SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I10P121

Volume 11 Issue 10, 258-265, October 2024

Original Article

An Efficient Authentication for IoT Devices Using Fuzzy Trust Privacy-Preserving Scheme

T. Yuvarani[1], A. R. Arunachalam[2]

[1,2]*Department of Computer Science and Engineering, Dr. M.G.R. Educational and Research Institute, Tamilnadu, India.*

[1]*Corresponding Author : yuvarani.2182@gmail.com*

Received: 21 August 2024 Revised: 22 September 2024 Accepted: 21 October 2024 Published: 30 October 2024

Abstract *- The Internet of Things (IoT) improves everyday life by expanding interactions among gadgets. The spike in the assortment of gadgets connected exposes network infrastructure to a variety of dangers. IoT is widely used in the retail, business, manufacturing, construction and defence sectors. Concerns about protecting information and authentication of identities are becoming more and more important as applications for the IoT proliferate. The researchers faced additional challenges in implementing security systems in IoT networks due to resource constraints on sensor nodes. To help prevent such assaults, some expensive Privacy-Preserving (PP) techniques have been used in past research. To manage resource usage alongside information security problems, a unique Fuzzy Trust Privacy-Preserving Scheme (FTPPS) is presented for the IoT context. When the packet length exceeds 400, and the overall number of repetitions is 100, then the suggested FTPPS takes less than 1 second to execute. The recommended FTPPS approach achieves 98 percent trust. Safety and reliability studies demonstrate that our suggested approach is not only resistant to a variety of assaults but also extremely effective with respect to computational efficiency.*

Keywords *- Authentication, IoT, Privacy-preserving, Fuzzy trust, Attacks.*

1. Introduction

The infrastructure that makes it possible for ordinary items in our surroundings to be connected to networks and have the capacity to transmit and receive information is known as the IoT. The power supply, storage, and processing capacities of devices in IoT systems are typically restricted. Furthermore, the fact that IoT devices are frequently used in open and unsecured spaces puts them at risk of both physical and virtual assaults. Hence, it's critical that any safety mechanism created for IoT devices be both effective and able to identify any breaches of the devices' physical safety. Authentication techniques that rely solely on a shared secret, such as password-based or hidden-key-based strategies, are inadequate to tackle security issues in these cases.

Nevertheless, IoT is prone to various networking assaults, which can disrupt the data transfer process and consume more energy. The PP is obtained in IoT applications to ensure confidentiality when accessing sensitive information. The PP primarily contains cryptographic techniques for protecting data against anomalous activities [1]. Data access, session password transmission, encryption and decryption are all tracked [2]. This method's processing is as follows: if the user provides data, it is encrypted, and the recipient uses a confidential key for decoding the data. In addition, network coding technology has been incorporated into IoT to safeguard data privacy in situations where sensor data is split up into several generations. In fact, an identifier signs each of the numerous packets in any transmission. An internal or external adversary may introduce bogus or altered packets into the data flow through the process of network mixing, which is a feature of the network coding, increasing the information flow's susceptibility to contamination threats and making it impossible for IoT devices to distinguish between accurate and reliable data. Currently, two main types of technology are used to counteract pollution assaults in network coding: schemes based on information theory and schemes based on cryptography. The information theory system primarily avoids contamination attacks by identifying and fixing contaminated packets at the sink node.

Regarding efficiency, information theory methodologies cannot cause intermediary nodes to filter out bogus messages. Hence, they can only passively approve the sink node contamination attacks. Another remedy to the issue of contamination assaults is a validation technique based on passwords, which allows transmitters to validate the reliability of sequences received during transit. This approach allows intermediary nodes to detect and delete bogus packets during distribution, effectively reducing contamination assaults at the source [3]. In recent years, several research has represented nonlinear structures as trust-based fuzzy systems characterized by spatially linear time-invariable networks linked by if-then rules. As a result, trust-based fuzzy systems have received increasing attention. Contrary to prior research, we offer a fuzzy-based trusted grading mechanism for defence against rebellious IoT devices while developing an energy-efficient PP infrastructure. The fuzzy trust evaluation model considers the restricted bandwidth and power usage. Assuming IoT maintains adequate stability, our fuzzy-based trust

model can produce an enhanced credibility evaluation value. Thus, we presented a novel approach termed Effective PP and Fuzzy based trustworthiness for securely authenticating IoT devices in order to improve confidentiality and trustworthiness as well as to minimize computing complexity.

Below is a list of our work's contributions.

- In order to counteract contamination assaults, we first proposed an innovative PP scheme based on a fuzzy-based trust model, where the security is proven based on the periodic logarithm's hardness.
- Secondly, we establish the reliability of our PP-based fuzzy trust scheme through strict numerical derivation.
- Lastly, confirm the suggested FTPPS performance by defining the criteria, such as accuracy, False Positive Rate (FPR), energy consumption, PP operating time, and trustworthiness.

