Framework for Optimizing Multiparty Computation for Secure Authentication in Internet-of-Things

Divya K.S[1] ,Dr.Roopashree H.R[2] ,Dr.Yogeesh A.C[3]

Research Scholar, GSSS Institute of Engineering and Technology for Women, Mysuru, India

Associate Professor, GSSS Institute of Engineering and Technology for Women, Mysuru, India.

Assistance Professor, Government Engineering College, Kushalnagar India.
divyaks.phd@gmail.com, roopashree16@gmail.com, yogeesh13@gmail.com

Abstract— With the rising demands of secure and efficient data transmission in presence of uncertain vulnerabilities residing in large network of Internet-of-Things, the evolution of multiparty-based authentication system is spontaneously increasing. Review of existing research methodology on same direction is carried out to find that there are still wide opportunities of improvement owing to various identified research issues associated with it. Hence, the proposed scheme presents a novel and secure computation scheme for multiparty-based authentication in order to promote higher degree of privacy while retaining ownership of intellectual property. The scheme performs this task by introducing primary and secondary optimization method which is meant for strengthening the encryption system by constructing a robust trapdoor function for secure validation of signature acting as proof of transaction towards non-repudiation. The benchmarked outcome shows that proposed scheme offers better performance in contrast to existing scheme.

Keywords- *Internet-of-Things, Multiparty Authentication, Privacy, Trapdoor Function, Proof of Transaction, Non-Repudiation*

I. INTRODUCTION

Multiparty authentication in the context of the Internet of Things (IoT) refers to a mechanism where multiple entities or parties participate in the authentication process to establish trust and ensure the secure communication between IoT devices [1][2]. It goes beyond the traditional two-party authentication, which typically involves a client and a server. In IoT scenarios, multiparty authentication becomes relevant when multiple devices or entities need to authenticate each other before sharing sensitive data or engaging in secure transactions [3]. Here are some key aspects of multiparty authentication in IoT are as follows. The first key aspect is multiparty authentication that involves more than two entities participating in the authentication process [4]. These entities can include IoT devices, gateways, cloud services, or other entities involved in the IoT ecosystem. Each entity verifies the identities of others before establishing trust. In multiparty authentication, mutual authentication is performed, meaning that each entity verifies the identity and authenticity of others involved in the communication [5]. It ensures that all parties involved can trust each other before engaging in data exchange or other interactions. Further, the authentication process in multiparty authentication aims to establish trust between the participating entities [6]. Trust can be established through various means, such as digital certificates, shared secrets, cryptographic protocols, or trusted third parties. The next important aspect is about secure key exchange [7]. Multiparty authentication often involves the exchange of cryptographic keys between the entities to ensure secure communication. Key exchange protocols, such as Diffie-Hellman key exchange, are commonly used to establish shared secret keys securely [8]. The next essential aspect is hierarchical or distributed trust models [9]. In IoT ecosystems, multiparty authentication may involve hierarchical or distributed trust models. Hierarchical models utilize trusted entities or central authorities to authenticate and vouch for the identities of other entities. Distributed models leverage consensus algorithms or blockchain technology to establish trust among the entities without relying on a central authority. Multiparty authentication mechanisms in IoT should be scalable to handle large numbers of devices and entities [10]. As the number of IoT devices increases, the authentication process should be able to accommodate the growing ecosystem without compromising performance or security. Further, privacy is a crucial aspect of multiparty authentication in IoT [11]-[14]. The authentication process should ensure that entities can prove their identities without revealing unnecessary personal or sensitive information. Techniques like anonymous credentials or zero-knowledge proofs can be employed to address privacy concerns.

Hence, multiparty authentication in IoT plays a vital role in ensuring the security and trustworthiness of IoT deployments. By involving multiple entities in the authentication process, it strengthens the overall security posture and enables secure interactions within the IoT ecosystem. However, it involves various challenges too. Therefore, the proposed scheme contributes towards a novel design of multiparty authentication scheme which is meant to offer a good balance between potential security features as well as data transmission performance of IoT. The study further benchmarked its outcomes with existing scheme to showcase its strength and effectiveness. The organization of this manuscript is as follows: Section II presents discussion of review of literature followed by highlights of research problems in Section III. Section IV presents discussion of adopted research methodology while discussion of accomplished results is carried out in Section V while conclusive remarks of proposed model is carried out in Section VI.

II. REVIEW OF LITERATURE

At present, there are various multiparty-based authentication scheme being introduced in existing scheme focusing on use-case of IoT-based environment. Shu et al. [15] have presented a blockchain-based certificateless scheme towards signature focusing on securing cyber physical system. The idea of this implementation is towards authenticating varied entities along with sharing information in healthcare domain. Similar adoption of blockchain is also noted in work of Rathod et al. [16] for incorporating secure communication in 5G networks. The work carried out by Zhang et al. [17] have used certificateless encryption scheme for performing authentication associated with IoT devices to protect from various adversaries. Further adoption of certificateless scheme is witnessed in work of Xiang et al. [18] in order to resists replacement key attacks on certificateless signature schemes. Sahu et al. [19] have presented a key-agreement protocol for strengthening authentication of multiparty in IoT using identity-based encryption. Feng and Si [20] have used searchable cryptography using certificateless scheme for authentication of public key where a stochastic predictive model is constructed to resist guessing attack. The work of Wu et al. [21] have presented a unique authentication scheme using signcryption scheme for better stability and consistency in service delivery. Lee et al. [22] have presented a random scheme of signature management in IoT using certificateless scheme integrated with key generation center where aggregation is carried out in gateway node to resists replacement attack and rogue key generation center. Tan et al. [23] and Khalid et al. [24] have presented another set of unique schemes to strength the security perspective of IoT in order to improve authentication. Table 1 highlights the strength and weakness of existing schemes.

