IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 September 2023, accepted 8 October 2023, date of publication 17 October 2023, date of current version 27 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3325305

RESEARCH ARTICLE

NTRU and Secret Sharing Based Secure Group Communication for IoT Applications

SANCHITA SAHA[1,2], (Member, IEEE), ASHLESHA HOTA[1], BIKRAMJIT CHOUDHURY[1], (Member, IEEE), AMITAVA NAG[1], (Senior Member, IEEE), AND SUKUMAR NANDI[3], (Senior Member, IEEE)

[1]Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, Kokrajhar, Assam 783370, India
[2]Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, West Bengal 721657, India
[3]Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, Guwahati, Assam 781039, India

Corresponding author: Amitava Nag (amitava.nag@cit.ac.in)

This work was supported in part by PDA grant of the Central Institute of Technology Kokrajhar, India.

ABSTRACT In the technology driven era, automation and communication have attained new heights, which paved the way for an improved human lifestyle. The Internet of Things (IoT) is one of the key aspects of this domain that promises to connect real-world objects embedded with sensors, enable them to communicate, and aid in making informed decisions. However, the growth of technology for convenience has also attracted various attacks on privacy and confidentiality. Numerous classical public-key cryptography based security solutions have been adopted to evade the problems in group communication. Unfortunately, most of the solutions fail to meet computationally lightweight requirements. In this paper, we propose a lightweight NTRU (Nth Degree Truncated Polynomial Ring Units) and Secret Sharing Based Secure Group Communication Scheme that is suitable for low bandwidth communication over the Internet of Medical Things (IoMT), Vehicular Adhoc Networks (VANET) and Precision Agriculture. Theoretical analyses and illustrations demonstrate that the proposed scheme is superior in comparison to the existing schemes.

INDEX TERMS Internet of Things, NTRU, secret sharing, group communication.

I. INTRODUCTION

Internet of Things (IoT) is an interconnection of various real-world objects embedded with lightweight sensors that offers limited computations and actuations. These objects are capable of communicating with one another to exchange their sensor readings via the internet. IoT is increasingly applied to several spheres, including however, not limited to healthcare (IoMT) [1], VANET [2], and Underwater Internet of Things (UIoT) [3]. A brief application of IoT is shown in Figure 1. The exponential growth of IoT devices and its increasing applications in various spheres has generated massive amounts of data. Storing and analysing this huge amount of data is a major challenge [4]. Interpretation of sensor readings and knowledge of noisy readings add to it. IoT devices are also referred to as resource-constrained devices with regard to their limited capabilities in computation, processing, storage, and energy [5]. These limitations make them vulnerable to different attacks.

Predominantly, IoT devices are prone to various malware attacks. Malware (malicious software) is any program or file that is designed to corrupt the operating system of the sensing devices. It can also cause the dropping of packets traveling through an insecure network. These resource-constrained devices fail to accommodate complex security algorithms such as RSA or Elliptic Curve Diffie-Hellman (ECDH) [6] to run on their operating systems. Moreover, these devices do not support strong cryptographic encryption techniques. In such a situation, it becomes a cake walk for intruders to send ambiguous readings to the cloud while impersonating a genuine sensors. Tampering with a single node does not seem as a potential threat initially; however, when a series of nodes are compromised, the entire IoT network is deemed corrupted. Moreover, with the emergence of 6G networks and the growing popularity of edge computing [7], it becomes more important to secure the decisions computed at the

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

© 2023 The Authors. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

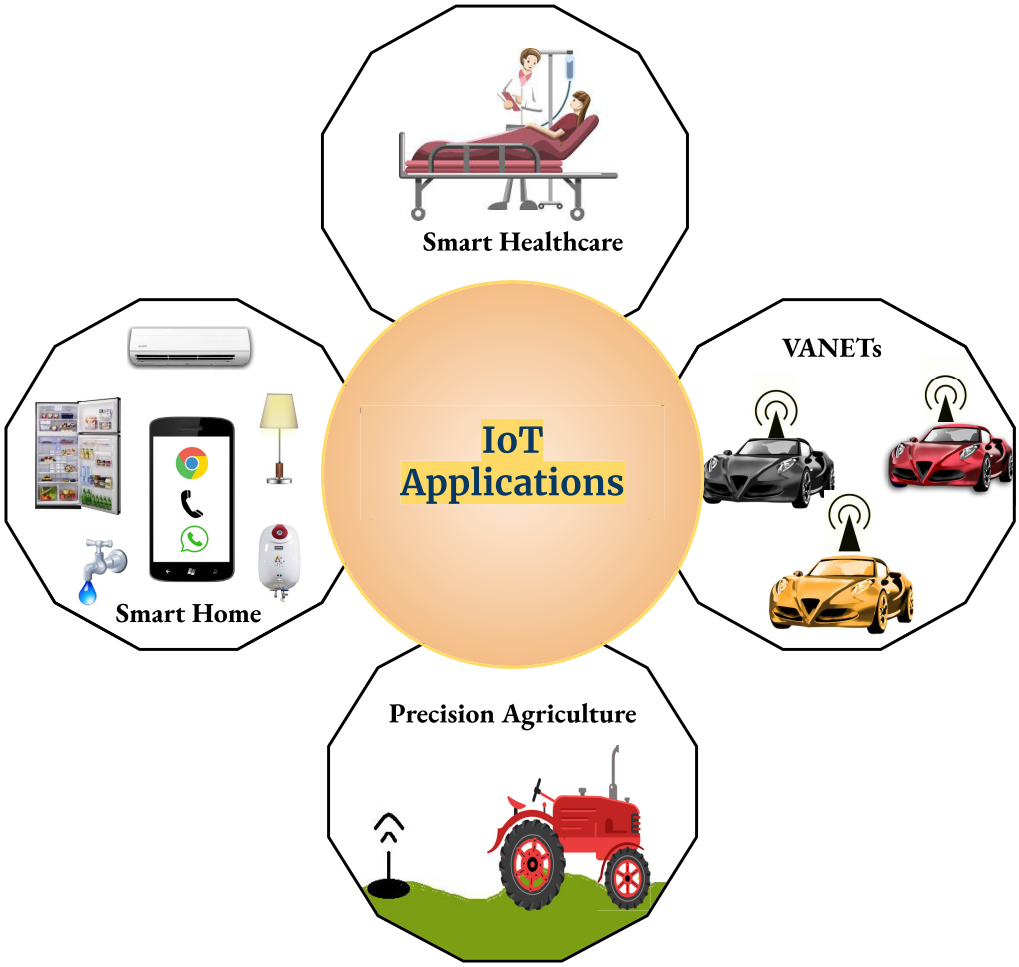


FIGURE 1. Applications of IoT.

local end while communicating those with the cloud servers. Edge computing allows remote nodes to perform more tasks than capturing environment parameters [8], [9]. This results in increased energy usage in the nodes. In such a context, a lightweight protocol is desired that compensates for the overhead of computation rather than draining itself while performing complex cryptographic operations.