2. Literature Review

In order to protect against pollution attacks, Laiche ng Cao and Min Zhu [4] used a T-S fuzzy trust theory and coded networks to direct information flows in an ideal clustering established by a specified recurring game concept. Next, demonstrate that, under data security conditions, the suggested concept exhibits a refined Nash equilibrium state and can increase the efficacy of resource usage. Consequently, compared to earlier research, this approach has a higher time and energy efficiency. An innovative authorization of users on a two-factor basis for permitting IoT medical environments in quantum-resistant processing contexts is presented by Al-saggaf et al. [5]. Additionally, the efficiency and safety of the suggested procedures are examined, demonstrating that they satisfy requirements for memoryless simplicity, confidentiality for users, shared authentication, and durability against attacks involving stolen smart cards, biometric template tampering, and resistance to privileged interior assaults. Estimates are made for the expenses of computing, storage and communicating requirements. The suggested protocol uses these computations to provide various important functionality and security aspects; hence, there is a natural increase in the overhead of our computational expenses. A unique technique to guarantee security and authentication in the VANET was presented by Jyothi and Patil [6]. By reducing computing complexity, the suggested solution improves the reliability of the VANET system.

Furthermore, fuzzy has been used to assess the reliability. According to the experimental research, the suggested solution offers 94% reliability and significantly reduces both time consumption and communication overhead. PP decision-making is presented for the data-sharing strategy by Almagrabi and Bashir [7]. By enhancing data sharing security without affecting communicating users through resource replication, this scheme is in charge. This technique uses categorization learning to autonomously identify replicas and access resources allocated to them. This classification is carried out repeatedly to increase the dependability of information sharing, which centres on the credibility level of the accessible resources. The Improved Two Factor Fuzzy Commitment method (ITFFCS), is an enhanced method for fuzzy commitment over IoT devices. It makes use of two different types of noisy factors that are present both within and outside of IoT devices. Even if an intruder has successfully gained access to an internal noise source through IoT devices, they are unable to precisely choose a key from the data that is available since the modules are similar. With an average of 0.18% and 0.28% in FAR and FRR, the suggested ITFFCS- Physical Unclonable Function (PUF) performs comparably better than the current approach.

In order to improve system security and privacy, Guo et al. [8] proposed a simple verification method that adds the PUF as the final element. Our approach is specifically developed to combat attacks such as wireless sensor node theft and digital card stealing by integrating PUF technology into sensors' integrated circuit chips and servers. In terms of computational costs, communication costs, storage costs and security needs, this approach performs better than current protocols. An effective, safe, and PP message authentication system for the IoT is presented by Wei et al. [9]. This work is more flexible and effective than the previous solutions since it enables connected devices with various encrypted setups and allows online/offline processing. PUFs are considered one of the authentication elements in Prosanta et al.'s [10] compact and PP dual-factor authorization approach for the IoT. In IoT contexts, Li et al. [11] presented three basic factors for the anonymity user verification approach that used flexible commitment to process customer biometric details. A Hyperledger Fabric architecture and identity authentication were created by Chi et al. [12] to enable safe data sharing in the IoT context. Powered by block chain sharing of information and public key infrastructure was suggested by Srivastava et al. [13] to address a number of IoT security needs, including sharing credentials, session password creation and defence from varied assaults. An enhanced identity-based signatory verification along with the safe exchange of data approach that guarantees information reliability, integrity, and secrecy is proposed by Fan et al. [14] for the IoT. According to a performance study, our system is probably safe, and when compared to Hong et al. [15], it cuts calculation costs by 15.34% and communication costs by 40.68%. A novel Message Authentication Protocol (MAP) created especially for IoT gadgets is presented by Anvesh Kumar and Bapuji [16], addressing the twin concerns of protecting user privacy and guaranteeing data integrity. It works computationally more efficiently than current systems and offers a strong defence against a range of frequent assaults, including replay attacks and message manipulation. In order to demonstrate how the design of the former block functions in an actual event, Nouredine Tamani and Yacine Ghamri-Doudane [17] first introduce a general methodology for users' habitual training as the foundation to detect anomalies. This algorithm is then implemented by inductive fuzzy set theory. The discussion of PP Data Aggregation strategies by Ali et al. [18] compares their effectiveness in helping researchers determine where to focus their efforts

while creating new PP techniques for the IoT with limited resources. This paper also offers a breakdown of every mathematical operation used in the various PP schemes.

3. Research Methodology

For effective sharing of resources between the user who requested them and the services in IoT applications, privacy is crucial. Mining data is seen to reduce difficult queries safely from the vast data set. In IoT applications, the PP is acquired to give privacy access to sensitive data. Cryptography techniques are mostly used in PP measures to safeguard data against unauthorized access. Data access and session key sharing are seen during encryption and decryption. This method's processing involves the user sending encrypted data, which is then decrypted by the recipient using the recipient's private key. Our suggested approach uses the FTPPS to analyze the computing and communication costs of the IoT device. Fuzzy analysis, which yields information regarding trustworthiness, can be used to analyze mutual authentication. Figure 1 displays the FTPPS flow diagram.