Table 1 Summary of Existing Approaches

Authors	**Problems**	**Methodology**	**Advantage**	**Limitation**
Shu et al. [15]	Secure storage in cyber physical system	Blockchain	Computationally efficient	No benchmarking
Rathod et al. [16]	Privacy in data sharing	Blockchain	Higher training accuracy	Computationally expensive with higher iteration
Zhang et al. [17]	Secure transmission	Certificateless encryption	Offers highly secure communication	Not applicable for heterogeneous network
Xiang et al. [18]	Secure communication	Certificateless, Elliptical Curve Encryption	Offers security from lethal threats	Induces complexity and overhead
Sahu et al. [19]	Key agreement	Identity-based encryption	Reduced power consumption	Not analyzed over heterogeneous nodes
Feng and Si [20]	Low adaptivity of certificateless scheme	Searchable encryption, Stochastic prediction	Simplified security model to implement	Attack-specific solution
Wu et al. [21]	Security issues due to concurrent users	Certificateless signcryption	Better stability and continuity of service	Demands memory to manage keys
Lee et al. [22]	Security threats in certificateless scheme	Certificateless Signature scheme	Strengthens non-repudiation	Attack-specific solution
Tan et al. [23]	Signature verification	Collaborative signature	Applicable for multi-device collaborative signing	Induce complexity, not scalable
Khalid et al. [24]	Edge security	Conventional public key encryption	Secure mutual authentication	Not applicable for heterogeneous network

III. RESEARCH PROBLEM

Multiparty authentication in IoT poses several challenges due to the complexity and diverse nature of IoT ecosystems. Here are some key challenges associated with multiparty authentication in IoT:

- **Scalability**: IoT systems often involve a large number of devices and entities, making scalability a significant challenge. Multiparty authentication mechanisms must be able to handle the increasing number of entities and devices efficiently without compromising security or introducing significant delays in the authentication process.
- **Heterogeneity**: IoT ecosystems consist of diverse devices, platforms, communication protocols, and authentication mechanisms. Integrating multiparty authentication across this heterogeneity can be challenging, as different devices may have varying capabilities and security requirements. Ensuring interoperability and seamless authentication among different entities is a complex task.
- **Resource Constraints**: Many IoT devices have limited computational power, memory, and energy resources. Multiparty authentication mechanisms need to be lightweight and resource-efficient to operate effectively on resource-constrained devices. Efficient cryptographic algorithms, optimized protocols, and smart resource management techniques are required to address these challenges.
- **Key Management**: Multiparty authentication often involves the exchange and management of cryptographic keys among multiple entities. Key distribution, storage, and revocation become complex tasks, particularly in large-scale IoT deployments. Robust key management mechanisms are necessary to ensure secure and efficient key exchange while considering the dynamic nature of IoT environments.
- **Trust Establishment**: Establishing trust among multiple parties is a critical aspect of multiparty authentication. However, determining and verifying the trustworthiness of each entity in a decentralized IoT ecosystem can be challenging. Ensuring the integrity and authenticity of each participating entity, especially in the absence of a centralized authority, requires careful design and use of trust models and mechanisms.
- **Privacy and Data Protection**: Multiparty authentication should address privacy concerns, as IoT systems often handle sensitive and personal data. Balancing the need for authentication while protecting user privacy becomes crucial. Privacy-enhancing techniques, such as anonymous credentials or secure protocols that minimize the disclosure of personal information, need to be incorporated into multiparty authentication schemes.
- **Security Vulnerabilities**: The complexity and interconnected nature of IoT ecosystems increase the attack surface and expose potential security vulnerabilities. Multiparty authentication mechanisms need to address various security threats, including impersonation attacks, man-in-the-middle attacks, replay attacks, and compromised devices. Robust security measures, such as strong authentication protocols, secure communication channels, and continuous monitoring, are essential to mitigate these risks.
- **Usability and User Experience**: IoT devices are often designed for user convenience and ease of use. However, multiparty authentication mechanisms should not introduce complexity or burdensome authentication procedures that hinder user experience. Striking a balance between security and usability is critical to ensure that users can easily authenticate multiple parties without compromising security.

Addressing these challenges requires a comprehensive approach that combines cryptographic techniques, standardized protocols, secure key management, efficient resource utilization, and robust trust models. As the IoT ecosystem continues to evolve, ongoing research and innovation are needed to overcome the challenges and ensure the secure and seamless authentication of multiple parties in IoT environments. The next section discusses about the proposed solution in terms of research methodology in order to address the above-mentioned research issues.

IV. RESEARCH METHODOLOGY

The core aim of the proposed study is to introduce a computational model in order to improve the non-repudiation perspective using multiparty computation system considering case study of IoT. In order to accomplish this research aim, following implementation objectives has been set:

