Received: 9 October 2021 | Revised: 9 April 2022 | Accepted: 20 April 2022

DOI: 10.1002/ett.4540

RESEARCH ARTICLE

WILEY

Secure cloud-based data storage scheme using postquantum integer lattices-based signcryption for IoT applications

Dharminder Dharminder[1] | Uddeshaya Kumar[1] | Ashok Kumar Das[2] | Basudeb Bera[2] | Debasis Giri[3] | Sajjad Shaukat Jamal[4] | Joel J. P. C. Rodrigues[5,6]

[1]Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Chennai, Tamil Nadu, India

[2]Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad, India

[3]Department of Information Technology, Maulana Abul Kalam Azad University of Technology, Nadia, West Bengal, India

[4]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

[5]College of Computer Science and Technology, China University of Petroleum (East China), Qingdao, China

[6]Instituto de Telecomunicações, Covilhã, Portugal

Correspondence
Ashok Kumar Das, Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India
Email: iitkgp.akdas@gmail.com

Funding information
Deanship of Scientific Research at King Khalid University, Grant/Award Number: R.G.P. 2/48/42; FCT/MCTES, Grant/Award Number: UIDB/50008/2020; Brazilian National Council for Scientific and Technological Development, Grant/Award Number: 313036/2020-9

Abstract

The primary objective of postquantum cryptography (also known as quantum-resistant cryptography) is to develop the cryptographic systems that need to be robust against both quantum and classical computers, and can also interoperate with the existing communications protocols and networks. In an Internet of Things (IoT) environment, the communicated messages contain sensitive information that are transmitted over an open channel, where message integrity and data privacy become challenging tasks. Although several traditional cryptographic security protocols can be applied for IoT security and data privacy, such as authentication, access control, key agreement, and digital signature, but they are not resilient against quantum attacks. To overcome these issues, in this article, we first present an advanced and efficient construction of postquantum lattice-based signcryption scheme, and then apply the constructed lattice-based signcryption in IoT applications, where data sensed by the deployed IoT smart devices is securely stored at the cloud, via the gateway nodes (aggregators). The data stored at the cloud servers cannot be even modified by them due to the involved signatures generated by the aggregators. The formal security analysis shows the robustness of our designed lattice-based signcryption scheme. Other detailed information security analysis and a performance analysis with the traditional number-theoretical based public key cryptosystems show the efficacy, and significantly better security and functionality features of the proposed scheme under the lattice-based postquantum context.

1 | INTRODUCTION

Cloud computing becomes the next growing step in the Internet based computing paradigm. It offers delivering "Information and Communications Technology (ICT)" resources as a service. Internet of Things (IoT) is a kind of networking environment where several smart devices (physical as well as virtual objects) can be deployed, which can sense the

information from their surrounding areas and the sensing information is then aggregated by their nearby gateway nodes (called the *aggregators*). The aggregator then analyzes the information and finally put the data in the semi-trusted cloud servers. As a result, IoT can definitely provide the scalability, performance and "pay-as-you-go" nature of cloud computing infrastructures.[1] In the following, we can classify the "IoT/cloud infrastructures" and their related services to the following models:[1]

- **Infrastructure-as-a-Service (IaaS) IoT/clouds**: Under this category, the services are provided by accessing all the deployed IoT smart devices and actuators in the cloud.
- **Platform-as-a-Service (PaaS) IoT/clouds**: In this case, PaaS IoT services are used to access to data, not to hardware. It is then clearly a differentiator as compared to that for IaaS.
- **Software-as-a-Service (SaaS) IoT/clouds**: The uses of SaaS IoT services are for accessing entire IoT-based software applications via the cloud, "on-demand" and in a "pay-as-you-go fashion." Usually, SaaS IoT applications are created over a PaaS infrastructure.

There are several IoT-based applications which can be also applied under the cloud infrastructures, such as healthcare systems;[2-8] wildlife monitoring;[9] smart agriculture;[10-12] drones;[13,14] blockchain-based supply chains,[15] and so on. Figure 1 also shows different applications related to IoT. Since the huge amount of data is gathered by the aggregators in an IoT application, the need for big data storage in cloud is very crucial for big data analytics. Thus, the techniques related to "secure storage", "verification", and "auditing" of Big data in a cloud computing environment are also necessary.[16]

In an IoT environment (eg, smart home applications, e-healthcare, and smart grids), the smart devices are connected via the Internet. The deployed IoT smart devices produce a huge amount of data that are mostly private and confidential. For instance, in the e-healthcare application, the data may be patient-related information. Therefore, the hardware, software as well as network connectivity will be secured enough for IoT objects to work effectively. Any connected equipment, from manufacturing to deployment, can be hacked if the security is not maintained in the IoT applications. Once an adversary or a hacker gains the control of an IoT environment, he or she can obtain the object's functionality and also steal the private and confidential data of the user. As a result, if the information is revealed to the adversary, it can affect the entire network. Hence, security and privacy are required in such IoT environments.[17,18]

An IoT environment is vulnerable to different kinds of security attacks/threats as the communication in such environment often occurs over the Internet.[19,20] Das et al[19] discussed several security and functionality requirements, and also provided several suggested security solutions to secure an IoT infrastructure. In addition, Sherali et al[20] discussed various technological solutions using cryptography and the protocol standards for IoT.

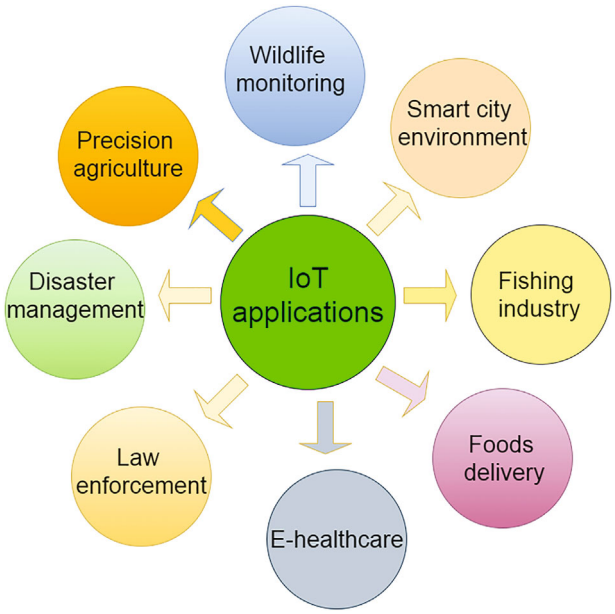

FIGURE 1 Various applications related to IoT enviromment

Public-key cryptosystem works under a pair of keys (public key, private key), whereas the public key is made public on the channel accessible by everyone during communication, and the private key is kept secret and only known to the owner. Both encryption and digital signature are highly essential tools that are used to guarantee a reliable connection on the public channel. In the cryptography, a method of first digitally signing a message, then encrypting the result has been introduced to ensure confidentiality and authenticity. In this step, the message's sender signs the message first, and then encrypts it with his private key; the number of cycles increases during signature generation and encryption, and message expansion results in transmission overhead. Signcryption combines signature and encryption into a single logical step to save time, and ensures data confidentiality and authenticity during transmission. A private-key generator (PKG) in an identity-based encryption is explained in Figure 2, where the sender (A) and the receiver (B) send their identities ID_A and ID_B to the trusted PKG, respectively. The PKG then generates the private (secret) keys SK_A and SK_B for the entities A and B, respectively.

In 1997, Zheng[21] introduced the most important concept of signcryption. Signcryption has been categorized in two scenarios: (1) two user phases and (2) multiuser phases. In the first scenario, there is a single sender and a user, whereas multiuser setting corresponds to multiple users and senders. In general, a multiuser setting describes the realistic model as single-user security (insider and outsider) is not necessarily followed in a multiuser setting. Moreover, both insider and outsider security have been defined in terms of an adversary's computation power as well. In outsider-case, the adversary obtains essentially public parameters and public keys of participating entities, whereas insider-case allows the adversary to obtain some of the private keys as well. The insider-case security model is stronger and covers all the security attributes. A complete definition of strong insider security model is introduced by Libert and Quisquater.[22] In this article, we consider two types of security attacks: (1) "indistinguishable against chosen cipher attack (IND-CCA)" and (2) "existential unforgeable against chosen message attack (EUF-CMA)".

Post-quantum cryptography (PQC) is a classical cryptography that can withstand attacks from a big quantum computer. It does not exploit any quantum properties as well as specialized hardware. It relies on hard mathematical problems, just like the traditional cryptography that we have today. However, PQC avoids using integer factorization problem (IFP) and discrete logarithm problem (DLP) for encrypting data. The classical cryptographic schemes based on IFP and DLP are vulnerable to attacks with respect to a quantum computer. For instance, PQC algorithms do not require any quantum hardware for encryption as well as decryption, and they are based on new mathematical problems (for instance, LWE, SIS, and shortest vector problem (SVP)) that are not vulnerable to known quantum computing attacks. In addition, the PQC includes building encryption around mathematical "structures", called lattices, using systems that are purely dependended on codes, solve complicated problems involving multiple variables, and many more.

In the last decade, the researchers are paying much attention to the lattice-based cryptography, because it provides better security even in modern quantum-era. Moreover, we are mainly considering two lattice-based problems: (1) "learning with errors (LWE)" and (2) "short integer solution (SIS)".

1.1 | Motivation

In general, if κ be a security parameter, the public key of a cryptosystem based on lattice is of $O(\kappa^2)$ and the computation time is of $O(\kappa^2)$. On the other side, in the number-theoretic classic cryptosystems (such as, RSA[23] and ElGamal[24]), the size of the public key used and computation time are of $O(\kappa)$ bits and $O(\kappa^3)$, respectively. By using the learning with errors

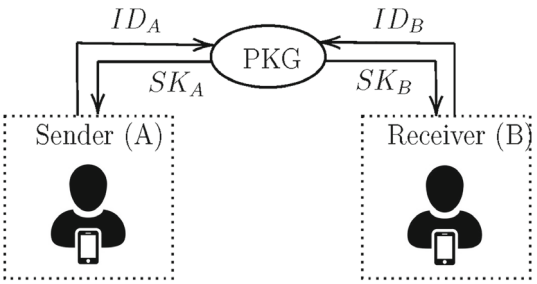

FIGURE 2 Private-key generator (PKG) in an identity-based encryption

(LWE), the size of public key can be further reduced to $\tilde{O}(\kappa)$. Therefore, in the lattice-based security schemes (eg, signcryption mechanism where both the encryption and signature of a message are jointly done by the sender and the receiver being the verifier can validate the signature and also retrieve the message simultaneously), there are computational advantages as compared to the usual number-theoretic classic cryptosystems.

Asif[25] reviewed the practicality of post-quantum cryptography in IoT, where the smart devices are resource constrained. A detailed comparative study of state of art postquantum key exchange protocols was done by analyzing the factors, like memory usage, computational time and clock cycle counts on hardware platforms. It was shown that LBC will be a very promising alternative for IoT-related networking environments. Consider a real IoT environment as mobile health (M-Health) system where an M-Health system can be integrated with IoT in order to support preventive/proactive healthcare services by connecting IoT-based wearable smart devices and persons. Ullah et al[26] suggested an efficient and provable secure certificate based signature, encryption and signcryption (CBCSES) scheme, where all these primitives are combined together. Since the LBC-based key exchange protocols are practical for IoT devices, the LBC-based signcryption schemes are also practical for IoT devices like the wearable devices in an M-Health system.

In an IoT application, majority of the deployed IoT smart devices are resource-limited in terms of their storage and computational power. Thus, it is viable to apply the lattice-based security solutions in IoT environment.[27] Furthermore, the lattice-based cryptosystems provide significantly better security as compared to the traditional public key cryptosystems as the lattice-based computational problems are resistant to quantum attacks. Due to these aforementioned issues, we propose a novel cloud-based data storage scheme using the integer lattices-based signcryption for IoT applications, where the cloud servers store the signcrypted information from the aggregators where the data are security gathered by the aggregators from their respective deployed IoT smart devices.

1.2 | Research contributions

In this article, we first propose an identity-based signcryption scheme in a well-studied lattice using learning with error. The security of the proposed scheme is based on the worst-case hardness of learning with error (LWE) problem that is proved in the standard model in a lattice. Also, the shorter identity based signature is used in the proposed construction in random lattice, as in signature, the proposed construction uses the nonzero bits only of a plaintext.[28] The proposed scheme ensures "multi-user indistinguishable under insider chosen cipher attack (MU-IND-iCCA2)" as well as "multi-user strong unforgeability under insider chosen message attack (MU-SUF-iCMA)" security attributes. Furthermore, the proposed signcryption scheme uses simple linear algebraic operations which require low computation. Next, we apply the constructed lattice-based signcryption scheme for secure data storage in cloud for IoT applications, where the data is stored in forms of signcrypted formats. Thus, the cloud servers in the cloud center cannot modify any store data as the signatures associated with the data are involved and the signatures are created using the secret (private) keys of the aggregators.

The main contributions are now listed below:

- Centered on the lattice problems, we have suggested a new signcryption approach without using a random oracle. Although, it has been observed that a simple structure of signcryption by merging IND-CCA2 secure encryption and SUF-CMA digital signature does not ensure MU-SUF-iCMA protection (See Section 4.3.1), but our proposed signcryption structure ensures both MU-SUF-iCMA and MU-IND-iCCA2 security (see Section 4.3.1).
- To improve the lattice-based signcryption, we have proposed a lattice-based advanced signcryption to ensure both MU-SUF-iCMA and MU-IND-iCCA2 protection under the assumptions of LWE and SIS.
- The constructed signcryption mechanism is then applied in a cloud-based IoT environment where the data from various IoT smart devices are securely gathered by the aggregator nodes in the network. The aggregators verify the signature of each message received from every IoT device in an IoT application, and after successful signature verification, the message is retrieved. Next, an aggregator makes signcryption of the retrieved messages using its own private key and the public key of the destination cloud server, and then sends the messages to the cloud server. The in-charge cloud server stores the received messages in the cloud after verifying the signatures on the received messages.
- A detailed security analysis has been done to show the robustness of the scheme. In addition, the proposed scheme is also resilient against other kinds of attacks, like "replay", "man-in-the-middle", "impersonation", "physical sensor nodes capture" and "priviledged-insider" attacks. In addition, the proposed scheme also supports untraceability and anonymity properties.

- A comparative performance with the existing public key cryptosystems has been also conducted to show the effectiveness of the proposed lattice-based signcryption scheme.

1.3 | Article outline

The article is organized as follows. The related work has been discussed in Section 2. In Section 3, we discuss the relevant basic preliminaries that are essential to discuss and analyze the proposed scheme. Section 4.3.1 then discusses the security model for multiuser setting secure IBSC. The formal model of an identity (ID)-based signcryption is also discussed in this section. Various phases related to the proposed construction of our lattice based signcryption are discussed in Section 5. A detailed formal security analysis for the proposed scheme is provided in Section 7. While the performance analysis of the proposed scheme with other competing public key cryptosystems is discussed in Section 8, the article is concluded in Section 9.

2 | RELATED WORK

Various cryptographic constructions have been proposed in the standard model based on LWE and SIS problems: (1) public key encryptions,[29-31] and (2) digital signature schemes.[32-39] Furthermore, there are some key encapsulations[34,40] and ID-based encryptions,[34,39] that are proposed in the literature.

In the following, we discuss some recently proposed existing state of art schemes related to signcryption that are associated to lattice-based cryptography.

In 2018, Sun and Zhang[41] presented an identity-based ring signcryption scheme. It was shown to be provably secure under the standard model and the assumption of the hardness of lattice problem, known as the "small integer solutions (SIS)". The authors mentioned that their approach is applicable in various applications, like "electronic cash payment system" and "security certification lightweight authentication".

In 2019, Yan et al[42] designed an attribute-based signcryption scheme that relies on the intractability of lattices. Their proposed scheme is proved as "indistinguishable against the inner adaptive-chosen ciphertext attacks (IND-CCA2)" as well as "existentially unforgeable against inner chosen-message attacks (EUF-CMA)".

In 2019, Yang et al[43] suggested a lattice-based signcryption method that is based on the standard model. Their scheme offers "indistinguishability against adaptive chosen ciphertext attacks (IND-CCA2)" and EUF-ACMA under the assumptions of the "ring learning with errors (RLWE)" and the "ideal short integer solution (ISIS)".