Parity, collaboration, and secure communication are the key drivers of a successful IoT network implementation. One of the major challenges that one must address is securing group communication. Group communication may not always refer to the sensor level however, also to access nodes or sink (gateways) nodes. sink (gateways) nodes have relatively higher computing power as compared to the edge nodes deployed in the field. Securing the communication over the sink (gateways) nodes is crucial, as these nodes serve as hubs for collecting sensor readings from edge nodes, processing the sensor data, and communicating it to the cloud server. These nodes are at the highest risk and vulnerable to attacks.

In the recent past, many contributions have been made in this field to address these challenges, with traditional public-key cryptography such as RSA, ECC at the forefront. However, traditional public-key cryptography based approaches have the following limitations for the IoT environment:

1) The traditional approaches are not resilient to quantum attack.
2) They necessitate large key sizes which adversely affects the computational cost.

The motivations of this work are to address the aforementioned issues and to propose a NTRU and Secret Sharing based robust and lightweight approach in order to secure IoT applications.

Hoffstein et al. [10] coined NTRU, based on the hard lattice problem. It offers resistance against quantum attacks. It has the advantage of performing very fast computations, and its security lies in the well known hard problem, the shortest vector problem, that is not breakable even by super or quantum computers in polynomial time. We found this encryption

scheme suitable for resource-constrained IoT applications. However, just encrypting the data cannot prevent security attacks like authentication and impersonation. We devised a scheme incorporating NTRU along with Secret Sharing to offer a more secure and reliable solution to tackle the security threats that are prominent in IoT systems.

A. MOTIVATION AND CONTRIBUTIONS

The various security challenges and the inefficiencies in the proposed solutions with respect to one or the other aspect motivated us to put forth our efforts in search of a lightweight group communication scheme that could meet the following requirements to be well suited for IoT systems:

1) Resists quantum attacks.
2) Avoids a secured channel.
3) Cuts down computational overheads.
4) Reduces communication overheads.
5) Enables Secure group communication in IoMT, VANETs, UIoT.

Our contributions are streamlined to achieve the aforementioned objectives. We present a NTRU and Secret Sharing based group communication protocol that is suitable for low-bandwidth communication channels and can be safely adopted in securing the communication between the gateway and the cloud. The proposed scheme is effective against quantum attacks and reduces the cost of encryption and decryption to $O(nlogn)$, where n denotes the length of the reading that is to be transmitted. The major contributions of the paper are summarized as follows:

1) A Secret sharing and NTRU based lightweight secure group communication protocol is proposed in the paper.
2) The proposed scheme facilities encryption of sensor readings in IoT, thereby eliminating the vulnerabilities to various security attacks.
3) The proposed scheme is verifiable and runs in $O(nlogn + tlog^2t)$ asymptotic time.

The proposed scheme is thus suitable to be operated over low bandwidth networks for the facilitation of the smooth processing of resource constrained applications like IoMT, VANETs and UIoT. The proposed scheme is elaborated in Section III.

B. ORGANIZATION OF THE PAPER

The rest of the paper is oriented in the following fashion: A detailed review of the works carried out in this realm is briefly discussed in Section II. In Section III, the essential prelims are described in brief. Section IV presents our proposed scheme. We discuss the correctness and security analysis of the scheme in Section V. The performance of the system is discussed in Section VI. We compare our system with a few recent approaches in Section VII. Finally, Section IX concludes our efforts.

II. RELATED RESEARCH

The phenomenal expansion of the IoT has resulted in application domains in which it is crucial to ensure users' privacy and safety [11]. IoT data may reveal private information, while data tampering may cause system malfunctions. It is necessary to ensure security in IoT without sacrificing efficacy and scalability. Secure group communication among IoT devices is an essential and demanding research concern in this context. The development of secure communication protocols has been significantly aided by the utilization of public-key cryptography. This section is devoted to discuss previous state-of-the-art security schemes particularly those focusing on IoT applications.

Public-key cryptosystems are extremely important for the security of IoT. Numerous researchers introduced different security schemes based on classical public-key cryptosystems such as RSA, ECC etc. Jose and Vijyalakshmi [12] presented a detailed review of the major challenges in IoT network systems and put forward a novel approach based on elliptic curve cryptography (ECC). ECC based schemes involve scalar multiplication, i.e., $Q = kP$, where a point P maps to a point Q when multiplied with k. This scheme can be extended through a series of point additions and multiplications on point P. For the choice of very large values of k, the problem becomes intractable. Wang et al. [13] focused on an application-based bilinear pairing security scheme for smart home fire emergencies. The scheme is efficient against the forged sender and tackled the man in the middle attack. Yan et al. [14] proposed an identity based encryption technique for secure access control to resist unauthorized access. This scheme is also built on the concept of bilinear pairing. Guo et al. [15] provided the idea to secure IoT systems with biometrics to prevent unregistered participants. However, this fails to withstand scenarios like - *"you cannot protect the one which you cannot see"*. The proposed scheme is applicable to the perceptron layer. However, it may not be efficient when scaled to the transport or routing layers. Hou et al. [16] developed a scheme that relied on bilinear pairing and used hash functions. However, the scheme is computationally inefficient and did not resist quantum attacks. Hsu et al. [17] proposed a user-oriented multi-group key establishment using secret sharing for secure and efficient communication in wireless body area networks. Their scheme is based on integer factoring, which is faster than public-key computations. Khasawneh and Kadoch [18] designed a security scheme that relied on ECC and hash function. It stood resilient against collusion attacks; however, it is computationally heavy and post-quantum challenges are not taken into consideration.

