International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/218513 Volume 10, Issue 1, January – February (2023)

RESEARCH ARTICLE

Framework of Multiparty Computation for Higher Non-Repudiation in Internet-of-Things (IoT)

Divya K.S
Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India.
divyaks.phd@gmail.com

Roopashree H.R
Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, India.
roopashree16@gmail.com

Yogeesh A.C
Department of Computer Science and Engineering, Government Engineering College, Kushalnagar, India.
yogeesh13@gmail.com

Received: 11 December 2022 / Revised: 23 January 2023 / Accepted: 26 January 2023 / Published: 26 February 2023

Abstract – Multiparty computation is essential in offering a better form of non-repudiation, which is not much explored in past research work. A review of existing non-repudiation-based approaches found various shortcomings that do not offer a good balance between robust security and algorithm efficiency. Therefore, the proposed study presents a novel yet simple multiparty computation framework to ensure a higher degree of non-repudiation considering a use-case of a highly distributed and large network, i.e., Internet-of-Things (IoT). The study implements a unique encryption mechanism that uses a transformation strategy to perform encoding while using split key management to retain maximal secrecy and multiparty authentication for enhanced security. The simulation outcome of the study showcases that the proposed scheme offers approximately a 48% reduction in computation overhead, 54% minimization in delay, and 58% faster processing in contrast to frequently reported non-repudiation schemes.

Index Terms – Multiparty Authentication, Encryption, Internet-of-Things, Key Management, Secrecy, Non-Repudiation.

1. INTRODUCTION

In information and security, the transmitting node must be facilitated with concrete and reliable evidence of the delivery of messages or services. In contrast, the receiving node must be facilitated with identity-based evidence of the transmitting node [1]. This operation will be essential to ensure that neither the transmitting node nor the recipient node can deny their assigned serviced undertaking [2]. This mechanism is termed non-repudiation and plays a crucial role while developing a security protocol or security-based application [3]. It is essential because, in the case of adversaries, the services or applications do not possess significant control over user actions, resulting in default permitting the intruder to introduce malicious activity termed a repudiation attack [4]. However, it should be noted that non-repudiation is just one of the security service standards demanded to incorporate a threat-free environment for securing enterprise networks, servers, or computers. Other important security service standards are confidentiality, authentication, availability, and integrity [5]. Usually, the concept of non-repudiation integrates data integrity and authentication [6]. One simple example to understand this is to consider a non-repudiation device a public key signature when the signature generation is restricted to only one party. Cryptography is one of the prime actors in accomplishing non-repudiation, e.g., logging, auditing, authentication, and digital signatures [7]. Besides its usage in the digital signature, email and digital contracts also deploy the principle of non-repudiation. However, ensuring effective and highly fail-proof non-repudiation services is not simpler. At present, there are various forms of non-repudiation approaches witnessed in existing schemes [8]-[10], where it is noted that digital signatures play a predominant role. However, explicit digital signature usage cannot offer complete assurance of non-repudiation or higher security. This is because there is a fair possibility of the signature being forfeited by an intruder by various means. With various malicious programs, it is quite feasible to break inside the network, steal information, and forge information about the digital signature. Hence, there is a need for the involvement of various trusted actors who can ensure that a singular-party system does not validate such security

RESEARCH ARTICLE

information. Hence, an evolution of multiparty computation schemes toward authenticating the security operation has occurred. However, developing a multiparty computation scheme for incorporating non-repudiation is yet to be seen, although some productive initiative has already been taken in the past. Such a scheme's prime challenge is ensuring consistent performance when exposed to a large-scale distributed network.

Therefore, the proposed scheme introduces a novel framework of a multiparty computation system for ensuring non-repudiation. The paper objectives / contributions are:

i) A novel computational model for a simplistic and yet robust multiparty-based authentication scheme.

ii) A lightweight encryption and unique decryption method are implemented when unique key splitting management is introduced for higher secrecy.

iii) An extensive simulation is carried out to benchmarked proposed scheme with most existing approaches of non-repudiation.

The paper's organization is as follows: Section 2 discusses the existing methodologies towards non-repudiation, followed by a briefing of the identified research problem in Section 3. An outline of the methodology is carried out in Section 4, while the illustration of algorithm implementation is carried out in Section 5. Section 6 discusses the accomplished result, while the summary of this paper is stated in Section 7 as a conclusion.

2. EXISTING TECHNIQUES OF NON-REPUDIATION

To date, there have been various evolving solutions for improvising the mechanism of non-repudiation in large-scale networks like IoT. The most familiarized approaches adopted are blockchain, certificateless cryptography, public key cryptography, signcryption, digital watermarking, and digital signature. From the security perspective of IoT, various layers are significantly affected due to potential threats, especially the perception layer, in the absence of non-repudiation [11]. Our prior work has reviewed various non-repudiation techniques [12], while this part of the study further updates it.

2.1. Blockchain

The contribution of blockchain is significant towards securing IoT with the majority of privacy standards, including non-repudiation [13]. A study towards accomplishing non-repudiation using blockchain was reported by Chen et al. [14], where a unique controller system is designed for interacting communication with the various modules with smart contracts. The technique also uses encryption to sign the message for the second layer of security. The work carried out by Sun et al. [15] has integrated immutable blockchain with attribute-based encryption, where the encrypted files are stored in a discrete file system for storage security. The study is found to be resistant to selected keyword attacks. The study carried out by Chen et al. [16] has also reported using blockchain to develop a framework capable of computing trust for cloud-based IoT applications. According to this study, the service is encrypted and retained as hash values within the blockchain. Further service provisioning is accomplished by using public key encryption by IoT clients.

2.2. Certificateless Cryptography/ Digital Signature

The existing system has witnessed the use of certificateless cryptography, where the digital signature is extensively used. Digital signature integrated with different methods is another prime approach towards ensuring non-repudiation of data [17]. Lee et al. [18] have developed a unique certificateless scheme that contributes towards the generation and verification of the newly generated message and signature. The signature size is reduced to using a gateway node in IoT and is claimed to resist key-based attacks. Similar adoption of the approach was presented by Kar et al. [19] and Shen et al. [20], considering a use-case of the sensory network. Along with non-repudiation, these studies also accomplish higher secrecy, anonymity, confidentiality, and data integrity. The work carried out by Sudharani, and Sakthivel [21] has adopted a proxy signature scheme using a certificateless approach to resist forgeability-based and message attacks. Harn et al. [22] have discussed discrete logarithmic-based signatures to address the key escrow problem. The scope of knowledge about the private key is only within the user; hence, this problem is sorted out along with its claimed resistivity against message attacks. Xiang et al. [23] have presented a unique certificateless signature scheme using an elliptical curve to improve the security coverage of conventional certificateless schemes and address storage issues.