In 2021, Yu and Bai[44] proposed a blind signcryption scheme that was based on the hardness of "learning with error (LWE)" problem as well as the "Chameleon hash function". Their scheme can be applied in several applications, such as e-commerce, smart cards, and mobile communication. In addition, their proposed protocol meets the "indistinguishability under adaptive chosen ciphertext attack (IND-CCA2)" and "unforgability against chosen-message attacks (UF-CMA) security requirements".

In 2021, Yu et al[45] suggested a certificate-less lattice-based signcryption scheme. Their scheme supports indistinguishability from IND-CCA2 under the intractability of the LWE problem as well as UF-CMA under the hardness of the short integer solution (SIS) problem.

In 2021, Hou et al[46] proposed a bilinear pairing based heterogeneous signcryption protocol for IoT environment. Their proposed scheme has the ability to transfer the data in a heterogeneous environment from public key infrastructure (PKI) to certificateless cryptosystem (CLC). In addition, they used a cloud server to execute the equality test on several ciphertexts. Their strategy achieves the "existential unforgeability against adaptive chosen message attacks (EUF-CMA)", "one-way chosen-ciphertext attacks (OW-CCA)", and IND-CCA.

Khasawneh and Kadoch[47] suggested an "elliptic curve cryptography (ECC) based signcryption scheme" for smart grid system in 2021. Their scheme is based on "ciphertext-policy attribute-based encryption (CP-ABE)" in order to achieve secure, fine-grained access control for multirecipient communication between the utility control center and a group of smart meters. However, their scheme does not resist the quantum attacks.

In 2021, Le et al[48] also proposed a lattice-based signcryption scheme. Their scheme is secure against insider attacks under the LWE assumption and the intractability of the SIS problem. Their suggested technique is resistant to the IND-iCCA1 and OW-iCCA1 insider attacks, as well as the "(strong) unforgeability under chosen message attack

(SUF-iCMA)". In Table 1, we have listed the cryptographic techniques, advantages and limitations of various existing state of art signcryption schemes.

3 | PRELIMINARIES

In this article, we have used the sets $\mathbb{Z}$ for integers, $\mathbb{R}$ for real numbers, and $\mathbb{Z}_q$ for the residue class modulo prime q, respectively, where $\mathbb{Z}_q = \{0, 1 \cdots, q-1\}$. Also, $\mathbb{Z}^n$ denotes set of n-tuple integer elements, $\mathbb{Z}_q^n$ denotes set of n-tuple integer elements modulo q, $\mathbb{Z}^{n\times m}$ represents the set of matrices having n rows and m column vectors. Furthermore, various notations and their significance are discussed in Table 2.

Assume that κ is a security parameter and $q = Poly(n)$ denotes an integer where n is necessarily the dimension of concerned lattice. A small letter denotes column vector and a capital letter corresponds to a matrix. The Euclidean length of a n-dimensional vector, say $\vartheta = (\vartheta_1, \vartheta_2, \ldots, \vartheta_n)$ is presented by $||\vartheta||^2 =< \vartheta, \vartheta >= \sum_{i=1}^{n} \vartheta_i.\vartheta_i$. A negligible function $\epsilon(n)$ represented as $\epsilon(n) = \log(n)$ and defined $\epsilon : \mathbb{N} \to [0, 1]$, where $\epsilon(n)$ follows the inequality $\epsilon(n) < \frac{1}{g(n)}$ for arbitrary function g and sufficiently large n. Additionally, if one consider two random variables X_1 and X_2, then the statistical distance between X_1 and X_2 is $\varsigma(X_1, X_2) = \frac{1}{2}\sum_{\omega\in\Omega} |Pr[X_1 = \omega] - Pr[X_2 = \omega]|$ and X_1, X_2 are ϵ close to each other if $\varsigma(X_1, X_2) \leq \epsilon$.

3.1 | Lattice

A two-dimensional (2D) lattice as shown in Figure 3, is treated as a discrete subgroup of R^n, where R^n denotes the "real space for some positive integer n." The following is a description of lattice.

Definition 1. Let $a_1, a_2, \ldots, a_m \in R^n$ be the "linearly independent tuples." Then, a lattice (Δ) generated by the basis vectors $A = \{a_1, a_2, \ldots, a_m\}$ is denoted $\Delta = L(a_1, a_2, \ldots, a_m) = \{Ax = \Sigma_i x_i\, a_i : x \in \mathbb{Z}^m\}$, where

$$\Delta = \mathbf{A}\cdot\mathbf{x} = \begin{bmatrix} | & | & & | \\ a_1 & a_2 & \ldots & a_m \\ | & | & & | \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix}$$

TABLE 1 Cryptographic techniques, advantages and limitations of some existing state of art signcryption schemes

Scheme	Year	Cryptographic techniques	Advantages	Drawbacks/limitations
Yu and Bai[44]	2021	* Lattice * Chameleon hash function	* Secure against IND-CCA2 and UF-CMA	* Can be improved with threshold signcryption algorithm from lattice
Yu et al[45]	2021	* Lattice * Universal hash functions	* Protected from IND-CCA2 and UF-CMA	* Certificate-less lattice-based approach
Hou et al[46]	2021	* Bilinear pairing Hash functions	Secure against EUF-CMA, OW-CCA, and IND-CCA	* Computationally heavy * Does not resist quantum attacks
Khasawneh and Kadoch[47]	2021	* ECC * Hash functions * ABE	* Secure against collusion attack	* Does not resist quantum attacks
Le et al[48]	2021	* Lattice * Hash function	* Resistant to the IND-iCCA1 and OW-iCCA1 insider attacks and SUF-iCMA	* Can be improved with signcryption with multiciphertext equality test and/or flexible multiciphertext equality test

TABLE 2 Used notations and there descriptions

Notation	Description
S	Sender of message
R	Receiver of message
$\mathcal{A}$	Adversary
C	Challenger
σ	Scaling factor of Gaussian
Ψ	Linear functional
Δ	Integer lattice
ϵ	Negligible function
ϑ	Integer n-tuple
$\mathbb{Z}$	Set of all integers
$\mathbb{R}$	Set of real numbers
q	Large prime number
$h(.)$	One-way hash function
$\oplus$	XOR operation
F_q	Finite field modulo prime q
LWE	Learning with Errors assumption
SIS	Short Integer Solution assumption
$\mathbb{PK}_x$	Lattice-based public key for an entity X
$\mathbb{SK}_x$	Lattice-based private key for an entity X
CS_k	kth cloud server in the cloud
$Appl_j$	jth IoT application
RA_j	jth trusted registration authority for $Appl_j$
$Aggr_j$	jth aggregator node (gateway node) for $Appl_j$
SN_i	ith IoT smart device associated with $Appl_j$
$Data_{SN_i}$	Sensing data related to an IoT smart device SN_i
TS_{SN_i}	Current timestamp created by SN_i
TS_{Aggr_j}	Current timestamp created by $Aggr_j$
ΔT	Maximum permitted transmission delay

The integers m represent the rank of the concerned matrix and n denotes the dimension of lattice.

The lattice Z_q^m that satisfies $Z_q^m \subseteq \Delta \subseteq Z^n$ for some integer q is called **q-ary lattice**, as "q times vector of lattice also belongs to it." Let $A \in Z_q^{n \times m}$ denotes a matrix modulo $q = poly(n)$, which depends only on the dimension of lattice. There are two types of n-dimensional q-ary lattices $\Delta_q^{\perp} = \{x \in Z^n \ : \ A\,x = 0 \ (mod\ q)\}$ and $\Delta_q^{u} = \{x \in Z^n \ : \ u = A\,x \ (mod\ q) |\ x \in Z^m\}$, where q and $m > n$ are denoted as integers. Various cryptographic techniques are constructed by using these q-ary lattices. Here, $A\,x = 0$ means

$$\mathbf{A} \cdot \mathbf{x} = \begin{bmatrix} | & | & & | \\ a_1 & a_2 & \dots & a_m \\ | & | & & | \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

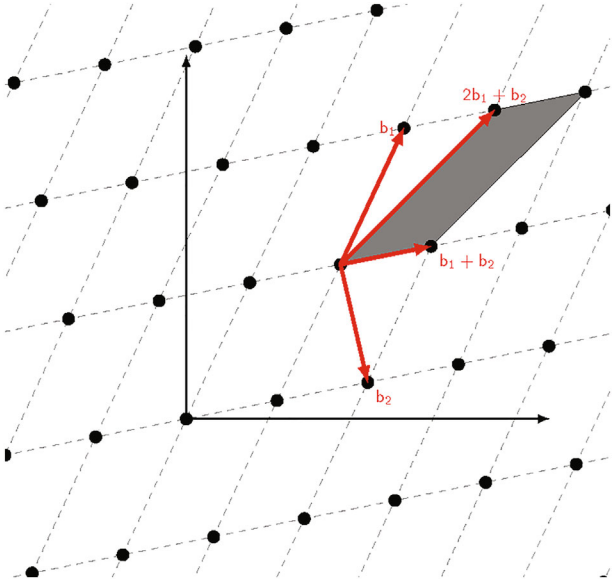

FIGURE 3 Two dimensional lattice spanned by tuples b_1 and b_2

and $u = A\ x$ means

$$\mathbf{A} \cdot \mathbf{x} = \begin{bmatrix} | & | & & | \\ a_1 & a_2 & \dots & a_m \\ | & | & & | \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{bmatrix}.$$

Since $\Delta_q^u(A) = \Delta_q^{\perp}(A) + z$ for arbitrary z where z satisfies $A\ z = u\ (mod\ q)$, so $\Delta_q^u(A)$ is a coset of $\Delta_q^{\perp}(A)$. If $b \in Z_q^n$, then $\Delta_b^{\perp}(A) = \{a \in Z^n : A\ a = b\ mod\ q\}$ be a coset of q-ary lattice. Now, suppose $n > 0$, $q > 2$ be some integers, ξ over Z_q be an arbitrary distribution and $\vartheta \in Z_q^n$, then "$_{\vartheta,\xi}$ is the distribution of $(a, a^t\vartheta + e) \in Z_q^n \times Z_q$", where $a \leftarrow Z_q^n$, and $e \leftarrow \xi$.

Definition 2 ((Learning with errors).). Given an integer $q = O(\kappa)$ depends on dimension of the lattice and a distribution ξ on Z_q, then $LWE_{q,\ \xi}$ has to distinguish between Uniform distribution $(Z_q^n \times Z_q)$ and $A_{\vartheta,\xi}$.

Let $\sigma > 0$ be given, then Φ_σ denotes the normal distribution on $[0, 1)$ along with mean 0 and standard deviation $\frac{\sigma}{\sqrt{2\pi}}$, under modulo one. When a normal random variable e follows distributions Φ_σ, then $\hat{\Phi}_\sigma$ is discrete normal random variable $[a.e]$ modulo q.

In the following, we now discuss the following:

- **Hardness of LWE**[31]: Suppose $\sigma = \sigma(m) \in (0, 1)$, $q = O(\kappa)$ (depends on dimension of the lattice) is a prime such that $\sigma q > 2\sqrt{n}$. If one can solve $LWE_{q,\hat{\Phi}_\sigma}$, then we can construct an algorithm for approximating the "shortest independent vector (SIVP)" within $\tilde{O}(\frac{n}{\sigma})$ in worst case.
- **Hardness of LWE**[31]: Let $n = n(\kappa)$, $q = q(\kappa)$, $m = m(\kappa)$, $p = p(\kappa)$ be integers, where κ (depends on lattice's dimension) be a security parameter. Then the problem $LWE_{n,m,p,q}$ is about to distinguish between $(A, [A\vartheta])$ and $(A, [u])$, where $A \in Z_q^{m\times n}$, $\vartheta \in Z_q^m$, $u \in Z_q^m$ are chosen randomly. The two distributions are indistinguishable, if the assumption $LWE_{l,q,n,\xi}$ is valid and $q > 2\alpha\gamma mnp$, $n > \frac{(l+\lambda+1)\log\ q}{\log\ 2\gamma+2\lambda}$, where "$\alpha$ is a bound on distribution ξ".
- **Small Integer Solution (SIS)**[49]: Let $q > 0$ be an integer and $\zeta > 0$ denoted a real number. Further, let $A \in Z_q^{n\times m}$. Then, $SIS_{q,\ \zeta}$ is about to find $z \in Z^m$ such that $Az = 0$ mod q, where $0 < ||z|| < \zeta$.
- **Indistinguishable property** Trap(m, n, q) gives an output $A \in Z_q^{m\times n}$, $S \in Z_q^{n\times n}$, for any given $n > m \log q(5 + 3\eta)$, $m, q > 2$, $\eta > 0$ and such that A is indistinguishable from $U(Z_q^{m\times n})$, for $||S|| < O(m\ \log q)$, $||\tilde{S}|| < O(\sqrt{m\ \log q})$.

3.2 | Understanding dual lattice and dual bases

If Δ is a lattice, then its dual is the set $\tilde{\Delta}$ consisting of tuples $x \in L(\Delta)$ that is, linear span of Δ such that inner product $< x,\ y >$ is an integer for all $y \in \Delta$. Following the definition, one can easily observe that the dual of $\mathbb{Z}^n$ is $\mathbb{Z}^n$. The inner product is defined as

$$< x,\ y >= x^t\ y = \sum_{i=1}^{n} x_i\ y_i, \tag{1}$$

where "$x = (x_1,\ x_2,\ \dots\ , x_n)$ and $y = (y_1,\ y_2,\ \dots\ , y_n)$ are tuples with real entries".

The dual space ($\tilde{\Delta}$) has same dimension as its primal space (Δ), and essentially both are isomorphic to each other. Therefore, a dual space $\tilde{\Delta}$ lies in the same space as primal Δ, not necessarily sublattice of Δ. The lattice $\tilde{\Delta}$ contains nonintegers even Δ contains only integers entries. The dual space is necessarily defined as follows in abstract vector space. Let $V \subseteq \mathbb{R}^n(R)$ be a vector space, then a function $\Psi\ :\ V \to R$ is called a linear functional satisfying: (1) $\Psi(\vartheta_1 + \vartheta_2) = \Psi(\vartheta_1) + \Psi(\vartheta_2)$, and (2) $\Psi(a\ \vartheta_1) = a\ \Psi(\vartheta_1)$, where $a,\ b \in R$ and $\vartheta_1,\ \vartheta_2 \in V$. The dual space of abstract vector space V is the set of all linear functional, where a function Ψ is represented as a tuple $\vartheta \in V$ such that $\Psi(x) =< \vartheta,\ x >$, but dual lattice is considered on set of integers $\mathbb{Z}$ instead set of reals one. The dual of lattice Δ is the collection of linear functionals $\Psi\ :\ V \to \mathbb{Z}$, represented as tuples in span(Δ). Each vector $\vartheta \in \tilde{\Delta}$ generates a linear functional $\Psi_\vartheta(x) =< \vartheta,\ x >$ satisfying $\Psi_\vartheta(\Delta) \subseteq \mathbb{Z}$ and partitions Δ into layers as $\Delta = \cup_{i\in\mathbb{Z}}\{\varrho \in \mathbb{Z}\ :\ \Psi_\vartheta(\varrho) = i\}$, where each layer $\Psi_\vartheta^{-1}(i) = \{\varrho \in \Delta\ :\ \Psi_\vartheta(\varrho) = i\}$ is necessarily a shifted copy of $\Delta \cap \vartheta^\perp = \{\varrho \in \Delta\ :< \vartheta,\ \varrho >= 0\}$ i. e. a lower dimensional sublattice orthogonal to ϑ with distance between layers $\frac{1}{||\vartheta||}$, implies sparser lattice has denser dual and vice-versa. Therefore, the dual of $c\Delta$ is $\frac{1}{c}\Delta$, where $c > 0$ is an arbitrary real.