NTRU is widely regarded as the most practical post-quantum public-key cryptosystem. Due to the fact that the development of quantum computing has rendered conventional public-key cryptosystems like RSA and ECC insecure, NTRU is the preferable cryptosystem. A number of different NTRU-based security approaches have been

proposed as potential solutions to the security issues that are present in resource-constrained IoT devices. Singh and Padhye [19] detailed the algebraic structures used in NTRU and their possible variations. Most of the variants of NTRU are based on addition and modular multiplication operations. Shuai et al. [20] proposed a NTRU-like public-key cryptographic paradigm to secure group communication. They scaled their approach to high performance Group-based nTRU (GTRU) and claimed that GTRU is more effective against lattice based attacks. Chaudhary et al. [21] formulated a lattice based mutual authentication scheme that incorporates a third-party key exchange protocol to perform encryption and decryption between users and cloud. The proposed solution withstand attacks like man in the middle and proved effective against data masquerading attack. Wang et al. [22] proposed a certificate-less authentication scheme based on NTRU. The scheme claimed to perform best and was carefully tailored for the Satellite Terrestrial Integrated Network. Gupta et al. [23] presented a lattice based small integer solution and in-homogeneous small integer solution to build a secure protocol applicable in IoMT. The protocol ensures the inevitable security requirements and addresses post-quantum security.

After a thorough review of the state of arts, we could figure out the following:

1) Most of the existing schemes are based on traditional public-key cryptographic schemes such as RSA and ECC that necessitate large key sizes, thereby increasing the cost of computation.
2) NTRU based existing schemes are effective against quantum attacks; however, they lack the notion of a common secret group key for a conductive IoT communication environment.
3) The running time of existing NTRU based schemes is surprisingly less, inspiring us further to explore a group communication protocol with secret sharing.

By investigating and analysing several recent related work on IoT security solutions, especially in the setting of lattice based cryptography,which has significant impact on post quantum challenges but little research attention, this study seeks to fill this gap.

III. ESSENTIAL PRELIMS OF NTRU AND SECRET SHARING BASED SCHEME

A. BACKGROUND

Lattice based cryptography is a public-key cryptographic system. It is based on the problem of finding the shortest vector between two points in a n-dimensional space. Lattice is a linear combination of independent vectors say $\{b_1, b_2, \ldots, b_n\}$ [24] and lattice $\mathrm{L} = \sum_{i=1}^{n} x.b_i$ where x is a random number. The different symbols used in this paper are recorded in Table 1.

B. REVIEW OF NTRU-KE KEY EXCHANGE PROTOCOL

The proposed scheme employs the NTRU-KE key exchange protocol introduced by Lei and Liao [25] for the common key establishment. Let us assume that the dealer $\mathcal{D}$ wants to establish a common key with each participant $\mathcal{P}_i$ from the set $\mathcal{P} = \{\mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3, \ldots, \mathcal{P}_n\}$. The following tasks are performed for the common key establishment:

- $\mathcal{D}$ must choose suitable public parameter N, p and q.
- $\mathcal{D}$ chooses two random polynomials f_i and g_i where the polynomial f_i must additionally satisfy the inverse property in the truncated polynomial ring R_q, where $R_q = \mathbb{Z}_q[X]/(X^N + 1)$.
- $\mathcal{P}_i$ computes $h_i \equiv f_i^{-1} * g_i (mod\ q)$ and communicates h_i to the dealer $\mathcal{D}$.
- Upon receipt of h_i, $\mathcal{D}$ chooses f_j such that it satisfies the inverse property in R_q, and g_j and r_j.
- $\mathcal{D}$ computes $h_j \equiv f_j^{-1} * g_j (mod\ q)$ and $e_j \equiv pr_j * h_i + f_j (mod\ q)$ and communicates h_j, e_j to $\mathcal{P}_i$.
- Upon receipt of h_j and e_j, $\mathcal{P}_i$ chooses r_i and computes $e_i \equiv pr_i * h_j + f_i (mod\ q)$ and communicates e_i to $\mathcal{D}$ and further computes $a_i = f_i * e_j (mod\ q)$, $K_i = a_i (mod\ p) = f_i * f_j (mod\ p)$.
- $\mathcal{D}_i$ receives e_i and computes $a_j = f_j * e_i (mod\ q)$, $K_j = a_j (mod\ p) = f_i * f_j (mod\ p)$
- The common key established is $K_i = K_j = f_i * f_j (mod\ p)$

The security of this algorithm is mapped to solving the *closest vector problem*. *Closest vector problem* is a computationally hard problem in lattice. NTRU-KE is quantum resistant, has better resistance to distributed attack, and is computationally faster than the ECDH algorithm [25].

C. THRESHOLD SECRET SHARING SCHEME

In the proposed scheme, authentication of the participating nodes is performed at the cloud server using secret sharing scheme. Shamir [26] and Blakley [27] are the first to independently propose two distinct secret sharing schemes. The scheme introduced by Shamir [26] is widely accepted and adopted. In this scheme, a secret, say $\mathcal{S}$ is encoded into n parts that are referred to as *shares*. The *shares* are distributed among a group of participants $\mathcal{P}_i$, for $(i = 1, 2, \ldots n)$, over the set $\mathcal{P}$ in such a way that:

- Each of the participants $\mathcal{P}_i$ holds exactly one *share*.
- No individual *share* reveals anything about the secret $\mathcal{S}$.
- A combination of t (t is referred to as threshold value) or more ($\leq n$) participants can reconstruct the secret $\mathcal{S}$ with their *shares*.
- A group of $(t - 1)$ or less participants does not reveal anything about the secret $\mathcal{S}$.