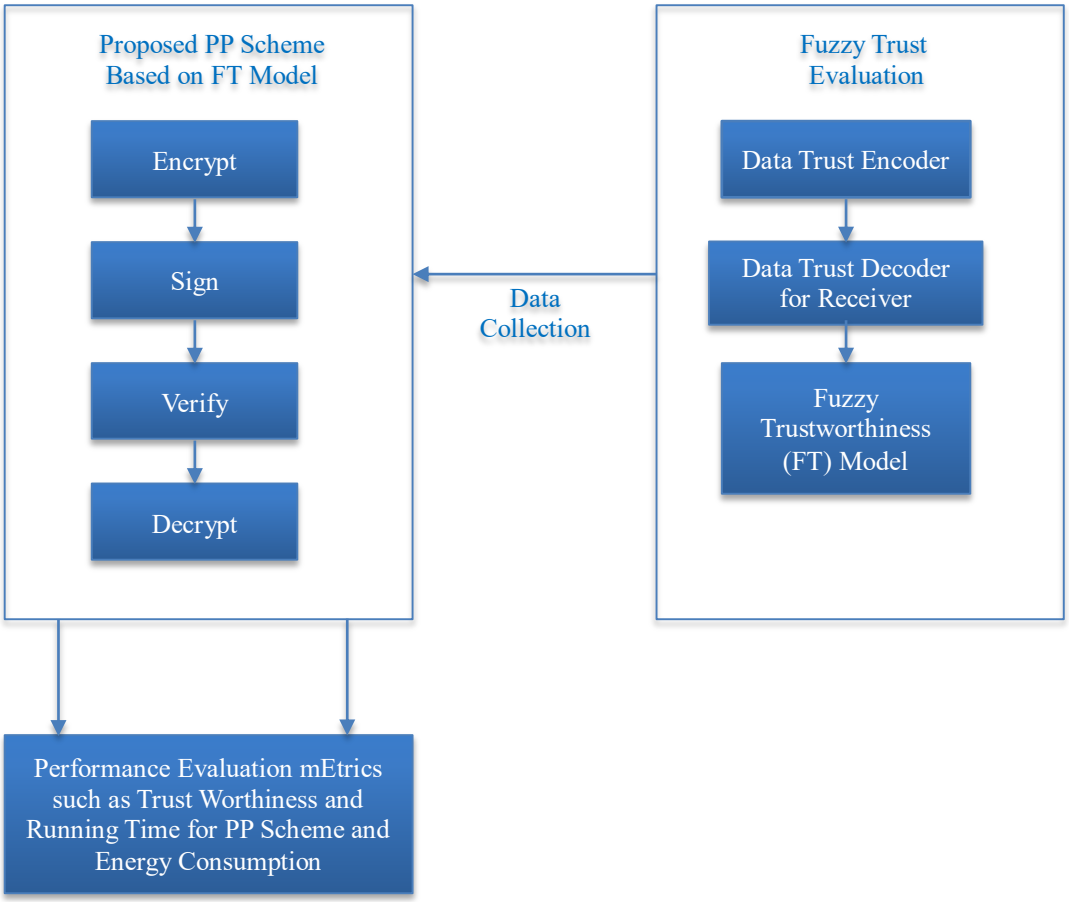

Fig. 1 The overall flow diagram of the proposed methodology

3.1. Network Model

This study examines a linear network coding approach that enables the IoT by having an IoT-connected gadget deliver a series of sequential instructions to several recipients. Each of the 'm' generations of transmitted messages can be thought of as a vector having N no of dimensions over the finite field f_p. Here, the prime number, p, is predetermined. In the meantime, there are M native messages in every generation.

Maintaining generality without reducing, an ρ-bit binary string is used to identify the i-th generation $Id_i \in \{0,1\}^{\rho}$, where $i \in \{1 \ldots m\}$ and $\rho \geq [log_2^m]$. Let $\Gamma = \{Id_{1,\ldots\ldots,} Id_m\}$ symbolize the collection of generational identifiers. Next, the collection of traditional messages from the i-th generation is defined as $\{D_{i,1,\ldots\ldots,} D_{i,M}\}$ in Equation (1).

$$D_{i,j} = (D_{i,j}^{(1)}, \ldots, D_{i,j}^{(n)}) \in f_p^n, j \in \{1, \ldots\ldots, M\} \quad (1)$$

The trust T between IoT gadgets is taken into account in this network architecture. The trust value generated in the previous exchange of information round is used to pick the reliable networking device in the subsequent round of information exchange.

3.2. Security Model

Consider a set of IoT devices D = {D_1, D_2, D_n} that communicate with the trustworthy server S of the data and control unit. The server executes a setup algorithm Setup(1^k)

for enrolling into a trusted environment, and a public parameter and secret key are generated for initialization.

In the model, IoT nodes U can execute the protocol repeatedly with BS V. We denote instance s of U (resp. V) by Π_U^s (resp. Π_U^s) for $s \in$ N, which models distinct executions of the protocol. The public parameters $params$ and identities ID = $\{ID_U, ID_v\}$ are also public.