2.3. Public Key Cryptography

The work carried out by Kim et al. [24] has presented a mechanism where the key is extracted from the recovery field of encrypted data. The technique also utilizes the proxy re-encryption technique to resist collusion attacks. Elamir et al. [13] have used public key encryption to construct a secure IoT model. The study used the RSA algorithm to encrypt the image data and report, followed by the second layer of security using gene-based encryption. The adoption of the RSA algorithm has also been reported in the work of Singh et al. [25], where a bilinear map has been used for implementing an identity-based certificateless scheme. Exponential operation and hash function has been used for further deploying an oracle model for assessing its security strength.

2.4. Signcryption

Toradmalle et al. [26] used an elliptical curve to construct a signcryption scheme using certificateless cryptography.

RESEARCH ARTICLE

However, the study did not talk highly about its implication or effectiveness. Selvi and Chandrasekaran [27] have developed a signcryption scheme assessed over an arbitrary oracle framework. The study model is independent of pairing operation for signcrypting the message. A different variant of the signcryption scheme has also been adopted, viz. certificateless signcryption scheme (Jin et al. [28], Zhang et al. [29], Meshram et al. [31], Lakshmanna et al. [32]), blind signcryption scheme (Abdullah et al. [33]), elliptical curve-based signcryption scheme (Zhang et al. [34]), quantum-based signcryption scheme (Ghosh et al. [34]), public-key based signcryption (Sarr et al. [35], Daniel et al. [36], Unal et al. [37], Witanto and Lee [38], Li et al.[39])

It is also noted that machine learning is predominantly used for securing IoT [40]; however, studies explicitly towards non-repudiation are few to find. There are also studies on transport layer security for improving non-repudiation schemes [41]. Apart from our reported review work [12], there is less work toward a multiparty-based non-repudiation system. Some of the reported work toward this direction was reviewed from the study model presented by Alper and Kupcu [42], Kalpana [43], Sharaf et al. [44], Kumar [45], Wang et al. [46], etc. Studies using multiparty offers various advantages in accomplishing non-repudiation, especially for large-scale networks. The challenges associated with the complexity of developing a network system that emphasizes a non-repudiation scheme demands something more than a conventional state of encryption.

Hence, it can be inferred that there are various reported studies in the existing system with different variants of security schemes to offer non-repudiation along with other security standards for addressing a specific set of problems; however, they are also characterized by shortcomings outlined in the next section in the form of the research problem.

3. RESEARCH PROBLEM

Following are the problems identified after reviewing the existing methodologies for improving non-repudiation.

- *Usage of Sophisticated Encryption*: The first and foremost criterion for developing a security scheme is to ensure its operation within the target device. In the case of an IoT, the devices often do not have sufficient resources; hence, processing high-end encryption techniques [28][32] will demand more space and computational resources. This will directly affect communication performance and adversely affect large-scale network security. Existing encryption approaches were not reported to be deployed, considering computation resources in mind [26][37][39].
- *Issues with Blockchain-based Approaches*: There is no doubt that blockchain is a better security alternative for the majority of upcoming applications. However, they, too, suffer from shortcomings. Typical designs of blockchain integrated with other approaches, e.g. [14][16], are featured with efficiently generating data blocks. However, when exposed to various attacks on large-scale networks, their performance consistency is still not reported. Apart from this, IoT devices are meant to carry out multiple applications and sensing, eventually using different protocols and data. Blockchain approaches are not implemented considering this aspect, and retrieving data blocks is also time-consuming and maximizes resource dependencies for emergency applications on IoT.
- *Less Emphasis Towards Key Management*: Adoption of public key encryption in existing schemes has not been reported working towards securing public keys and is more inclined towards strengthening the generation of private keys [19][22][25]. IoT devices are mainly wireless, so the circulation of public keys among the devices is quite vulnerable to being compromised. Apart from this, encryption and certificateless signature techniques have a larger memory even after the key is used. This saturates the internal memory. Even elliptical curve-based encryption [23] [34], which offers better key management, does not address this problem. It results in the generation of a massive number of keys with less security towards storing them properly over a distributed environment.
- *Less Modelling towards Multiparty Computation*: Existing approaches have much less standardized and few benchmark modeling using multiparty computation. Some of the studies using this concept [40][42][46] have been proven for attack-specific security, but they are not purely towards achieving non-repudiation. The prime focus was always on data integrity and less on non-repudiation.

Hence, there is a need for an effective solution to address the abovementioned research. The next section discusses problem solutions in the form of research methodology.

4. RESEARCH METHODOLOGY

The core goal of the proposed framework is to develop a comprehensive computation using a multi-party computation system considering the case study of IoT. The secondary goal of this module will be to develop a novel encryption mechanism that mainly targets achieving adequate non-repudiation while performing secure data transmission.

The implementation of the proposed system has been carried out using analytical research methodology where the core emphasis is mainly on multiparty computation towards achieving non-repudiation in IoT. Figure 1 highlights the

RESEARCH ARTICLE

process flow of the proposed system, where the first step will be to incorporate the design of an IoT environment system considering a certain set of IoT devices, gateway nodes, edge servers, and cloud storage at the end. The study also considers the inclusion of the trusted authority required to undergo a specific configuration. The next part of the implementation is associated with the secret key generation, which is mainly meant for the user. As a novelty, the proposed system introduces a split key mechanism where the one split of the key bearing a user's identity information and certain other parameters will be considered. The next split of the secret key will be generated by transforming the prior set of split keys to generate another split key. Finally, a novel authentication mechanism will be introduced, including multi-parties (MP) to perform authentication.