D. OVERVIEW OF HOMOMORPHISM ENCRYPTION BASED SECRET SHARING

Zhang et al. [28] proposed one verifiable secret sharing scheme by combining the property of homomorphism

encryption with secret sharing. The scheme is described briefly as follows:

1) Initialization:
   a) The dealer $\mathcal{D}$ randomly selects $x_1, x_2, \ldots, x_n$ in the finite field $GF(q)$ and distributes them among the participants $\mathcal{P}_i$, for $(i = 1, 2, \ldots n)$.
   b) $\mathcal{D}$ randomly selects $t-1$ elements $\{a'_1, a'_2, \ldots, a'_{t-1}\}$ in the finite field $GF(q)$ and constructs the $(t-1)^{\text{th}}$ degree polynomial $f(x)'$ as:

$$f(x)' = a'_0 + \sum_{i=1}^{t-1} a'_i x^i \ (mod\ q) \tag{1}$$

   where, a'_0 is the random number and the corresponding shares are generated as $y'_i = f(x_i)'$, for $1 \leq i \leq n$. $\mathcal{D}$ distributes the random number a'_0 among the participants $\mathcal{P}_i$, for $(i = 1, 2, \ldots n)$.
2) Secret distribution:
   a) The dealer $\mathcal{D}$ randomly selects $t-1$ elements $\{a_1, a_2, \ldots, a_{t-1}\}$ in the finite field $GF(q)$ and constructs the $(t-1)^{\text{th}}$ degree polynomial $f(x)$ as:

$$f(x) = a_0 + \sum_{i=1}^{t-1} a_i x^i \ (mod\ q) \tag{2}$$

   where, a_0 is the secret and the corresponding shares are generated as $y_i = f(x_i)$, for $1 \leq i \leq n$.
   b) $\mathcal{D}$ performs the following computation according to the property of (+, +) - homomorphism secret sharing:
   $s_i = y_i \oplus y'_i$, for $1 \leq i \leq n$ and distributes s_i among the participants $\mathcal{P}_i$, respectively.
   c) $\mathcal{D}$ also distributes $h(a_0)$ among $\mathcal{P}_i$, where $h(.)$ is a one-way function.

IV. SYSTEM MODEL

The proposed model is a three-tier architecture, with the lowest layer containing field sensor nodes. These nodes are deployed on the field whose attributes are to be recorded. The task of these sensor differs from application to application, such as humidity sensors in precision agriculture, wearable wrist watch pulsometers in healthcare, or speedometers in VANETs. A brief application of IoT is shown in Figure 1.

The intermediate layer, consisting of sink (gateways) nodes, is responsible for communicating the sensor data with the cloud server. The cloud server is assumed to be at the topmost layer. In the rest of the paper, the cloud is denoted as the dealer $\mathcal{D}$ and each sink (gateways) node is treated as a participant, $\mathcal{P}_i$. A pictorial representation of the system is shown in Figure 2.

We assume the notation of a trusted key generation center (KGC), the dealer $\mathcal{D}$, and the set of participants $\mathcal{P}_i$, for $(i = 1, 2, \ldots n)$. KGC is responsible for the registration of participants willing to be a part of the group communication. KGC computes the session key for the participants and shares

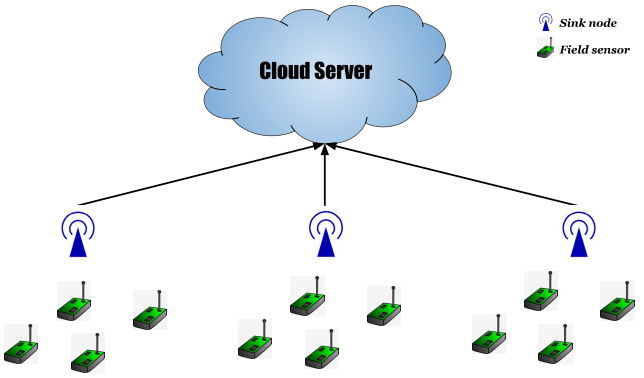


FIGURE 2. IoT system model.

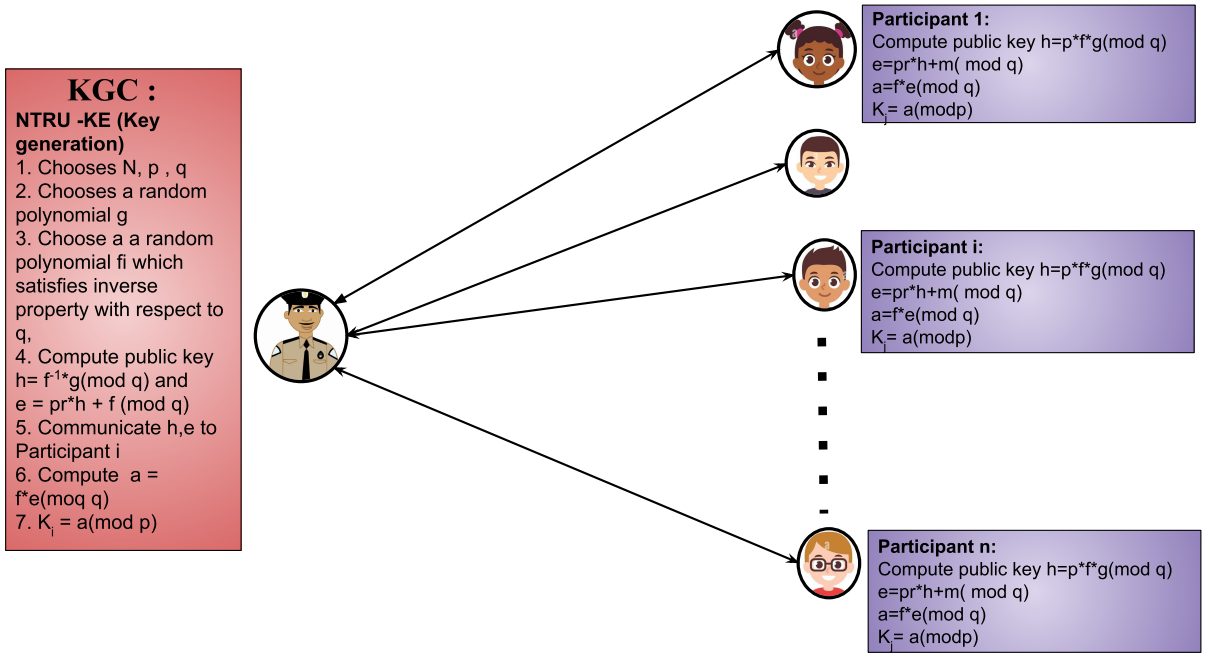
TABLE 1. List of symbols.

Symbol	Meaning
$\mathcal{D}$	Dealer
$\{\mathcal{P}_i\}_{i=1}^{n}$	Set of n participants
N, p, q	Public parameters
$GF(q)$	Finite field with order q
$UID_i,\ 1 \leq i \leq n$	Unique identifier of i^{th} participant
$\mathcal{K}_i$	Shared key between $\mathcal{P}_i$ and $\mathcal{D}$
$\mathcal{S}$	Original group secret
$\mathcal{S}_0, \mathcal{S}_1$	Partial group secrets
$\mathcal{S}_2$	Noise to be distributed to all participants
$\mathcal{S}_3$	Partial secret $\mathcal{S}_1$ combined with noise $\mathcal{S}_2$
$hash(\cdot)$	One way hash function

it with the dealer $\mathcal{D}$ and each of the participants $\mathcal{P}_i$. The proposed method includes three phases: (i) initialization, (ii) registration, and (iii) group key generation.

