Journal of Theoretical and Applied Information Technology
31st July 2025. Vol.103. No.14

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SELF-ADAPTIVE TRANSIENT GENERALIZED FUNCTIONAL REGRESSIVE CRYPTOSYSTEM BASED AUTHENTICATION FOR SECURED DATA TRANSMISSION IN PERSONAL AREA NETWORK

R.ABARNA SRI [1], K.DEVASENAPATHY[2]

Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-641021

Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore-641021

[1]abarnasrirajaganesh@gmail.com, [2]drdevasenapathy.k@kahedu.edu.in

ABSTRACT

Personal Area Network (PAN) is to connect electronic devices. Personal devices namely laptops, wearable devices, and other peripherals employed in PAN.During the communication, PAN is susceptible to different attacks caused by the malicious device within the network. Security plays an important role in preserving the data from different attacks during communication. Secure transmission was discussed with numerous researches. But higher confidentiality was major challenging issues. Self-Adaptive Transient Generalized Functional Regressive Cryptographic Authentication (SATGFRCA) technique is designed to enhance data confidentiality in PANs. The SATGFRCA technique employs the Benaloh Public Key Homomorphic Cryptosystem to achieve improved data confidentiality. In SATGFRCA technique, nodes or devices register their information with the base station (BS) to facilitate authentication. The BS then generates a Self-Adaptive Transient key pair (public and private keys) for each registered node. Upon receiving the key pair, sender node encrypts data packets via public key as well as transmits toward receiver node. Upon receiving the data, the receiver node verifies its authenticity using Generalized Functional Regressive Analysis. Once authenticity is confirmed, the authorized receiver node decrypts the data using its private key. This process ensures data packets remain secure, enhancing both security and confidentiality through the SATGFRCA technique. An experimental evaluation was conducted based on factors such as authentication accuracy, authentication time, data confidentiality rate, and data delivery ratio, considering varying numbers of nodes and data samples. Outcome of SATGFRCA provides higher data confidentiality rate, data delivery ratio, and reduced authentication time. This finding confirms the SATGFRCA technique efficiency and effectiveness compared to existing approaches

Keywords: *Personal Area Network, security, authentication, Benaloh Public Key Homomorphic Cryptosystem, Self-Adaptive Transient key, Generalized Functional regression*

1. INTRODUCTION

A wireless network is a communication system that enables devices to connect and transmits data without the use of physical cables. This setup allows for a greater mobility and flexibility, as devices communicates over various distances using radio frequency signals. Wireless networks offer numerous benefits, and also present security challenges due to their broadcast nature. Implementing robust security and strong authentication methods are essential to protect data and prevent unauthorized access.

An enhanced Ghost Bidirectional Gated Recurrent Network (Ghost_BiNet) model was developed in [1] for intrusion detection, aiming to enhance information security and detection accuracy using Homomorphic encryption. However, it failed to improve intrusion detection while also protecting data confidentiality and security in various cybersecurity scenarios. A lightweight authentication protocol was designed in [2] with the aim of improving security during communication. The protocol was more robust against numerous attack vectors. However, the time consumption during authentication was not minimized. Different cryptographic algorithms were designed in [3] to enhance security during data communication. But a machine learning model was not applied to perform authentication and further enhance security. Lightweight symmetric and asymmetric encryption

integrated [4] with Hybrid Lightweight Cryptographic Approach (HLCA). But, it failed to restrict access to key information solely to authorized users, thus compromising the security of the data. The Light Weight Integrated Elliptic Curve Cryptographic model was developed in [5] for secure data transmission and intrusion detection, offering high security and minimal delay.

Hybrid encryption approach was developed in [6] that combine symmetric Blowfish encryption with elliptic curve cryptography to ensure security while minimizing execution time. However, the encryption process requires larger key sizes to achieve the highest level of security. Additionally, accommodate a large number of IoT devices proves to be challenging. A hybrid cryptographic mechanism was developed in [7] by integrating the Ant Lion Optimization algorithm with a cryptography model for secure data transmission. However, it failed to address the reduction of computational complexity in secure data transmission. Intrusion detection enhanced [8] via new fuzzy model by achieving better accuracy, increasing the packet delivery rate, and decreasing network delay. However, it failed to apply cryptographic techniques to enhance the accuracy.

A Blockchain and Secure Federated Learning method was developed in [9] to enhance privacy and address security attack issues. However, it failed to improve the system's reliability. A neural network integrated with Homomorphic Encryption (HE) was introduced in [10] to enhance robustness against attacks. But, it failed to include the design of a more powerful algorithm to further enhance security. A homomorphic encryption and blockchain technology were developed in [11] to guarantee the accuracy of normal and anomalous behaviors. However, the confidentiality level was not improved. The Trust-Based Intrusion Detection System was designed in [12] to enhance the efficiency of detecting and isolating malicious nodes while minimizing packet loss. But, it failed to detect a wider range of attacks, including neighbor attacks. An adaptive hybrid IDS was developed in [13] to efficiently distinguish and recognize a wide range of attacks. However, it failed to ensure robust security while minimizing unnecessary computational burdens.

A federated learning-based approach was developed in [14] for decentralized DDoS attack detection to enhance detection efficiency. But, it failed to improve its applicability and robustness in securing IoT networks against a wide range of cyber threats. A new approach called the blockchain and quantum cryptography model was introduced in [15] to establish communication authenticity and integrity. However, it failed to enhance the security, scalability, and privacy of the framework for its successful implementation in diverse attack detection.

1.1 Major contribution

SATGFRCA contribution given by,

- Novel SATGFRCA technique is introduced with achieving intrusion detection in PAN through the integration of the Benaloh Public Key Homomorphic Cryptosystem and Generalized Functional Regression.
- To enhance authentication accuracy, a generalized functional regression model is employed to analyze the node features during data transmission and distinguish between normal and attack behaviors. This process takes minimal time to authenticate the node within the PAN.
- To enhance the confidentiality rate, the SATGFRCA technique utilizes the Benaloh Public Key Homomorphic Cryptosystem to perform self-adaptive transient key generation, data encryption, and decryption. This process ensures that only authorized nodes access the data, thereby guaranteeing security and improving data delivery between the sender and receiver.
- Simulation performed forSATGFRCA as well as related works. The results show that our SATGFRCA technique was evaluated using various performance metrics, including authentication accuracy, authentication time, data confidentiality rate and data delivery rate.