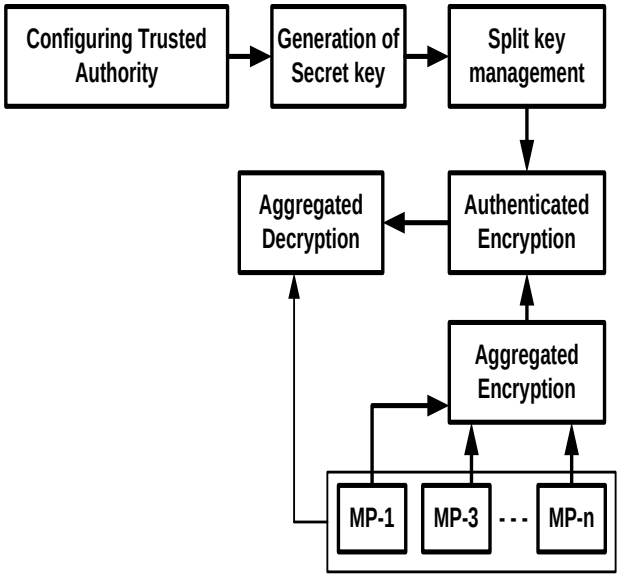

Figure 1 Proposed Research Methodology

The prime novelty of this mechanism is that by incorporating a split key mechanism, the process of multi-party computation is aimed to be faster, directly impacting non-repudiation performance. One of the proposed study's significant outcomes is that apart from non-repudiation, the proposed study will also achieve integrity and confidentiality. The effectiveness of the study is anticipated to offer reduced computation overhead, reduced delay in operation, and faster algorithm processing time. Apart from this, the proposed scheme balances privacy and non-repudiation. The next section discusses the algorithm design adopted to implement it.

5. ALGORITHM DESIGN

This section discusses the algorithm constructed to retain a higher deal of non-repudiation considering transmitting and receiving nodes in an IoT environment. The proposed scheme implements this using three different algorithms, i.e., i) Algorithm for Profile Enrollment, ii) Algorithm for Encrypting Message, and iii) Algorithm for Decrypting Message. An elaborated discussion of all the above-mentioned algorithms is as follows:

5.1. Algorithm for Profile Enrollment

The term profile will mean all the basic information related to the user that can establish their identity in a multiparty authentication system. Such private information must be effectively protected in distributed cloud storage to safeguard its privacy. Therefore, this algorithm-1 is the primary step toward safeguarding the user's private details. The steps of the proposed algorithm-1 are as follows:

Input: *fn*, *ln*, *ag*, *un*, *ps*
Output: *up*
Start
1. For i=1:u_{max}
2. ud_i=[*fn*, *ln*, *ag*, *un*, *ps*]^i
3. If ud_i=*ud_db*
4. flag 'user detail exists.'
5. Else
6. e_p=f_1(ud_i(*ps*))
7. [*r*, *c*]=size(update(*i*));
8. *up*=[ud_i, e_p]
9. *i.up*(*r*, *c*)=*up*
10. End
End

Algorithm 1 Profile Enrollment

The algorithm-1 takes the input of all the essential user details, i.e., *fn* (first name), *ln* (last name), *ag* (age), *un* (user name), *ps* (password), which upon processing yields a resultant of *up* (updated encrypted profile). Considering u_{max}, i.e., the maximum number of users (Line-1), the proposed scheme constructs a matrix *ud* for retaining all the elements of user details in it (Line-2). In enrolling the user, if the entered user details ud_i for i^{th} specific user is found to match with user details already stored in database *ud_db* (Line-3). The proposed scheme declares a flag message stating its existence (Line 4). Otherwise, the proposed scheme encrypts the password *ps* using a discrete function $f_1(x)$ (Line-6). The next part of the algorithm-1 obtains a size of all i^{th} user details individually and stores them in row *r* and column *c* (Line-7). Finally, the algorithm-1 constructs an updated matrix *up* that stores all the user details ud_i along with encrypted password e_p (Line-8). The algorithm-1 also assigned the obtained updated details matrix *up* and construct a data structure to retain all the updated information row-wise. The internal operation carried out by the $f_1(x)$ is as follows: The function is designed on the transposition of the strings, which is implemented by encoding each character present in the secret message by the number of strings. It also permits decryption using equivalent

RESEARCH ARTICLE

transpositions in the opposite direction. The system performs the initial transformation of the strings of the message in the form of a discrete number using modular arithmetic. Therefore, the encryption of the strings in the proposed system using f1(x) is represented as shown in equation (1)

$$f_i(x)=(n+x).\ \mathrm{mod}(A) \quad (1)$$

In the above expression (1), the encryption function $f_1(x)$ is implemented using its dependable parameters x string and n number of shifts. At the same time, the variable A represents the total number present in the complete string. For the alphabet, it is 26; however, it can be customized to any value depending on the length of the message. The decryption can be carried out as shown in equation (2).

$$f_2(x)=(x-n).\ \mathrm{mod}(A) \quad (2)$$

The encryption function $f_1(x)$ takes two different forms of an input viz. i) n, i.e., integer number representing the demanded shift, and ii) x, i.e., messages to be encrypted. According to this encryption function, the given messages are traversed one at a time concerning each character. Transformation is carried out for specified characters based on the rule while the generated new string represents an encrypted message, i.e., e_p (Line-6). After the process of profile enrollment is carried out, the next step of the proposed system is towards selecting the

5.2. Algorithm for Encryption Message

This algorithm-2 is responsible for securing the user's message, which undergoes encryption before forwarding it to the next node. The algorithmic steps of the proposed scheme are as follows:

Input: *udo*, *cuo*
Output: U_{tx}
Start
1. *init* udo, cuo
2. user←cuo
3. tx=f_1(msg)
4. [a, b]=size(ca)
5. If c=0
6. cuo.up(i, c+1)=tx
7. Else
8. j=1: count
9. If ($cond_1$=T && $cond_2$=T)
10. cuo.up(i, j+6)=tx, U_{tx}=*cuo*;
11. End
12. End
End

Algorithm 2 Encrypting Message

The algorithm-2 considers its input file to be *udo* (user detail object) and *cuo* (the current user), which, after processing, yields a result of U_{tx} (uploaded encrypted message). To carry out authentication, the algorithm-2initially constructs two object files viz. *udo* (user detail object) and *cuo* (the current user) (Line-1). The object file acts as a split key related to user detail and is assigned to a matrix user (Line-2). A similar encryption function $f_1(x)$ is used to secure the message *msg* to be propagated (Line-3) that leads to encrypted message *tx*. The next part of the algorithm-2 constructs a temporary matrix *ca* that consists of updated information about user details. The size of this *ca* matrix is obtained and stored in two arrays of *a* and *b* (Line-4). Further, a string comparison is carried out between the user details and the message to confirm the message's ownership. A condition for temporary counter *c* to be equivalent to zero (Line-5) is constructed. Upon finding a truth statement, allocates the obtained encrypted message to the updated current detail and objects (Line-6). Considering all the count of objects (Line-8), the proposed scheme constructs a conditional statement where it assesses two discrete conditions, i.e., $cond_1$ and $cond_2$ (Line-9). The first condition, $cond_1$, assesses if the new matrix *ca* is empty, and the second condition, $cond_2$, assesses if the counter is set to zero. It means that the condition is looking for valid user details confirmed to be legitimate. Upon finding a positive confirmation, the obtained encrypted message *tx* is allocated to the current user object (Line-10). This encrypted message is forwarded to the next node, where the decryption algorithm-3 is initiated.