In our proposed scheme, we split the original secret $\mathcal{S}$ into two parts: $\mathcal{S}_0$ and $\mathcal{S}_1$. These split secrets, $\mathcal{S}_0$ and $\mathcal{S}_1$, are shared via different methods to ensure enhanced double-layer security. The communication flow of the proposed security scheme is as shown in Figure 3 and described as follows:

1) *Initialization:* KGC chooses suitable values of the public parameters N, p, q to initialize the NTRU-KE [25] exchange.
2) *Registration:* Participants who want to take part in group communication must register themselves and obtain a *Unique Identifier*, *UID*. This is private to the participant, and knowledge of this *UID* is limited to the participant and the KGC. KGC is tasked with communicating the UID_i of each participant $\mathcal{P}_i$ to $\mathcal{D}$, who is responsible thereon for client authentication and the exchange of messages.
   In a likely situation when a faulty node or participant is to be removed from the group, $\mathcal{D}$ must trigger a message to the KGC to do the needful task. KGC then removes the faulty participant and recomputes the group session key again. In the case of the addition of new participants, a similar procedure is followed.
3) *Group Key Generation:* The generation of the group key is carried out in the following way:



The subscripts mentioned in text are avoided in the above pictorial representation.

FIGURE 3. Communication-flow of proposed scheme.

a) *Sharing of UID and partial group secret* $\mathcal{S}_0$

i) KGC establishes a common key by the NTRU-KE [25] with each of the participant $\mathcal{P}_i$, for $i = 1, 2, \cdots, n$, as discussed in Section III-B. Now KGC has a set of keys corresponding to each participant $\mathcal{P}_i$ i.e, $\mathcal{K} = \{ \mathcal{K}_1, \mathcal{K}_2, \mathcal{K}_3, \cdots, \mathcal{K}_n \}$

ii) KGC generates UID_i for each participant $\mathcal{P}_i$ and the partial group secret $\mathcal{S}_0$.

iii) The XOR and Sum of UID_i and $\mathcal{S}_0$ is then transmitted to the participant $\mathcal{P}_i$ through the common key established as mentioned in Step i) and discussed in Section III-B.

b) *Noise calculation and broadcasting*

i) KGC uses Shamir's secret sharing scheme [26] to distribute a *noise*, $\mathcal{S}_2$ to all the participants as:

$$y' = f(x) = \mathcal{S}_2 + a'_1 x + a'_2 x^2 + a'_3 x^3 + \cdots + a'_{n-1} x^{n-1}, \tag{3}$$

where, $\mathcal{S}_2$ is the *noise*, and $a'_1, a'_2, a'_3, \cdots, a'_n$ are the coefficients of the polynomial $f(x)$ randomly chosen by KGC. Here, KGC uses *UID*s of the participants to compute the value of y'_i for i^{th} participant. Considering the number of participants, say t willing participants to communicate, the equation (3) becomes,

$$f(x) = \mathcal{S}_2 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{t-1} x^{t-1} \tag{4}$$

the value of x is chosen in such a way, so that $f(x_i) \neq f(x_j)$. This is ensured by choice of values of $x_i = UID_i$. As a result, KGC obtains a set of tuples where elements are in the form $(x, f(x))$ i.e., $\{ (UID_1, f(UID_1)), (UID_2, f(UID_2)), (UID_3, f(UID_3)), \ldots, (UID_t, f(UID_t)) \}$

ii) Using the keys, from the set $\mathcal{K}$, KGC transmits the share value of $f(x_i)$ to each participant $\mathcal{P}_i$ by encrypting the share value with key as the UID_i of the corresponding participant.

c) *Additive Secret Sharing*

i) KGC uses the additive secret sharing scheme [28] to distribute y and $\mathcal{S}_2$ among the participants. KGC constructs the polynomial $f(x)$ as:

$$y = f(x) = \mathcal{S}_3 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{n-1} x^{n-1}, \tag{5}$$

where, $\mathcal{S}_3$ is the sum of *noise* and partial secret $\mathcal{S}_1$, and $a_1, a_2, a_3, \cdots, a_n$ are the coefficients of the polynomial $f(x)$ randomly chosen by KGC. Here, the KGC uses the UID_i of the participants to compute the value of y_i for i^{th} participant. Considering the number

of participants, say t willing participants to communicate, the equation (5) becomes,

$$y = f(x) = \mathcal{S}_3 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{t-1} x^{t-1} \quad (6)$$

the value of x is chosen in such a way that $f(x_i) \neq f(x_j)$. This is ensured by the choice of values of $x_i = UID_i$.

ii) KGC then computes individual shares s_i' as: s_i' = $y_i + y_i'$ and hash($\mathcal{S}$), the one way hash of the original secret $\mathcal{S}$.

iii) KGC transmits (s_i', hash($\mathcal{S}$)) to each of participant $\mathcal{P}_i$.

iv) KGC shared the set of unique identifiers and the hash of the secret value $\mathcal{S}$ to $\mathcal{D}$.

v) A group of t or more participants willing to share their updates with $\mathcal{D}$, must come together and reconstruct the group secret to establish their authenticity.

d) *Secret Reconstruction*

i) The secrets can be reconstructed using *Lagrange's Interpolation* as follows:

$$noise = \sum_{i=0}^{t-1} y_i' \prod_{\substack{j=0 \\ j\neq i}}^{t-1} \frac{x - x_j}{x_i - x_j} \quad (7)$$

and

$$\mathcal{S}_3 = \sum_{i=0}^{t-1} s_i \prod_{\substack{j=0 \\ j\neq i}}^{t-1} \frac{x - x_j}{x_i - x_j} \quad (8)$$

where $x_i = UID_i$; The *UID* is computed from the information received from the KGC.

ii) The participants compute $\mathcal{S}_1 = \mathcal{S}_3$ - *noise*.

iii) The original secret $\mathcal{S} = \mathcal{S}_0 + \mathcal{S}_1$.

iv) Participant $\mathcal{P}_i$ computes the hash value of $\mathcal{S}$ and verifies it with the value of hash($\mathcal{S}$), already received from KGC.

e) *Communication over Cloud*

i) The interested t group of participants submits their *UIDs* and group secret $\mathcal{S}$ to the cloud.

ii) The cloud checks the hash value of the received secret, compares that with the computed one, and discards it upon disagreement; otherwise, accept.

iii) After establishing their identities, participants submit their data in NTRU encrypted form to $\mathcal{D}$.

iv) $\mathcal{D}$ decrypts the data and analyzes it to make decisions.