3.3 | The closest vector problem

In the "closest vector problem (CVP)", one inputs a "lattice Δ" and also a "target vector τ", and the goal is to search $\vartheta \in \Delta$ such that $||\tau - \vartheta||$ is minimum, where $\tau \in \mathbb{R}^n$. We can define the CVP in any norm, but the Euclidean remains the common one. In general τ is in the linear span of lattice, but this is not necessary. Finally, one can assume that τ is in linear span of lattice and projects τ orthogonally to span(B) without disturbing the solution. Equivalently, the CVP is to find a lowest norm vector in coset $\tau + \Delta$ that is, if $e = \tau + \vartheta \in \tau + \Delta$ is such point, then $-\vartheta = \tau - e \in \Delta$ is closest to target (CVP solution). One can observe a highly important characteristic of dual lattice is to define lattice cosets. Let $\tilde{B} \in \mathbb{R}^{n\times k}$ be essentially a random generating set for dual lattice $L(\tilde{B}) = \tilde{\Delta} \subset \mathbb{R}^n$, then $\tau \in \mathbb{R}^n$ and $\tilde{B}^t\tau\ mod\ 1 \in [0,\ 1)^k$ is necessarily syndrome of τ under $\tilde{B}$, which is essentially depending on both $\tilde{\Delta}L(\tilde{B})$ and $\tilde{B}$. Furthermore, the syndrome depends component of τ in $span(\tilde{B}) = span(\Delta)$ implies $\tau \in span(\Delta)$. Let $\Delta \subset \mathbb{R}^n$ and $\tilde{B}$ be generating set corresponding to $L(\tilde{B}) = \tilde{\Delta}$, then $e,\ \tau$ satisfy $\tilde{B}^t\ e = \tilde{B}\ \tau\ (mod\ 1)$ and belongs to same affine-span $e \in \tau + span(\Delta) \Leftrightarrow e \in \tau + \Delta$, where $\tau,\ e \in \mathbb{R}^n$. Therefore, a vector $e \in \tau + span(\Delta) = \mathbb{R}^n$ holds trivially when Δ has full rank.

Definition 3. The decoding of syndrome $\tau \in [0,\ 1)^n$ under matrix $H \in \mathbb{R}^{n\times n}$, where $det(H) \neq 0$ asks one to find a solution to $H\ x = \tau\ (mod\ 1)$ of possible smallest norm.

3.4 | The Gaussian measures

Let $\vartheta,\ c \in \mathbb{R}^n$ and $\sigma > 0$ be arbitrary, then $\rho_{\sigma,\ c}(\vartheta) = e^{-\pi||(\vartheta - c)/\sigma||^2}$ defines a Gaussian distribution function with center c and scaling σ, where the total measure corresponding to $\rho_{\sigma,\ c}$ is

$$\int_{\vartheta\in\mathbb{R}^n} \rho_{\sigma,\ c}(\vartheta)d\vartheta = \sigma^n. \tag{2}$$

Therefore, Gaussian distribution $\rho_{\sigma,\ c}$ can be defined using its probability density function $D_{\sigma,\ c}(\vartheta) = \frac{\rho_{\sigma,\ c}(\vartheta)}{\sigma^n}$, where $\vartheta \in \mathbb{R}^n$. The estimated square distance of a vector from c chosen in this distribution is clearly $n\ \sigma^2/2\pi$, implying that $D_{\sigma,\ c}$ is basically a sphere with radius $\sigma\ \sqrt{n/(2\pi)}$ around the middle point c.

In general, one can also observe $D_{\sigma,\, c}$ can be represented as the sum of n-orthogonal one-dimension Gaussian distributions, and essentially each of them can be approximated so is $D_{\sigma,\, c}$, using standard techniques. If one assume all the entries real, then $D_{\sigma,\, c}$ can be sampled exactly one. In case of finite precision, $D_{\sigma,\, c}$ can be estimated by selecting points with a probability nearly proportional to $D_{\sigma,\, c}$ on a fine grid. For a countable set S, the distribution is defined as:

$$\rho_{\sigma,\, c}(S) = \sum_{\vartheta \in S} \rho_{\sigma,\, c}(\vartheta). \tag{3}$$

For a lattice Δ, one can define distribution

$$D_{\Delta,\, \sigma,\, c}(\vartheta) = \frac{D_{\sigma,\, c}(\vartheta)}{D_{\sigma,\, c}(\Delta)} = \frac{\rho_{\sigma,\, c}(\vartheta)}{\rho_{\sigma,\, c}(\Delta)}, \tag{4}$$

where vectors $\sigma > 0$, c has real entries. We refer $D_{\Delta,\, \sigma,\, c}$ as a discrete Gaussian (see Figure 4) and follow a close connection between $D_{\sigma,\, c}$ and $D_{\Delta,\, \sigma,\, c}$ as: if ϑ follows the distribution $D_{\sigma,\, c}$, then we condition on ϑ and the "conditional distribution of ϑ is $D_{\Delta,\, \sigma,\, c}$". To observe the fact, recall that ϑ is really chosen from a fine grid, then chance to obtain a grid point ϑ sampled in $D_{\sigma,\, c} \approx \alpha D_{\sigma,\, c}(\vartheta)$, where α is the "volume of one cell" in concerned grid, whereas the "probability $\vartheta \in \Delta$ is very close to $\alpha D_{\sigma,\, c}(\Delta)$". One can also show that $D_{\Delta,\, \sigma,\, c}$ resembles continuous Gaussian $D_{\sigma,\, c}$ when σ is large enough. Specifically, the "vectors in $D_{\Delta,\, \sigma,\, c}$ have an average value very close to c and expected squared distance essentially $\sigma^2 n/2\pi$". Therefore, we define a new parameter called smoothing parameter helps to choose σ for this to happen.

3.5 | Fourier transform

We discuss some valuable characteristics of the Fourier transform and depth could be found in References 50 and 51. The Fourier transform of $\eta \;:\; \mathbb{R}^n \to \mathbb{R}$ is defined as

$$\hat{\eta}(\varrho) = \int_{\mathbb{R}^n} \eta(\vartheta) e^{-2\pi i <\vartheta,\, \varrho>} d\vartheta \tag{5}$$

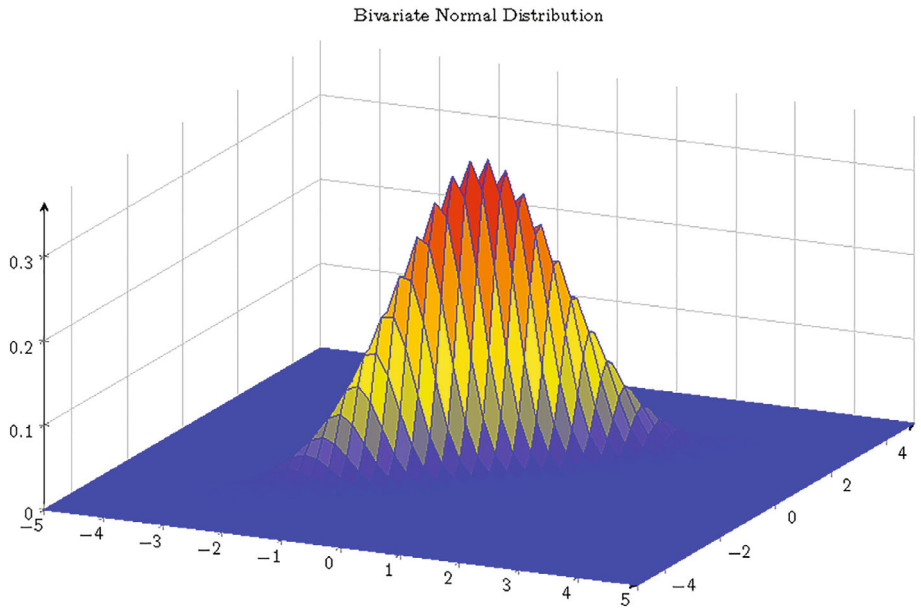

FIGURE 4 Gaussian distribution in multidimensions

which helps in obtaining various formulas, if for some vector v, $\eta(\vartheta) = h(\vartheta + v)$ where h is some function then $\hat{\eta}(\varrho) = e^{2\pi\imath<v,\ \varrho>}\hat{h}(\varrho)$.

Following the same lines, if $\eta(\vartheta) = e^{2\pi\imath<\vartheta,\ v>}h(\vartheta)$, then $\hat{\eta(\varrho)} = \hat{h}(\varrho - v)$. Furthermore, one can define η^u is the derivative of η in the direction of unit vector u then its Fourier is $\hat{\eta^u}(\varrho) = 2\pi\imath < u,\ \varrho > \hat{\eta}(\varrho)$. Another essential fact about Gaussian is that the Gaussian is its own Fourier transformation (i. e. $\hat{\rho} = \rho$) and $\hat{\rho}_\sigma = \sigma^n \rho_{\frac{1}{\sigma}}$, where $\sigma > 0$ is real. It has been observed that any lattice Δ and any $f\ :\ \mathbb{R}^n \to \mathbb{C}, f(\Delta) = det(\tilde{\Delta})\,\hat{f}(\tilde{\Delta})$, where $\hat{f}$ is Fourier transformation of function f. Given a $\sigma > 0$ and vector c, $\rho_{\sigma,\ c}(\Delta) \leq \rho_\sigma(\Delta)$ holds, because

$$\begin{aligned}
\rho_{\sigma,\ c}(\Delta) &= det(\tilde{\Delta})\hat{\rho}_{\sigma,\ c}(\tilde{\Delta}) \\
&= det(\tilde{\Delta})\sum_{y\in\tilde{\Delta}}\hat{\rho}_{\sigma,\ c}(y) \\
&= det(\tilde{\Delta})\sum_{y\in\tilde{\Delta}}e^{-2\pi\imath<c,\ y>}\hat{\rho}_\sigma(y) \\
&= det(\tilde{\Delta})\sum_{y\in\tilde{\Delta}}\hat{\rho}_\sigma(y) \\
&= \rho_\sigma(\Delta),
\end{aligned}$$

where $\hat{\rho}_\sigma = \sigma^n\ \rho_{\frac{1}{\sigma}}$ is treated as a positive function. The Banaszczyk's lemma[52] ensures if $c > \frac{1}{\sqrt{2\pi}}$ and Δ is n-dimensional lattice, then

$$\rho\left(\frac{\Delta}{c\ \sqrt{n}\ \mathcal{B}}\right) < C^n\ \rho(\Delta), \tag{6}$$

$$\rho\left(\frac{\Delta + v}{c\ \sqrt{n}\ \mathcal{B}}\right) < 2\ C^n\ \rho(\Delta), \tag{7}$$

where $\mathcal{B}$ is closed ball with centered origin and $C = c\ \sqrt{2\pi e}\ e^{-\pi c^2} < 1$ holds.

3.6 | The smoothing parameter

We need to introduce an advanced lattice parameter (smoothing parameter[49]) related to Gaussian measures on random lattices.

Definition 4. Let Δ be a lattice of dimension n and $\epsilon > 0$ be an arbitrary small real number, then one can define smoothing parameter $\xi_\epsilon(\Delta)$ to be the smallest σ following $\rho_{\frac{1}{\sigma}}(\tilde{\Delta} - \{0\}) \leq \epsilon$.

It has been observed that $\rho_{\frac{1}{\sigma}}(\tilde{\Delta} - \{0\})$ is decreasing continuous function in σ that is, $lim_{\sigma\to 0}\ \rho_{\frac{1}{\sigma}}(\tilde{\Delta} - \{0\}) = \infty$ and $lim_{\sigma\to\infty}\ \rho_{\frac{1}{\sigma}}(\tilde{\Delta} - \{0\}) = 0$. Therefore, the essential parameter $\xi_\epsilon(\Delta)$ is defined for $\epsilon > 0$, where $\epsilon \to \xi_\epsilon(\Delta)$ is inverse function of $\sigma \to \rho_{\frac{1}{\sigma}}(\tilde{\Delta} - \{0\})$. Moreover, we are interested in smoothing parameters $\xi_{\epsilon(n)}(\Delta_n)$ corresponding to $\{\Delta_n\}_{n\in N}$, where $\epsilon(n)$ is negligible function and n is dimension of concerned lattice. Therefore, $\xi_{\epsilon(n)}(\Delta_n)$ is required smallest σ such that Gaussian necessarily on $\tilde{\Delta}_n$ with $\frac{1}{\sigma}$ gives all but negligible weight to origin corresponding to $\epsilon(n)$, where $\epsilon(n)$ is negligible function in dimension of the lattice.

4 | SYSTEM MODELS

In this section, we elaborate the network model along with the threat (attack) model that are useful in discussing the proposed signcryption scheme and its use in data storage in cloud for IoT applications.

4.1 | Network model for secure cloud data storage in IoT applications

Figure 5 illustrates a generic architecture for data storage in cloud in IoT environment with the help of lattice based signcryption mechanism. The network entities of this model are considered as: (1) a trusted registration authority (*RA*), (2) IoT smart (sensor) nodes (*SN*), (3) aggregators (gateway nodes, *GWN*), and (4) cloud server(s), *CS*. The *RA* has a mission to register all the entities (*GWN*, *SN*s and *CS*) for an IoT application by the "Set-up phase," "Extraction-S phase," and "Extraction-R phase" described in Section 5 prior to deployment in their functioning field. Once the registration process is over, the *RA* loads the private (secret) and public parameters in their memory. The sensor nodes SN_j(s) are deployed in the IoT application and they start the communication with the associated aggregator *GWN* over the public channel. The secure communication can be done between SN_j and *GWN* by executing the proposed signcryption scheme. SN_j (called the sender) sends the information to the receiver *GWN* (aggregator node). After receiving the message from SN_j, *GWN* applies unsigncryption algorithm for retrieving the original message as well as to verify the authenticity of the message. After successfully verification, *GWN* also applies same signcryption process to hide the original message and maintain the legitimacy of it, and then forwards the signcrypted message to the linked cloud server *CS*. Finally, *CS* verifies the authenticity of message using unsigncryption algorithm and stores the data into its storage database.

4.2 | Formal model of ID-based signcryption

The proposed construction is necessarily consisting of four different phases: (a) Setup, (b) Extraction, (c) Signcryption, and (d) Unsigncryption. A brief understanding of the proposed design is executed in four phases illustrated below.

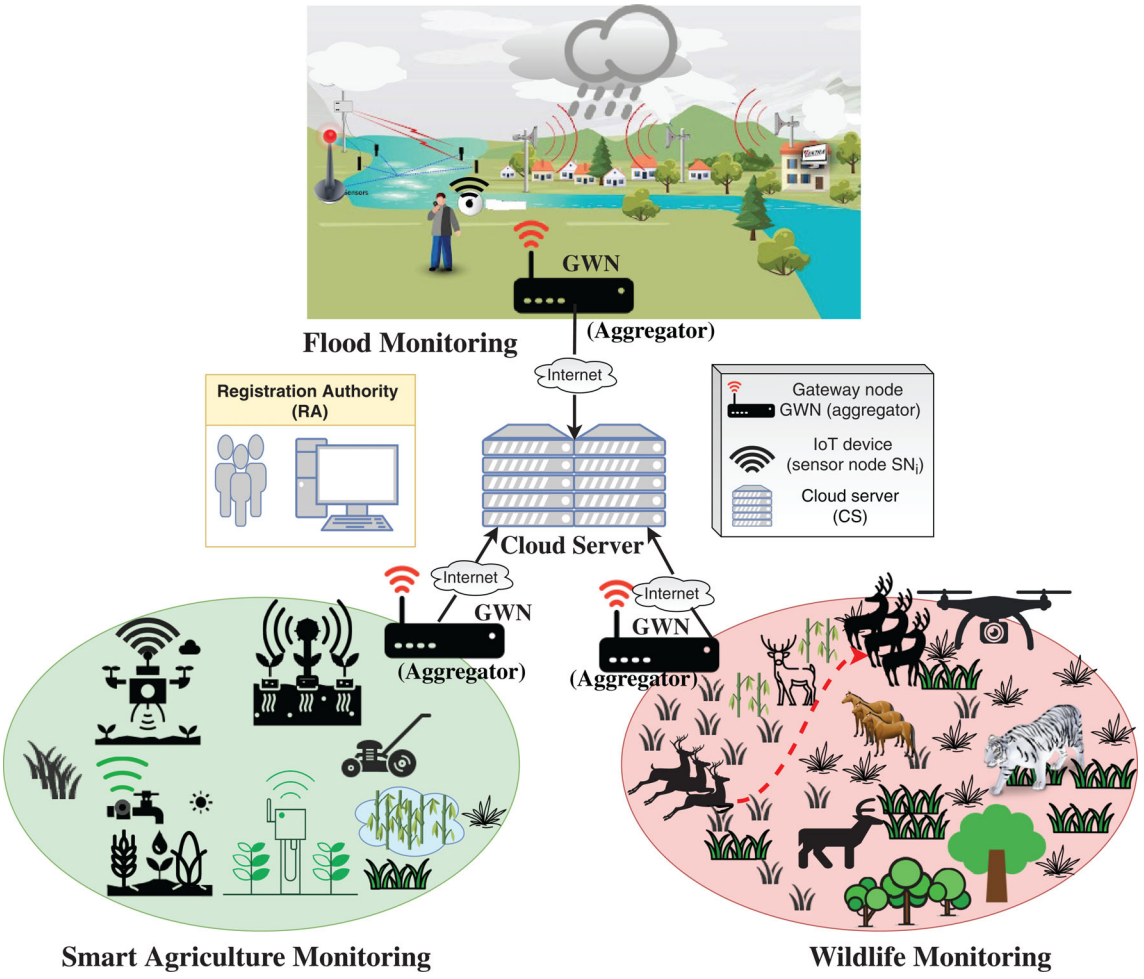

FIGURE 5 A network model for secure cloud data storage in IoT applications

- **Setup(1^λ)**: This is essentially a "randomized algorithm" inputs the "security parameter (λ)", and outputs corresponding public parameters $\mathcal{P}$.
- **Extraction($1^\lambda, \mathcal{P}$)**: Both sender and receiver execute extraction algorithm using λ, $\mathcal{P}$, where a sender/receiver gets corresponding public/private keys.
- **Signcryption**: The sender S executes Signcryption($\mu, \mathbb{PK}_r, \mathbb{SK}_s$) = c and sends the output c to R.
- **Unsigncryption**: After receiving c, the receiver R executes Unsigncryption($c, \mathbb{PK}_s, \mathbb{SK}_r$) = μ and gets the message.