5.3. Algorithm for Decrypting Message

The decryption of the proposed message is carried out completely differently from any existing decryption mechanism. This algorithm-3 obtains the input from the receiver node, an encrypted file, and involves multiple parties to extract the decrypted message. The steps of this algorithm-3 are as follows:

Input: U_{tx}
Output: Dec_{msg}
Start
1. For i=1: *m*
2. For j=1: *n*
3. k=f_2(v)
4. If size(k≤T)
5. If (Φ(msg, u)<β)
6. a←msg
7. b←u
8. Dec_{msg}←[cuo(a), udo(b)]
9. End
10. End
11. End
End

Algorithm 3 Decrypting Message

The algorithm-3 mentioned above takes the input of U_{tx} (uploaded encrypted message) that offers an outcome of Decmsg (extracted message) upon processing. For this

RESEARCH ARTICLE

purpose, the algorithm-3considers all the *m* incoming traffic to the receiver node (Line-1) and stream of data *n* (Line-2). The next part of the algorithm-3 assesses an available number of multi-parties *v* (Line-3) using a simplified counting function $f_2(x)$, which ultimately yields available active multi-parties that can carry out the authentication of the legitimacy of the received data packet without involving the participation of the receiver node. The outcome of several multi-parties is maintained in the *k* matrix. Conditional logic is constructed to check if the size of k is within a threshold limit to resist any form of the overhead of multi-parties participation (Line-4). This assists in faster operation. The v multi-parties assess the message msg and user u and check if their size and elements within it Φ are less than the size of encoded keys used by multi-parties during encryption (Line-5). This operation is vital as it not only yields conformity of similar keys that are uniquely deployed during encryption but also ensures that the message is being originated via genuine user *u* (Line-5). Finally, the array consisting of encoded elements of messages a and b are obtained from message msg and *u* matrix (Line-6 and Line-7). The decrypted message is obtained by further confirming the usage of the original split keys *cuo* and *udo* (Line-8). The outcome of the decrypted message is obtained in this process. The overall flow of the complete algorithm-3 is showcased in Figure 2.

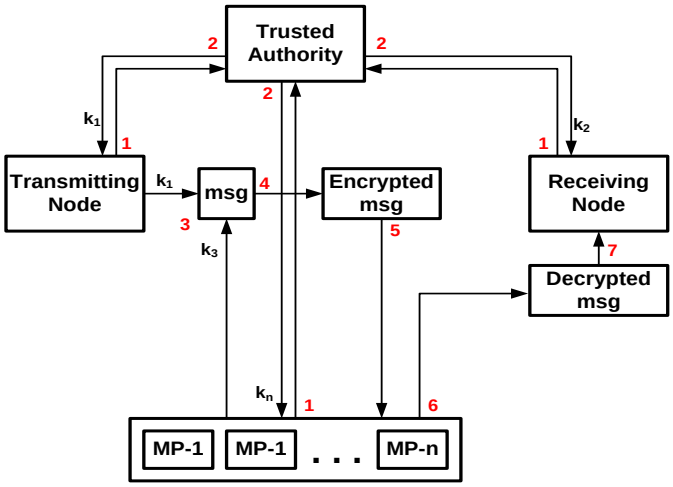

Figure 2 Operational Flow of Proposed Algorithm

According to Figure 2, the first step calls for the transmitting node, receiving node, and multi parties are required to enroll themselves with a trusted authority. The trusted authority forwards a unique key back to the transmitting node, receiving node, and multi-parties as a second step. However, multi-parties generate a further secret key based on the number of available multi-parties. These keys are retained within multi-parties, and it does not need updating to the trusted authority. In the third step, the message propagated by the transmitting node is primarily encrypted with the proposed encryption algorithm-2.

Further, it is encoded with a new key generated by multi-parties. In the fourth step, the system generates an encrypted message forwarded to the receiving node in the IoT environment. However, the receiving node does not perform decryption by multi-parties using the decryption algorithm-3.

It should be noted that the same multi-parties involved in encryption do not also need to perform decryption. For this purpose, the proposed scheme maintains a shared memory system where all the key-based information is stored in the matrix. After getting themselves authenticated by a trusted authority, any active multi-parties can easily participate in decryption. The next section discusses the result obtained from the proposed scheme.

6. RESULTS AND DISCUSSIONS

The proposed scheme introduces a novel solution for addressing the existing problems associated with incorporating a non-repudiation system taking the use case of the IoT ecosystem. This section discusses the outcome of implementing the proposed multiparty non-repudiation scheme. The discussion concerns the strategy adopted for accomplishing the study methodology and resultant obtained from implementation.