On successful completion of these steps, each participant $\mathcal{P}_i$ can claim its authenticity to the dealer $\mathcal{D}$ and share the update with it.

V. CORRECTNESS AND SECURITY ANALYSIS

We validate the proposed scheme with subject to its correctness and security.

A. CORRECTNESS ANALYSIS

During the registration phase, KGC assigns a UID_i to each participant $\mathcal{P}_i$ in the group. KGC then distributes the shares to each participant in that group. Each participant $\mathcal{P}_i$ has the pair $(UID_t, f(UID_t))$. We know that KGC has constructed a $t-1$ degree polynomial to allow t or more participants to communicate. Any combination of t or more participants can recover the secret $\mathcal{S}$ to establish their identity. The participant must share the value of their share and each unique registration identifier allocated to them by KGC to the dealer $\mathcal{D}$. This is sufficient for reconstruction when t participants come together and compute the secret using Lagrange interpolation. The secret is reconstructed as discussed in Section IV 3d.

The correctness of the original secret $\mathcal{S}$ is validated by participants and cloud both. They compute the hash value of $\mathcal{S}$ and verifies it with the value of hash($\mathcal{S}$), already received from KGC.

Let us assume an attacker outside the group tries to establish communication by sharing his fake UID_k such that UID_k does not belong to the set of *UIDs* maintained by KGC and submits his share $\mathcal{S}$. When the dealer $\mathcal{D}$ receives (UID_k, $\mathcal{S}_k$), it computes the secret $\mathcal{S}''$ that is not equivalent to $\mathcal{S}$. Moreover, it verifies if UID_k belongs to *UIDs* or not. If not, then the attacker is not entertained.

B. SECURITY ANALYSIS

The security of the proposed scheme while reconstructing $f(x)$ from fewer than t participants is based on Shamir's secret sharing scheme [26]. Without the knowledge of the private key parameter (i.e. f_i), the participants $\mathcal{P}_i$ cannot determine the *UIDs* of one another. If a participant wants to break this scheme with known parameters, its difficulty is equal to solving the hard problem, the *shortest vector problem*, that is not breakable even by super or quantum computers in polynomial time. The *UIDs* of the participants are known only to the dealer $\mathcal{D}$, as it provides *UID* to each participant during the registration phase. The proposed scheme withstands the following attacks performed by any adversary:

1) INSIDER AND OUTSIDER IMPERSONATION ATTACK

The proposed scheme prevents unauthorized access by an adversary. During the registration phase, KGC assigns *UID* to each of the participants. The values of the secrets are encrypted using the NTRU-KE. The secret $\mathcal{S}$ is not visible to anyone outside the group. Insider curious participants cannot impersonate as other participants without the knowledge of the *UID* that is private to KGC, dealer $\mathcal{D}$, and corresponding participant.

2) FORWARD AND BACKWARD SECRECY OF GROUP COMMUNICATION

The proposed scheme maintains the forward and backward secrecy of the group communication. Forward secrecy

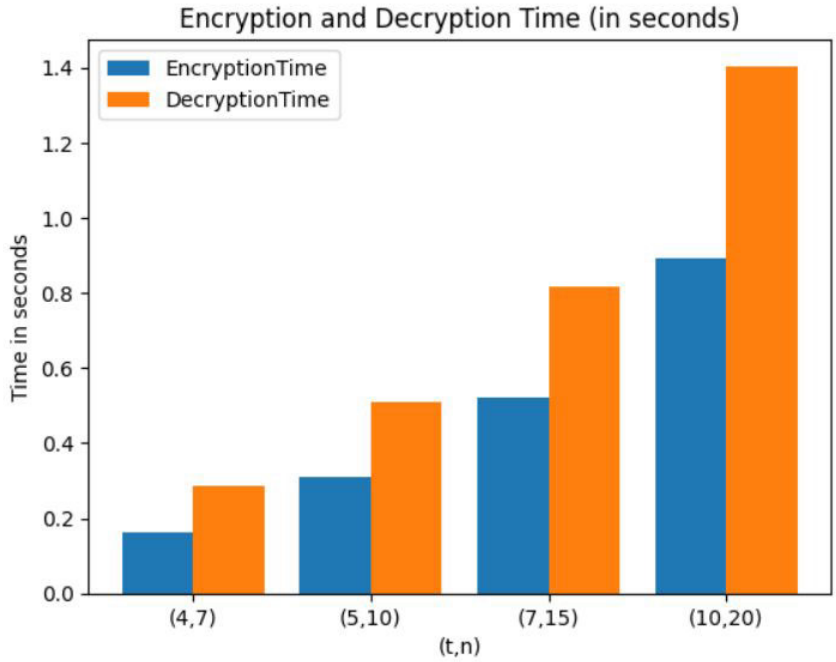


FIGURE 4. Time required for (t,n) clients for encryption and decryption with N = 100, p = 3, q = 32.

signifies that any new participant in the group cannot access the messages of the past communication records, and Backward secrecy signifies that the participant who has been removed or has decided to opt out cannot access the communication updates any longer. Both the secrecy are maintained by KGC. The dealer $\mathcal{D}$ requests KGC to distribute a new group key after the addition or removal of a participant in the group. This is essential in some cases where, in the IoT system, one or more sensors from a sensor suite may drain out of battery, or are physically tampered with or damaged, and it is not possible for these sensors to take part in the communication any longer.

VI. SIMULATION RESULTS AND PERFORMANCE EVALUATION

This section is devoted to assess our proposed methodology. The simulation is carried out on an AMD processor with 8 GB of RAM and Python 3. Our experiment demonstrates that the choice of values of 100, 3, and 32 for the public parameters N, p, and q, respectively, is in good agreement with theoretical analysis and claims. Figure 4 illustrates the time consumed in seconds for encryption and decryption in various case studies. The values on the X-axis pertain to the (t,n) tuple, where n is the total number of clients and t is the minimum number of clients whose collaboration is mandatory for the secret reconstruction.