- **Framework for Multi-Party Computation System for IoT**: A novel baseline architecture has been constructed towards multiparty computation in IoT. The model is characterized by novel key management, shared memory-based computation, transformation-based encryption. The study outcome has shown reduced delay, faster algorithm processing time, and minimal overhead. A research journal by title "Framework of Multiparty Computation for Higher Non-repudiation in Internet-of-Things (IoT)" is published for this objective most recently [25].
- **Framework for Optimizing Multi-party Computation**: The prime goal of the current work being carried out is to perform further optimization of the multi-party based non-repudiation system. This part of the study focuses on the fact that cloud computing, which basically host IoT environment is highly vulnerable to various threats as well as various other threats associated with it. This part of the proposed system is basically intended for incorporating optimization process in the multi-parties validation scheme targeting better form of non-repudiation along with privacy. Fig.1 highlights the schematic diagram which shows that a transmitting IoT node forwards its data to the

authentication module which further process this data to the multi-parties. This processing generates a multi-party data which will be subjected to the primary optimization, a kind of a trap door function development to ensure for forward as well as backward secrecy. The idea is also to ease down the process of encryption approach to be followed in next step. The proposed system also offers a novel encryption mechanism using modified public key encryption. This is further processed for secondary optimization that ensures that a better form of key management can be constructed. The secondary optimization block is responsible for ensuring the privacy factors of all the multi-parties involved in it. Finally, the encrypted data goes to the receiving IoT nodes.

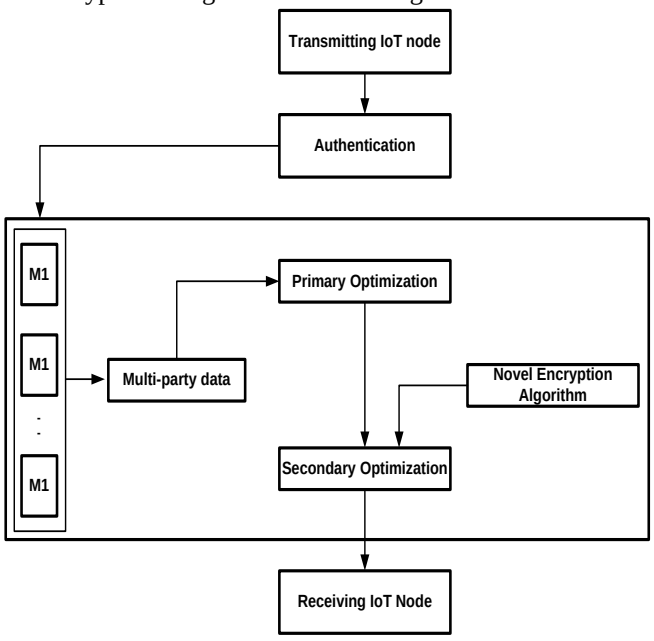

Fig.1 Proposed Research Methodology

The prime novelty of this part of implementation is about the mechanism of authentication being carried out by multi-parties' modules. This makes the process run over distributed system where authentication and authorized data / service relay is carried out concurrently, which is an indicator of better form of non-repudiation performance over cloud environment.

Algorithm for Primary Optimization

Input: n(number of IoT nodes), m (number of multiparty nodes)

Output: Enc_{data} (transmission of encrypted data)

Start

1. **For** i=1:n
2. **For** j=1:m
3. $j \rightarrow f_1(i)$
4. $i \leftarrow priv_{key}$
5. $i \rightarrow ds(b_1, b_2)$
6. **If** $cond_1=cond_2$
7. flag '*authenticate msg*'
8. **End**
9. $j \rightarrow f_2(i)$
10. $CN \leftarrow f_3(i)$
11. $CN \rightarrow j(Enc_{data})$
12. **End**
13. **End**

End

The discussion of the above algorithm is as follows: The algorithm takes the input argument of *n* (number of IoT nodes) and *m* (number of multiparty nodes) in a defined simulation area which after processing yields an outcome of Enc_{data} (transmission of encrypted data). The complete internal operational steps of the algorithm can be discussed under following sequential processes:

- **Initialization of Primary Optimization**: Under this process, the proposed scheme considers that secure encryption and key management process is being carried out by core node and multiparty authority and not the other regular IoT nodes. An explicit function $f_1(x)$ is developed (Line-3) which carries out following operation on its input of *i* IoT device viz. i) a security key s_t is generated in order to carry out a simplified public key encryption of the data packet, ii) the function generates pairing attributes (a_1, a_2, a_3, a_4, a_5, a_6, and a_7), iii) the function selects dual methods for performing hashing i.e., P (=a_{10})and p (=a_{12}) for that maps the data in a_5 attribute and maps input towards an output with uniform constant length respectively. iv) configures a public key $Pub_{key}=r.\gamma$, where r and γ represents a random number and generator of a_5 attribute respectively, v) finally an IoT device is loaded with all these system attributes. It should be noted that multiparty authority performs this task of pre-allocating the security tokens to all the IoT devices prior to communication.
- **Management of Secret Key**: In this process, the IoT node *i* extracts its private key $priv_{key}$ (Line-4). The private key is obtained by multiplying random number *r* with hashed value obtained by concatenating identity of specific IoT node and its timestamp. This information of private keys can be obtained from the supreme token β and identity information of the specific IoT device. The next consecutive process is related to generation of two attributes b_1 and b_2 as follows:

$$b_1=p.\text{concat}(Enc_{data}, t, \pi)$$

$$b_2=b_1.priv_{key}+rand_{IoTnode}.\gamma \quad (1)$$

In the above expression (1), the computation of first attribute b_1 is carried out considering specific hash function p over the value obtained by concatenating encrypted data Enc_{data}, time stamp t, and a variable π obtained by exponential operation i.e., $\pi = (\gamma, \gamma)^{r1}$. The algorithm generates digital signature *ds* using b_1 and b_2 attribute which is computed by the IoT node *i* (Line-5). The next part of the implementation is associated with the verification process by formulating two logical condition $cond_1$ and $cond_2$ which are both associated with verifying