1.2 Organization of the paper

It is given by: literature survey explained in Section 2. Section 3 introduces the proposed SATGFRCA technique providing an in-depth explanation along with a diagram. Simulation as well as dataset used for evaluation in Section 4. Performance of SATGFRCA, existing approaches analyzed in Section 5 across different parameters. Lastly, conclusion presented in Section 5.

2. LITERATURE SURVEY

For boosting security, adversarial neural network with cryptographic techniques was developed in [16]. But, it struggled with detecting more powerful attacks and handling longer keys.Spoofing attacks determined [17] by DNN with minimal time

consumption. However, it did not make advancements in network security strategies for creating secure and reliable environments. Principal Component Analysis (PCA) and a machine learning classifier model were developed in [18] to enhance the accuracy of DDoS attack detection. However, the time complexity of attack detection was high. The new Collaborative Intrusion Detection (CID) approach developed in [19] aimed to enhance intrusion detection accuracy. However, it did not improve the performance of the IDS model as expected.Anomaly detection and ML were applied [20] via IDS defense. But, it failed to ensure the robustness of the model.

DNN identifies intrusions [21] within computer networks. But the performance of intrusion detection was not improved. An integration of Gaussian Naive Bayes and Random Forest was developed in [22] to achieve impressive accuracy in attack detection. However, it failed to be applied to larger-scale datasets for attack detection. An efficient encrypted control system was developed in [23] for detecting man-in-the-middle attacks with minimal processing time. But, it failed to explore timestamp-based attack detection methods to enhance cybersecurity against various attacks. The machine learning algorithms were developed in [24] for securely scanning the wireless network to enhance data delivery with minimal latency. However, the cryptographic method was not applied to enhance the level of confidentiality. A Deep Belief Network (DBN) model was developed in [25] to construct an intelligent detection model with improved accuracy. But, it failed to apply the updated architectures to enhance network performance.

A dynamic symmetric key generation model was designed in [26] to enhance the security of the wireless network. However, the computational time of the model was not reduced. To minimize computational time, a Teaching-Learning-Based Optimization (TLBO) enabled Intrusion Detection System (IDS) was developed in [27] to efficiently protect IoT networks from intrusion attacks. However, it failed to incorporate various encryption standards to further enhance its performance. A Convolutional Neural Network (CNN) was developed in [28] to enhance model performance. But, the computational complexity of the model was high in resource-constrained environments. A distributed and cooperative signature-based intrusion detection approach was developed in [29] within the wireless network to detect malicious traffic patterns. However, authentication was not addressed to enhance the level of confidentiality.In [30], asymmetric cryptography model was designed from source to destination. But, higher safety not achieved.

3. PROPOSAL METHODOLOGY

Personal Area Networks (PAN) represent a novel approach in the field of information technology, designed to connect personal devices within a short range and fulfill end-users' requirements for seamless communication and data exchange between devices. Security is the most critical concern in PANs. In PANs, devices need to ensure secure communication during the exchange of sensitive information. However, traditional PAN setups do not fully guarantee secures data access.Proposed SATGFRCAdeigns higher data access security and communication among devices in a PAN by utilizing cryptographic techniques. The architecture of the SATGFRCA technique is illustrated in Figure 1.

Figure 1 demonstrates the detailed process involved in the SATGFRCA technique, which is designed to guarantee robust security for data transmission within the Personal Area Network (PAN) environment. A PAN typically includes interconnected devices to facilitate seamless communication and data exchange. The architectural design of the proposed SATGFRCA technique is designed on achieving seamless and secure interaction between devices within the PAN. This design incorporates advanced security mechanisms called Benaloh Public Key Homomorphic Cryptosystem to protect sensitive information while ensuring efficient device communication. Four primary steps included in SATGFRCA technique. Each process plays a vital role in securing the PAN. This initial step establishes trust within the network. Devices within the PAN undergo a secure registration process to authenticate their identity. During this phase, cryptographic keys are generated and distributed for communication between devices and data protection against unauthorized access. Encryption is the process of secure data transmission within the PAN. Data generated by devices is encrypted using advanced cryptographic algorithms before transmission. Third process is an authentication in which each device is authenticated to verify its identity. This process prevents unauthorized devices (i.e. attacks) access the data. This process ensures that only legitimate devices and users access the network. For enabling certified devices, decryption achieves original shape. Decryption ensures that sensitive data accessed by authorized devices with the proper decryption keys. This guarantees the confidentiality and integrity of data within the PAN. The following subsection

provides deeper explanation within the SATGFRCA technique.