6.1. Strategies Adopted Towards Assessment

The primary strategy adopted for the proposed study is to deploy an environment of IoT considering 500-1000 sensors deployed in a simulation area of 1000x1000 m^2. The environment consists of sensors playing the role of both transmitting node and receiving node, a trusted authority, and a set of multiparty nodes. The involvement of the trusted authority is only in the preliminary round of communication for enrolling both sensor nodes (also known as IoT devices) and multiparty nodes. The complete analysis is simulated in MATLAB considering a normal 64-bit windows environment. The overall size of the aggregated and transmitted data is retained at a test value of 1000 GB. The assessment is carried out by considering that each sensor acting as an IoT device is a personal belonging of a user. Hence, the initial enrollment process consists of considering all the user's personal details, followed by encrypting them. The secondary strategy of the proposed assessment is to mainly consider the specific set of performance parameters, viz. computation overhead, delay, and processing time. The assessment concerning all individual performance metrics is carried out by considering all non-repudiation approaches influenced by a set of test aggregated data of 250 GB, 500 GB, 750 GB, and 1000 GB. The idea is to understand the impact of traffic load on the encryption and decryption operation. To carry out benchmarking, the proposed scheme is compared with frequently exercised schemes of non-repudiation observed from Section II, i.e.,

RESEARCH ARTICLE

Rivest-Shamir Algorithm (RSA) [24][25], Signature Based Scheme (SBS) [17][18], Blockchain (BC) [14][16], Certificateless-based Scheme (CLBS) [21][23], Signcryption based Scheme (SGBS) [26][27], and Public Key Based Scheme (PKBS) [13][24]. All these schemes are implemented on a similar test environment of 1000GB of overall aggregated data, which the transmitting node forwards to the receiving node. Observation is carried out over split data concerning various iterations. The proposed scheme's tertiary strategy is to observe and arrive at inference based on the overall experiment by executing the operation for 1000 simulation rounds. The parameters involved in simulation environment are highlighted in Table 1.

Table 1 Simulation Environment

Parameter	Values
Sensors	500-1000
Simulation Area	1000x1000 m^2
Simulation Rounds	1000
Data	1000 GB

This analysis aims to showcase the impact of a variable traffic data set over the discreet performance metric. The assessment also evaluates the performance analysis of computational complexity concerning temporal factors to signify the study model's effectiveness. The next section discusses the outcomes arrived at from the experiment.

6.2. Result Analysis

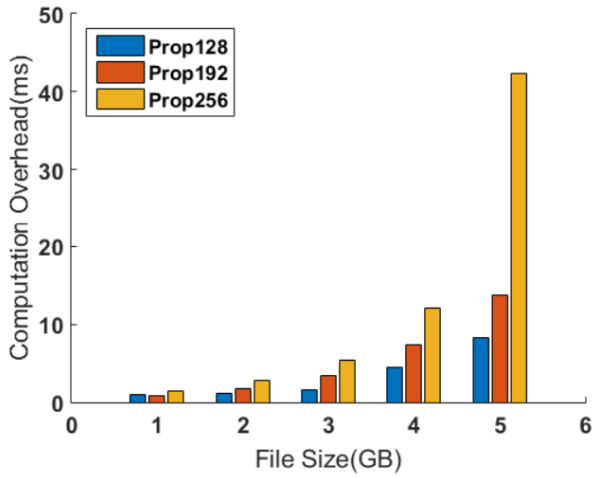

Figure 3 Impact of Key Size on Overhead

The analysis of the results is carried out to determine the impact of various critical parameters on the effectiveness of the proposed scheme. The primary evaluation parameter to observe is the impact of different key sizes on computational overhead. The evaluation of the computational overhead is carried out by assessing various resources involved in the execution of the proposed algorithms. The term resource will specifically mean memory, energy, and bandwidth here. For this purpose, the configuration of standard MicaZ mote is considered [47]. The analysis is carried out on three sets of key sizes for the proposed scheme, i.e., 128-bit, 192-bit, and 256-bit. Although the proposed system is an analytical model, any key size can be programmed to be executed because sensor nodes are more analyzed with either a secured hash algorithm or advanced encryption standard owing to their supportability of hardware acceleration. The outcome is shown in Figure 3.

From the outcome observed in Figure 3, the proposed scheme does not require maximizing the size of keys to accomplish better non-repudiation performance with increasing size of files. With the increasing traffic load, although the computation overhead increases, performance is still better when the proposed scheme utilizes a 128-bit key size. Similar performance is also noted when the key sizes are changed to different values on increasing trends. Following is the inference:

- Contribution: The proposed scheme contributes towards an effective encryption algorithm that uses split key management to balance increased security demand and reduced computation overhead demand.
- Novelty: Unlike conventional encryption, the simplified proposed scheme offers a better multiparty authentication scheme for lowered key size. Majority of the existing schemes carry forward this operation within a node which increases overhead while this operation is migrated by the multi-party in proposed scheme. Hence, overhead is significantly controlled in proposed model.
- Quantified Outcome: The adoption of a 128-bit key size offers approximately 30% and 42% of reduction of computation overhead in contrast to the adoption of a 192-bit key size and 256-bit key size, respectively.

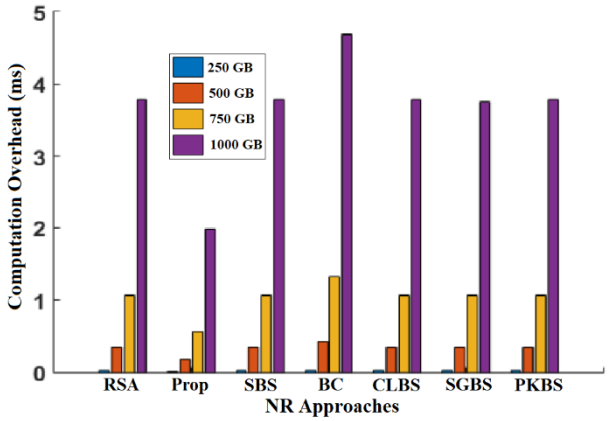

Figure 4 Comparative Analysis of Computation Overhead

RESEARCH ARTICLE

Figure 4 highlights the comparative analysis of the proposed scheme with the existing scheme concerning computation overhead. The outcome shows that the proposed scheme offers significantly reduced overhead over increasing traffic load. Following is the inference of this outcome:

- Contribution: The contribution of this finding is manifold, viz. i) the scheme of BC has higher dependencies on resources which increases memory consumption from the resource-limited IoT devices resulting in higher overhead. Hence, BC schemes are required to be more investigated to make them further lightweight for supporting such nodes, ii) there is not much significant difference between the overhead performance of RSA, SBS, CLBS, SGBS, and PKBS over increasing traffic, iii) proposed scheme scored well as neither the transmitting node nor the receiving node is required to perform any form of authentication, which is carried out by actively available multiparty resulting in enough reserved resources This contributes towards reduced computational overhead. The algorithm is not iterative; hence, less internal memory consumption is seen during execution.
- Novelty: The prime novelty of this outcome is that without using a complex encryption mechanism, the encryption function $f_1(x)$ discussed in the algorithm section ensures significantly reduced overhead, even compared to the most frequently adopted schemes. The encryption carried out in existing scheme are mainly iterative which induces computational burden. However, proposed scheme uses non-iterative scheme which significantly controls this computational burden resulting in reduced overhead among all the participating node. Irrespective of any size of the network, the presence of multiparty is another reason for reduced overhead.
- Quantified Outcome: The proposed scheme offers approximately 48% reduced computational overhead compared to the existing non-repudiation (NR) scheme.