π attributes (Line-6). For this purpose, the attribute π is split into two part i) original π_i and ii) computed π_i'.[π_i'=(γ, $\gamma)^{r1}$=π_i]. The condition $cond_1$ will represent hashed value of concatenation of Enc_{data}, t, and π_i' while condition $cond_2$ will represent hashed value of concatenation of Enc_{data}, t, and π_i which is also equivalent to b_1 attribute of digital signature (Line-6). If these conditions are found to be valid than the system flags that message is authenticated (Line-7). In the consecutive steps, the multiparty j broadcast its identity, a single-session random number, and initiating time to be used for signing the digital signature using a function $f_2(x)$ as exhibited in Line-9. Finally, a core node CN is selected from the normal IoT device randomly consisting of higher resources. A new function $f_3(x)$ is used for this purpose which performs. In order to choose a role of CN, all the IoT devices chooses an arbitrary number and compares this with a threshold. For all the nodes whose value is found to be less than this threshold is considered as CN. Finally, CN forwards the encrypted data Enc_{data} to the multiparty which then forward it to the gateway node (Line-11) and this completes the primary optimization operation.

Algorithm for Secondary Optimization

Input: n(number of IoT nodes), m (number of multiparty nodes)

Output: Enc_{data} (transmission of encrypted data)

Start

1. **For** i=1:n
2. **For** j=1:m
3. $j \rightarrow f_4(i)$
4. i$\leftarrow priv_{key}$
5. $\lambda_{off} \rightarrow (c_5)^{-ti}$
6. $\lambda_{on} \rightarrow (c5)^{\lambda off}$
7. **If** $cond_3$=$cond_4$
8. flag '*authenticate msg*'
9. **End**
10. CN$\rightarrow$j(Enc_{data})
11. **End**
12. **End**

End

The prime task of the above-mentioned secondary optimization algorithm is towards optimizing the operation of the internal processing associated with proposed IoT based communication system. The agenda of the secondary optimization algorithm is to minimize the cost of signing of signature along with storage and computational burden of primary optimization algorithm.

- **Initialization of Secondary Optimization:** Nearly similar steps are performed during secondary optimization where the multiparty authority implement a function $f_4(x)$ as exhibited in Line-3 which is nearly equivalent to prior function $f_1(x)$ with slight changes as following: i) a security token s_t is generated by the proposed encryption method, ii) an arbitrary generator c_5 is selected from the multiplicative group of finite field c_3 followed by selection of r random number with supreme token β, iii) an arbitrary number c_7 is selected for generating a private key for each IoT device considering P as hash operator, iv) finally, the IoT is preloaded with attributes *attr*. In case of secondary optimization, the attributes selected are *attr*(SO)=(c_1, c_2, c_3, c_4, c_5, c_6, c_7, c_8), where eight attribute elements represent security token s_t, integer corresponding number of security token, multiplicative group, q prime order, arbitrary generator of multiplicative group, arbitrary number selected by key generator, random number for private key generation, and hash operator for mapping strings of multiplicative group P respectively. In the prior discussion of primary optimization algorithm, it was stated in initialization step that pairing attributes (a_1, a_2, a_3, a_4, a_5, a_6, and a_7) which represents first prime order, second prime order, elliptical curve, finite field, subgroup of elliptical curve and finite field, subgroup of finite field, and generator of pair map. While the discussion of the secondary optimization scheme has been carried out considering initialization step of attributes (c_1, c_2, c_3, c_4, c_5, c_6, c_7, and c_8). One important fact to be known is there are 7 pairing attributes and 12 system attributes *attr*(PO) used in primary optimization (Fig.2(b)), while there are only 8 system attributes *attr*(SO) used in secondary optimization (Fig.2(a)). Therefore, there is difference in attributes opted in previous primary optimization algorithm and secondary optimization algorithm, which is as shown in Fig.2.

a_1	a_2	a_3	a_4	a_5	a_6
Prime order p	Prime order q	Elliptical Curve E	Finite Field F_p	G1:Subgroup of E/Fp	G2: Subgroup of Fp
a_7	a_8	a_9	a_{10}	a_{11}	a_{12}
σ: generator of pair map	Security token s_t	Integer to represent s_t size	P: Hash operator for string mapping for G1	r: random number	p: input mapping for output with constant length

(a) system attributes for primary optimization, *attr*(PO)

c_1	c_2	c_3	c_4	c_5
Security token s_t	Integer to represent s_t size	G:finite cyclic group	Prime order q	g: random generator of G
c_6	c_7		c_8	
r: random number	r_i: random number for private key generation		P: Hash operator for string mapping for G1	

(b) system attributes for secondary optimization, *attr*(SO)

Fig.2 Elements involved in system attributes *attr*

Therefore, from Fig.2, it can be said that secondary optimization has inclusion of a smaller number of system attributes compared to primary optimization. It should be noted that attributes are preloaded within the IoT device prior to communication as a part of security configuration in proposed scheme in both the optimization schemes. The next part of the implementation is associated with extraction of private key (Line-4) by the i^{th} IoT device, however, there is a difference the security token st in

secondary optimization is considered with two attributes i.e.,

$$s_t(SO)=(y_1, y_2) \quad (2)$$

In the above expression (2), the first variable y_1 represents random generator of multiplicative group G while the second variable y_2 represents summation of ri i.e., random number for private key generation and hashed value for y_1 and identity information of IoT node multiplied by random number r and modulus of second prime order q.

