the earlier section. Finally, the pack loss ratio is evaluated. It is clear from the evaluation the proposed model more accurately transfers the data without any loss.

Table 2: Performance Evaluation Result of The Proposed Approach

No. of nodes	Throughput	PDR	Remaining Energy	Packet loss
50	1843	1.00	98.66	0
100	2942	0.98	98.18	0.03
150	3678	0.97	97.57	0.04
200	4453	0.975	96.8	0.04
250	4907	0.973	96.37	0.04
300	5611	0.982	95.7	0.03
350	6210	0.972	94.1	0.05
400	6812	0.975	93.1	0.04
450	7400	0.969	93.38	0.04
500	8032	0.975	93.2	0.04

7.0 CONCLUSION

This paper aimed to design and implement a novel intrusion detection and prevention model for heterogeneous networks. Each abnormal node's activities are deployed in all the relay stations, where the communication data is verified at all the RS because all the heterogenous network communications have occurred only at relay stations. The data about the node, data used in the transmission, and other attributes are verified based on authentication, trust value calculation, the format of the data, and other functions of the nodes and the routes. It helps to decide whether any malicious node activity is occurred in the network. It also verifies the inter and intra-communication among the nodes in the networks. In order to do the above-said processes, an RNN-based authentication routing protocol is created and simulated in NS2 software to verify the outputs. From the outputs, it is found that the proposed routing protocol proved that it is highly efficient and fulfills the networks' QoS. In future enhancement, this paper is that the performance of the proposed approach is compared with the other existing approaches reviewed in the literature survey and proves its better-ness.

REFERENCES

[1] Ahmad, Awais, et al. "Data transmission scheme using mobile sink in static wireless sensor network." *Journal of Sensors,* 2015.

[2] Yang, Ding-Xin, et al. "Through-metal-wall power delivery and data transmission for enclosed sensors: A review." *Sensors*, Vol. 15, No. 12, 2015, pp. 31581-31605.

[3] Bhandari, Rupesh, and V. B. Kirubanand. "Enhanced encryption technique for secure IoT data transmission." *International Journal of Electrical and Computer Engineering*, Vol. 9, No. 5, 2019, pp. 3732.

[4] Oh, Sung-Min, and JaeSheung Shin. "An efficient small data transmission scheme in the 3GPP NB-IoT system." *IEEE Communications Letters*, Vol. 21, No. 3, 2016, pp. 660-663.

[5] Dynes, James F., et al. "Ultra-high bandwidth quantum secured data transmission." *Scientific reports*, Vol. 6, No. 1, 2016, pp. 35149.

[6] Mohanty, Prabhudutta, and Manas Ranjan Kabat. "Energy efficient reliable multi-path data transmission in WSN for healthcare application." *International journal of wireless Information Networks*, Vol. 23, No. 2, 2016, pp. 162-172.

[7] Yazdeen, Abdulmajeed Adil, et al. "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review." *Qubahan Academic Journal*, Vol. 1, No. 2, 2021, pp. 8-16.

[8] Ezeofor, C. J., and A. G. Ulasi. "Analysis of network data Encryption & Decryption techniques in communication systems." *International Journal of Innovative Research in Science, Engineering and Technology,* Vol. 3, No.12, 2014, pp. 17797-17807.

[9] Manohar, N., and Peetla Vijay Kumar. "Data encryption & decryption using steganography." *2020 4th international conference on intelligent computing and control systems (ICICCS)*. IEEE, 2020.

[10] Baagyere, Edward Yellakuor, et al. "A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers." *IEEE Access*, Vol. 8, 2020, pp. 100438-100447.

[11] Mota, Aquino Valentim, et al. "Comparative analysis of different techniques of encryption for secured data transmission." *2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*. IEEE, 2017.

[12] Ahmed, Abdulghani Ali, et al. "Dynamic reciprocal authentication protocol for mobile cloud computing." *IEEE Systems Journal*, Vol. 15, No. 1, 2020, pp. 727-737.

[13] Ostad-Sharif, Arezou, et al. "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme." *Future Generation Computer Systems*, Vol. 100, 2019, pp. 882-892.

[14] Mishra, Dheerendra, et al. "Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks." *Multimedia Tools and Applications*, Vol. 77, 2018, pp. 18295-18325.

[15] Nyangaresi, Vincent Omollo, Anthony J. Rodrigues, and Nidhal Kamel Taha. "Mutual authentication protocol for secure VANET data exchanges." *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures*. Cham: Springer International Publishing, 2021.

[16] Ahmed, S. T., M. Sandhya, and S. Sankar. "TelMED: Dynamic User Clustering Resource Allocation Technique for MooM Datasets Under Optimizing Telemedicine Network. Wireless PersCommun, Vol. 112, 2020, pp. 1061–1077.

[17] Kumar, S. Sreedhar, et al. "Unstructured Oncological Image Cluster Identification Using Improved Unsupervised Clustering Techniques." *Computers, Materials & Continua,* Vol. 72, No. 1, 2022.

[18] Ahmed, Syed Thouheed, et al. "A generalized study on data mining and clustering algorithms." *New Trends in Computational Vision and Bio-inspired Computing: Selected works presented at the ICCVBIC 2018, Coimbatore, India*, 2020, pp. 1121-1129.