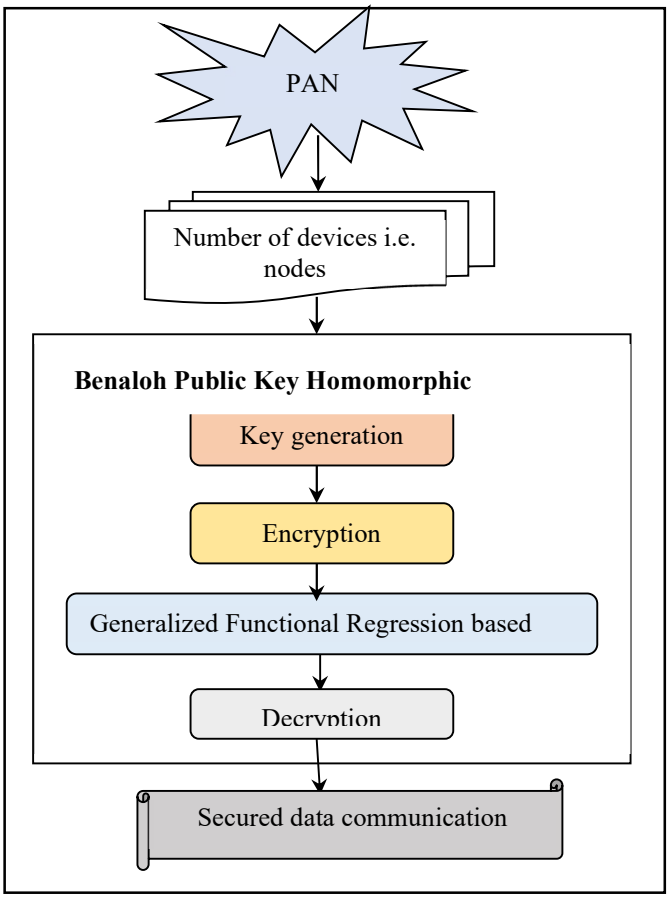

Figure 1 Architecture diagram of the SATGFRCA technique

3.1 System model

The PAN structural design comprises various entities such as devices or nodes, Base station, contributing to secure data transmission. The architecture of SATGFRCA includes multiple PAN devices$N_1, N_2, N_3, \ldots . N_n$ which generate the data $D_1, D_2, D_3, \ldots . D_m$ within the network. These devices communicate with a central base station'BS' to manage data transmission. The PAN device ensures seamless and secure services for all connected devices, enabling efficient interaction and data communication within the network.

3.2 Registration and key generation

User submitting their personal details is registered to central server or base station (BS), registration carried out.Device provides information such as their ID, and other relevant details, which are then stored securely on BS. It generates Self adaptivetransient keysfor both registered device. Withsuccessfully storing device during the registration process, the base station initiates the generation of Self-Adaptive Transient Keys for each registered device. These keys, which include both private and public components, play a vital role in establishing secure and dynamic communication within the network.

The publicly accessible key shared with other network devices for secure communication. Private Key is a confidential key unique to the device, securely stored and never showed to other network devices. The self-adaptive nature ensures that the keys remain robust against evolving cyber threats and unauthorized access attempts.

Transient Keys are not permanent and are designed to be regenerated over specific time (i.e., session expiration).This transient nature minimizes the risk of long-term key publicity or compromise. Keys are regenerated when a communication session between the device and the base station ends. This ensures that each new session starts with a new key for preventing attackers and enhances confidentiality. The use of transient keys ensures that data exchanged between devices and the network remains unaltered and confidential.

This transient keys generation process is carried out using the Benaloh Cryptosystem to ensure secure communication and data protection. Assume two prime numbers X as well as$Y$. Transient keys are generated s follows,

$$Q = X * Y \quad (1)$$

$$\varphi = (X-1)(Y-1) \quad (2)$$

$$\beta = \omega^{\varphi/b} \, mod \, Q \quad (3)$$

From (1) (2) (3),(ω, Q) denotes a self adaptive transient public key, (φ, β) represents the self adaptive transientprivate key, b denotes a block size, ω denotes an integer number. After the keys generation, the base station distributes the self adaptive transient public key and private key for every registered device.

3.3 Encryption

After generating the key, the proposed SATGFRCA technique performs encryption on the sender's side, transforming plaintext into ciphertext to prevent access by malicious devices (i.e. attacks). The encryption process in the SATGFRCA technique is designed to secure data transmission by converting plaintext into ciphertext, ensuring that unauthorized entities cannot access the original information. This process begins at the sender's end, where the sensor node encryptsinformation. By utilizing public key cryptography, the possessing the corresponding private key decrypt and access the data. The sender node, performs this encryption to prevent attacker nodes from intercepting sensitive information during transmission. This approach maintains data integrity and confidentiality in the communication process.

The data encryption is done at the sender side (i.e. cloud service provider) whereas the

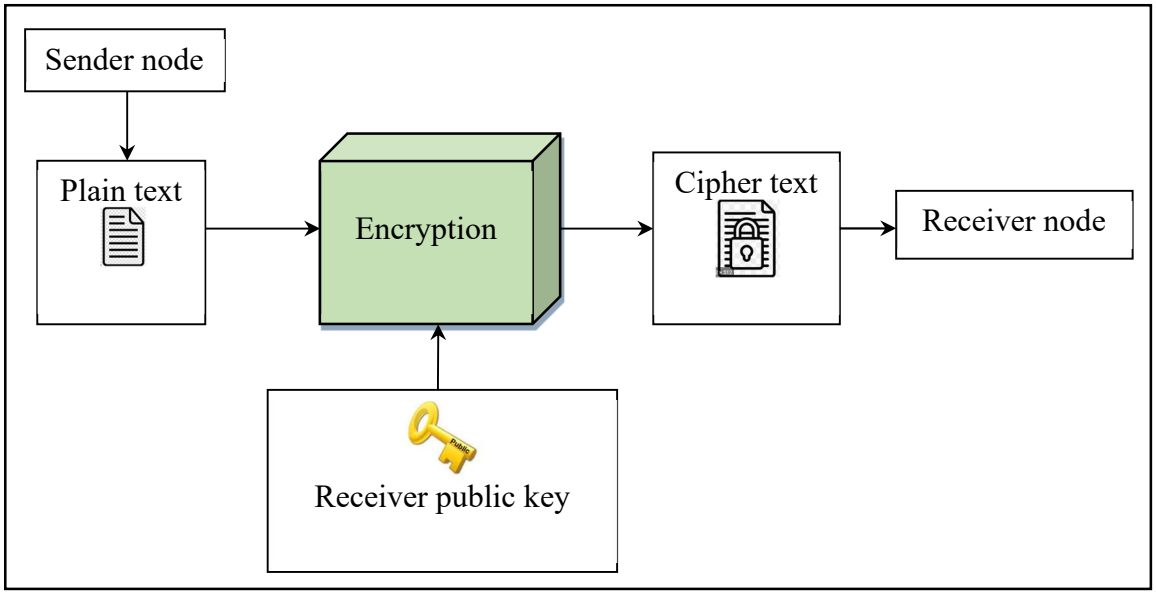

Figure 2 Encryption

Encryption process has portrayed in Figure 2 with improving security from sender nodes to receiver. Let us consider the sensed data samples 'D' and it is changed to ciphertext as given below,

$$C = \omega^D R^b \, mod \; Q \quad (4)$$

Where, C indicates a ciphertext, D represents a input data packets, ω denotes a public key, R indicates a random number, b represents a block

size, Q indicates a product of two prime numbers. Once the sender node has encrypted, plaintext information transmits to receiver node resulting ciphertext securely via public key. This process helps to maintain synchronization between the nodes and allow the receiver to verify the integrity and authenticity of the input data packets.