4.3 | Threat model

In the following, we discuss the associated security models.

4.3.1 | Security model for multiuser setting secure IBSC

A signcryption ensures both confidentiality and authenticity in a single logical step. In the two user framework, an adversary ($\mathcal{A}$) requires to get query on secret key at the starting of the game. In a multiuser framework, $\mathcal{A}$ is allowed to get query on secret key and he can submit polynomial times queries to the signcryption as well as unsigncryption Oracle. Moreover, an insider attacker possesses a secret key of the sender/receiver in the challenge phase for the corresponding output phase of the IND-CCA2/SUF-CMA phases respectively.

In a multiuser setting, we will discuss two important notions of security: (1) "multiuser indistinguishable under insider chosen cipher attack (MU-IND-iCCA2)" and (2) "multiuser strong unforgeability under insider chosen message attack (MU-SUF-iCMA)".

Phase-1: In MU-IND-iCCA2 queries, a polynomial bounded adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ play a game, where $\mathcal{C}$ performs the setup for parameters generation and sends the parameters to $\mathcal{A}$, but keeps the master key secret. Now, $\mathcal{A}$ executes the queries as follows:

1) Key-generation: $\mathcal{A}$ picks an identity ID and sends it to $\mathcal{C}$. $\mathcal{C}$ then runs Key-generation(ID) = K_{ID} and generates corresponding private key and sends to $\mathcal{A}$.

2) Query 1: $\mathcal{A}$ submits a cipher (c) and an identity ID_A to $\mathcal{C}$. $\mathcal{C}$ computes K_{ID_B} = Key-generation(ID_B), and runs Unsigncryption(c, K_{ID_B}, ID_A) and sends it back to $\mathcal{A}$.

3) Challenge: Let $\mathcal{A}$ choose two random m_0, m_1 and $(ID_A^*, K_{ID_A^*}$. In addition, $\mathcal{C}$ picks a bit, say $b \in \{0, 1\}$ and runs $Signcrypt(m_b, K_{ID_A}, ID_B^*) = c^*$ and sends c^* to $\mathcal{A}$.

4) Query 2: $\mathcal{A}$ chooses ID_A and a cipher c, and queries to $\mathcal{C}$. $\mathcal{C}$ answers as in Query (1), except $(ID_A, c) \neq (ID_A^*, c^*)$.

Output: At last, $\mathcal{A}$ guesses a bit $b' \in \{0, 1\}$, where $Adv_{\mathcal{A}}^{MU-IND-iCCA2}(\kappa) = |Pr[b' = b] - \frac{1}{2}|$ denotes the "gained advantage in the MU-IND-iCCA2 game".

MU-SUF-iCMA-phase: A MU-SUF-iCMA game is played as in the above Phase 1. $\mathcal{C}$ executes the setup under the security parameter κ, generates corresponding parameters and sends to $\mathcal{A}$. $\mathcal{A}$ also executes queries as in Phase 1. At last, $\mathcal{A}$ will guess a tuple (c', ID_B', K_{ID_B}') as a forgery tuple, and he can win the game under the condition: $(c', ID_B', m') \neq (c^i, ID_B^i, m^i) \wedge m'$ for a polynomial number of queries.

4.3.2 | Trapdoor with algorithms

Micciancio and Peikert[53] proposed the following algorithm with trapdoor. If $n \geq 1$, $q \geq 2$ and $m = O(n \log q)$, then $Gen - trap(1^n, 1^m, q)$ is a randomized algorithm generates $A \in \mathbb{Z}_q^{n \times m}$ called parity check matrix and secret trapdoor T such that $A \in \mathbb{Z}_q^{n \times m}$ follows almost uniform distribution. Furthermore, there are efficient algorithms *Invert* and $Sample - D$ with the "overwhelming probability over all random choices" with the following characteristics:

i) Let T, A and $b^t = \varrho^t + e^t$ be the input, where $\vartheta \in \mathbb{Z}_q^n$ and $||e|| < \frac{q}{O(\sqrt{n \log q})} \leftarrow D_{\mathbb{Z}^m, \alpha q}$, $\frac{1}{\alpha} \geq \sqrt{n \log q}.\omega(\sqrt{\log n})$, then the deterministic procedure $Invert(T, A, b)$ gives outputs as ϑ and e.

ii) Let T, A and $\varrho \in \mathbb{Z}_q^n$ and $\vartheta = O(\sqrt{n \log q})$ be the input, then randomized procedure $Sample - D(T, A, \varrho, \vartheta)$ samples according to negl(n) distribution statistically close to $D_{\Delta_q^{\varrho}, \vartheta.\omega(\sqrt{\log n})}$.

4.3.3 | Security model for communication

For communication between various entities in the IoT network, we consider the widely applied Dolev-Yao threat model (popularly, known as the DY model).[54] This model permits an adversary (either a passive or an active adversary), say $\mathcal{A}$, not only read/eavesdrop all the messages during communication among the entities, but also to update, erase or push fake contents in the messages. The adversary $\mathcal{A}$ can physically compromise some of the installed IoT sensor nodes from the deployment field, and using the "power analysis attacks",[55] the credentials stored in compromised nodes' memory can be easily extracted. The extracted information can be utilized for some other attacks, such as sensor node impersonation attack on behalf of other noncompromised sensor nodes. However, it is assumed that both the *GWN*s and *CS*s are semi-trusted, and will not be compromised by the adversary $\mathcal{A}$. For this purpose, we further assume that the aggregators (*GWN*s) can be also placed under a locking system as it was the case in Reference 56.

5 | PROPOSED CONSTRUCTION OF LATTICE-BASED SIGNCRYPTION

Our proposed construction follows sign-then-encryption approach, but it can be observed that a scheme combining both IND-CCA secure encryption and SUF-CMA secure signature does not necessarily implies MU-SUF-CMA security.[57,58]

A communication model related to the proposed construction is provided in Figure 6. In this process, an insider adversary ($\mathcal{A}$) can use receiver's public key to perform unsigncryption using the signcryption Oracle and obtains a valid forgery on the message. To get rid of this problem, we do not put signature (ε) on μ and $\mathbb{PK}_r$ only, but also the output $(\hat{c_0}, \hat{c_1})$ using learning with errors trapdoor $g_A(\vartheta, e) = \vartheta^t A + e^t \ (mod\ q)$, where $A \in \mathbb{Z}^{n \times m}$, $\vartheta \in \mathbb{Z}_q^n$ and $e \in \mathbb{Z}^m$ respectively. Furthermore, if $\hat{c_0} = g_A(\vartheta, e_0)$ and $\hat{c_1} = g_U(\vartheta, e_1)$, then it further processes encryption on the signature and corresponding message as $c_0 = \hat{c_0} + \varepsilon \ (mod\ q)$ and $c_1 = \hat{c_1} + \mu[\frac{q}{2}] \ (mod\ q)$. Therefore, $\mathcal{A}$ has to produce a valid forgery (c_0^*, c_1^*) in breaking the MU-SUF-CMA security. The proposed construction is described mainly in five phases: (1) Set-up, (2) Extraction-R, (3) Extraction-S, (4) L-Signcryption, and (5) L-Unsigncryption.

5.1 | Set-up phase

Set-up $(\mathbf{1}^{\lambda})$: The public parameters are chosen as: (1) an integer $n >> \lambda$, (2) $q = poly(n)$, (3) $\hat{m} = O(n \log q)$, (4) $m = \hat{m} + n \log q$, (5) $\sigma^{-1} = O(n \log q)^2 \cdot \omega(\sqrt{\log n})$, (6) $\delta = O(\sqrt{n^2 \log^2 q}) \cdot \omega(\sqrt{\log n})^2.l$ is message-length, and (7) $p = \Omega(q\ \delta^{-1}) > 0$ is an integer. Let G be a diagonal matrix as

$$G = \begin{bmatrix} g^t & & \\ & \ddots & \\ & & g^t \end{bmatrix} \in \mathbb{Z}_q^{n \times n \log q},$$

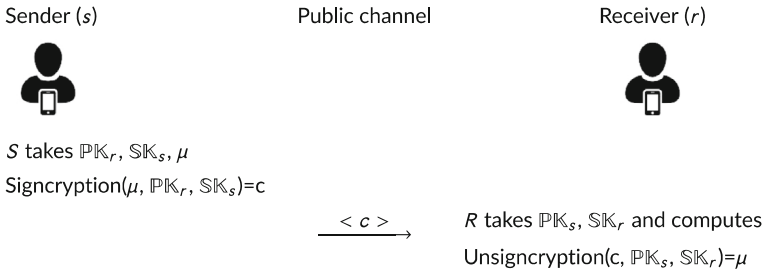

FIGURE 6 Illustration of the proposed construction's communication model

where $g^t = 2^0,\ 2^1,\ 2^2,\ \ldots,2^{\log\ (q-1)} \in \mathbb{Z}_q^{1\times \log\ q}$, $H\ :\ \mathbb{Z}_q^n \to \mathbb{Z}_q^{n\times n}$ be full-rank difference encoding,[53,59] and $A_0,\ A_1,\ \leftarrow \mathbb{Z}_q^{n\times n\ \log\ q},\ B \leftarrow \mathbb{Z}_q^{n\times m},\ U \leftarrow \mathbb{Z}_q^{n\times l},\ u_s \leftarrow \mathbb{Z}_q^n$ are uniform random. Finally, all the public parameters are $params = \{\ n,\ q, \lambda,\ \hat{m},\ m,\ \sigma,\ l,\ p,\ \delta,\ G,\ H,\ A_0,\ A_1,\ B,\ U,\ u_s\}$.

5.2 | Extraction-R phase

Extraction-R(params): This phase generates key pair $(\mathbb{PK}_r,\ \mathbb{SK}_r) \leftarrow Extraction(params)$ via following steps:

- Select $\hat{A}_r \xleftarrow{u} \mathbb{Z}_q^{n\times \hat{m}},\ T_r \leftarrow D_{\mathbb{Z},\ \log\ n}^{\hat{m}\times n\ \log\ q}$.
- Calculate $A_r = [\hat{A}_r| - \hat{A}_r T_r] \in \mathbb{Z}_q^{n\times n}$.
- Finally, compute $\mathbb{PK}_r = A_r$ and $\mathbb{SK}_r = T_r$.

5.3 | Extraction-S phase

Extraction-S(params): This phase generates key pair $(\mathbb{PK}_s,\ \mathbb{SK}_s) \leftarrow Extraction(params)$ via following steps:

- Choose $\hat{A}_s \xleftarrow{u} \mathbb{Z}_q^{n\times \hat{m}},\ T_s \leftarrow D_{\mathbb{Z},\ \log\ n}^{\hat{m}\times n\ \log\ q}$.
- Compute $A_s = [\hat{A}_s|G - \hat{A}_s T_s] \in \mathbb{Z}_q^{n\times n}$.
- Finally, calculate $\mathbb{PK}_s = A_s$ and $\mathbb{SK}_s = T_s$.

5.4 | L-Signcryption phase

L-Signcryption on a string $\mu \in \{0,\ 1\}^{\ell}$ is executed in the following steps:

1. Pick $r_e,\ r_s \leftarrow D_{\mathbb{Z},\ \log\ n}^m$ and then compute $t = f_{\hat{A}}(\mathbb{PK}_s) + f_B(r_e) \in \mathbb{Z}_q^n$.
2. Calculate $A_{r,\ t} = [\hat{A}_r|H(t)G - \hat{A}_r T_r] \in \mathbb{Z}_q^{n\times m}$.
3. Set $s \xleftarrow{u} \mathbb{Z}_q^n, x_0 \leftarrow D_{\mathbb{Z},\ \sigma q}^m, x_1 \leftarrow D_{\mathbb{Z},\ \sigma q}^{\ell}$.
4. Compute $\hat{c_0} = s^t\ A_{r,\ t} + px_0^t \in \mathbb{Z}_q^m, c_1 = s^t U + px_1^t \in \mathbb{Z}_q^{\ell}$.
5. Output is $\hat{C} = \{\hat{c}_0,\ \hat{c}_1,\ r_e\}$.
6. Perform a signature on $\mu||\mathbb{PK}_r||\hat{C}$ via executing the steps:
   - Calculate $h = f_{\hat{A}_s}(\mu||\mathbb{PK}_r||\hat{C}) + f_B(r_s) \in \mathbb{Z}_q^n$,
   - Compute $A_{s,\ h} = [A_s|A_0 + (\prod_{i\in\mathcal{H}} 2^i)A_1] \in \mathbb{Z}_q^{m+n\ \log\ q}$, where $\mathcal{H}$ is the set of positions in bit representation of string h,
   - Compute $e \leftarrow Samples - D(T_s,\ A_{s,\ h},\ u_s,\ \delta)$,
   - Set $< e,\ r_s > \in \mathbb{Z}^{m+n\ \log\ q} \times \mathbb{Z}^m$. as the desired signature.
7. $c_0 = \hat{c}_0 + r_s \in \mathbb{Z}_q^m, c_1 = \hat{c}_1 + p.\mu[\frac{q}{2}]$.
8. Finally, output is $C = \{c_0,\ c_1,\ r_e,\ e\}$.

5.5 | L-Unsigncryption phase

The receiver signcrypts $C = \{c_0,\ c_1,\ r_e,\ e\}$ via executing the following steps:

- Calculate $t = f_{\hat{A}_r}(\mathbb{PK}_s) + f_B(r_e) \in \mathbb{Z}_q^n, A_{r,\ t} = [\hat{A}_r|H(t)G - \hat{A}_r T_r] \in \mathbb{Z}_q^{n\times m}$,
- Set $(z,\ r_s) \leftarrow Invert(T_r,\ A_{r,\ t},\ c_0)$,
- Compute $E \in \mathbb{Z}^{m\times \ell}$ satisfying $A_{r,\ t}E = U\ (mod\ q)$ under $Sample - D$,

- Calculate $v^t = c_1^t - (c_0 - r_s)^t E = p(x_1^t + \mu^t[\frac{q}{2}] - x_0^t E)$ and recovers μ from $\frac{v}{p}$ $(mod\ q)$,
- Compute $\hat{c}_0 = c_0 - r_s\ (mod\ q),\ \hat{c}_1 = c_1 - p\ \mu\ [\frac{q}{2}]\ (mod\ q), \hat{C} = \{\hat{c}_0,\ \hat{c}_1,\ r_e\}$ and computes $h = f_{\hat{A}_s}(\mu||\mathbb{PK}_r||\hat{C}) + f_B(r_s) \in \mathbb{Z}_q^n, A_{s,\ h} = [A_s|A_0 + (\prod_{i\in\mathcal{H}} 2^i)A_1] \in \mathbb{Z}_q^{m+n\ \log\ q}$, where $\mathcal{H}$ is the set of positions in bit representation of string h,
- Message μ is valid if $A_{s,\ h}.e = u_s\ (mod\ q)\ \wedge\ ||e|| \leq \delta\ \sqrt{m + n\ \log\ q}$, where $\wedge$ is "and" operation.

6 | APPLYING CONSTRUCTED SIGNCRYPTION FOR SECURE CLOUD DATA STORAGE IN IOT APPLICATIONS

In this section, we propose a secure cloud-based data storage scheme using the constructed lattice-based signcryption for IoT applications. In short, we call it as SCDS-LBSIoT. We utilize the same notations as provided in Table 2 to discuss various related phases of SCDS-LBSIoT. To resist the replay attack protection, it is assumed as in References 13,14,56 that the network entities are synchronized with their clocks.