3.3. Threats Model

The Probabilistic Polynomial Time (PPT) adversary *A* is allowed to control all communications in the network through access to a set of oracle queries as follows. The attack process is modelled through the Oracle queries and answers back to *A*. Extract, Execute, Send, Reveal, Corrupt, and test are the queries for ID-based authentication and key exchange protocol.

3.4. Data Trust Encoder

Concerning the j-th native messaging $D_{i,j}$ in the *i*-th generations, a unit vector in t dimensions represents p_j, with the *j*-th item being the measured reliability $T_{i,j}$for 0 is attached to the native messaging for IoT devices. The corresponding enhanced block $c_{i,j}$is then provided as follows in Equation (2).

$$c_{i,j} = (p_j, D_{i,j}) \tag{2}$$

The matching encrypted block is provided by the bi-linear map polynomial-time technique is given in Equation (3).

$$E_{i,j} = encrpt\ (h, Id_i\ , c_{i,j}) \tag{3}$$

When the total count of IoT devices is expressed by Id_i, and h is the variable in the Bi-linear chart dividing distinct progressive cyclical groups.

3.5. Data Trust Decoder for Receiver

The information block is initially decoded and saved in the buffer by the network controller upon receiving the encoded data. Gaussian elimination allows the network controller to retrieve the native message after acquiring *m* non-linearly coupled information blocks. Subsequently, the sender will receive an acknowledgement message to verify the successful transmission of the subsequent batch of messages.

3.6. Fuzzy Trustworthiness (FT) Model

The data-PP model between IoT devices is presented here. Nonetheless, we must also take data transfer routing security concerns into account. In order to protect against malevolent nodes in the IoT, Li et al. [19] investigated the reliability relaying model rather than the conventional encrypted approach due to the advancement of trust-evaluating technologies in safe routing. The level of trustworthiness amongst IoT devices is typically difficult and changeable in real-world applications. We logically presume a trust-based fuzzy model in this part to reduce the impact of personal aspects on the assessment of trust.

In Definition 1, $A = \{a_1, a_2, \ldots, a_n\}$ is a group of IoT. In order to objectively characterize the trustworthiness of IoT devices, we selected the communication trust T_c and the energy trust T_e as the fuzzy characters z_k. Then, the vector $v\ (x_{ij}) = v_{ji} = (\mu_{1i}\ , \mu_{2i}\ , \ldots\ , \mu_{mi})$ is created by taking into account each competitor's membership degree for these limited fuzzy characteristics z_k is employed as the vector for the trust evaluation of $\mu_{ji} \in [0, 1]$, (j = 1, 2, . . ., l) for x_i , while v_{ji} is the trust vector of node j to node i for evaluation, and μ_{ki}(k = 1, 2, . . ., m) is the degree of node membership i (x_i) to node j evaluates the fuzzy parameter z_k. Finally, the fuzzy rule definition is provided as follows:

3.7. The Proposed PP Scheme Based on the Fuzzy Trustworthiness (FT) Model

We present the foundation of our PP plan in this section. In this case, energy consumption, defence attack capabilities, and other metrics are examples of network performance indicators.

As a result, IoT data may be delivered reliably and with minimal energy usage. The following section presents a PP method based on the fuzzy trust model to defend against attacks compromising data privacy when encrypting IoT networks. First, four steps constitute the overall strategy. Detailed steps are as follows:

3.7.1. Registration Phase

When an IoT node joins the IoT networks, it transmits unique identifiers ID_{IoT} and other secret identity information for registration. After verifying the validity of the IoT node, the trust set T generates the IoT node's private key.

- Encrypt (h, T, Id_i c) Definition 1 states that the trust set T consists of 0 and 1. Coding data is received when the trustworthiness of IoT devices is 1. After that, a sequence of t-bit binary strings denoted as $\{ s_j \}_{j=1}^{t}$, are produced as the source. To create the encryption matrix, a keyed pseudo-random function *f:* {0, 1} * {0, 1} * K $\rightarrow f_p$ is used.

  Therefore, Equation (4) as follows,

  $$E_{i,j} = Encrypt\ (h, T, Id_i, c_{i,j}) = (E_{c,T} D_{i,j}) \tag{4}$$

- Sign (k, Id_i, c). Consider a full-domain encrypted algorithm.

  H: {0, 1} * $\rightarrow$ f_p as a random oracle. The source C signature is provided by

  Where *sk* represents the signature key such that *sk* = $\{sk_1, \ldots.., sk_{t+n+1}\}$, $sk_i \overset{R}{\leftarrow} f_p$. Then, the data blocks $\{ c_i \}_{i-1}^{\sigma}$ and $\{ \Delta_i \}_{i-1}^{\sigma}$ of the *i*-th generation are combined as follows in Equation (5).

  $$\Theta_i = \left(\sum_{i=1}^{\sigma} T_i c_i, \prod_{i=1}^{\sigma} \Delta^{T_i\ ,\ Id_i} \right) \tag{5}$$

3.7.2. Authentication Phase

When an IoT node enters a domain covered by a BS1 for the first time, it generates a signature using its private key.

- Verify (pk, c, Id_i, Δ). When the pk represents public key, Id_i represents generation, c represents a data block, and the Δ represents signature; the compared computation is given by Equation (6).

$$\eta_1 = e(\Delta, o) \quad (6)$$

Where o denotes G's generator.