3.3 Authentication

Authentication is a significantprocess of the SATGFRCA technique, ensuring that only legitimate devices participates in the communication process. It establishes trust between the sender and receiver nodes and prevents unauthorized access, and other security threats. The proposed technique utilizes the generalized functional regressive analysis. It is an advanced analytical method that applies regression models to functional data, enabling precise modeling and prediction of user behavior in authentication systems. This technique is suitable for distinguishing between normal and attack by analyzing a history of samples in device.Let us consider the history of data samples for each deviceis formulated as follows,

$$IV = \begin{bmatrix} D_1f_1 & D_1f_2 & \dots & D_1f_k \\ D_2f_1 & D_2T_f & \dots & D_2f_k \\ \dots & \dots & \dots & \dots \\ D_nf_1 & D_nf_2 & \dots & D_mf_k \end{bmatrix} \quad (5)$$

Where, 'IV' is input vector matrix defined by taking into considerations of the history of sample 'D_m' for the corresponding device 'N_n' and node features$f = \{f_1, f_2, \dots, f_k\}$. The generalized functional regression function analyses the history of sample devices in order to detect the normal (i.e. benign) or attacks (i.e. DDos). The regression analyses between the data samples of the node are analyzed as given below,

$$Y = \delta_0 + \sum_{j=1}^{m} D_{jk}\ \delta + \varepsilon \quad (6)$$

Where Y denotes a regression outcomes, δ_0, δ denotes a regression coefficient used to determine which features are most influential in detecting attacks or normal, ε denotes a random error with mean zero and finite variance, D_{jk} denotes a j^{th} data samples for k^{th} features of the device or node within the network.

$$Y = \begin{cases} 1\ ;\ attack\ nodes \\ 0\ ;\ normal\ nodes \end{cases} \quad (7)$$

The above equation (7) indicates that the regression outcome 'Y'is binary. A value of '1' corresponds to a node being in an attack state (i.e. DDoS attack), while a value of 0 corresponds to the node being normal or benign. Therefore, the generalized functional regression model helps in analyzing the behavior of network nodes by identifying the significant features through the coefficients and distinguishes between normal operation and attack states. This process helps to enhance the authentication of the node for enhancing the confidential data transmission.

3.4 Decryption

Finally, the normal node received the cipher text and performs decryption to get the original data.Decryption is the reverse process of encryption and is essential for ensuring that only authorized node access the original data.

Decryption process demonstrated in Figure 3through receiver private key.

$$D = \log_{\beta}\ (M) \quad (8)$$

$$M = C^{\varphi/b}\ mod\ M \quad (9)$$

Where D denotes an original text, β, φindicates a private keys, C denotes a cipher text, b denotes a block size.Finally, the authorized receiver node successfully decrypts the ciphertext to obtain the original data packets, ensuring that the data remains confidential throughout the transmission. This decryption process is crucial for preserving data confidentiality, as only the authorized receiver, utilizing the correct decryption key and accesses the original information. By employing secure encryption methods, unauthorized nodes or attackers are prevented from the sensitive data. As a result, confidentiality of the data is significantly enhanced and protect it from unauthorized access or malicious activities during transmission. SATGFRCA pseudo code presented by,