We have various phases that applies our proposed constructed signcryption for secure cloud data storage in IoT applications, such as (1) registration, (2) secure data aggregation, and (3) secure cloud data storage. The registration phase includes the three subphases: (a) IoT smart device enrollment, (b) aggregator (gateway node) registration, and (c) cloud server registration. In the IoT smart device enrollment phase, a trusted registration authority executes the **Extraction-S phase** described in Section 5.3. An aggregator being a gateway node executes the **Extraction-R phase** described in Section 5.2 during the aggregator (gateway node) registration process. During the cloud server registration phase, a cloud server needs to execute **Extraction-R phase** described in Section 5.2. Now, for Secure data aggregation a smart device executes the **L-Signcryption** phase (described in Section 5.4) and an aggregator applies the **L-Unsigncryption** phase (described in Section 5.5). Finally, for secure cloud data storage a cloud server needs to run the **L-Unsigncryption** phase described in Section 5.5.

The detailed description of each phase is given in the following subsections.

6.1 | Registration phase

Under this phase, we consider the following three subphases.

6.1.1 | IoT smart device enrollment

This phase is done in offline mode by the in-charge registration authority. Note that this process is one-time activity only. In order to enroll a new IoT smart (sensor) node (device), say SN_i associated under an aggregator node, being the gateway node (GWN), $Aggr_j$ for a particular IoT application $Appl_j$, the associated registration authority, say RA_j, picks its identity ID_{SN_i}. By executing the **Extraction-S phase** described in Section 5.3, the RA_j computes the lattice-based private and public keys pair $(\mathbb{SK}_{SN_i}, \mathbb{PK}_{SN_i})$ and makes the public key $\mathbb{PK}_{SN_i}$ as public. Then RA_j deletes the private key $\mathbb{SK}_{SN_i}$ of each deployed sensor node SN_i from its database. The RA_j pre-loads the credentials $\{ID_{SN_i}, (\mathbb{SK}_{SN_i}, \mathbb{PK}_{SN_i})\}$ into the memory of SN_i before its deployment in the network.

6.1.2 | Aggregator (gateway node) registration

The associated registration authority RA_j is responsible to register an aggregator, say $Aggr_j$ for a particular application, via a secure channel. The $Aggr_j$ first picks its identity ID_{Aggr_j} and sends a registration request message including its identity to the RA_j via secure channel. After registering $Aggr_j$, the RA_j send registration reply to $Aggr_j$ via secure channel. Once the registration reply is received, $Aggr_j$ runs the **Extraction-R phase** described in Section 5.2, to compute its lattice-based private and public keys pair $(\mathbb{SK}_{Aggr_j}, \mathbb{PK}_{Aggr_j})$, stores the private key $\mathbb{SK}_{Aggr_j}$ in its secure database, and makes the public key $\mathbb{PK}_{Aggr_j}$ as public. The RA_j also pre-loads $\mathbb{PK}_{Aggr_j}$ into the memory of the attached deployed IoT sensor node SN_i, before the deployment of SN_i.

6.1.3 | Cloud server registration

A cloud server CS_k associated with the registration authority RA_j first picks its own identity ID_{CS_k} and sends a registration request message including its identity to the RA_j via secure channel. After getting registration reply from the RA_j, CS_k also runs **Extraction-R phase** described in Section 5.2, to derive its lattice-based private and public keys pair $(\mathbb{SK}_{CS_k}, \mathbb{PK}_{CS_k})$, stores the private key $\mathbb{SK}_{CS_k}$ in its secure database, and makes the public key $\mathbb{PK}_{CS_k}$ as public.

6.2 | Secure data aggregation phase

This phase is executed between the IoT sensor nodes SN_i and their associated aggregator $Aggr_j$ for each application $Appl_j$. The following steps are needed to serve the secure data aggregation:

- **Step 1.** Suppose an IoT sensor node SN_i has sensing data, say $Data_{SN_i}$. SN_i then creates a current timestamp TS_{SN_i} and applies the **L-Signcryption** phase (described in Section 5.4) on $Data_{SN_i}$, ID_{SN_i} and TS_{SN_i} to create signcryption as $C_{SN_i} = \text{L-Signcryption}(Data_{SN_i}, ID_{SN_i}, TS_{SN_i})$, where the signature is created using the private key $\mathbb{SK}_{SN_i}$ of SN_i and the information $(Data_{SN_i}, ID_{SN_i}, TS_{SN_i})$ is encrypted using the public key $\mathbb{PK}_{Aggr_j}$ of $Aggr_j$. SN_i sends the message $Msg_{SNData} = \{C_{SN_i}, TS_{SN_i}\}$ to the $Aggr_j$ via public channel.
- **Step 2.** After receiving Msg_{SNData} at time TS'_{SN_i}, $Aggr_j$ first validates the received timestamp ST_{SN_i} by $|TS'_{SN_i} - TS_{SN_i}| < \Delta T$, where ΔT is the "maximum allowable transmission delay" associated with a message. Note that the timestamp validation allows to protect the replay attack in the proposed scheme. If the timestamp validation is successful, $Aggr_j$ applies the **L-Unsigncryption** phase (described in Section 5.5) to verify the signature using the public key $\mathbb{PK}_{SN_i}$ of SN_i and also to extract the data $Data_{SN_i}$, identity ID_{SN_i} and timestamp TS_{SN_i} using its own private key $\mathbb{SK}_{Aggr_j}$. If the extracted timestamp matches with the received timestamp, $Aggr_j$ further proceeds to generate the current timestamp TS_{Aggr_j} and applies the **L-Signcryption** phase on the information $Data_{SN_i}$, ID_{SN_i}, ID_{Aggrj}, TS_{SN_i}, TS_{Aggr_j} to create signcryption as $C_{SN_i,Aggr_j} = \text{L-Signcryption}(Data_{SN_i}, ID_{SN_i}, ID_{Aggrj}, TS_{SN_i}, TS_{Aggr_j})$, where the signature is created using the private key $\mathbb{SK}_{Aggr_j}$ of $Aggr_j$ and the information $(Data_{SN_i}, ID_{SN_i}, ID_{Aggrj}, TS_{SN_i}, TS_{Aggr_j})$ is encrypted using the public key $\mathbb{PK}_{CS_k}$ of CS_k. Finally, $Aggr_j$ sends the message $Msg_{SNAggrData} = \{C_{SN_i,Aggr_j}, TS_{Aggr_j}\}$ to the concerned cloud server CS_k via public channel.

6.3 | Secure cloud data storage phase

This phase is executed by the concerned cloud server CS_k after receiving the message $Msg_{SNAggrData} = \{C_{SN_i,Aggr_j}, TS_{Aggr_j}\}$ from an aggregator node $Aggr_j$ for an IoT application $Appl_j$. The following steps are then needed for secure data storage at the cloud:

- **Step 1**. If the CS_k receives the message $Msg_{SNAggrData}$ at time TS'_{Aggr_j}, it first checks the timestamp validation by the condition: $|TS'_{Aggr_j} - TS_{Aggr_j}| < \Delta T$. If the timestamp is invalid, the phase will be terminated.
- **Step 2**. Upon successful timestamp verification, CS_k applies the **L-Unsigncryption** phase to verify the signature using the public key $\mathbb{PK}_{Aggr_j}$ of $Aggr_j$ and also to extract the information $Data_{SN_i}$, ID_{SN_i}, ID_{Aggrj}, TS_{SN_i} and TS_{Aggr_j} using its own private key $\mathbb{SK}_{CS_k}$. Now, if the extracted timestamp of $Aggr_j$ is same as the received timestamp of $Aggr_j$, CS_k proceeds to store the signcrypted data $C_{SN_i,Aggr_j} = \text{L-Signcryption}(Data_{SN_i}, ID_{SN_i}, ID_{Aggrj}, TS_{SN_i}, TS_{Aggr_j})$ in its database.

It is worth to note that the cloud server CS_k cannot modify $C_{SN_i,Aggr_j}$ in the database, because it involves the signature of $Aggr_j$ using the private key $\mathbb{SK}_{Aggr_j}$ of $Aggr_j$. The overall scheme is summarized in Figure 7.

7 | SECURITY ANALYSIS

In the first part, we provide the formal security analysis of our constructed signcryption scheme. In the second part, we show the proposed SCDS-LBSIoT is resilient against several potential attacks through informal security analysis.

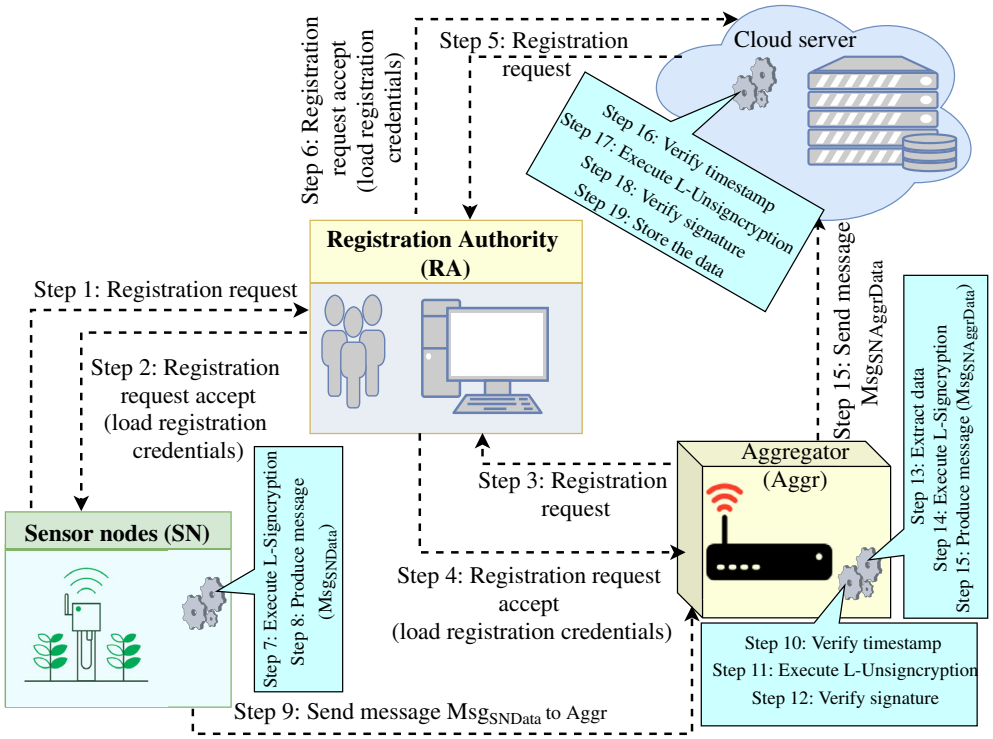

FIGURE 7 Overall secure cloud data storage in SCDS-LBSIoT

7.1 | Formal security analysis

The proposed signcryption follows sign-then-encryption approach, but it can be observed that a scheme combining both IND-CCA2 secure encryption and SUF-CMA secure signature does not necessarily implies MU-SUF-iCMA security.[57,58] The validness of the proposed scheme comes under the fact of learning with errors. Theorems 2 and 3 discuss the essential security of the proposed signcryption.

It is worth noticing that we cannot prove the correctness with equality. This is based on assumption: "learning with errors" that gives an approximate way to decrypt the encrypted message. Micciancio and Peikert[53] proposed an algorithm with trapdoor that is provided in Theorem 1. This proves the validity of our proposed signcryption algorithm.

Theorem 1 (53). *If $q \geq 2$, $n \geq 1$, and $m = O(n \log q)$, then $Gen - trap(1^n, 1^m, q)$ is a "randomized algorithm" that generates $A \in \mathbb{Z}_q^{n \times m}$, called a parity check matrix, and a secret trapdoor T such that $A \in \mathbb{Z}_q^{n \times m}$ follows almost uniform distribution. Furthermore, there are efficient algorithms Invert and $Sample - D$ with the "overwhelming probability over all random choices" with the following characteristics:*

i) Let T, A and $b^t = \varrho^t + e^t$ be the inputs, where $\vartheta \in \mathbb{Z}_q^n$ and $||e|| < \frac{q}{O(\sqrt{n \log q})} \leftarrow D_{\mathbb{Z}^m, \alpha q}$, $\frac{1}{\alpha} \geq \sqrt{n \log q}.\omega(\sqrt{\log n})$. Then, the deterministic procedure $Invert(T, A, b)$ gives output as (ϑ, e).

ii) Let T, A and $\varrho \in \mathbb{Z}_q^n$ and $\vartheta = O(\sqrt{n \log q})$ be the inputs. Then, the randomized procedure $Sample - D(T, A, \varrho, \vartheta)$ samples according to $negl(n)$ distribution statistically close to $D_{\Delta_q^{\varrho}, \vartheta.\omega(\sqrt{\log n})}$.

Theorem 2. *If $\sigma \geq 2\frac{\sqrt{n}}{q}$ and LWE holds for the given σ and q, and hash function is collision resistant, then our construction is MU-IND-iCCA2 secure.*

Proof. Let an attacker $\mathcal{A}$ play a game to breach the security of the proposed construction. We define the MU-IND-iCCA2 games, say $\mathcal{G}_i$, $i \in \{1, 2, 3, 4, 5\}$. The detailed description of these game is as follows.

1. Game $\mathcal{G}_1$: This is natural MU-IND-iCCA2 game.

2. Game $\mathcal{G}_2$: This game follows the steps as in $\mathcal{G}_1$ except that if $\mathcal{A}$ sends an unsigncryption query $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$ satisfying $t^* = f_{\hat{A}_r}(\mathbb{PK}_s) + f_B(r_e)$, then terminates the process.
3. Game $\mathcal{G}_3$: This game follows the steps as in $\mathcal{G}_2$ except that B corresponding to f_B is replaced with a trapdoor $T_B \in \mathbb{Z}^{\hat{m} \times \log\ q}$.
4. Game $\mathcal{G}_4$: This game follows the same steps as in $\mathcal{G}_3$ except that C generates c_0^* corresponding to challenge cipher C^*:
   - Set $s \xleftarrow{u} \mathbb{Z}_q^n, \hat{x}_0 \leftarrow D_{\sigma q}^{\hat{m}}, \hat{c}_0^t = s^t\ \hat{A}_r + p\hat{x}_0^t\ (mod\ q)$.
   - Select $\hat{x}_0' \leftarrow D_{\sigma q}^{n\ \log\ q}$, and calculate $c_0'^t = -\hat{c}_0^{\ t}\ T_r + p\ x_0'^t = (s^t(-A_r T_r)) + p(-\hat{x_0} T_r + x_0') \in \mathbb{Z}_q^{n\ \log\ q}$.
   - Finally, set $\hat{c_0}^{*t} = \hat{c_0}^t || c_0'^t$.
5. Game $\mathcal{G}_5$: This game follows the steps as in $\mathcal{G}_4$ except that in place of $\hat{c}_0 = s^t \hat{A}_r + p\ \hat{x_0}\ (mod\ q),\ \hat{c}_1 = s^t\ U + p\ x_1\ (mod\ q), < \hat{c_0},\ \hat{c_1} > \in \mathbb{Z}_q^{\hat{m}} \times \mathbb{Z}_q^{n \times \ell}$ is an arbitrary tuple.

Now, we define the following events ($1 \leq i \leq 5$) to illustrate the MU-IND-iCCA2 security of the concerned $\mathcal{LBSCS}$ as follows.

- $\mathcal{S}_i$: Event $\mathcal{S}_i$ corresponds to $\mathcal{A}'s$ success in $\mathcal{G}_i$.
- $\mathcal{V}_i$: Event $\mathcal{V}_i$ corresponds to $\mathcal{G}_i$, where $\mathcal{A}$ sends unsigncryption query $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$ satisfying $t^* = f_{\hat{A}_r}(\mathbb{PK}_s) + f_B(r_e) \in \mathbb{Z}_q^n$.
- $\mathcal{CR}_i$: Event $\mathcal{CR}_i$ corresponds to $\mathcal{G}_i$, where $\mathcal{A}$ sends unsigncryption query $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$ satisfying $< \mathbb{PK}_s,\ r_e > \neq < \mathbb{PK}_s^*,\ r_e^* > \wedge\ t^* = f_{\hat{A}_r}(\mathbb{PK}_s) + f_B(r_e) \in \mathbb{Z}_q^n$.
- $\mathcal{F}_i$: Event $\mathcal{F}_i$ corresponds to $\mathcal{G}_i$, where $\mathcal{A}$ sends unsigncryption query $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$ satisfying $< \mathbb{PK}_s,\ r_e > \neq < \mathbb{PK}_s^*,\ r_e^* > \wedge\ \wedge\ ||e|| \leq \delta\sqrt{m + n\ \log\ q} \wedge A_{s,\ h}.e = u_s\ (mod\ q)$, where $h \leftarrow f_{\hat{A}_s}(\mu || \mathbb{PK}_r || \hat{C}) + f_B(r_s) \in \mathbb{Z}_q^n$.