- **Management of Secret Key:** The part of proposed scheme is to perform the signing process considering two network condition:
    - **Signing during peak traffic condition**: This process of signing is carried out during the situation when the normal data transmission is affected temporary due to variable reasons. In this case, the IoT device generates λ_{off} signature considering timestamp associated with the transmission while the information of signature is stored to be processed during normal traffic condition. The signature generated is represented with respect to timestamp t_i of IoT device while the process of signing can be carried out by IoT device or by multiparty authority too during peak traffic condition (Line-5).
    - **Signing during normal traffic condition**: This process of signing is carried out during the normal stream of transmission among the IoT devices in regular case of networking. According to this scheme, a signature λ_{on} is generated using two parameters viz. i) c_5 i.e., random generator of cyclic group and first hashing operator P applied on encrypted data Enc_{data} and identity of IoT node to offer a dual layer of encryption-based security (Line-6).

The next task is associated with the authentication of the validity of the signature which acts like a proof in order to ensure non-repudiation. Similar to primary optimization, two different conditions are assessed and compared i.e., $cond_3$ and $cond_4$ (Line-7). The first condition $cond_3$ and second condition $cond_4$ is shown in expression (3)

$$cond_3=\lambda_{on}, rand(P).c_5(p_i, P(rand, \text{identity of node}))$$

$$cond_4=(c_5) \quad (3)$$

If the above both conditions are found to be valid, then system consider it as authenticate message (Line-8) followed by transmitting the encrypted data from core node to multiparty node j which further forwards it to gateway node. It should be noted that multiparty authorities are many in number which is designated as single entity as it is a part of service provider. The next section discusses about the accomplished outcome of this algorithmic implementation.

V. Result Discussion

The assessment of the proposed work is carried out considering nearly similar implementation scenario as noted in first implementation objective with minor amendments. The simulation parameters considered for the assessment are as follows: i) number of IoT devices: 100-500, ii) location of multiparty authority, iii) percentage of IoT nodes to play the role of CN: 5-50%, iv) initialized energy of IoT device=1 as a probability value to represent highest resource value. The comparison of the proposed scheme is carried out with existing scheme *Exist* which represent certificateless authentication scheme which is frequently deployed in existing multiparty-based schemes in IoT [17]. The discussion of the outcomes are as follows:

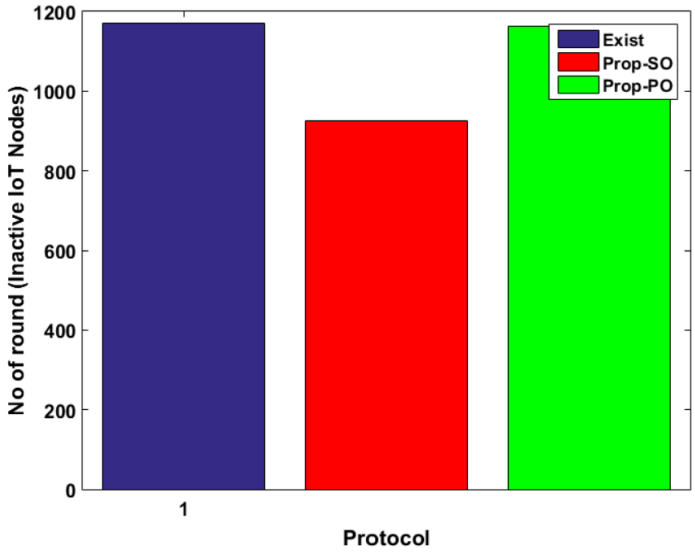

Fig.3 Comparative Analysis of Inactive IoT Nodes

Fig.3 highlights the number of inactive IoT nodes which represents non-participating nodes due to complete saturation of their respective resources. The outcome shows that proposed secondary optimization (Prop-SO) offers a smaller number of inactive IoT nodes in comparison to proposed primary optimization (Prop-PO) and existing certificateless authentication scheme (Exist). The prime reason behind this is Prop-SO offers much reduced number of system parameters which lightens up the burden during authentication and hence a greater number of active nodes are retained. *Exist* scheme incurs too much sophisticated operation resulting in higher number of inactive IoT nodes.

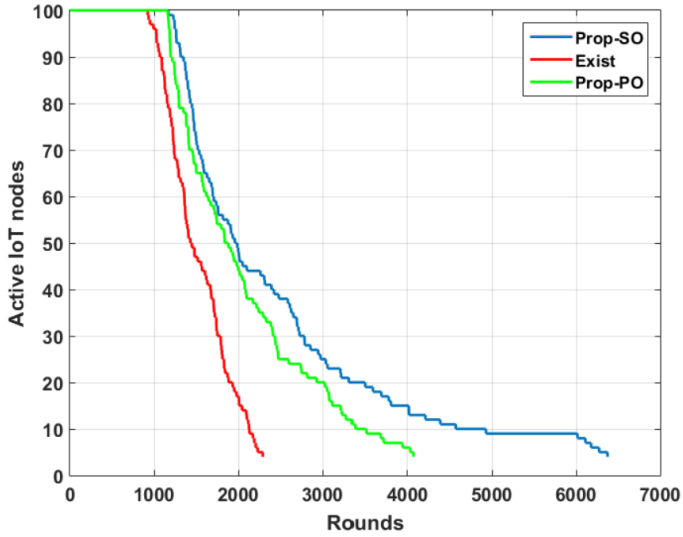

Fig.4 Comparative Analysis of Active IoT Nodes

The outcome shown in Fig.4 is in agreement with inactive nodes present in Fig.3, whereas the current outcome in Fig.4 showcase secondary optimization (Prop-SO) to benefit retention of more active nodes compared to existing scheme *Exist*. Similar justification can be offered for this; moreover, *Exist* consist of higher number of operational steps to in performing secure aggregation followed by signcryption. Although, this scheme offers strong security, but it also consumes additional resources from resource-constraints IoT devices.