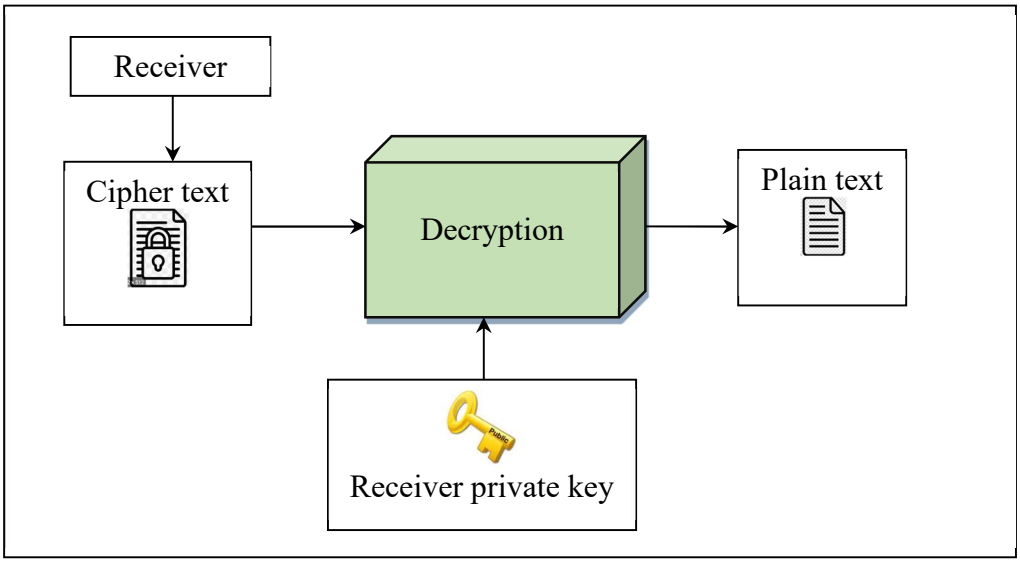

Figure 3 Decryption procedure

// Algorithm 1:Self-Adaptive Transient Generalized Functional Regressive Cryptographic Authentication
Input:PAN devices$N_1, N_2, N_3, \ldots . N_n$, data samples $D_1, D_2, D_3, \ldots . D_m$ within the network. central base station 'BS'
Output: Enhance data communicationsafety
Begin
Step 1: for each 'device or node 'N_n' in the network
Step 2: Register their details to 'BS''
Step 3: BS'**g**eneratesSelf-Adaptive Transient private and public key by (2) (3)
Step 4: End for
Step 5:For each data 'D_i' transmission
Step 6: Sender node carry out data encryption
Step 7: Convert plain text into ciphertext using (4)
Step 8: Send ciphertext into receiver
Step 9: **End for**
Step 10: For each receiver node
Step 11: Perform authentication using (6)
Step 12: if $(Y = 1)$**then**
Step 13: Node is said to be an attacker
Step 14: **else**
Step 15: Node is said to be an normal
Step 16: **End if**
Step 17: **End for**
Step 18: For each normal node **do**
Step 19: Perform data decryption using (8) (9)
Step 20: Authorized receiver obtain the original data 'D'
Step 21: **End for**
End

SATGFRCA algorithm procedure is described. Initially, nodes or devices are deployed across the network to collect data. Each node registers their details to the bases station for further processing. After the successful registration, the base station generates the pair of Self-Adaptive Transient keys for secure communication. Once the keys are generated, the node begins transmitting the data to the receiver. Before sending, the node encrypts the data to ensure privacy based on the receiver public key. For each transmission, the base station performs the receiver node authentication with the help of the generalized functional regression method. After performing the authentication, the authorized node or normal node performs the data decryption. Upon receiving the encrypted data, the authorized receiver node decrypts the data using its private key. This process helps to preventing unauthorized access to the data. This approach significantly enhances the confidentiality of data transmission in wireless network.

4. SIMULATION

SATGFRCA as well as two conventional methods namely Enhanced Ghost_BiNet [1], lightweight authentication protocol [2] are implemented in the python programming language. Network Intrusion detection evaluation dataset CIC-IDS2017 taken from http://www.unb.ca/cic/ datasets/IDS2017.html. It collects network traffic captured during different days of the week with various attack scenarios. This dataset includes 2 classes such as Normal and attack. The main aim of this datae is to detect the anomaly

using labelled data samples. The dataset contains 85 features, including flow features, time-based features, and statistical features. The number of data samples ranges from 10,000 to 100,000, while the number of devices ranges from 1,000 to 10,000.

5. PERFORMANCE ANALYSIS

SATGFRCA, traditional [1], [2], are discussed with respect to various parameters. The assessment of these metrics is presented using both tabular and graphical representations.

5.1 Evaluation metrics

Authentication accuracy: It is determined by the ratio of correctly identified authorized devices or attacks.

$$AA = \sum_{i=1}^{n} \left(\frac{CIN}{N_i}\right) * 100 \quad (10)$$

Where, 'AA' denotes authentication accuracy, 'N_i' indicates the number of nodes or devices as input for experimentation. AA determined by percentage (%).

Authentication time: It refers to time duration required by the algorithm to authenticate a devices or nodes. Therefore, the authentication time is calculated by as follows

$$AT = \sum_{i=1}^{n} N_i * Time\ (NA) \quad (11)$$

Where 'AT' indicates the authentication time, 'B' denotes the number of nodes or devices, '$Time\ (NA)$' is the time taken for node authentication. ATestimated by milliseconds (ms).

Data confidentiality rate: Number of data samples accessed with authorized devices or nodes and it is protected from unauthorized devices or attacks. It is measured as given below,

$$DCR = \sum_{j=1}^{m} \left(\frac{DAND}{D_j}\right) * 100 \quad (12)$$

Where 'DCR' represents the data confidentiality rate, $DAND$ denotes a data samples accessed by normal (i.e. authorized) device.

Data delivery ratio: It referred to as number of information samples successfully delivered at authorized receiver and it is protected from unauthorized devices or attacks. This process helps to evaluate the security of the model as given below,

$$DDR = \sum_{j=1}^{m} \left(\frac{DSD}{D_j}\right) * 100 \quad (13)$$

Where 'DDRrepresents the data delivery rate, DCR denotes adata samples successfully delivered at the receiver.

5.2 Comparative analysis of different methods

SATGFRCA, Enhanced Ghost_BiNet [1], lightweight authentication protocol [2] are analyzed in this secion with different performance metrics.

5.2.1 Performance analysis of authentication accuracy

In this section, a comparative analysis of the proposed SATGFRCA technique and two existing methods, referred to as Enhanced Ghost_BiNet [1], lightweight authentication protocols [2] is conducted using authentication accuracymetrics.

Table I comparison of authentication accuracy

Number of nodes	Authentication accuracy (%)		
	SATGFRCA	Enhanced Ghost_BiNet	lightweight authentication protocols
1000	98.6	93.3	91.8
2000	98.36	92.65	90.36
3000	97.58	93.05	91.66
4000	98.11	92.63	90.21
5000	97.36	93.07	91.36
6000	98.22	93.37	91.48
7000	97.36	92.88	90.21
8000	98.05	93.05	91.74
9000	98.66	92.78	90.36
10000	97.36	93.1	91.52

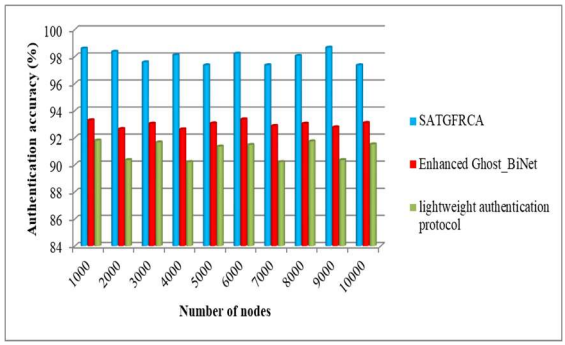

Figure 4 Graphical illustration of authentication accuracy

Figure 4 presents the node authentication accuracy achieved by three models.Number of nodes or wireless devices is denoted as horizontal axis. AA indicated as vertical axis. The SATGFRCA consistently achieves higher accuracy than the other methods. For example, in the first iteration with 1000 nodes or devices, the SATGFRCA technique attained an accuracy of 98.6%, and the accuracies of [1] [2] was observed to be 93.33% and the 91.8% respectively. To allow a comprehensive assessment, ten separate results were generated for each method by varying the number of input nodes. The analysis reveals that the SATGFRCA technique achieved an

average improvement of 5% and 8% over [1] and [2], respectively. This improvement is achieved through the application of Generalized Functional Regressive Analysis within the wireless network. The regression function analyzes the features of each node during transmission to verify authenticity. Based on this analysis, nodes are accurately classified as either normal or malicious. Consequently, the SATGFRCA technique exhibits superior accuracy in node authentication.