Now, we try to show that $Adv_{\mathcal{A}}^{MU-IND-CCA}(\lambda)$ is negligible under following three facts:

- **Fact (1)**: $Pr[\mathcal{CR}_1] \leq negl(\lambda)$. **Discussion**: With the help of $\mathcal{A}$, one can construct a polynomial times algorithm $\mathcal{B}$ which breaks collision problem in $f_{\hat{A}_r} + f_B$ in the following steps:
  - **Set-up**: This algorithm takes input $< B,\ \hat{A}_r > \in \mathbb{Z}_q^{n \times (m + \hat{m})}$ and generates A_r by sampling $T_r \in \mathbb{Z}_q^{\hat{m} \times n\ \log\ q}$ from $D_{\sqrt{\log\ n}}^{\hat{m} \times n\ \log\ q}$, computes $A_r \leftarrow [A_r | - A_r T_r]$. It furthers chooses an arbitrary $U \in \mathbb{Z}_q^{n \times \ell}$ and adds $< U,\ B >$ to public parameters, where $\mathbb{PK}_r = A_r$ and $\mathbb{SK}_r = T_r$. Finally, one runs $\mathcal{A}(params,\ \mathbb{PK}_r)$ as:
    1. **Queries-phase 1**: If $\mathcal{A}$ sends a query $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$ to the concerned unsigncryption Oracle, then repeat the process as in $\mathcal{G}_1$.
    2. **Challenge**: If $\mathcal{A}$ sends a challenge $< \mathbb{PK}_s^*,\ \mathbb{SK}_s^*,\ \mu_0,\ \mu_1 >$, then $\mathcal{B}$ computes $t^* = f_B(r_e^*) + f_{\hat{A}_r}(\mathbb{PK}_s^*) \in \mathbb{Z}_q^n$ and chooses arbitrary $b \in \{0,\ 1\}$ to generate C^* on μ_b using $\mathcal{LBSCS}$ signcryption.
    3. **Queries-phase 2**: If $\mathcal{A}$ sends a query $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$ to the unsigncryption Oracle, then $\mathcal{B}$ checks whether $\mathcal{CR}_1$ occurs, if yes then stops and outputs $(< r_e^*,\ \mathbb{PK}_s^* >, < r_e,\ \mathbb{PK}_s >)$, otherwise stops unsigncryption algorithm.
  - **Output**: Finally, $\mathcal{A}$ outputs arbitrary $b' \in \{0,\ 1\}$.

  One can observe that $\mathcal{B}$ essentially simulates the view of $\mathcal{A}$. If $\mathcal{A}$ sends a query $t^* = f_B(r_e) + f_{\hat{A}_r}(\mathbb{PK}_s) \in \mathbb{Z}_q^n$ and $(< r_e^*,\ \mathbb{PK}_s^* > \neq < r_e,\ \mathbb{PK}_s >)$, then output of $\mathcal{B}$ is a collision to $f_{\hat{A}_r + f_B}$.
- **Fact (2)**: $|Pr[\mathcal{S}_2] - Pr[\mathcal{S}_3]| \leq negl(\lambda)$, $|Pr[\mathcal{F}_2] - Pr[\mathcal{F}_3]| \leq negl(\lambda)$, $|Pr[\mathcal{S}_3] - Pr[\mathcal{S}_4]| \leq negl(\lambda)$ and $|Pr[\mathcal{F}_3] - Pr[\mathcal{F}_4]| \leq negl(\lambda)$.

  Discussion: One can observe that both $|Pr[\mathcal{S}_2] - Pr[\mathcal{S}_3]| \leq negl(\lambda)$ and $|Pr[\mathcal{F}_2] - Pr[\mathcal{F}_3]| \leq negl(\lambda)$ are true by Theorem 1. Both $|Pr[\mathcal{S}_3] - Pr[\mathcal{S}_4]| \leq negl(\lambda)$ and $|Pr[\mathcal{F}_3] - Pr[\mathcal{F}_4]| \leq negl(\lambda)$ are true under the facts:

  Fact-(a)(31): Let $r_1,\ r_2 > 0$ be two real numbers and $z,\ u \in \mathbb{R}^n$, where $\frac{1}{\sqrt{\frac{1}{r_1^2} + (||z||/\alpha)^2}} \geq \xi_\epsilon$ with $\epsilon < \frac{1}{2}$. Then the distribution $< z,\ \vartheta > + e$, where ϑ distributed under $D_{\Delta + u,\ r_1}$ and e from Gaussian with mean zero and deviation $\frac{\sigma}{2\pi}$ follows statistical distance always less than 4ϵ of normal variable with mean zero and deviation $\frac{\sqrt{(r_1 ||z||^2) + \alpha^2}}{\sqrt{2\pi}}$.

Fact-(b)(60): Let $E,\ F$ be two positive definite matrices satisfying $\sum = E + F > 0$ and $\sum_3^{-1} = E^{-1} + F^{-2} > 0$. Let $\Delta_1,\ \Delta_2$ be two lattices satisfying condition $\sqrt{E} \geq \xi_\epsilon(\Delta_1)$ and $\sqrt{\sum_3} \geq \xi_\epsilon(\Delta_2)$, where $\epsilon \leq \frac{1}{2}$ and $r_1,\ r_2 \in \mathbb{R}^n$. Now, one consider $x_2 \leftarrow D_{\Delta_2+r_2,\ \sqrt{F}}$, then chooses $x_1 \leftarrow x_2 + D_{\Delta_1+r_1+-x_2,\ \sqrt{E}}$. The marginal distribution of x_1 has statistical distance less than 8ϵ of $D_{\Delta_1+r_1,\ \sqrt{\sum}}$.

- **Fact (3)**: $|Pr[S_4] - Pr[S_5]| \leq negl(\lambda)$, $Pr[\mathcal{F}_4] - Pr[\mathcal{F}_5]| \leq negl(\lambda)$, $|Pr[S_5] - \frac{1}{2}| \leq negl(\lambda)$, $Pr[\mathcal{F}_5] \leq negl(\lambda)$.

Discussion: It can be observed that $|Pr[S_5] - \frac{1}{2}| \leq negl(\lambda)$, $Pr[\mathcal{F}_5] \leq negl(\lambda)$ holds as μ and r_s are hidden (statistically) in $\mathcal{G}_5$. Furthers, one can prove $|Pr[S_4] - Pr[S_5]| \leq negl(\lambda)$ by designing polynomial times model $\mathcal{B}'$, which can break LWE assumption and discussed in the following steps:

1. **Set-up**: $\mathcal{B}'$ takes an LWE challenge $\{\hat{A}_r,\ U,\ \hat{c}_0,\ \hat{c}_1\} \in \mathbb{Z}_q^{n\times(\ell+\hat{m})} \times \mathbb{Z}_q^{(\hat{m}+\ell)}$ and chooses arbitrary $t^* \in \mathbb{Z}_q^n$, furthers generate $< B,\ T_B > \leftarrow Trap - gen(1^\lambda)$, samples $T_r \in \mathbb{Z}_q^{\hat{m}\times n\ \log\ q} \leftarrow D_\delta^{\hat{m}\times n\ \log\ q}$. Let $A_r = [\hat{A}_r| - H(t^*)G - \hat{A}_r T_r] \in \mathbb{Z}_q^{n\times m}$, and $\mathbb{PK}_r = A_r, \mathbb{SK}_r = (T_r,\ T_B)$, then adds $(\hat{A},\ U,\ B)$ and runs $\mathcal{A}(params,\ \mathbb{PK}_r)$.
2. **Queries-phase 1**: If $\mathcal{A}$ sends $< \mathbb{PK}_s,\ c_0,\ c_1,\ r_e,\ e >$, the it is answered same as in $\mathcal{G}_4$ by $\mathbb{SK}_r$ under proposition (1).
3. **Challenge**: If $\mathcal{A}$ sends $< \mathbb{PK}_s^*,\ \mathbb{SK}_s^*,\ \mu_0,\ \mu_1 >$, then $\mathcal{B}'$ follows the steps:
   a. Chooses arbitrary $b \in \{0,\ 1\}, r_e^* \leftarrow sample - D(T_B,\ B,\ (t^* - f_{\hat{A}_r}(\mathbb{PK}_s^*))\ (mod\ q),\ \log\ n)$.
   b. Computes $c_0'^t = \hat{c_0}^t T_r + x_0'^t,\ \hat{c_0}^{*t} = p(\hat{C_0}^{'t} || \hat{c_0}'^t) \in \mathbb{Z}_q^m$ and $\hat{c_1}^* = p\hat{c_1} \in \mathbb{Z}_q^\ell$.
   c. Computes $< c_0^*,\ c_1^*,\ r_e^*,\ e^* >$ using $< \mathbb{PK}_s^*,\ \mathbb{SK}_s^* >$ under the signcryption algorithm.
   d. Finally, returns $C^* =< c_0^*,\ c_1^*,\ r_e^*,\ e^* >$.
4. **Queries-phase 2**: Following the **Queries-phase 1**, furthers $\mathcal{A}$ sends $< \mathbb{PK}_s, C >$, where $< \mathbb{PK}_s, C > \neq < \mathbb{PK}_s^*, C^* >$.
5. Finally, $\mathcal{A}$ guesses a bit $b' \in \{0,\ 1\}$.

Whenever $\mathcal{A}$ sends queries $t \neq t^*$, then unsigncryption is possible due to $H(t) - H(t^*) = H(t - t^*) \in \mathbb{Z}_q^{n\times n}$ is invertible under full rank decoding.[59] In **Queries-phase 1**, $\mathcal{A}$ sends a query with $t = t^*$ has negligible probability as t^* is hidden (statistically) in set-up phase. Therefore, one can use output of $\mathcal{A}$ and $\mathcal{B}'$ to decide $< \hat{c_0},\ \hat{c_1} >$ is the sample of LWE problem. Furthermore, it can be observed that $|Pr[\mathcal{F}_4] - Pr[\mathcal{F}_5]| \leq negl(\lambda)$ constructing $\mathcal{B}''$ under LWE problem, where $\mathcal{B}$ is same as $\mathcal{B}'$ except $\mathcal{B}''$ verifies unsigncryption under condition $||e|| \leq \delta\sqrt{m + n\ \log\ q}$ and $A_{s,\ h}.e = u_s\ (mod\ q)$ and guesses "b=0", otherwise, "b=1". Therefore, the advantage $Adv_{\mathcal{A}}^{MU-IND-CCA}(\lambda)$ is negligible.

■

Theorem 3. *When $SIS_{q,\ \zeta}$ holds for $\zeta = O((n\ \log\ n)^{\frac{5}{2}})\ .\omega(\log\ n^{\frac{3}{2}})$ and hashing is collision resistant, then the proposed signcryption is MU-SUF-iCMA secure.*

Proof. In MU-SUF-iCMA game, $\mathcal{A}$ is polynomial times, message $m = \mu||\mathbb{PK}_r||c_0$ and x_i be access to $Oracle_i$, where $i \in [Q]$. However, $\mathcal{A}$ is classified in to two categories as follows:

- **Type-1**: $\mathcal{A}$ forges the message using a collision of $f_{\hat{A}_s} + f_B$.
- **Type-2**: $\mathcal{A}$ forges the message without using a collision of $f_{\hat{A}_s} + f_B$ as follows:
  - $\mathcal{A}$ forges the message without submitting queries on the message.
  - $\mathcal{A}$ forges the message by submitting polynomial times queries on the message.

If $\mathcal{A}$ is type-1 adversary, then one can design a model S to find a collision of $f_{\hat{A}_s} + f_B$ and $ADv_{\mathcal{A}}^{MU-SUF-CMA}(\lambda) \leq Adv_S^{cr}(\lambda)$, where S_{cr} is designed as follows:

1. **Set-up**: Let $\hat{A}_s \in \mathbb{Z}_q^{n\times\hat{m}}$ and $B \in \mathbb{Z}_q^{n\times m}$ be the inputs, then parameters are generated same as Set-up and Extraction same as in Theorem 2, and $< \mathbb{PK}_s,\ \mathbb{SK}_s > =< (A_s,\ u_s),\ T_s >$ using $\hat{A}$ and B, then run(params, $\mathbb{PK}_s$).
2. **Queries-phase**: If $\mathcal{A}$ sends $< \mathbb{PK}_r,\ \mu >$, then S computes $c_0 =$ under public key $\mathbb{PK}_r$. Furthermore, S chooses an arbitrary r_s and computes $h = f_{\hat{A}_s}(\mu||\mathbb{PK}_r||c_0) + f_B(r_s)$, $C = \{c_0,\ c_1,\ r_e,\ e\}$ on message μ and sends C to $\mathcal{A}$.
3. **Output**: $\mathcal{A}$ generates a forgery $\{\mathbb{PK}_r^*,\ \mathbb{SK}_r^*,\ C^*\}$, and computes μ^* using unsigncryption and outputs $< m^*,\ r_s^* >$, $< m^{(i)},\ r_s^{(i)} >$ satisfying $f_{\hat{A}_s}(m^*) + f_B(r_s^*) = f_{\hat{A}_s}(m^{(i)}) + f_B(r_s^{(i)})$, where $< m^*,\ r_s^* > \neq < m^{(i)},\ r_s^{(i)} >$.

Now, one can observe that S_{cr} essentially simulates $\mathcal{A}$ and the forgery $\{\mathbb{PK}_r^*,\ \mathbb{SK}_r^*,\ C^*\}$ is constructed with the help of collision in corresponding $f_{\hat{A}_s} + f_B$ implies $ADv_{\mathcal{A}}^{MU-SUF-CMA}(\lambda) \leq Adv_S^{cr}(\lambda)$ holds.

In type-2 adversary, we show a reduction from $SIS_{q,\ \zeta}$, where $\zeta = O(2(\log\ q)^{\frac{3}{2}}).\omega(\sqrt{\log\ n})^3$ to MU-SUF-iCMA security of our proposed construction. Now, $\mathcal{A}$ cannot distinguish the change of B in $< B\ T_B >$ (parameter, trapdoor) and B of hashing function.

In type-2 (a), $\mathcal{A}$ outputs a forgery without submitting any query. If this happens, then one can construct $\mathcal{S}'$ who solves $SIS_{q,\ \zeta}$ with inputs $A = [\hat{A}_s|A'] \in \mathbb{Z}_q^{n\times\hat{m}+\log\ q}$ and $u \in \mathbb{Z}_q^n$, outputs $z \in \mathbb{Z}^m$ satisfying $Az = u\ (mod\ q)$, where $||z|| \le \zeta - 1$. A polynomial time $\mathcal{S}'$ who solves $SIS_{q,\ \zeta}$ is constructed as follows:

- **Set-up**: It takes input $A = [\hat{A}_s|A'] \in \mathbb{Z}_q^{n\times\hat{m}+\log\ q}$ and generates $< \mathbb{PK}_s,\ \mathbb{SK}_s >$ as:
  - It takes arbitrary messages $h^{(1)},\ h^{(2)},\ \dots,h^{(Q)} \in \{0,\ 1\}^\lambda$ and $\mathcal{P}$ be the set of strings p_i of length at most λ and no $h^{(i)}$ has prefix $p_i \in \mathcal{P}$.
  - It computes $< A_s,\ A_0,\ \dots,\ A_\lambda,\ u >$ as $A_i = H_iG + \hat{A}Ts,\ i$, where $Ts,\ i \leftarrow D_{\log\ n}^{m\times n\ \log\ q}$ and

$$H_i = \begin{cases} H(0) = 0 & \text{if } i > t \\ (-1)^{p_i}H(u^{(i)}) & \text{if } i \in [t] \\ -\sum\limits_{j\in[t]} p_jH(u^{(j)}) & \text{if } i = 0 \end{cases}. \tag{8}$$

  - Signature is generated with corresponding $h^{(i)}$ as $A_{s,\ h^{(i)}} \leftarrow [A|A_0 + \sum_{j\in[\lambda]} h_j^{(i)}A_j] = \hat{A}_s|A'|HG - \hat{A}(T_{(s,\ 0)} + \sum_{j\in[\lambda]} h_j^{(i)}T_{(s,\ j)})$ and $T_s^{(i)} = T_{(s,\ 0)} + \sum_{j\in[\lambda]} h_j^{(i)}T_{(s,\ j)}$ is trapdoor for $A_{s,\ h^{(i)}}$. Finally, it computes a signature $e^{(i)} \leftarrow sample - D(T_s^{(i)},\ A_{s,\ h^{(i)}},\ u_s,\ \delta)$.