- Decrypt (h, T, Id_i, c). Given the pseudo-random function f and the secret key k, the decoding vector can be calculated as $DE_{c,T}$

3.7.3. Data Transmission Phase

Before an IoT node requests a specific application service, it provides the necessary attributes and information to an IoT node. Then, a token is generated by the application supplier, which allows the IoT node to get a symmetric key K for the specific service.

4. Results and Discussion

This section discusses the suggested FTPPS's IoT performance. The Contiki Cooja Simulator simulates the experimental setting for evaluating performance. Contiki is a lightweight, event-based platform for IoT. In the above simulation, node identification is done using Rime addresses from Contiki. Rime addresses can be either 2 or 8 bytes by default. Given the compact size of our clusters, 2-byte addresses should be adequate. In this scenario, 60 IoT gadgets are randomly deployed and connected to 12 infrastructural modules to build a networking framework that includes malicious activities and quantifies the credibility of each IoT device. Furthermore, our proposed technique utilized fuzzy to assess trustworthiness and maintain the link between trust T and IoT devices while attempting to evade the attackers. In order to analyze the efficiency of the suggested FTPPS, we establish metrics in the simulation parameter setup, such as accuracy, consumption of energy, PP scheme operating time, trustworthiness, and FPR. The proposed plan is added to the current NCS0 scheme, NCS1 scheme, and ID-based scheme for statistical comparison.

4.1. Measurement of Trustworthiness

Our major technique is to assess the trustworthiness of messages accepted and disseminated. It is a crucial component to analyze for optimum interaction among IoT devices. Each IoT device's level of trust is defined by its direct trust T_{direct} and indirect trust $T_{indirect}$. Following is a definition of total trust:

$$T_{total} = \lambda_1 T_{direct} + \lambda_2 T_{indirect}$$

Where $\lambda 1 + \lambda 2 = 1$ is satisfied by the weight variables of direct and indirect trust, $\lambda 1$ and $\lambda 2$. The method used to evaluate trust, which includes direct and indirect trust, is possibly explained in [20].

Figure 2 shows that the proposed FTPPS approach assures 98% trust, while the NCS0 system gives 82%, NCS1 offers 68%, and the ID-based strategy allows for 80% trustworthiness.

4.2. Running Time of the Proposed FTPPS Method

The operating time of the FTPPS indicates the success of our scheme, which can operate more rapidly than earlier schemes [21, 22] despite fulfilling the need for data privacy. In Figure 3, our suggested FTPPS approach has the least runtime when weighed against the other three approaches. Furthermore, based on the extent of the running time shift, our approach exhibits greater stability.