5.2.2 Performance analysis of authentication time

Authentication time is a critical metric. It measures time taken by a system to verify the identity of nodes.

Table II AT

Number of nodes	AT (ms)		
	SATGFRCA	Enhanced Ghost_BiNet	Lightweight authentication protocol
1000	43	48	53
2000	47.6	51.3	55.6
3000	51.3	55.8	60.3
4000	55.9	60.3	63.5
5000	62.3	65.7	70.4
6000	68.2	72.5	75.6
7000	71.8	80.6	83.6
8000	74.6	82.3	84.7
9000	78.2	85.4	87.5
10000	82.5	86.7	90.6

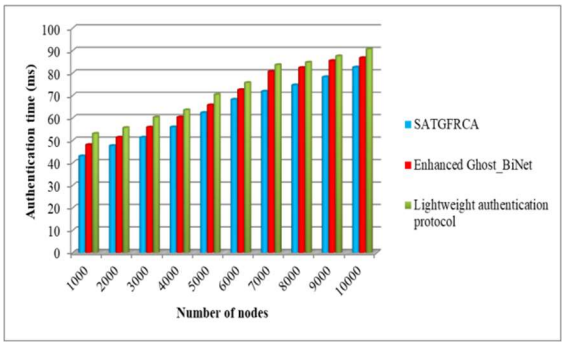

Figure 5 Graphical illustration of AT

Figure 5 illustrates the authentication time. Node increases, overall authentication time also increased. However, the SATGFRCA technique demonstrates lower authentication time compared to other existing techniques. For experimentation with 1000 nodes, the authentication time for SATGFRCA technique was recorded as $43ms$, whereas the existing [1] and [2] methods required $48ms$ and $53ms$, respectively. Different volumes of input nodes provided better performance across all three approaches. The results indicate that the SATGFRCA technique achieved a significant reduction in authentication time by 8% and 13% compared to [1] and [2], respectively. The reduction in time complexity and improved performance is achieved through Generalized Functional Regression (GFR). Node features were examined. It utilizes coefficient analysis to identify key relationships between features. The regression approach enhances the authentication process with minimal time consumption.

5.2.3 Performance analysis of DCR

DCR crucial metric by evaluating security efficacy. It measures system ability fordefendresponsiveinformation as ofnot permitted access during transmission.

Table III DCR

Number of data samples	DCR (%)		
	SATGFRCA	Enhanced Ghost_BiNet	Lightweight authentication protocol
10000	94.36	92.41	90.78
20000	93.85	91.26	89.56
30000	94.21	91.33	88.78
40000	93.98	91.05	89.08
50000	94.22	92.78	90.12
60000	94.65	92.35	90.42
70000	93.75	91.05	89.05
80000	93.44	91.47	88.45
90000	94.66	91.64	89.15
100000	94.12	91.33	89.35

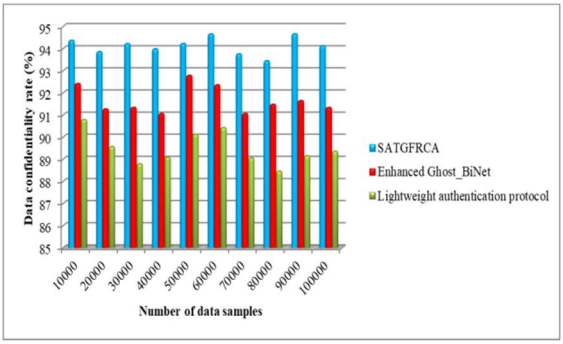

Figure 6 Graphical illustration of DCR

DCR of three methods demonstrated in Figure 6. The SATGFRCA technique demonstrates obviously higher data confidentiality rate compared to the other approaches. For instance, in the first iteration with 10000 samples, the namely SATGFRCA technique achieved an accuracy of 94.36%, outperforming the existing models [1] and [2], which recorded accuracies of 92.41% and 90.78%, respectively. Ten different results were generated for each method by varying the number of data samples, allowing a comprehensive comparison of their performance.

The comparative analysis exposes that the SATGFRCA technique outperformed [1] and [2] by 3% and 5%, respectively. This improvement is achieved by applying the Benaloh Public Key Homomorphic Cryptosystem for encrypting the data samples. The source node encrypts the data is then transmitted toward receiver. Upon receiving ciphertext, the base station verifies the authenticity. Finally, original data samples are retrieved with authorized receiver to decrypts information. This process enhances the confidentiality of the data.

5.2.4 Performance analysis of DDR

Performance ofSATGFRCA,[1], [2]of DDR is estimated. It measures effectiveness and reliability of a system in delivering data packets from the source to the intended destination.