- **Queries-phase**: A query $< \mu^{(i)},\ \mathbb{PK}_r^{(i)} >$ is submitted to signcryption Oracle, which proceeds as it chooses $r_s^{(i)} \leftarrow sample - D(T_B,\ B,\ h^{(i)} - f_{\hat{A}_s}(m^{(i)}\ (mod\ q),\ \log\ n)$. Furthers, it computes $< c_0^{(i)},\ c_1^{(i)} >$ using $< r_s,\ e^{(i)} >$ and essentially returns $C^{(i)} = \{c_0^{(i)},\ c_1^{(i)},\ r_e^{(i)},\ e^{(i)}\}$.
- **Output**: If $\mathcal{A}$ generates a forgery $\{\mathbb{PK}_r^*,\ \mathbb{SK}_r^*,\ C^* = (c_0^*,\ c_1^*,\ r_e^*,\ e^*)\}$, then it is confirmed to unsigncrypt μ^* using unsigncryption and it furthers computes $e,\ h^* \leftarrow f_{\hat{A}_s}(m^*) + f_B(r_s^*)\ (mod\ q)$.

Further, one can show that $\mathcal{S}'$ solves SIS problem using $< h^*,\ e^* >$. Since p is the prefix of h^*, then following holds: $As,\ h^* = [\hat{A}_s|A'| - \hat{A}_sT_{s,\ h^*}]$ implies

$$[\hat{A}_s|A'] = \begin{bmatrix} I_m & -T_s^* \\ I_n & \log\ q \end{bmatrix} \cdot \begin{bmatrix} y^* \end{bmatrix} = u_s\ (mod\ q),$$

where $||y^*|| \le \delta\ \sqrt{m} = O(\sqrt{\lambda}\ n\ \log\ q).\omega(\sqrt{\log\ n})^2$ holds trivially and $||T_s^*|| \le \sqrt{\lambda+1}.O(\sqrt{\hat{m}} + \sqrt{n\ \log\ q})$ holds as in Reference 53, and $||z|| \le \zeta - 1$.

In type-2 (b), $\mathcal{A}$ outputs a forgery by submitting query h^*. If this happens, then one can construct $\mathcal{S}''$ who solves $SIS_{q,\ \zeta}$ following the same as $\mathcal{S}'$ except set-up and outputs phases. The algorithm is executed for a given $A \in \mathbb{Z}_q^{n\times m}$ and $u \in \mathbb{Z}_q^n$, outputs $z \in \mathbb{Z}^m$ satisfying $Az = 0\ (mod\ q)$, where $||z|| \le \zeta$. A polynomial times $\mathcal{S}''$ who solves $SIS_{q,\ \zeta}$ is constructed as:

- It takes arbitrary messages $h^{(1)},\ h^{(2)},\ \cdot, h^{(Q)} \in \{0,\ 1\}^\lambda$ and $\mathcal{P}$ be the set of strings p_i of length at most λ and no $h^{(i)}$ has prefix $p_i \in \mathcal{P}$.
- It computes $< A_s,\ A_0,\ \cdot,\ A_\lambda,\ u_s >$ as in $\mathcal{S}'$ and $p \leftarrow h, y \leftarrow D_{\mathbb{Z}_\delta}$, where $u_s = A_h\ y\ (mod\ q)$. It generates a signature $e^{(i)}$ on $h^{(i)}$ as by $\mathcal{S}'$ except for h and assumes y is signature on h.
- **Output**: If $\mathcal{A}$ generates a forgery $\{\mathbb{PK}_r^*,\ \mathbb{SK}_r^*,\ C^* = (c_0^*,\ c_1^*,\ r_e^*,\ e^*)\}$, compute $< h^*,\ e^* >$ using unsigncryption. If $h^* = h$, then it is confirmed to unsigncrypt μ^* using unsigncryption and it furthers computes $As,\ h^* = [\hat{A}_s|A'| - \hat{A}_sT_{s,\ h^*}]$ implies

$$[\hat{A}_s|A'] = \begin{bmatrix} I_m & -T_s^* \\ I_n & \log\ q \end{bmatrix} \cdot \left[y^* - y\right] = 0\ (mod\ q),$$

where $||y^*|| \leq \delta\ \sqrt{m} = O(\sqrt{\lambda}\ n\ \log\ q).\omega(\sqrt{\log\ n})^2$ holds trivially and $||T_s^*|| = O(\sqrt{\lambda\ n\ \log\ q}).\omega(\sqrt{\log\ q})$ holds.

Both type-2 (a) and type-2 (b) adversaries complete the short integer solution reduction, and hence, the proof follows. ∎

7.2 | Informal security analysis

In the following propositions, we show that the proposed SCDS-LBSIoT is resilient against different attacks.

Proposition 1. *SCDS-LBSIoT is secure against replay attack.*

Proof. In the proposed SCDS-LBSIoT, the lattice-based signcrypted messages $Msg_{SNData} = \{C_{SN_i}, TS_{SN_i}\}$ and $Msg_{SNAggrData} = \{C_{SN_i,Aggr_j}, TS_{Aggr_j}\}$ are transmitted over the public channel. Each of these messages is injected with current timestamps TS_{SN_i} and TS_{Aggr_j}, and after receiving the messages the receiver verifies the timestamps with the receiving time. Therefore, if an adversary $\mathcal{A}$ tries to replay the old messages, the receiver can easily detect the old ones by verifying the timestamps attached with the messages. In this way, $\mathcal{A}$ cannot succeed with the "replay attack", and hence, SCDS-LBSIoT is protected from such type of attack. ∎

Proposition 2. *SCDS-LBSIoT is secure against privileged-insider attack.*

Proof. During the registration process in SCDS-LBSIoT, each trusted registration authority RA_j loads the private and public credentials into the network enteritis's memory only. Furthermore, the registered entities do not supply any further credentials to the RA_j. Once the registration process is over, RA_j deletes all the private information of the entities from its own memory. Therefore, even if a privileged-insider user of the RA_j, acting as an adversary $\mathcal{A}$, cannot obtain any of the private keys and as a result, the privileged-insider attack is resisted in SCDS-LBSIoT. ∎

Proposition 3. *SCDS-LBSIoT is secure against man-in-the-middle (MiTM) attack.*

Proof. In the proposed SCDS-LBSIoT, two messages are communicated over the public channel, which are $Msg_{SNData} = \{C_{SN_i}, TS_{SN_i}\}$ and $Msg_{SNAggrData} = \{C_{SN_i,Aggr_j}, TS_{Aggr_j}\}$. The messages are constructed by the lattice-based **L-Signcryption** process with the help of sender's private key as well as receiver's public key. The private key is generated based on the lattice-based hardness assumption and it is quantum resistance. An adversary $\mathcal{A}$ cannot then guess the private key online by eavesdropping the messages to generate a fake (modified) message on the fly, and therefore, $\mathcal{A}$ cannot extract the original data from the messages. Thus, SCDS-LBSIoT is secure against MiTM attack. ∎

Proposition 4. *SCDS-LBSIoT is secure against impersonation attacks.*

Proof. The transmitted messages Msg_{SNData} and $Msg_{SNAggrData}$ are constructed based on the lattice-based **L-Signcryption** process which need the private key of the sender. The private key is also quantum resistance and it is infeasible to derive the private with knowledge of the public key and other public information. In addition, SCDS-LBSIoT is able to hide the private keys in the communicated messages. Now, an adversary $\mathcal{A}$ cannot reveal the private key offline for disclosing the messages as well as generate the fake message(s) on behalf of either an IoT sensor node SN_i or an aggregator $Aggr_j$. Hence, SCDS-LBSIoT is protected against the IoT sensor node impersonation attack as well as aggregator impersonation attack. ∎

Proposition 5. *SCDS-LBSIoT provides both anonymity and untraceability properties.*

Proof. In the SCDS-LBSIoT, the sender sends a message to the receiver by applying the lattice-based **L-Signcryption** process with the help of its own identity, lattice-based private and public keys along with current timestamp. The identity is hidden to the messages and revealing this identity from the messages is computationally infeasible. Therefore, an adversary $\mathcal{A}$ cannot know the identity of the sender from the transmitted messages, and hence, SCDS-LBSIoT is able to support the anonymity property. Additionally, every time the messages are built by the fresh timestamps which makes the old

message is different from a new message. $\mathcal{A}$ cannot then trace the messages during communication. Thus, SCDS-LBSIoT provides the untraceability property. ∎

Proposition 6. *SCDS-LBSIoT is resilient against physical IoT sensor nodes capture attack.*

Proof. In the proposed SCDS-LBSIoT, assume that an IoT sensor node SN_i is physically compromised by an adversary $\mathcal{A}$ as monitoring IoT fields 24×7 is not always possible. Based on the security model defined in Section 4.3.3, using the power analysis attacks[55] $\mathcal{A}$ will have the extracted credentials $\{ID_{SN_i}, (\mathbb{SK}_{SN_i}, \mathbb{PK}_{SN_i}), \mathbb{PK}_{Aggr_j}\}$. It is worth noticing that all the $\{ID_{SN_i}, (\mathbb{SK}_{SN_i}, \mathbb{PK}_{SN_i})\}$ are distinct and unique for each deployed IoT sensor node SN_i. As a result, $\mathcal{A}$ cannot create messages on behalf of other noncompromised IoT sensor nodes in the network and cannot also send the messages to the aggregator node(s). Thus, compromise of a sensor node in the network does not reflect to compromise the secure communications happen among other noncompromised sensor nodes and the aggregators. As a result, $\mathcal{A}$ is resilient against physical IoT sensor nodes capture attack. ∎

Proposition 7. *SCDS-LBSIoT is resilient against potential quantum attacks.*

Proof. In a hybrid lattice-reduction attack, an adversary needs to break the shortest vector problem (SVP) where given a basis of vectors of a lattice such that the vectors are of fixed-length tuples of integers, to find a nonzero vector whose length is same as that for the length of the shortest vector. If we combine the hybrid lattice-reduction attack and meet-in-the middle attack together, a hybrid attack is formed. There is also other quantum attacks, such as a quantum MiTM attack, where an adversary may block all the calibration signals and then sends the tampered calibration signals to disturb the activation timing calibration of the detectors. In our proposed SCDS-LBSIoT, we have utilized fresh timestamp, identity and message for generating the signcrypted ciphertext by using the lattice-based **L-Signcryption** process with the help of sender's private key as well as receiver's public key. Thus, hybrid attack is resisted in SCDS-LBSIoT. Moreover, in SCDS-LBSIoT, a quantum MiTM attack is also resisted due to use of the LBC-based signcryption approach. As a result, SCDS-LBSIoT resists quantum MiTM attack and hybrid attack. ∎

8 | PERFORMANCE ANALYSIS

It is very important to observe that the proposed construction is helpful in reducing the size of public parameters. Let n be a security parameter with bit size κ, τ be a prime, a positive integer $m = O(n\ log(\log\ \tau))$ be dimension of lattice, $d << \tau$ be a value of sample from Gaussian in $\mathbb{Z}$. Our proposed construction takes $mn\ \log\ \tau, mn \log\ \tau\ \log\ d, mn\ \log\ \tau, mn \log\ \tau\ \log\ d, (m+k) \log\ \tau + 2m \log\ d + |\mu|$, in the receiver public-key, receiver secret-key, sender public-key, sender secret-key, and cipher-size respectively.

We first discuss the cost of computation for our proposed design and then elaborate a comparative study with the classical RSA/ECC based protocols. In general, for a security parameter κ, a lattice based cryptosystem has a public key of size $O(\kappa^2)$ and the computation time $O(\kappa^2)$, whereas the size of the public key used in a number theoretic classic cryptosystem (eg, in RSA and ElGamal systems) is $O(\kappa)$ and then computation time is $O(\kappa^3)$.[65] Furthermore, a lattice based cryptosystem using learning with rounding[31] can reduce the size of public key as $\tilde{O}(\kappa)$. We have provided a comparative analysis among the relevant classical schemes of Chiba et al,[61] Ducas and Micciancio,[35] Sato et al,[62] Gupta and Biswas,[63] Dharminder and Mishra,[64] Sun and Zhang,[41] Yan et al,[42] Yang et al,[43] Yu and Bai,[44] and the proposed signcryption scheme in Table 3. λ is a parameter chosen in Yan et al's scheme.[42] It is observed that the proposed construction performs better than other schemes of Chiba et al, Sato et al, Gupta and Biswas, and Dharminder and Mishra, except the scheme of Ducas and Micciancio, in terms of sender and receiver public keys sizes. Moreover, our proposed signcryption scheme is also equally comparable with the schemes of Sun and Zhang,[41] Yan et al,[42] Yang et al,[43] and Yu and Bai.[44] However, our construction works better than Ducas and Micciancio's construction[35] when it is considered for the cipher size. Overall, the proposed construction has better performance as compared to other schemes.

We analyze performance of the proposed design, and we take the LWE problem under suitable parameters as: $q = O(\kappa), x = O(\kappa \log q), n = O(\kappa \log q)$ for a security parameter κ. For the simplicity, we take $q = \kappa^2, x = \kappa \log q, n = 2\kappa \log q$. The communication cost for $x + r^T E, Ar$ becomes $n|q|$ or $m|q|$ and for a matrix A it is $16\kappa^2 log^3 k$ bits. For the discrete logarithm, storage and communication costs are $\log(p)$ bits with $p \approx 2^\kappa$ bits. The complexity of computation of a public key is $O(\kappa^3 log^5 \kappa)$ and for $x'^t + rE$ as well as verification will be $O(\kappa^2 log^4 \kappa)$. Our proposed construction has a secret key

TABLE 3 Performance comparison of our construction with relevant schemes

Protocol	Sender public key-size	Receiver public key-size	Cipher size
Chiba et al[61]	$3\ n\ m\ \log(q)$	$3\ n\ m\ \log(q)$	$(n+\kappa).\log(q)+3\ n\ \log(\rho)+\lvert\mu\rvert$
Ducas and Micciancio[35]	$n\ m\ \log(q)$	$n\ m\ \log(q)$	$(n+\kappa).\log(q)+3\ n+m+\mu\ \log(q)$
Sato et al[62]	$3\ n\ m\ \log(q)$	$3\ n\ m\ \log(q)$	$(n+\kappa).\log\ (q)+2\ n\log(\rho)+\lvert\mu\rvert$
Gupta and Biswas[63]	$3\ n\ m\ \log(q)$	$3\ n\ m\ \log(q)$	$(n+\kappa).\log(q)+3\ n\ \log(\rho)+\lvert\mu\rvert$
Dharminder and Mishra[64]	$3\ n\ m\ \log(q)$	$3\ n\ m\ \log(q)$	$(n+\kappa).\log\ (q)+2\ n\ \log(\rho)+\lvert\mu\rvert$
Sun and Zhang[41]	$(m\ \kappa+1)\log(q)$	$(m\ \kappa+1)\log(q)$	$2m\ \kappa^2\ n\ (\log(q))^2$
Yan et al[42]	$\kappa\ (\kappa+1)^2\ m^2\ \lambda\ (\log(q))^2$	$\kappa\ (\kappa+1)^2\ m^2\ \lambda\ (\log(q))^2$	$m\ \kappa\ n^2\ (\log(q))^2$
Yang et al[43]	$m^2\ n\ \log(q)$	$m^2\ n\ \log(q)$	$2m^2\ n\ (\log(q))^2$
Yu and Bai[44]	$2n^2\ \log(q)$	$2n^2\ \log(q)$	$m\ n^2\ (\log(q))^2$
Proposed	$2\ n\ m\ \log(q)$	$2\ n\ m\ \log(q)$	$(n+\kappa).\log(q)+2\ n\log(\rho)+\lvert\mu\rvert$

TABLE 4 Performance comparison of our construction with classical DLP scheme

Protocol	Primitive	Bit-size
DLP storage	$g \in Z_p^*$	$k' = \log p$
DLP communication	$g^r, r^{-1}(P - X_A h) \in Z_p^*$	$k' = \log p$
LWE-storage	$A \in Z_q^{m\times n}$	$((5+\kappa)n+\tau_5+1)m\log q$
LWE-signcryption	$\omega_1 \leftarrow SamplePre(T'_{\mathbb{ID}_s}, b-z, \vartheta_1), Z_q^*$	$m^2n+4nm+m\tau_5$
LWE-unsigncryption	$\omega_1 \leftarrow SamplePre(T'_{\mathbb{ID}_r}, b-z, \vartheta'_1), Z_q^*$	$m^2n+4nm+3\tau_5 n$

size nm as in shown in Table 4 and the verification key size $4n^2 \log q$. Moreover, the sizes of public and secret keys are $O(\kappa^2 \log \kappa)$ bits and $n^2 \log q$ bits, respectively.