The next observation is carried out for delay, calculated by the lag of duration caused when an encrypted message is forwarded over the IoT-distributed network to be extracted by the receiver. Note that delay should usually include the time to transmit the data and the time when the encrypted data is received. However, for effective analysis, the time to transmit the data is considered right from the beginning during the request stage of the transmitting node.

In contrast, the end time is considered when the multiparty has successfully decrypted the data. This analysis will offer the true value of delay caused when an IoT device allocates a variable traffic load in one cycle of data aggregation. The comparative analysis of delay is showcased in Figure 5.

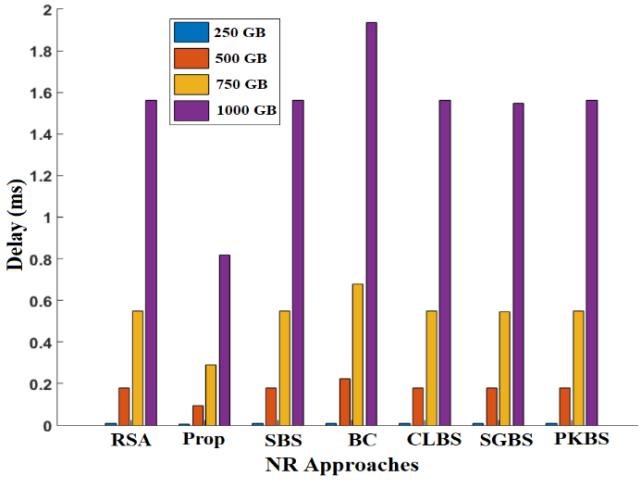

Figure 5 Comparative Analysis of D

Figure 5 highlights that the delay score for the proposed system is significantly less compared to existing approaches. Following is the inference of this outcome:

- Contribution: The prime contribution of the proposed scheme towards delay reduction are i) the mechanism and steps of decryption are completely different from encryption, unlike any existing security approaches that result in lowering the dependency on retrieving (or computing) the keys from the network causing faster decryption and ii) the proposed scheme uses shared memory for the multiparty that results in the availability of multiparty even if some might be busy in current task causing faster authentication and delivery of decrypted data.
- Novelty: Existing schemes has single key-based operation, which although can offer better security; however, its distributed operation is significantly affected. This also results in extensive delay for large scale network too. However, the proposed scheme exhibits significant delay control, even in increasing traffic load. The primary reason behind this is that the proposed scheme lowers the dependency on using singular authentication, which consumes time by splitting the speedily available keys. The secondary reason behind this is that the proposed scheme uses only two split keys but is updated every time in data forwarding. This controls memory saturation issues without compromising key generation operation.
- Quantified Outcome: The proposed scheme exhibits approximately 54% reduced delay compared to existing approaches.

The next and final part of the assessment is to evaluate processing time which is calculated by summing up the complete time duration involved in initiating the variables in

RESEARCH ARTICLE

the IoT scenario till the final accomplishment of decrypted data by the receiving node. In increasing order, the network is allocated a similar traffic load at a step size of 250 GB. At the same time, individual observation is carried out towards each time duration involved in processes. The overall outcome of processing time based on a comparison with the existing scheme is shown in Figure 6.

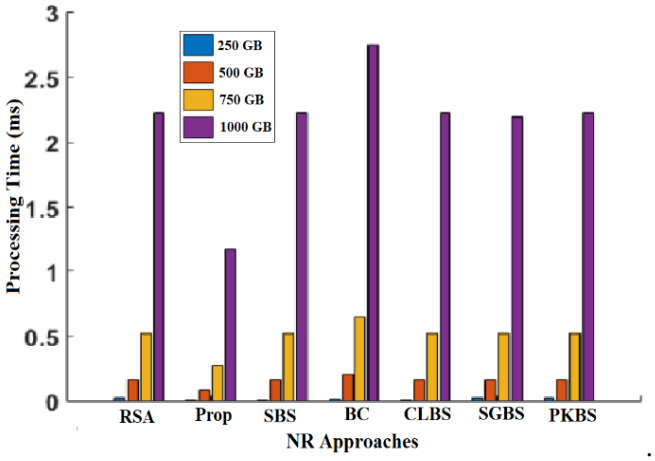

Figure 6 Comparative Analysis of Processing Time

Figure 6 highlights that the proposed multiparty non-repudiation scheme performs better with processing time than the existing scheme. Following is the conclusive inference of this outcome:

- Contribution: The core contribution of this outcome is that it states that the proposed model can undertake any number of traffic loads. At the same time, the distributed environment of multiparty can successfully assist in generating a second key for encryption and authenticating the legitimacy of the message being received. Another contributing finding is that BC, one of the most adopted approaches, is witnessed to have higher processing time when exposed to the increased traffic load. Another contribution of the study is that SGBS and CLBS also offer better performance; however, owing to their potential dependencies of key computation during the retrieval stage, the process does not support distributed environment of IoT much. Although it may work quite well in clustered-form of communication, they incur more processing time when deployed over large distributed IoT environment. PKBS approach cannot be stated as secured as they have no amendments in their public key despite various evolving private key generation techniques
- Novelty: Existing encryption mechanism has spontaneous and iterative key management operation, which not only takes up storage but also consumes higher algorithm processing time. Hence, security is ensured at the cost of higher processing time in existing scheme which renders them non-applicable in application with streaming data. The prime novelty factor associated with this outcome is that the proposed scheme can be termed a lightweight encryption scheme as it does not use any ciphering techniques reported in existing cryptography approaches. This causes lesser dependencies on complex key management operations leading to faster processing time.
- Quantified Outcome: The proposed scheme's processing time is approximately 58% reduced compared to the existing non-repudiation scheme.