Table IV DDR

Number of data samples	DDR(%)		
	SATGFRCA	Enhanced Ghost_BiNet	Lightweight authentication protocol
10000	96.25	92.65	91.36
20000	97.11	93.65	90.45
30000	96.84	92.33	90.01
40000	95.05	93.31	90.33
50000	96.33	93	91.45
60000	95.74	93.32	91.22
70000	96.22	92.36	90.45
80000	96.37	93.05	89.46
90000	95.65	92.56	90.04
100000	96.03	93.58	90.41

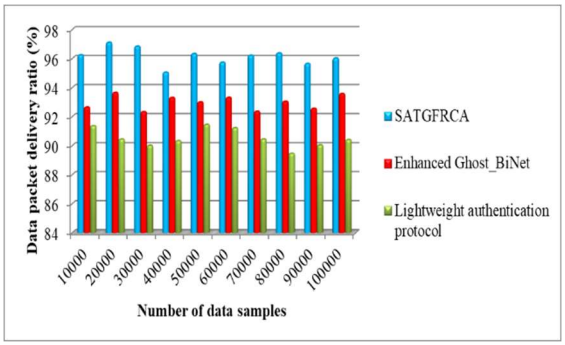

Figure 7 Graphical illustration of DDR

DDR illustrated in Figure 7. Number of data samples taken ranged from 10000 to 100000. Three methods were evaluated namely SATGFRCA technique and two existing methods Enhanced Ghost_BiNet [1], lightweight authentication protocol [2] to evaluate Data packet delivery ratio during data transmission. The horizontal axis represents the data sample count, while the vertical axis indicates data packet delivery ratio performance. The experimental findings reveal that the SATGFRCA technique consistently achieved superior performance compared to the other two approaches. For example, with 10000 samples from the dataset, the SATGFRCA techniquerecorded a delivery ratio of 96.25%, outperforming [1] and [2], which achieved Data packet delivery ratio of 92.65% and91.36%, respectively. A range of data packet delivery results were observed for all three methods with varying data sampled, enabling a complete comparison. The overall analysis indicates that the SATGFRCA techniqueimproved data packet delivery ratio by 3% over [1] and 6% over [2] in accurately performing the data transmission between sender and receiver. This enhanced performance is achieved through the use of the Benaloh Public Key Homomorphic Cryptosystem, which maximizes the confidentiality of the data samples at the receiver. Furthermore, the authentication process of the SATGFRCA technique eliminates attackers, ensuring that the data samples are delivered only to the authorized node, thereby enhancing data delivery.

6. CONCLUSION

Implementing advanced Intrusion Detection Systems (IDS), such as the SATGFRCA technique, enables effective monitoring of network traffic and identification of malicious activities within wireless networks. The Benaloh Public Key Homomorphic Cryptosystem is employed in the SATGFRCA technique to enhance data confidentiality in Personal Area Networks**)**. Encryption used in this cryptosystem. The data preserved during transmission.Additionally, the SATGFRCA technique utilizes a generalized functional regression function to verify the authenticity of nodes, thereby improving security levels and data confidentiality. By simulation, SATGFRCA performance validated, comparing it with conventional methods using various metrics. Outcome of SATGFRCA significantly outperforms traditional methods, demonstrating notable improvements in accuracy, data confidentiality, and data delivery ratio. Furthermore, the SATGFRCA technique reduces authentication time compared to conventional approaches.

REFERENCES

[1] Om Kumar Chandra Umakantham, Sudhakaran Gajendran, Suguna Marappan, "Enhancing Intrusion Detection Through Federated Learning With Enhanced Ghost_BiNet and Homomorphic Encryption", IEEE Access, Volume 12, 2024, Pages 24879 – 24893. DOI: 10.1109/ACCESS. 2024.3362347

[2] Vincent Omollo Nyangaresi, Ganesh Keshaorao Yenurkar, "Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor network", High-Confidence Computing, Elsevier, Volume 4, Issue 2, 2024, Pages 1-14. https:// doi.org/10.1016/j.hcc.2023. 100178

[3] Catarina Silva, Vitor A. Cunha, João P. Barraca & Rui L. Aguiar, "Analysis of the Cryptographic Algorithms in IoT Communications", Information Systems Frontiers, Springer, Volume 26, 2024, Pages 1243–1260. https://doi.org/10. 1007/s10796-023-10383-9

[4] Viral H. Panchal, Bhavesh K. Patel, and Nikita V. Panchal, "An Efficient Security Enhancement in Wireless Technologies for IoT with Hybrid Approach", International Journal of Future Computer and Communication, Volume 13, Issue 1, 2024, Pages 1-5.DOI: 10.18178/ijfcc.2024. 13.1.610

[5] Ranjith J, Mahantesh K, Abhilash C N, "LW-PWECC: Cryptographic Framework of Attack Detection and Secure Data Transmission in IoT", Journal of Robotics and Control (JRC),Volume 5, Issue 1, 2024, Pages 228-238.DOI: 10.18196/jrc.v5i1.20514

[6] Limin Zhang & Li Wang, "A hybrid encryption approach for efficient and secure data transmission in IoT devices", Journal of Engineering and Applied Science, Springer, Volume 71, 2024, Pages 1-18.https://doi.org/10.1186/s44147-024-00459-x

[7] Abdulmohsen Almalawi, Shabbir Hassan, Adil Fahad & Asif Irshad Khan, "A Hybrid Cryptographic Mechanism for Secure Data Transmission in Edge AI Networks", International Journal of Computational Intelligence Systems, Springer, Volume 17, 2024, Pages 1-15.https://doi.org/10.1007/s44196-024-00417-8

[8] P. Sathishkumar, A. Gnanabaskaran , M. Saradha , R. Gopinath, "Dos attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network", Ain Shams Engineering Journal, Elsevier, Volume 15, Issue 12, 2024, Pages 1-16.https://doi.org/10. 1016/j.asej.2024.103052

[9] Jianping Yu, Hang Yao, Kai Ouyang, Xiaojun Cao, Lianming Zhang, "BPS-FL: Blockchain-Based Privacy-Preserving and Secure Federated Learning", Big Data Mining and Analytics, Volume 8, Issue 1, 2025, Pages 189 – 213. DOI: 10.26599/BDMA.2024.9020053

[10] Oscar Fontenla-Romero, Bertha Guijarro-Berdiñas, Elena Hernández Pereira, Beatriz Pérez-Sánchez, "FedHEONN: Federated and homomorphically encrypted learning method for one-layer neural networks", Future Generation Computer Systems, Elsevier, Volume 149, 2023, Pages 200-211. https://doi.org/10.1016/j.future.2023.07.018