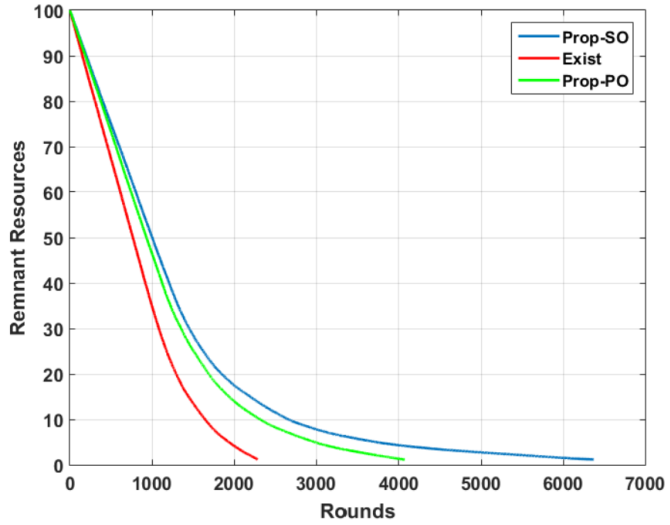

Fig5. Comparative Analysis of Remnant Resources

Fig.5 highlights that Prop-SO offers significantly better retention of residual resources in comparison to Exist. The mechanism adopted in *Exist* scheme consists of increasing operational steps right from generation of user key to validation of signature on the basis of identity. However, all these operations are mainly carried out by IoT device itself, whereas proposed scheme introduced the complete operation to be performed by distributed multiparty (only after ensuring their legitimacy), which curtains maximum resource depletion from IoT device causing more remnant resources.

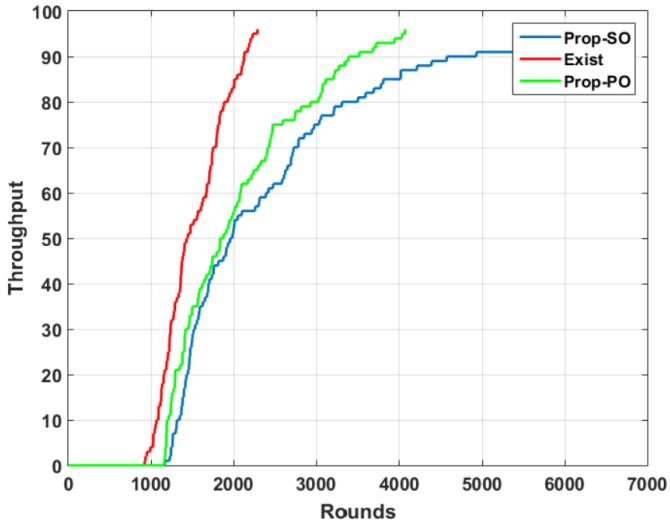

Fig.6 Comparative Analysis of Throughput

Fig.6 showcases that Prop-SO offers higher and consistent throughput compared to other schemes. It is because the proposed scheme introduces a mechanism of selection of CN out of all IoT devices just on the basis of random number declaration and comparing with threshold. The process is very faster while the CN node obtains all information and forward to multiparty who performs the task of authentication. One multiparty can have concurrent transmission with multiple CN and this consideration results in superior increment of throughput with higher consistency. This form of outcome is not reflected in existing scheme, where multiple form of aggregation followed by authentication encryption and decryption is highly an iterative step. Hence, significant amount of effort is used for securing the routes without much consideration of data transmission performance in existing scheme.

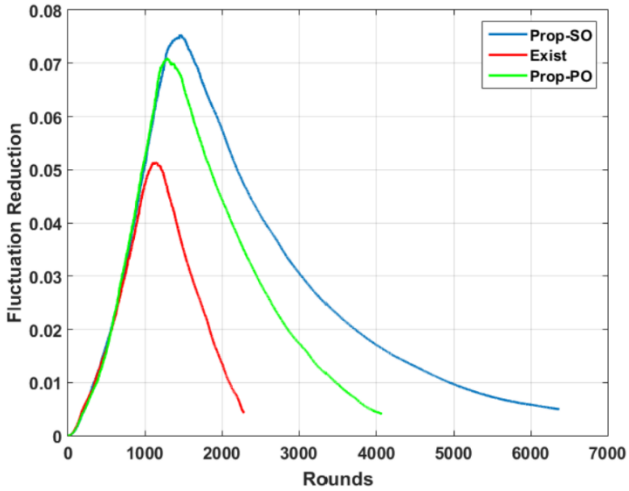

Fig.7 Comparative Analysis of Fluctuation Reduction

Fluctuation of variance in distribution of energy attribution is highly detrimental for improving network lifetime as well as to gain a similar control of algorithmic performance for all heterogeneous IoT device. Hence, the difference in statistical variance is computed before and after the data propagation process to find out fluctuation reduction as performance parameters in Fig.7. The outcome showcase that proposed scheme of Prop-SO offers superior reduction of fluctuation followed by Prop-PO. However, *Exist* scheme is witnessed to offer reduced capability to deal with fluctuation. It is imperative to anticipate fluctuation of energy consumption in heterogeneous IoT system and hence it must be suppressed. The proposed scheme controls fluctuation of energy by i) constructing faster mechanism of CN selection, ii) pre-allocation of system parameters even before communication starts, iii) consideration of resources for selection of CN node apart from the random number declaration process. For this purpose, the synchronization of multiparty entities is well-established with proper syncing with the IoT nodes that results in streamlining reduction of resource dependencies towards performing any sorts of security-based task. *Exist* scheme introduces usage of partial key generation followed by differential authentication without considering heterogeneity aspect. Hence, energy fluctuates from one to another group of communicating IoT devices.