7. CONCLUSION

Multiparty computation plays an essential role in security, especially suitable for large-scale environments like IoT. The proposed scheme has introduced a novel yet simplified security scheme that uses a multiparty computation approach to facilitate effective encryption and decryption for non-repudiation. The contribution of the proposed study are as follows:

i) The proposed scheme introduces a novel transformation-based encryption scheme that is not only simple but also effective for encrypting larger size of messages,

ii) novel key management is implemented in the proposed scheme, which splits the core key to offer a higher degree of secrecy while performing encryption or decryption,

iii) the model implements a shared memory for all the multiparty involved in computation which offers higher accessibility towards secret keys as well as other security-related information in case different multiparty are involved,

iv) the outcome exhibits that proposed scheme offers reduced overhead, minimal delay, and faster processing time in contrast to existing non-repudiation scheme.

The future work direction will be continued to optimize the non-repudiation performance further.

REFERENCES

[1] J. Tian, G. Ruifang and X. Jing, "Stern–Brocot-Based Non-Repudiation Dynamic Provable Data Possession," in IEEE Access, vol. 7, pp. 96686-96694, 2019, doi: 10.1109/ACCESS.2019.2916173.

[2] D. Goyal, O. P. Verma, S. Balamurugan, Sheng-Lung Peng, Design and Analysis of Security Protocol for Communication, Wiley, ISBN: 9781119555643, 1119555647, 2020

[3] D.C. Wilson, Cybersecurity, MIT Press, ISBN: 9780262542548, 0262542544, 2021

[4] I.Pekaric, C.Sauerwein, S.Haselwanter, M.Felderer, "A taxonomy of attack mechanisms in the automotive domain," Elsevier-Computer Standards & Interfaces, Volume 78, October 2021

RESEARCH ARTICLE

[5] R. Khatoun, Cybersecurity in Smart Homes-Architectures, Solutions and Technologies, Wiley, ISBN: 9781119987444, 111998744X, 2020
[6] L. Bock, Modern Cryptography for Cybersecurity Professionals, Packt Publishing, ISBN: 9781838644352, 1838644350, 2021
[7] A. Wirth, C. Gates, J. Smith, Medical Device Cybersecurity for Engineers and Manufacturers, Artech House, ISBN: 9781630818166, 163081816X, 2020
[8] M. Faisal, I. Ali, M.S. Khan, J. Kim, and S.M. Kim, "Cyber Security and Key Management Issues for Internet of Things: Techniques, Requirements, and Challenges," Hindawi-Complexity, Article ID 6619498, DOI: https://doi.org/10.1155/2020/6619498
[9] G. Jayabalasamy, S.Koppu, "High-performance Edwards curve aggregate signature (HECAS) for nonrepudiation in IoT-based applications built on the blockchain ecosystem," Journal of King Saud University - Computer and Information Sciences, 2021
[10] M. Sookhak, H. Tang, Y. He, F.R. Yu, "Security and Privacy of Smart Cities: A Survey, Research Issues, and Challenges," IEEE Communications Surveys & Tutorials, VOL. 21, NO. 2, SECOND QUARTER 2019
[11] H. A. Khattaka, M. A. Shah, S. Khan, I.Ali, M. Imran, "Perception layer security in Internet of Things," Future Generation Computer Systems, Vol.100, pp.144-164, 2019
[12] Divya K.S, Roopashree H.R, Yogeesh A C, "Non-Repudiation-based Network Security System using Multiparty Computation," International Journal of Advanced Computer Science and Applications, Vol. 13, No. 3, 2022
[13] M. M. Elamir, M. S. Mabrouk, and S. Y. Marzouk, "Secure framework for IoT technology based on RSA and DNA cryptography," Egyptian Journal of Medical Human Genetics, vol.23, No.116, 2022
[14] Chen, C.-L.; Lim, Z.-Y.; Liao, H.-C.; Deng, Y.-Y. A Traceable and Authenticated IoTs Trigger Event of Private Security Record Based on Blockchain. Appl. Sci. 2021, 11, 2843. https://doi.org/10.3390/app11062843
[15] J. Sun, X. Yao, S. Wang, and Y. Wu, "Non-Repudiation Storage and Access Control Scheme of Insurance Data Based on Blockchain in IPFS," in IEEE Access, vol. 8, pp. 155145-155155, 2020, doi: 10.1109/ACCESS.2020.3018816.
[16] F. Chen, J. Wang, J. Li, Y. Xu, C. Zhang, T. Xiang, "TrustBuilder: A non-repudiation scheme for IoT cloud applications", ACM-Computer and Security, vol.116, No.C, 2022. DOI: https://doi.org/10.1016/j.cose.2022.102664
[17] W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, G. Wang, "Digital signature scheme for information non-repudiation in the blockchain: a state of the art review," EURASIP Journal on Wireless Communications and Networking volume 2020, Article number: 56, 2020
[18] D-H Lee, K. Yim, I-Y Lee, "A Certificateless Aggregate Arbitrated Signature Scheme for IoT Environments," PubMed Central-Sensors(Basel). vol.20, No.14, 2020. doi: 10.3390/s20143983
[19] J. Kar, X. Liu, F. Li, "CL-ASS: An efficient and low-cost certificateless aggregate signature scheme for wireless sensor networks," Journal of Information Security and Applications, Vol.61, Issue C, Sep 2021. DOI: https://doi.org/10.1016/j.jisa.2021.102905
[20] J. Shen, Z. Gui, X. Chen, J. Zhang, and Y. Xiang, "Lightweight and Certificateless Multi-Receiver Secure Data Transmission Protocol for Wireless Body Area Networks" in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 03, pp. 1464-1475, 2022.
[21] K. Sudharani, P. N. K. Sakthivel, "A Secure Encryption Scheme Based on Certificateless Proxy Signature," Springer, 2018
[22] L. Harn, J. Ren, C. Lin, "Design of DL-based certificateless digital signatures," Journal of Systems and Software, Vol.82, Issue 5, pp.789-793, 2009
[23] D. Xiang, X. Li, J. Gao, X. Zhang, "A secure and efficient certificateless signature scheme for Internet of Things," Elsevier- Ad Hoc Networks, Volume 124, 1 January 2022.
[24] Kim, T.; Kim, W.; Seo, D.; Lee, I. Secure Encapsulation Schemes Using Key Recovery System in IoMT Environments. Sensors 2021, 21, 3474. https://doi.org/10.3390/s21103474
[25] J. Singh, V. Kumar, R. Kumar, "An Efficient and Secure RSA Based Certificateless Signature Scheme for Wireless Sensor Networks," Springer, 2016
[26] D. Toradmalle, J. Muthukuru, B Sathyanarayana, "Lightweight Certificate less Signcryption Scheme Based on Elliptic Curve," International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-10, August 2019
[27] S. Sharmila Deva Selvi, Pandu Rangan Chandrasekaran, "Efficient and provably secure certificateless multi-receiver signcryption," IIT Madras Conference, Volume: 5324 LNCS, pp.52 - 67, 2008, DOI: 10.1007/978-3-540-88733-1-4
[28] C. Jin, H. Zhu, W. Qin, Z. Chen, Y. Jin, J. Shan, "Heterogeneous online/offline signcryption for secure communication in Internet of Things," Elsevier-Journal of Systems Architecture, Volume 127, June 2022
[29] W. Zhang, Y. Zhang, C. Guo, Q. An, Y. Guo, X. Liu, S. Zhang, J. Huang, "Certificateless Hybrid Signcryption by a Novel Protocol Applied to Internet of Things," PubMed Central-Comput Intell Neurosci. 2022. 10.1155/2022/3687332
[30] Meshram, C.; Imoize, A.L.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S.; Barve, S.K. An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps. Sensors 2021, 21, 7039. https://doi.org/10.3390/s21217039
[31] Nayab, S. Hussain, A. Alabrah, S. S. Ullah, H. Khattak, T. M. Alfakih, I. Ullah, "An Efficient Online/Offline Signcryption Scheme for Internet of Things in Smart Home," ACM-Wireless Communications & Mobile ComputingVolume 2022, DOI: https://doi.org/10.1155/2022/4215441
[32] A. M. Abdullah, I. Ullah, M. A. Khan, M. H. Alsharif, S. M. Mostafa, and J. M-T Wu, "An Efficient Multidocument Blind Signcryption Scheme for Smart Grid-Enabled Industrial Internet of Things," Hindawi-Next-Generation Wireless Networks (NGWN) for Autonomous Intelligent Communications, Article ID 7779152, 2022, DOI:https://doi.org/10.1155/2022/7779152
[33] P. Zhang, Y. Li, H. Chi, "An Elliptic Curve Signcryption Scheme and Its Application," Hindawi-Wireless Communications and Mobile Computing, Article ID 7499836, 2022, DOI: https://doi.org/10.1155/2022/7499836
[34] Ghosh, S.; Zaman, M.; Plourde, B.; Sampalli, S. A Quantum-Based Signcryption for Supervisory Control and Data Acquisition (SCADA) Networks. Symmetry 2022, 14, 1625. https://doi.org/10.3390/sym14081625
[35] A. P. Sarr, P. B. Seye, T. Ngarenon, "A Practical and Insider Secure Signcryption with Non-interactive Non-repudiation", Springer-2019
[36] R. M. Daniel, E.B. Rajsingh, S. Silas, "A forward secure signcryption scheme with ciphertext authentication for e-payment systems using conic curve cryptography," Journal of King Saud University - Computer and Information Sciences, Vol.33, No.1, pp.86-98, 2021, DOI: https://doi.org/10.1016/j.jksuci.2018.02.004
[37] Witanto, E.N.; Lee, S.-G. Cloud Storage Data Verification Using Signcryption Scheme. Appl. Sci. 2022, 12, 8602. https://doi.org/10.3390/app12178602
[38] L. Li, X. Lu, K. Wang, "Hash-based signature revisited," SpringrOpen-Cybersecurity, vol.5, Article number: 13, 2022
[39] Abbas, G.; Mehmood, A.; Carsten, M.; Epiphaniou, G.; Lloret, J. Safety, Security and Privacy in Machine Learning Based Internet of Things. J. Sens. Actuator Netw. 2022, 11, 38. https://doi.org/10.3390/jsan11030038
[40] S. Capkun, E. Ozturk, G, Tsudik, K. Wust, "ROSEN: RObust and SElective Non-repudiation (for TLS)", ACM-Proceedings of the 2021 on Cloud Computing Security Workshop, November 2021, Pages 97–109, DOI: https://doi.org/10.1145/3474123.3486763
[41] H. K. Alper, A. Küpçü, "Optimally Efficient Multi-party Fair Exchange and Fair Secure Multi-party Computation," ACM Transactions on