[11] Marco Arazzi, Serena Nicolazzo, Antonino Nocera, "A Fully Privacy-Preserving Solution for Anomaly Detection in IoT using Federated Learning and Homomorphic Encryption", Information Systems Frontier, Springer, 2023, Pages 1-24. https://doi.org/10.1007/s10796-023-10443-0

[12] S. Remya, Manu J. Pillai, C. Arjun, Somula Ramasubbareddy and Yongyun Cho, "Enhancing Security in LLNs Using a Hybrid Trust-Based Intrusion Detection System for RPL", IEEE Access, Volume 12, April 2024, Pages 58836 – 58850.DOI: 10.1109/ACCESS. 2024.3391918

[13] Aryan Mohammadi Pasikhan, John A. Clark and Prosanta Gope, "Incremental hybrid intrusion detection for 6LoWPAN",Computers & Security, Elsevier, Volume 135, December 2023, Pages 1-15. https://doi.org/10.1016/j.cose.2023.103447

[14] Yaser Alhasawi and Salem Alghamdi, "Federated Learning for Decentralized DDoS Attack Detection in IoT Networks", IEEE Access, Volume 12, 2024, Pages 42357 – 42368. DOI: 10.1109/ACCESS.2024.3378727

[15] Shalini Dhar, Ashish Khare, Ashutosh Dhar Dwivedi, Rajani Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography", Internet of Things, Elsevier, Volume 25, 2024, Pages 1-16.https://doi.org/10.1016/j.iot.2023.101019

[16] Min Li, "Application of GAN-Based Data Encryption Technology in Computer Communication System", Informatica, Volume 48, 2024, Pages 17–34. https://doi.org/10.31449/inf.v48i15.6390

[17] VanlalruataHnamte, Jamal Hussain, "Enhancing security in Software-Defined Networks: An approach to efficient ARP spoofing attacks detection and mitigation", Telematics and Informatics Reports, Elsevier, Volume 14, June 2024, Pages 1-19.https://doi.org/10.1016/j.teler.2024.100129

[18]Sanjit Kumar Dash, Sweta Dash, Satyajit Mahapatra, Sachi Nandan Mohanty, M. Ijaz Kha, Mohamed Medani, Sherzod Abdullaev, Manish Gupta, "Enhancing DDoS attack detection in IoT using PCA", Egyptian Informatics Journal, Elsevier, Volume 25, 2024, Pages 1-10. https://doi.org/10.1016/ j.eij.2024.100450

[19]Vu Tuan Truong and Long Bao Le, "MetaCIDS: Privacy-Preserving Collaborative Intrusion Detection for Metaverse based on Blockchain and Online Federated Learning", IEEE Open Journal of the Computer Society , Volume 4, 2023, Pages 253 – 266. DOI: 10.1109/OJCS.2023.3312299

[20]Esra Altulaihan, Mohammed Amin Almaiah and Ahmed Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms", Sensors, Volume 24, Issue 2, 2024, Pages 1-30.https://doi.org/10.3390/ s24020713

[21]Edosa Osa, Patience E. Orukpe, UsiholoIruansi, "Design and implementation of a deep neural network approach for intrusion detection systems", e-Prime - Advances in Electrical Engineering, Electronics and Energy, Elsevier, Volume 7, 2024, Pages 1-6. https://doi.org/10. 1016/j.prime.2024.100434

[22]Furqan Rustam, Ali Raza, Muhammad Qasim, Sarath Kumar Posa, Anca Delia Jurcut, "A Novel Approach for Real-Time Server-Based Attack Detection Using Meta-Learning", IEEE Access, Volume 12, 2024, Pages 39614 – 39627. DOI: 10.1109/ACCESS.2024.3375878

[23]Akane Kosugi, Kaoru Teranishi, Kiminao Kogiso, "Experimental Validation of the Attack-Detection Capability of Encrypted Control Systems Using Man-in-the-Middle Attacks", IEEE Access ,Volume 12, 2024, Pages 10535 – 10547. DOI: 10.1109/ACCESS. 2024.3353289

[24]P Senthilraja, P Nancy, J Sherine Glory & G Manisha, "Enhancing IoT security in wireless local area networks through dynamic vulnerability scanning", Sādhanā, Springer, Volume 49, 2024, Pages 1-19.https://doi.org/ 10.1007/s12046-024-02534-8

[25]Putra Wanda & Marselina Endah Hiswati, "Belief-DDoS: stepping up DDoS attack detection model using DBN algorithm", International Journal of Information Technology, Springer, Volume 16, 2024, Pages 271–278. https://doi.org/10.1007/s41870-023-01631-x

[26]David Samuel Bhatti, Shahzad Saleem, Heung-No Lee & Ki-Il Kim, "A dynamic symmetric key generation at wireless link layer: information-theoretic perspectives", EURASIP Journal on Wireless Communications and Networking, Springer, volume 2024, 2024, Pages 1-39.https://doi.org/10.1186/s13638-024-02396-y

[27]Ajay Kaushik & Hamed Al-Raweshidy, "A novel intrusion detection system for internet of things devices and data", Wireless Networks, Springer, Volume 30, 2024, Pages 285–294.https://doi.org/10.1007/s11276-023-03435-0

[28]Estabraq Saleem Abduljabbar Alars& Sefer Kurnaz, "Enhancing network intrusion detection systems with combined network and host traffic features using deep learning: deep learning and IoT perspective", Discover Computing, Springer, Volume 27, 2024, Pages 1-19.https://doi.org/10.1007/s10791-024-09480-3

[29]Manesh Thankappan, Helena Rifà-Pous & Carles Garrigues, "A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks", International Journal of Information Security, Springer, Volume 23, 2024, Pages 3527–3546. https://doi.org/10.1007/s10207-024-00899-9

[30]Bhanu Priyanka Valluri, Nitin Sharma, "Exceptional key based node validation for secure data transmission using asymmetric cryptography in wireless sensor networks", Measurement: Sensors, Elsevier, Volume 33, June 2024, Pages 1-11.https://doi.org/10.1016/ j.measen.2024.101150