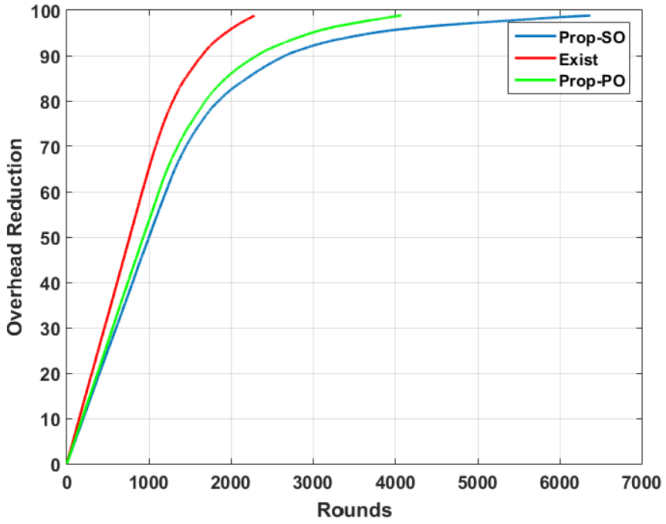

Fig.8 Comparative Analysis of Overhead Reduction

Fig.8 highlights that Prop-SO offers higher overhead reduction in comparison to other schemes. The prime reason behind this outcome is that *Exist* scheme of certificateless authentication involves a large step for system initialization in comparison to proposed system where a common algorithm is executed by the key generation center. This is heavily time-consuming as well as requires multiple set of information from varied resources for analysis. Hence, the first step itself introduces overhead when it is exposed to variable and dynamic traffic situation. Whereas, the initialization steps of proposed scheme is quite simplified and highly reduced with lesser dependency of information to be acquired from any environment. Hence, protocol implementation becomes faster when exposed to any form of traffic and no additional data is required apart from payload information resulting in reduced overhead.

VI. CONCLUSION

The proposed scheme presents a novel framework where the prime focus is towards optimizing the securing features of data transmission while performing multiparty authentication in IoT. The contribution of the proposed scheme is presented in the form of following novelty as:

- The proposed scheme can perform multiparty authentication in any form of traffic condition of IoT.
- The mechanism of encryption and management of evidence (or proof) in the form of digital signature actually creates a robust trapdoor function.
- The proposed scheme has no iteration, nor it has any complex encryption steps in comparison to existing schemes of non-repudiation and privacy control in IoT environment.
- The outcome of the proposed scheme shows that proposed scheme (Prop-PO and Prop-SO) offers approximately 20% less inactive IoT nodes, approximately 45% more retention of active IoT nodes, approximately 37% more remnant resources, approximately 68% more throughput, and approximately 62% of reduced energy fluctuation in comparison to most frequently used existing scheme of certificateless authentication.

REFERENCES

[1] H. Smajlović, A. Shajii, B. Berger, H. Cho, and I. Numanagić, "Sequre: a high-performance framework for secure multiparty computation enables biomedical data sharing," Genome Biol., vol. 24, no. 1, p. 5, 2023, doi:https://doi.org/10.1186/s13059-022-02841-5

[2] K. Şahinbaş and F. O. Catak, "Secure multi-party computation based privacy preserving data analysis in healthcare IoT systems," arXiv [cs.CR], 2021, doi: https://doi.org/10.48550/arXiv.2109.14334

[3] S. Garg and R. Vashisht, "A permissioned blockchain system for secure multiparty computation," J. Phys. Conf. Ser., vol. 1998, no. 1, p. 012003, 2021.doi:10.1088/1742-6596/1998/1/012003

[4] X. Li, K. Zhang, L. Zhang, and X. Zhao, "A new quantum multiparty simultaneous identity authentication protocol with the classical third-party," Entropy (Basel), vol. 24, no. 4, p. 483, 2022.https://doi.org/10.3390/e24040483

[5] R.-K. Sheu, M. S. Pardeshi, and L.-C. Chen, "Autonomous Mutual Authentication Protocol in the Edge Networks," Sensors, vol. 22, no. 19, p. 7632, Oct. 2022, doi: 10.3390/s22197632.

[6] O. O. Olakanmi and K. O. Odeyemi, "Trust-aware and incentive-based offloading scheme for secure multi-party computation in Internet of Things," Internet of Things, vol. 19, no. 100527, p. 100527, 2022.doi:https://doi.org/10.1016/j.iot.2022.100527

[7] S. Mawlood Hussein, J. A. López Ramos, and J. A. Álvarez Bermejo, "Distributed Key Management to Secure IoT Wireless Sensor Networks in Smart-Agro," Sensors, vol. 20, no. 8, p. 2242, Apr. 2020, doi: 10.3390/s20082242.

[8] V. S. Naresh, M. M. Nasralla, S. Reddi, and I. García-Magariño, "Quantum Diffie–Hellman Extended to Dynamic Quantum Group Key Agreement for e-Healthcare Multi-Agent Systems in Smart Cities," Sensors, vol. 20, no. 14, p. 3940, Jul. 2020, doi: 10.3390/s20143940

[9] A. De Salve, L. Franceschi, A. Lisi, P. Mori, and L. Ricci, "L2DART: A Trust Management system integrating blockchain and off-chain computation," ACM Trans. Internet Technol., vol. 23, no. 1, pp. 1–30, 2023.https://doi.org/10.1145/3561386

[10] K. Mrabet, F. El Bouanani, and H. Ben-Azza, "Dynamic Decentralized Reputation System from Blockchain and Secure Multiparty Computation," Journal of Sensor and Actuator Networks, vol. 12, no. 1, p. 14, Feb. 2023, doi: 10.3390/jsan12010014.