RESEARCH ARTICLE

Privacy and Security, Vol.25, Issue 1, February 2022, Article No.: 3, pp 1–34, DOI: https://doi.org/10.1145/3477530
[42] P. Kalpana, "Amalgam Of Hamming Weight-Based RSA And Multi-Party Computations To Enhance Security In Multi-Cloud Ambience," International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol.8, Issue-10, August 2019
[43] 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.
[44] M. Sharaf, J. Chen, E. Keedwell, "Non-repudiation and privacy-preserving sharing of electronic health records," Taylor & Francis Online, Cogent Engineering, Vol.9, Iss.1, 2022. DOI: https://doi.org/10.1080/23311916.2022.2034374
[45] A. Kumar, "A cloud-based buyer-seller watermarking protocol (CB-BSWP) using semi-trusted third party for copy deterrence and privacy-preserving," Springer-Multimedia Tools and Applications, vol.81, pages 21417–21448, 2022.
[46] L. Wang, J. Li, L. Zuo, Y. Wen, H. Liu, W. Liu, "T-Tracer: A Blockchain-Aided Symbol Mapping Watermarking Scheme for Traitor Tracing in Non-Repudiation Data Delivery," ACM-Proceedings of the Fourth ACM International Symposium on Blockchain and Secure Critical Infrastructure, May 2022, Pages 23–34, DOI: https://doi.org/10.1145/3494106.3528674
[47] http://www.cmt-gmbh.de/MICAz.pdf (Accessed on 17-November, 2022).

Authors

Ms. Divya K. S is a Research scholar at GSSS Computer institute of engineering and technology for Women, Mysuru, under VTU, working as Assistant Professor in Computer Science Department at Kristu Jayanti College, Bengaluru, India. She has completed her B.Tech and MTech in CS. She is currently pursuing Ph.D. in the area of Network Security at VTU. She has 14 years of teaching experience.

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

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

How to cite this article:

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 (IJCNA), 10(1), PP: 84-94, 2023, DOI: 10.22247/ijcna/2023/218513.