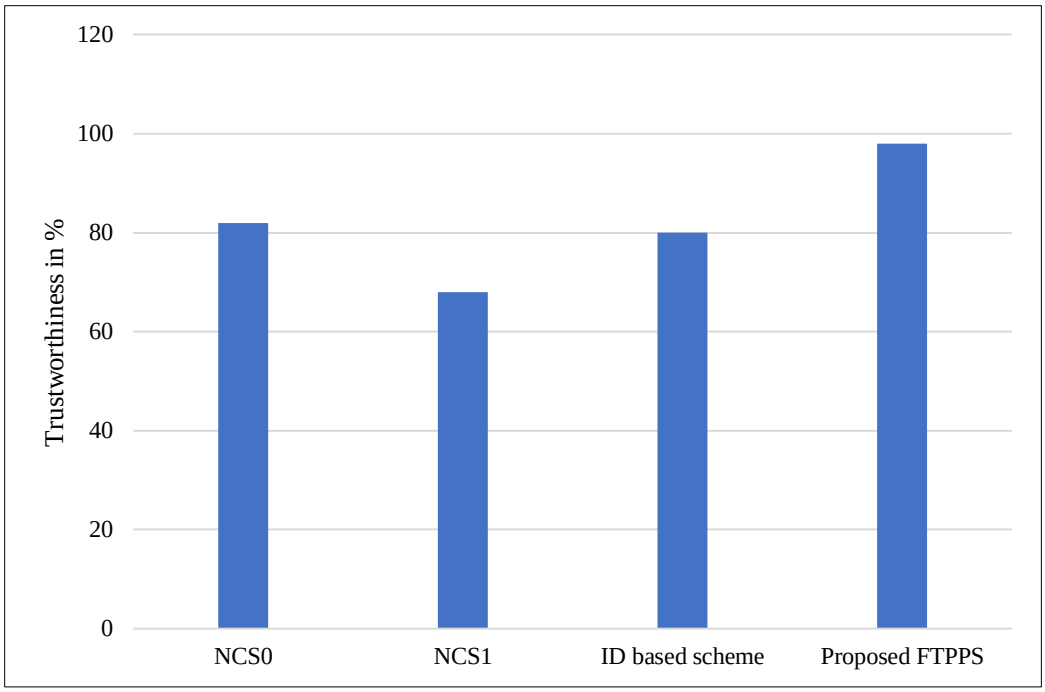

Fig. 2 Evaluation of trustworthiness for various schemes

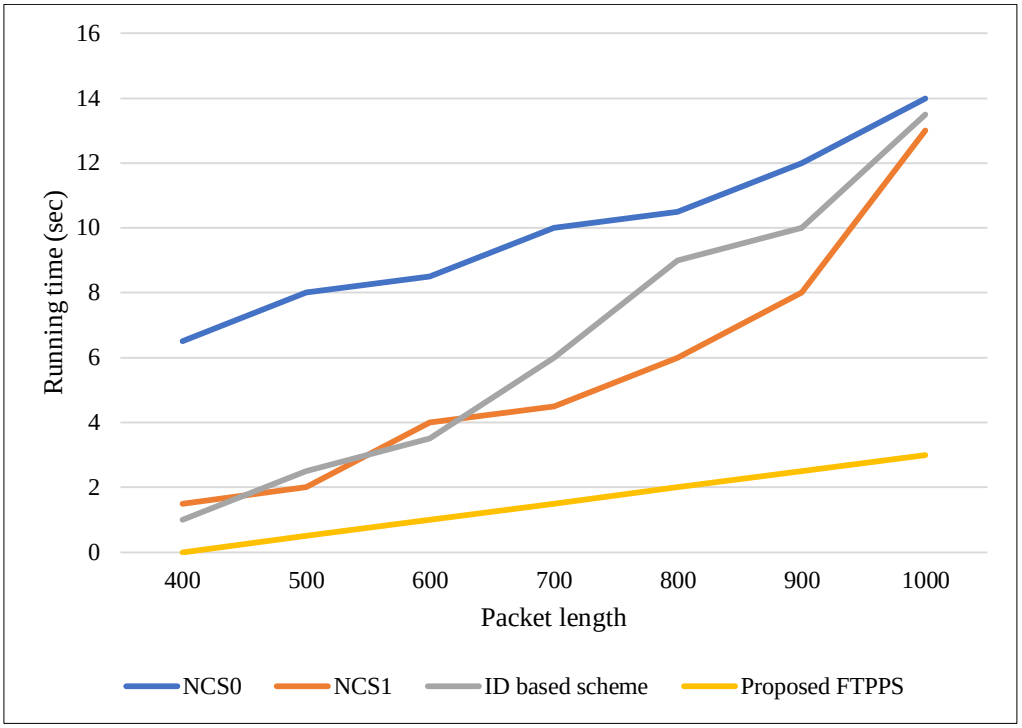

Fig. 3 Running time against packet length

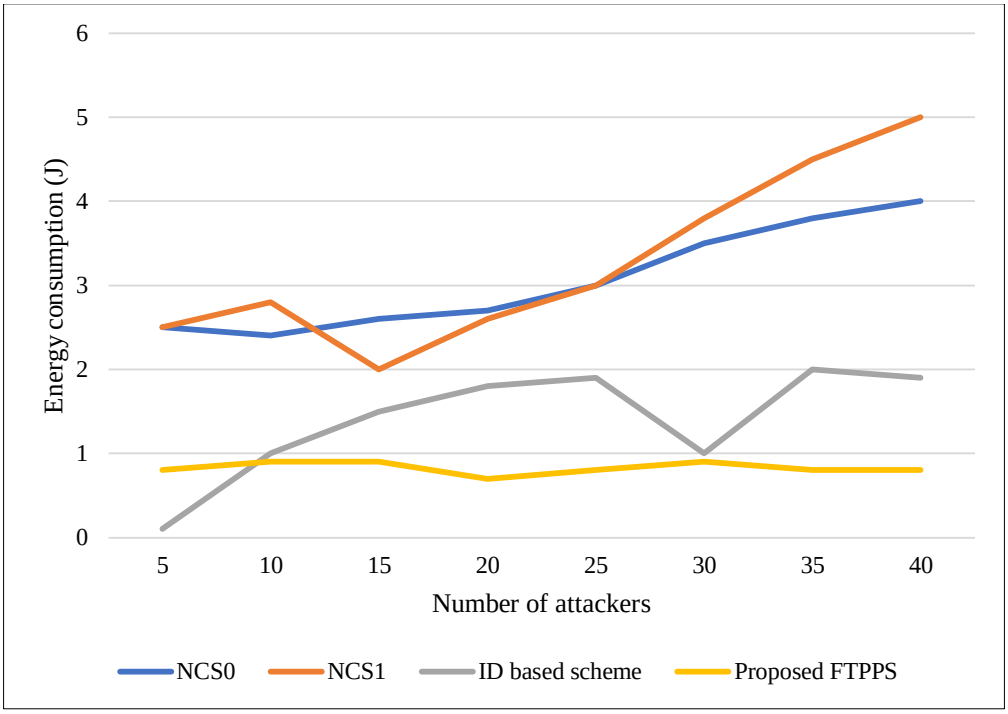

Fig. 4 Energy consumption

4.3. Energy Consumption

Figure 4 compares FTPPS energy usage to the NCS0-, NCS1-, and ID-based approaches. The simulation's outcome demonstrates that our approach uses the least amount of energy. The energy needed for trust analysis progressively escalates as the number of attack points in the IoT rises. Yet, the energy usage of our approach has remained consistent, with no considerable growth. At this point, when the iteration is set to 30-100, our approach has the most leftover energy than any other method.