[11] D.-E. Fălămaş, K. Marton, and A. Suciu, "Assessment of Two Privacy Preserving Authentication Methods Using Secure Multiparty Computation Based on Secret Sharing," Symmetry, vol. 13, no. 5, p. 894, May 2021, doi: 10.3390/sym13050894.

[12] J. Zhou, Y. Feng, Z. Wang, and D. Guo, "Using Secure Multi-Party Computation to Protect Privacy on a Permissioned Blockchain," Sensors, vol. 21, no. 4, p. 1540, Feb. 2021, doi: 10.3390/s21041540.

[13] T. Geng, L. Njilla, and C.-T. Huang, "Delegated Proof of Secret Sharing: A Privacy-Preserving Consensus Protocol Based on Secure Multiparty Computation for IoT Environment," Network, vol. 2, no. 1, pp. 66–80, Jan. 2022, doi: 10.3390/network2010005.

[14] M. Anagreh, P. Laud, and E. Vainikko, "Parallel Privacy-Preserving Shortest Path Algorithms," Cryptography, vol. 5, no. 4, p. 27, Oct. 2021, doi: 10.3390/cryptography5040027

[15] H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, and L. Sun, "An efficient certificateless aggregate signature scheme for blockchain-based Medical Cyber Physical Systems," Sensors (Basel), vol. 20, no. 5, p. 1521, 2020.

[16] T. Rathod et al., "Blockchain-driven intelligent scheme for IoT-based public safety system beyond 5G networks," Sensors (Basel), vol. 23, no. 2, p. 969, 2023.

[17] Y. Zhang, F. Ren, A. Wu, T. Zhang, J. Cao, and D. Zheng, "Certificateless multi-party authenticated encryption for NB-IoT terminals in 5G networks," IEEE Access, vol. 7, pp. 114721–114730, 2019

[18] D. Xiang, X. Li, J. Gao, and X. Zhang, "A secure and efficient certificateless signature scheme for Internet of Things," Ad Hoc Netw., vol. 124, no. 102702, p. 102702, 2022.

[19] A. K. Sahu, S. Sharma, and D. Puthal, "Lightweight multi-party authentication and key agreement protocol in IoT-based E-healthcare service," ACM Trans. Multimed. Comput. Commun. Appl., vol. 17, no. 2s, pp. 1–20, 2021.

[20] T. Feng and J. Si, "Certificateless searchable encryption scheme in multi-user environment," Cryptography, vol. 6, no. 4, p. 61, 2022.

[21] X. Wu, F. Ren, Y. Li, Z. Chen, and X. Tao, "Efficient authentication for Internet of Things devices in information management systems," Wirel. Commun. Mob. Comput., vol. 2021, pp. 1–14, 2021.

[22] D.-H. Lee, K. Yim, and I.-Y. Lee, "A certificateless aggregate arbitrated signature scheme for IoT environments," Sensors (Basel), vol. 20, no. 14, p. 3983, 2020.

[23] L. Tan, X. Shang, L. Zou, H. Yang, Y. Wen, and Z. Liu, "Multi-party co-signature scheme based on SM2," PLoS One, vol. 18, no. 2, p. e0268245, 2023.

[24] H. Khalid, S. J. Hashim, S. M. S. Ahmad, F. Hashim, and M. A. Chaudhary, "SELAMAT: A new secure and lightweight multi-factor authentication scheme for cross-platform industrial IoT systems," Sensors (Basel), vol. 21, no. 4, p. 1428, 2021

[25] Divya K.S, Roopashree H.R, Yogeesh A.C, "Framework of Multiparty Computation for Higher Non-Repudiation in Internet-of-Things (IoT)", International Journal of Computer Networks and Applications, vol.10, Iss.1, pp.84-94, 2023.DOI: 10.22247/ijcna/2023/218513

[26] Divya K.S,Dr.RoopaShree H.R,Dr.Yogesh A.C, "Non-Repudiation-based Network Security System using Multiparty Computation ", International Journal of Advanced Computer Science and Applications, Vol. 13, No. 3, 2022,PP 282-289,DOI:10.14569/IJACSA.2022.0130335.

Authors

Ms. Divya K. S is a Research scholar in GSSS Computer institute of engineering and technology for Women,Mysur under VTU, working as Assistant Professor in Computer Science Department in Kristu Jayanti College, Bengaluru, India. She has completed her B.Tech and MTech in CS. She is currently pursing Ph.D in the area of Network Security in VTU.She has 15 years of teaching experience

Dr. Roopashree H.R. has completed B.E (E&C) in M.Tech (CS&E) in from VTU, Belagavi, Karnataka, India and PhD from CHRIST (Deemed to be University) Bengaluru, Karanataka, India. She has around 13 years of Industrial experience and 2 years of teaching experience. she is presently working as Associate professor in Dept of CSE at GSSSIETW,Mysuru,India and supervising 6 PhD research scholars in V TU.

Dr.Yogesh A.C has completed B.E, M.Tech and PhD from Visvesvaraya Technological University Belagavi,Karnataka,India. Presently working as Assistant Professor in Dept. of CS&E, Government Engineering College,Kushalnagar, Karnataka, India. His area of interest is Wireless sensor network, IOT and Machine learning.