The proposed scheme is computationally faster than ECDH-based schemes. It incorporates NTRU encryption to send data updates to the cloud that take $O(nlogn)$ using Fast Fourier transformations. The proposed scheme is resilient to quantum attacks and is computationally lighter than ECDH and RSA-based schemes. It involves matrix computations and is thus more suitable for resource-constrained applications in IoT systems. It is also communication efficient, as the secret key does not need to be computed every time for the same group of participants. Moreover, the proposed scheme overcomes impersonation attacks and maintains the secrecy of forward and backward communication records in group communication.

VII. COMPARATIVE ANALYSIS

The proposed scheme is compared with some recent research available in the literature. The parameters against which the performance of our technique is compared are as follows:

- *The cryptographic technique*: Our proposed scheme is based on NTRU and Secret Sharing. The schemes [16], [18], [29] relies on other cryptographic techniques such as bilinear pairing, ECC, hash function & verifiable secret sharing techniques.
- *Post-quantum security*: Quantum computers are high-speed computers that can solve many difficult problems in polynomial time. NTRU is based on SVP problem that still stands to be unsolved by a supercomputer in polynomial time.
- *Computationally inexpensive*: Our proposed technique takes $O(tlog^2t)$ for the reconstruction of the secret, where t is the threshold value. NTRU performs the complex encryption and decryption operations very quickly.
- *Verifiable*: Our proposed scheme involves verification at both the participant side and cloud server.
- *Forward and Backward secrecy in group communication*: Forward secrecy means that the new participant in the group cannot access the messages of the past

TABLE 2. Comparison of the proposed scheme with [16], [18], and [29].

Basis for comparison	[16]	[18]	[29]	Our scheme
Cryptographic technique	Bilinear pairing and hash function	ECC and hash function	Verifiable secret sharing scheme	NTRU and Secret Sharing
Year	2021	2021	2022	-
Resilient to quantum attacks	No	No	No	Yes
Computationally inexpensive	No	No	Yes	Yes
Effective against Impersonation attack	Yes	Yes	Yes	Yes
Computational costs	NA	NA	$O((t+1)\|q\|+r)$	$O(nlogn+tlog^2t)$
Forward and Backward secrecy	NA	NA	NA	Yes

Here 't' denotes the threshold value, 'n' denotes the length of message and 'NA' means either the aspect is not applicable to or available in the scheme

communication records, and Backward secrecy means that the participant who has been removed or has decided to opt out cannot access the communication updates any longer.

- *Impersonation attack*: When a participant $\mathcal{P}_i$ pretends to be participant $\mathcal{P}_j$ with a concealed motive to capture the private data or send updates with $\mathcal{P}_j$'s credential. The scheme is effective against impersonate attacks as the *UIDs* of each participant are a private asset to the corresponding participant and KGC.

Table 2 displays the comparison of our proposed scheme with a few other schemes reported in the literature. It is evident from Table 2 that our proposed scheme outperforms the existing schemes with regard to the aforementioned parameters.

VIII. APPLICATION AREAS OF THE PROPOSED SCHEME

The proposed scheme has vivid applications in different spheres. Owing to its computational advantage, it can be deployed in several sectors. For instance, in a VANET, two vehicles desirous of communication may exchange their location coordinates. However, it is possible for an adversary to capture this information, which endangers the privacy and safety of the two vehicles. The response time in such a highly dynamic system is very low, and NTRU becomes extremely handy in such cases where the vehicles do not necessarily spend much time in cryptographic operations. The second application area of the proposed scheme is the IoMT network. In an ideal IoMT network, we expect the health parameters of a patient situated in a remote area to be communicated to the diagnostic center or to the cloud for the detection of health ailments. The proposed scheme not only maintains the confidentiality of health parameters by encrypting them but also ensures that the health attributes are communicated to the desired addressee through an access control feature offered by secret sharing. The third application area is precision agriculture, where the time constraints are too strict. For instance, if stormy weather is likely to be predicted by the sensors, it is equally important to communicate this message to the concerned person so that precautionary measures can be taken to avoid the crops being flooded with excessive rain. The other prospective use is to establish effective and trusted group communication among the sensor nodes so that failure or malfunction of one node can be timely communicated to others in the group without disclosing it to non-trusted nodes.

IX. CONCLUSION

IoT devices are prone to several security attacks that intend to exploit the normal functioning of the system. To address a few security concerns, we have proposed a novel verifiable NTRU and Secret Sharing Based Secure Group Communication Scheme that prevents the unauthorized access and exploitation of secret messages that are being transmitted from the sink (gateways) nodes to the cloud server while maintaining Forward and Backward secrecy. The data updates are encrypted before being transmitted to the cloud server. The proposed scheme is computationally more efficient than RSA and ECDH based schemes and can be adopted for resource-constrained devices in IoT applications.

REFERENCES

[1] S. Panja, A. K. Chattopadhyay, A. Nag, and J. P. Singh, "Fuzzy-logic-based IoMT framework for COVID19 patient monitoring," *Comput. Ind. Eng.*, vol. 176, Art. no. 108941, Dec. 2023.

[2] S. M. Hatim, S. J. Elias, N. Awang, and M. Y. Darus, "VANETs and Internet of Things (IoT): A discussion," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 12, no. 1, pp. 218–224, Oct. 2018.

[3] T. Qiu, Z. Zhao, T. Zhang, C. Chen, and C. L. P. Chen, "Underwater Internet of Things in smart ocean: System architecture and open issues," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4297–4307, Jul. 2020.

[4] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, Dec. 2015, pp. 336–341.

[5] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, 2010.

[6] D. R. Stinson and M. Paterson, *Cryptography: Theory and Practice*. Boca Raton, FL, USA: CRC Press, 2018.

[7] Q. V. Khanh, V.-H. Nguyen, Q. N. Minh, A. D. Van, N. Le Anh, and A. Chehri, "An efficient edge computing management mechanism for sustainable smart cities," *Sustain. Comput. Inform. Syst.*, vol. 38, Art. no. 100867, Apr. 2023.