4.4. Accuracy and FPR

System functionality in an IoT environment is greatly impacted by the ability to obtain necessary data quickly, safely, and effectively.

This is especially true for real-time applications. In this case, the percentage of all accurate findings and outcomes determines overall accuracy. It is calculated using the following standardized formula:

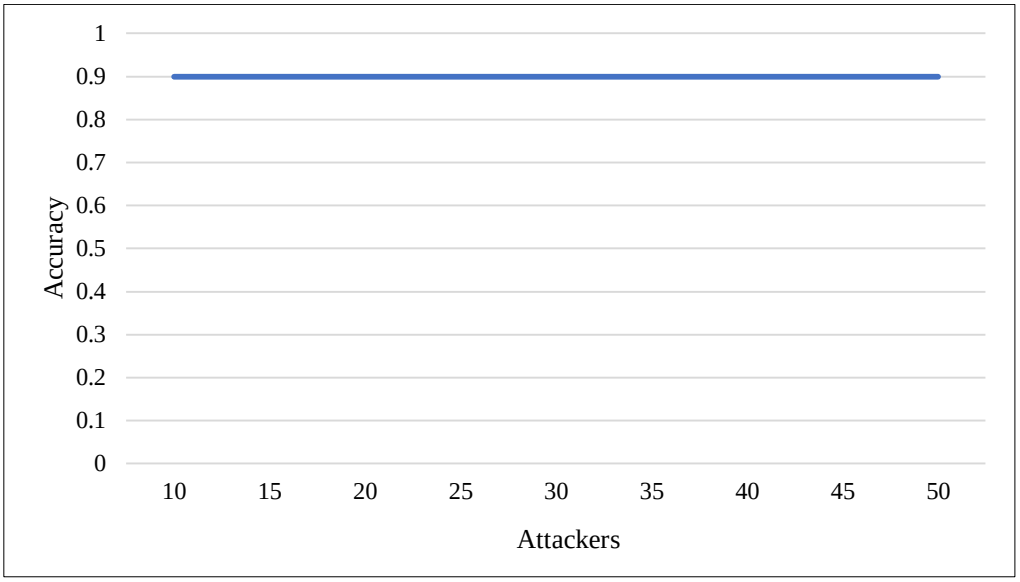

Fig. 5 Overall accuracy

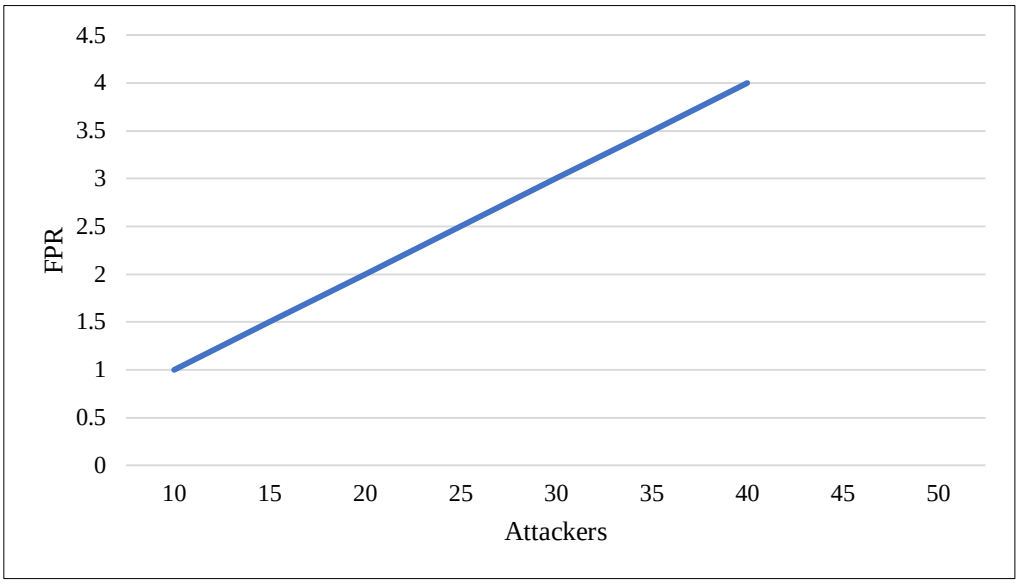

Fig. 6 FPR of proposed FTPPS

Figure 5 illustrates that our scheme's average accuracy under varying attackers' participation percentages is 89%.

4.4.1. FPR

In this study, the reliability of our technique in identifying fabricated communications is demonstrated through the application of FPR. It is calculated using the following standardized formula.

Where TN is a count of fake messages that our technique properly identified, and FP is the count of forged messages mistakenly identified as real communications. As illustrated in Figure 6, the varying proportions of hackers injecting fraudulent messages result in an average FPR of approximately 4%.