In our proposed construction, a Gaussian sample is considered with a dimension n, and a preimage sample is considered in dimension $2m$. The multiplication cost over Z_q is roughly $m^2n + 4nm + m\tau_5$, whereas the unsigncryption cost becomes $m^2n + 4nm + 3\tau_5 n$, and the number of multiplications turns out to be $3\tau_5 n$ over Z_q. The ciphertext in the proposed scheme is $c = (t, c_0, c_1, c_2)$, where size of c_2 is $|c_2| = |r_1| + |r_2| + |\mu|$. The length of signcryption output is then $|t| + |c_0| + |c_1| + |r_1| + |r_2| + |\mu|$ as shown in Table 4. Moreover, the signcryption phase of the proposed scheme needs n "discrete Gaussian samplings" and $2n$ "pre-image samplings". On the receiver end, $3mn$ multiplications over Z_q are necessary. A solution to $Ae = b$ also requires the Gaussian elimination method, and thus, the resultant matrix needs to be stored for efficient computation purpose. The total number of multiplicative operations over Z_q during the back substitution process becomes "$[n-(m-1)] + [n-(m-2)+\cdots+n+(m-m)] = mn - \frac{1}{2}m(m-1)$". One can readily observe the relationship between the length of keys in bits and generation time in milliseconds.

TABLE 5 Computation costs comparative study: RSA vs Lattice based key generation

Approach	Key-length (in bits)	Key generation time (in milliseconds)
RSA	512	360
	1024	1280
	2048	4195
Lattice-based	1169	4
	1841	7.5
	4024	17.5

In Table 5, we have shown a computation costs comparative study among RSA and lattice based public key cryptosystems for key generation. In RSA, key lengths 512, 1024, 2048, takes 360, 1280, and 4195 milliseconds respectively, whereas in lattice based, key lengths 1170, 8140, 4024, take generation time 4, 7.5, and 17.5 milliseconds, respectively.[66]

9 | CONCLUSION AND FUTURE WORK

In this article, we have constructed a postquantum secure identity based signcryption. Our construction is postquantum secure and it has shorter size of public parameters as compared to the existing schemes, and offers low computation and communication costs as compared to those for the fundamental schemes based on ordinary number system. The proposed signcryption has better security in the era of quantum computers as compared to the number system based schemes. We then applied the constructed lattice-based signcryption for secure cloud based data storage in IoT applications (SCDS-LBSIoT). The proposed SCDS-LBSIoT allows secure data transfer among the IoT sensor nodes and the aggregators, and also among the aggregators and the cloud servers. In addition, the data put in the cloud cannot be modified/updated even by the cloud servers because of involvement of the signatures on the data signed by the private keys of the aggregators. As a result, SCDS-LBSIoT is resilient against replay, impersonation, man-in-the-middle, physical IoT senor nodes capture and privileged-insider attacks. Moreover, SCDS-LBSIoT offers untraceability and anonymity preservation properties. Thus, SCDS-LBSIoT is very much applicable in real-life applications, like IoT applications.

Some future research works can be as follows. We would like to study and analyze the threshold signcryption algorithm from lattice that can be applied in IoT environment for secure data storage at the cloud center. In addition, we would like to refine our proposed SCDS-LBSIoT for better efficiency in terms of public key size as well as cipher size.

ACKNOWLEDGMENTS

The authors thank the anonymous reviewers, the associate editor and the editor-in-chief for their valuable feedback on the article, which helped us to improve its quality and presentation.

CONFLICT OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

FUNDING INFORMATION

Deanship of Scientific Research at King Khalid University for funding this work through research groups program under grant number R.G.P. 2/86/43. FCT/MCTES through national funds and when applicable co-funded EU funds under the Project UIDB/50008/2020; and by Brazilian National Council for Scientific and Technological Development—CNPq, via Grant No. 313036/2020-9.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Dharminder Dharminder https://orcid.org/0000-0002-4478-5706
Joel J. P. C. Rodrigues https://orcid.org/0000-0001-8657-3800

REFERENCES

1. Soldatos J. The Internet of Things in the Cloud; 2017. https://www.kdnuggets.com/2017/05/internet-of-things-iot-cloud.html. Accessed October 2021.
2. Saha S, Sutrala AK, Das AK, Kumar N, Rodrigues JJPC. *On the Design of Blockchain-Based Access Control Protocol for IoT-Enabled Healthcare Applications*. Dublin, Ireland: IEEE International Conference on Communications (ICC'20); 2020:1-6.
3. Srinivas J, Das AK, Kumar N, Rodrigues JJPC. Cloud centric authentication for wearable healthcare monitoring system. *IEEE Trans Depend Secure Comput*. 2020;17(5):942-956.
4. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues JJPC. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. *IEEE Trans Ind Inform*. 2019;15(1):457-468.
5. Fotouhi M, Bayat M, Das AK, Far HAN, Pournaghi SM, Doostari MA. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Comput Netw*. 2020;177:107333.

6. Jindal A, Dua A, Kumar N, Das AK, Vasilakos AV, Rodrigues JJPC. Providing healthcare-as-a-service using fuzzy rule based big data analytics in cloud computing. *IEEE J Biomed Health Inform*. 2018;22(5):1605-1618.
7. Yang X, Li X, Li T, Wang X, Wang C, Li B. Efficient and anonymous multi-message and multi-receiver electronic health records sharing scheme without secure channel based on blockchain. *Trans Emerg Telecommun Technol*. 2021;32(12):e4371.
8. Alzubi OA, Alzubi JA, Shankar K, Gupta D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. *Trans Emerg Telecommun Technol*. 2021;32(12):e4360.
9. Mitra A, Bera B, Das AK. *Design and Testbed Experiments of Public Blockchain-Based Security Framework for IoT-Enabled Drone-Assisted Wildlife Monitoring*. Vancouver, BC, Canada: IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); 2021:1-6. doi:10.1109/INFOCOMWKSHPS51825.2021.9484468
10. Bera B, Vangala A, Das AK, Lorenz P, Khan MK. Private blockchain-envisioned drones-assisted authentication scheme in IoT-enabled agricultural environment. *Comput Stand Interfaces*. 2022;80:103567.
11. Vangala A, Das AK, Kumar N, Alazab M. Smart secure sensing for IoT-based agriculture: blockchain perspective. *IEEE Sens J*. 2021;21(16):17591-17607.
12. Vangala A, Das AK, Lee JH. Provably secure signature-based anonymous user authentication protocol in an Internet of Things-enabled intelligent precision agricultural environment. *Concurr Comput Pract Exp*. 2021;e6187. doi:10.1002/cpe.6187
13. Bera B, Saha S, Das AK, Kumar N, Lorenz P, Alazab M. Blockchain-Envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment. *IEEE Trans Veh Technol*. 2020;69(8):9097-9111.
14. Bera B, Chattaraj D, Das AK. Designing secure blockchain-based access control scheme in IoT-enabled internet of drones deployment. *Comput Commun*. 2020;153:229-249.
15. Jangirala S, Das AK, Vasilakos AV. Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. *IEEE Trans Ind Inform*. 2020;16(11):7081-7093.
16. Aujla GS, Chaudhary R, Kumar N, Das AK, Rodrigues JJPC. SecSVA: secure storage, verification, and auditing of big data in the cloud environment. *IEEE Commun Mag*. 2018;56(1):78-85.
17. Atoui R, *The Importance of Security by Design for IoT Devices*. Cleveland: IIoT World; 2018. https://iiot-world.com/ics-security/cybersecurity/the-importance-of-security-by-design-for-iot-devices/
18. Yao X, Farha F, Li R, Psychoula I, Chen L, Ning H. Security and privacy issues of physical objects in the IoT: challenges and opportunities. *Digital Commun Netw*. 2021;7(3):373-384.
19. Das AK, Zeadally S, He D. Taxonomy and analysis of security protocols for Internet of Things. *Futur Gener Comput Syst*. 2018;89:110-125.
20. Zeadally S, Das AK, Sklavos N. Cryptographic technologies and protocol standards for Internet of Things. *IoT*. 2021;14:100075.
21. Zheng Y. Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption). *Advances in Cryptology — CRYPTO '97*. Santa Barbara, CA, Berlin, Heidelberg: Springer; 1997:165-179.
22. Libert B, Quisquater JJ. *Efficient Signcryption with Key Privacy from Gap Diffie-Hellman Groups. Public Key Cryptography – PKC*. Vol 2004. Singapore, Berlin Heidelberg: Springer; 2004:187-200.
23. Rivest RL, Shamir A, Adleman LM. A method for obtaining digital signatures and public-key cryptosystems. *Commun ACM*. 1978;21(2):120-126.
24. Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans Inf Theory*. 1985;31(4):469-472.
25. Asif R. Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms. *IoT*. 2021;2(1):71-91.
26. Ullah I, Amin NU, Khan MA, Khattak H, Kumari S. An efficient and provable secure certificate-based combined signature, encryption and signcryption scheme for internet of things (IoT) in mobile health (M-Health) system. *J Med Syst*. 2020;45(1):1-4.
27. Chaudhary R, Jindal A, Aujla GS, Kumar N, Das AK, Saxena N. LSCSH: lattice-based secure cryptosystem for smart healthcare in smart cities environment. *IEEE Commun Mag*. 2018;56(4):24-32.
28. Waters B. Efficient identity-based encryption without random oracles. Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques; 2005:114-127; Springer, New York, NY.
29. Lindner R, Peikert C. *Better Key Sizes (and Attacks) for LWE-Based Encryption. Topics in Cryptology – CT-RSA*. Vol 2011. San Francisco, CA, Berlin Heidelberg: Springer; 2011:319-339.
30. Peikert C, Vaikuntanathan V, Waters B. *A Framework for Efficient and Composable Oblivious Transfer. Advances in Cryptology – CRYPTO*. Vol 2008. Santa Barbara, CA, Berlin Heidelberg: Springer; 2008:554-571.
31. Regev O. On lattices, learning with errors, random linear codes, and cryptography. *J ACM (JACM)*. 2009;56(6):34.
32. Boyen X. Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more. Proceedings of the 13th International Conference on Practice and Theory in Public Key Cryptography; 2010:499-517; Paris, France, Springer-Verlag.
33. Boyen X, Li Q. Towards tightly secure lattice short signature and id-based encryption. Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security; 2016:404-434; Springer, New York, NY.
34. Cash D, Hofheinz D, Kiltz E, Peikert C. Bonsai trees, or how to delegate a lattice basis. Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques; 2010:523-552; Springer, New York, NY.
35. Ducas L, Micciancio D. Improved short lattice signatures in the standard model. Proceedings of the Annual Cryptology Conference; 2014:335-352; Springer, New York, NY.
36. Lyubashevsky V, Micciancio D. Asymptotically efficient lattice-based digital signatures. Proceedings of the Theory of Cryptography Conference; 2008:37-54; Springer, New York, NY.
37. Lyubashevsky V, Micciancio D. Asymptotically efficient lattice-based digital signatures. *J Cryptol*. 2018;31(3):774-797.

38. Rückert M. Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles. Proceedings of the International Workshop on Post-Quantum Cryptography; 2010:182-200; Springer, New York, NY.
39. Zhang J, Chen Y, Zhang Z. Programmable hash functions from lattices: short signatures and IBEs with small key sizes. Proceedings of the Annual International Cryptology Conference; 2016:303-332; Springer, New York, NY.
40. Peikert C. Public-key cryptosystems from the worst-case shortest vector problem. Proceedings of the 41st Annual ACM Symposium on Theory of Computing; 2009:333-342; ACM, New York, NY.
41. Sun Y, Zheng W. An identity-based ring signcryption scheme in ideal lattice. *J Netw Intell*. 2018;3(3):152-161.
42. Yan J, Wang L, Li M, Ahmad H, Yue J, Yao W. Attribute-based signcryption from lattices in the standard model. *IEEE Access*. 2019;7:56039-56050.
43. Yang X, Cao H, Li W, Xuan H. Improved lattice-based signcryption in the standard model. *IEEE Access*. 2019;7:155552-155562.
44. Yu H, Bai L. Post-quantum blind signcryption scheme from lattice. *Front Inf Technol Electron Eng*. 2021;22(6):891-901.
45. Yu H, Bai L, Hao M, Wang N. Certificateless signcryption scheme from lattice. *IEEE Syst J*. 2021;15(2):2687-2695.
46. Hou Y, Huang X, Chen Y, Kumar S, Xiong H. Heterogeneous signcryption scheme supporting equality test from PKI to CLC toward IoT. *Trans Emerg Telecommun Technol*. 2021;32(8):e4190.
47. Khasawneh S, Kadoch M. 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*. 2021;32(8):e4102.
48. Le HQ, Duong DH, Roy PS, Susilo W, Fukushima K, Kiyomoto S. Lattice-based signcryption with equality test in standard model. *Comput Stand Interfaces*. 2021;76:103515.
49. Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. *SIAM J Comput*. 2007;37(1):267-302.
50. Ebeling W. *Lattices and Codes: A Course Partially Based on Lectures by Friedrich Hirzebruch*. Wiesbaden: Springer Fachmedien Wiesbaden; 2013:1-32.
51. Winograd S. On computing the discrete Fourier transform. *Math Comput*. 1978;32(141):175-199.
52. Banaszczyk W. New bounds in some transference theorems in the geometry of numbers. *Math Ann*. 1993;296(4):625-636.
53. Micciancio D, Peikert C. Trapdoors for lattices: Simpler, tighter, faster, smaller. Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques; 2012:700-718; Springer, New York, NY.
54. Dolev D, Yao A. On the security of public key protocols. *IEEE Trans Inf Theory*. 1983;29(2):198-208.
55. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans Comput*. 2002;51(5):541-552.
56. Wazid M, Das AK, Odelu V, Kumar N, Susilo W. Secure remote user authenticated key establishment protocol for smart home environment. *IEEE Trans Depend Secure Comput*. 2020;17(2):391-406.
57. An JH, Dodis Y, Rabin T. On the security of joint signature and encryption. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques; 2002:83-107; Springer, New York, NY.
58. Matsuda T, Matsuura K, Schuldt JC. Efficient constructions of signcryption schemes and signcryption composability. Proceedings of the International Conference on Cryptology in India; 2009:321-342; Springer, New York, NY.
59. Agrawal S, Boneh D, Boyen X. Efficient lattice (H) IBE in the standard model. Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques; 2010. p. 553-572; Springer, New York, NY.
60. Peikert C. An efficient and parallel Gaussian sampler for lattices. Proceedings of the Annual Cryptology Conference; 2010:80-97; Springer, New York, NY.
61. Chiba D, Matsuda T, Schuldt JCN, Matsuura K. Efficient generic constructions of signcryption with insider security in the multi-user setting. Vol. 6715 of Lecture Notes in Computer Science Nerja, Spain: 9th International Conference on Applied Cryptography and Network Security (ACNS'11); 2011:220-237; Springer, New York, NY.
62. Sato S, Shikata J. *Lattice-Based Signcryption Without Random Oracles. Post-Quantum Cryptography*. Cham: Springer International Publishing; 2018:331-351.
63. Gupta DS, Biswas G. Design of lattice-based ElGamal encryption and signature schemes using SIS problem. *Trans Emerg Telecommun Technol*. 2018;29(6):e3255.
64. Dharminder D, Mishra D. Construction of identity based signcryption using learning with rounding. Proceedings of the International Conference on Machine Learning, Image Processing, Network Security and Data Sciences; 2020:612-626; Post-Quantum Cryptography; Springer, New York, NY.
65. Goldreich O, Goldwasser S, Halevi S. Public-key cryptosystems from lattice reduction problems. Proceedings of the Annual International Cryptology Conference; 1997:112-131; Springer, New York, NY.
66. Gagnidze A, Iavich M, Iashvili G. Analysis of post quantum cryptography use in practice. *Bull Georgian Natl Acad Sci*. 2017;11(2):29-36.

How to cite this article: Dharminder D, Kumar U, Das AK, et al. Secure cloud-based data storage scheme using postquantum integer lattices-based signcryption for IoT applications. *Trans Emerging Tel Tech*. 2022;33(9):e4540. doi: 10.1002/ett.4540