[8] V. K. Quy, A. Chehri, N. M. Quy, N. D. Han, and N. T. Ban, "Innovative trends in the 6G era: A comprehensive survey of architecture, applications, technologies, and challenges," *IEEE Access*, vol. 11, pp. 39824–39844, 2023.

[9] V. K. Quy, N. T. Ban, D. Van Anh, N. M. Quy, and D. C. Nguyen, "An adaptive gateway selection mechanism for MANET-IoT applications in 5G networks," *IEEE Sensors J.*, vol. 23, no. 19, pp. 23704–23712, Oct. 2023.

[10] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*. Portland, OR, USA: Springer, Oct. 2006, pp. 267–288.

[11] R. Billure, V. M. Tayur, and V. Mahesh, "Internet of Things—A study on the security challenges," in *Proc. IEEE Int. Advance Comput. Conf. (IACC)*, Jun. 2015, pp. 247–252.
[12] D. V. Jose and A. Vijyalakshmi, "An overview of security in Internet of Things," *Proc. Comput. Sci.*, vol. 143, pp. 744–748, 2018.
[13] C. Wang, J. Shen, Q. Liu, Y. Ren, and T. Li, "A novel security scheme based on instant encrypted transmission for Internet of Things," *Secur. Commun. Netw.*, vol. 2018, pp. 1–7, Jan. 2018.
[14] H. Yan, Y. Wang, C. Jia, J. Li, Y. Xiang, and W. Pedrycz, "IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT," *Future Gener. Comput. Syst.*, vol. 95, pp. 344–353, Jun. 2019.
[15] Z. Guo, N. Karimian, M. M. Tehranipoor, and D. Forte, "Hardware security meets biometrics for the age of IoT," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2016, pp. 1318–1321.
[16] Y. Hou, X. Huang, Y. Chen, S. Kumar, and H. Xiong, "Heterogeneous signcryption scheme supporting equality test from PKI to CLC toward IoT," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 8, p. e4190, Aug. 2021.
[17] C.-F. Hsu, L. Harn, and B. Zeng, "UMKESS: User-oriented multi-group key establishments using secret sharing," *Wireless Netw.*, vol. 26, no. 1, pp. 421–430, Jan. 2020.
[18] S. Khasawneh and M. Kadoch, "ECS-CP-ABE: A lightweight elliptic curve signcryption scheme based on ciphertext-policy attribute-based encryption to secure downlink multicast communication in edge envisioned advanced metering infrastructure networks," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 8, p. e4102, Aug. 2021.
[19] S. Singh and S. Padhye, "Generalisations of NTRU cryptosystem," *Secur. Commun. Netw.*, vol. 9, no. 18, pp. 6315–6334, Dec. 2016.
[20] L. Shuai, H. Xu, L. Miao, and X. Zhou, "A group-based NTRU-like public-key cryptosystem for IoT," *IEEE Access*, vol. 7, pp. 75732–75740, 2019.
[21] R. Chaudhary, A. Jindal, G. S. Aujla, N. Kumar, A. K. Das, and N. Saxena, "LSCSH: Lattice-based secure cryptosystem for smart healthcare in smart cities environment," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 24–32, Apr. 2018.
[22] S. Wang, G. Zhao, C. Xu, Z. Han, and S. Yu, "A NTRU-based access authentication scheme for satellite terrestrial integrated network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2022, pp. 3629–3634.
[23] D. S. Gupta, N. Mazumdar, A. Nag, and J. P. Singh, "Secure data authentication and access control protocol for industrial healthcare system," *J. Ambient Intell. Humanized Comput.*, vol. 14, no. 5, pp. 4853–4864, May 2023.
[24] C. Ma and J. Ao, "NTRU based group oriented signature," Cryptol. EPrint Arch., Tech. Rep., 2009.
[25] X. Lei and X. Liao, "NTRU-KE: A lattice-based public key exchange protocol," Cryptol. ePrint Arch., Tech. Rep., 2013.
[26] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.
[27] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl. (MARK)*, Jun. 1979, pp. 313–318.
[28] E. Zhang, J. Peng, and M. Li, "Outsourcing secret sharing scheme based on homomorphism encryption," *IET Inf. Secur.*, vol. 12, no. 1, pp. 94–99, 2018.
[29] A. Shivhare, M. K. Maurya, J. Sarif, and M. Kumar, "A secret sharing-based scheme for secure and energy efficient data transfer in sensor-based IoT," *J. Supercomput.*, vol. 78, no. 15, pp. 17132–17149, Oct. 2022.

SANCHITA SAHA (Member, IEEE) received the B.Tech. and M.Tech. degrees in CSE. She is currently pursuing the Ph.D. degree with the Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, Kokrajhar, Assam, India. She is also an Assistant Professor with the Department of Computer Science and Engineering, Haldia Institute of Technology, Haldia, West Bengal, India. She has a number of research publications in international journals and conference proceedings. Her research interests include information security and federated learning. She is a member of the Institution of Engineers, India.

ASHLESHA HOTA received the B.Tech. degree in computer science and engineering from the Central Institute of Technology Kokrajhar, Assam, India. Her research interests include machine learning, deep learning, and their applications.

BIKRAMJIT CHOUDHURY (Member, IEEE) is currently an Assistant Professor with the Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, with more than ten years of experience in teaching and research. He has published research articles in many international conferences and journals. His research interests include the Internet of Things security, blockchain, and network security. He is a member of ACM and IEI.

AMITAVA NAG (Senior Member, IEEE) is currently a Professor of computer science and engineering with the Central Institute of Technology Kokrajhar, Assam, India. He has more than 50 research publications in various international journals and conference proceedings. His research interests include the IoT, information security, and machine learning. He is a fellow of IEI.

SUKUMAR NANDI (Senior Member, IEEE) received the Ph.D. degree in computer science and engineering from the Indian Institute of Technology Kharagpur, India, in 1995. He was a Visiting Senior Fellow with NTU, Singapore, from 2002 to 2003. He is currently a Senior Professor with the Department of Computer Science and Engineering, Indian Institute of Technology Guwahati, India. He has more than 450 international journals and international conferences publications. His research interests include computer networks, computer and network security, machine learning, VLSI, computer architecture, and computational linguistic. He is a Senior Member of ACM. He is a fellow of the Indian National Academy of Engineering, the Asia–Pacific Artificial Intelligence Association, the Institution of Engineers, India, and the Institution of Electronics and Telecommunication Engineers, India.