5. Conclusion

In order to protect IoT devices from threats while balancing data security and energy efficiency, this research examines a unique fuzzy-based PP scheme. IoT energy usage can be decreased by proposing a fuzzy trust evaluation technique in the place of existing cryptographic method. The trust-based PP method is subsequently provided, where the distinct logarithm's difficulty determines the level of security.

Additionally, fuzzy analysis has been used to assess the reliability. Based on the experimental research, the suggested strategy offers 98% reliability and significantly reduces the required time. With varying attacker percentages, our scheme's average accuracy is 90%. It may be inferred that, compared to alternative methods, our suggested strategy assures great security and minimizes all computing difficulties.

Hence, in our next study, we will take into account more types of strikes on IoT data and create more potent fuzzy methods based on PP.

References

[1] Alexander Yohan, and Nai-Wei Lo, "FOTB: A Secure Blockchain-Based Firmware Update Framework for IoT Environment," *International Journal of Information Security*, vol. 19, pp. 257-278, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] S.K. Sathya Lakshmi Preeth et al., "An Adaptive Fuzzy Rule Based Energy Efficient Clustering and Immune-Inspired Routing Protocol for WSN assisted IoT System," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-13, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[3] Peiying Zhang et al., "A Security and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems," *IEEE Transactions on Computational Social Systems*, vol. 9, no. 1, pp. 97-108, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[4] Laicheng Cao, and Min Zhu, "Fuzzy-Based Privacy-Preserving Scheme of Low Consumption and High Effectiveness for IoTs: A Repeated Game Model," *Sensors*, vol. 22, no. 15, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Alawi A. Al-saggaf et al., "Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing," *Arabian Journal for Science and Engineering*, vol. 48, pp. 2347-2357, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] N. Jyothi, and Rekha Patil, "A Fuzzy-Based Trust Evaluation Framework for Efficient Privacy Preservation and Secure Authentication in VANET," *Journal of Information and Telecommunication*, vol. 6, no. 3, pp. 270-288, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[7] Alaa Omran Almagrabi, and A.K. Bashir, "A Classification-Based Privacy-Preserving Decision-Making for Secure Data Sharing in IoT Assisted Applications," *Digital Communications and Networks*, vol. 8, no. 4, pp. 436-445, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ping Guo, Wenfeng Liang, and Shuilong Xu, "A Privacy Preserving Four-Factor Authentication Protocol for Internet of Medical Things," *Computers & Security*, vol. 137, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[9] Jiannan Wei, Tran Viet Xuan Phuong, and Guomin Yang, "An Efficient Privacy Preserving Message Authentication Scheme for Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 617-626, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Prosanta Gope, and Biplab Sikdar, "Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580-589, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Xiong Li et al., "A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments," *Journal of Network and Computer Applications*, vol. 104, pp. 194-204, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[12] Jiancheng Chi et al., "A Secure and Efficient Data Sharing Scheme based on Blockchain in Industrial Internet of Things," *Journal of Network and Computer Applications*, vol. 167, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Gautam Srivastava et al., "Data Sharing and Privacy for Patient IoT Devices using Blockchain," *Smart City and Informatization, Communications in Computer and Information Science*, pp. 334-348, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Qing Fan et al., "A Secure and Efficient Authentication and Data Sharing Scheme for Internet of Things based on Blockchain," *Journal of Systems Architecture*, vol. 117, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] Hanshu Hong, Bing Hu, and Zhixin Sun, "Toward Secure and Accountable Data Transmission in Narrow Band Internet of Things Based on Blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, pp. 1-10, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[16] Boddupalli Anvesh Kumar, and V. Bapuji, "Efficient Privacy Preserving Communication Protocol for IOT Applications," *Brazilian Journal of Development*, vol. 10, no. 1, pp. 402-419, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Nouredine Tamani, and Yacine Ghamri-Doudane, "Towards a User Privacy Preservation System for IoT Environments: A Habit-Based Approach," *2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE)*, Vancouver, BC, Canada, pp. 2425-2432, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[18] Inayat Ali, Eraj Khan, and Sonia Sabir, "Privacy-Preserving Data Aggregation in Resource-Constrained Sensor Nodes in Internet of Things: A Review," *Future Computing and Informatics Journal*, vol. 3, no. 1, pp. 41-50, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] Yuzhe Li, Ling Shi, and Tongwen Chen, "Detection Against Linear Deception Attacks on Multi-Sensor Remote State Estimation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 846-856, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[20] Chunyang Qi et al., "A Novel Privacy-Preserving Mobile-Coverage Scheme Based on Trustworthiness in HWSNs," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, pp. 1-11, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Dan Boneh et al., "Signing a Linear Subspace: Signature Schemes for Network Coding," *Proceedings of the International Workshop on Public Key Cryptography*, Irvine, CA, USA, pp. 68-87, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[22] Qun Lin et al., "An ID-Based Linearly Homomorphic Signature Scheme and its Application in Blockchain," *IEEE Access*, vol. 6, pp. 20632-20640, 2018. [CrossRef] [Google Scholar] [Publisher Link]