IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON EMERGING APPROACHES TO CYBER SECURITY

Received April 25, 2020, accepted May 15, 2020, date of publication May 18, 2020, date of current version June 2, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995443

CASCF: Certificateless Aggregated SignCryption Framework for Internet-of-Things Infrastructure

TAI-HOON KIM[1], (Member, IEEE), GULSHAN KUMAR[2], RAHUL SAHA[2], MAMOUN ALAZAB[3], (Senior Member, IEEE), WILLIAM J. BUCHANAN[4], MRITUNJAY KUMAR RAI[5], G. GEETHA[2], AND REJI THOMAS[6]

[1]School of Economics and Management, Beijing Jiaotong University, Beijing 100044, China
[2]School of Computer Science and Engineering, Lovely Professional University, Phagwara 144411, India
[3]College of Engineering, IT and Environment, Charles Darwin University, Casuarina NT 0810, Australia
[4]BlockPassID Lab, Edinburgh Napier University, Edinburgh EH11 4DY, U.K.
[5]School of Electronics and Electrical Engineering, Lovely Professional University, Phagwara 144411, India
[6]Division of Research and Development, Lovely Professional University, Phagwara 144411, India

Corresponding authors: Rahul Saha (rsahaaot@gmail.com) and Mamoun Alazab (mamoun.alazab@cdu.edu.au)

ABSTRACT The increasing number of devices in the age of Internet-of-Thing (IoT) has arisen a number of problems related to security. Cryptographic processes, more precisely the signatures and the keys, increase and generate an overhead on the network resources with these huge connections. Therefore, in this paper we present a signcryption framework to address the above problems. The solution highlights the use of aggregate signcryption and certificaless approach based on bilinear pairings. The use of signcryption with aggregation and certificateless authentication reduces the time consumption, overhead and complexity. The solution is also able to solve the key staling problems. Experimental results and comparative analysis based on key parameters, memory utilization and bandwidth utilization have been measured. It confirms that the presented work is efficient for IoT infrastructure.

INDEX TERMS Authentication, signature, signcryption, security, IoT, confidentiality.

I. INTRODUCTION

Internet-of-Thing (IoT) is a technology enabler in present world. It derives an ecosystem made up of people, process and technology; with more insights, the infrastructure of IoTs uses web enabled smart devices with embedded systems, cloud storages, underlying internet structure and applications used by the users [1]. The objectives of making life smoother and easier have craved the pathway of IoT in out technology. It is able to shape both the industrial and consumer worlds. The advantages of IoTs have showed potentials in various domains such as healthcare, agriculture, finance, logistics, supply chains, education and many more [2]. With the increasing number of applications and forecasting of increased device connections also posing severe challenges [3]. Security is one of the major concerns among the all [4], [5].

The associate editor coordinating the review of this manuscript and approving it for publication was Muhammad Imran.

Inheriting the security problems of wireless networks, IoT also faces some severe security issues such as: authentication attacks, denial-of-services, camouflages, espionages, routing attacks and others [6]. Authentication attacks take another dimension in IoT where heterogeneous devices are connected to the network. Therefore, the security mechanism should be strict enough to provide sufficient strength to the network without reducing the performance. Such a solution for IoT security has been provided in the present work. In the following subsections discussion is made on some background of the existing security mechanism and technology and relevant security derivations in recent years.

A. BACKGROUND OF SECURITY

Security is defined by a logical interpretation of being free from threats. It is obvious in this present world of internet technology that the attacks are present everywhere and making strategies for gaining access to the network data. Therefore, it is required that any system requires some security parameters to be obtained by using security

tools. In IoT perspectives, the security requirements are as follows [7].

Confidentiality: The data in communication should not be accessed by a third party.

Authentication: The sender and receiver must prove their identity for data access.

Integrity: The data sent by the sender should be received by the receiver without any modification or alteration.

Non-repudiation: The sender or the receiver cannot deny about their responsibility of sending or receiving the data.

Availability: The data should be available always by the authenticated users in the network whenever and wherever required.

Apart from these access control and accountability are also required for IoT to manage the network properly. To accomplish these requirements cryptographic protocols are used rigorously. Hash functions, symmetric/asymmetric key cryptography, digital signatures are used by all the IoT infrastructures [8]. Such cryptographic functionalities make security backbone overall and therefore, such algorithms need to be robust enough. Encryption techniques provide confidentiality, digital signatures provide integrity, authentication and non-repudation. In generic security frameworks, these two techniques are processed separately. However, researches have been conducted to integrate these two in single logical step and thus, signcryption processes come into existence in cryptography [9].

B. SIGNCRYPTION, AGGREGATES AND RECENT DEVELOPMENTS

Signcryption, as single logical step for digital signature and encryption, is able to reduce the computational costs and communication overheads as compared with the traditional signature-then-encryption schemes. Correctness, efficiency, security in terms of forward secrecy, unforgeability are some of the essential features of signcryption [10]. Various signcryption algorithms have been developed in recent years. A standard model of signcryption is shown in [11]. Various hyper elliptic curve based signcryption techniques are researched which prove their efficiency in terms of security [12]. Some other significant use of signcryption in various IoT based infrastructures are also worth mentioning [13]–[20]. To enhance the performance of signcryptions blockchain based signcryption is also derived [21]. With the need of post quantum resistance, lattices are introduced in signcryption [22].

The successful implementation of signcryption for reducing computation and communication overhead in IoTs has been processed forward by aggregating the signatures. Signature aggregation schemes allow multiple signatures generated by multiple public keys for multiple messages to be aggregated into a single signature and verified accordingly [23]. Various aggregate signature schemes are researched in recent times. Significant use of aggregate signatures in vehicular ad hoc networks are observed [24], [25]. Another such scheme for healthcare-based application is researched [26].

Aggregation schemes can be enhanced further by doing aggregations on the overall signcryptions. The objective of providing required security with reduced overhead and computation has led to such developments. An obfuscating aggregate signcryption development for IoT is worth mentioning here [27]. An application specific use of signcryption aggregation is shown in [28] Another recent construction of such aggregation is shown in [29]. The algorithms shown in [27]–[29] are chosen for the comparison with the proposed certificateless scheme. Emphasizing on the last three research works, some problems are identified. Firstly, the algorithms of [27] and [28] are unable to provide a certificateless scheme therefore, having a scope of improvement with certificateless schemes. Secondly, key staling is a problem in all these three algorithms. These identified problems have motivated us to find a signcryption solution for IoT framework.

The rest of the paper is organized as follows. Section II explain the proposed approach/scheme detailing about the preliminaries and phase wise descriptions with algorithms. Section III explains the experimental results, comparative analysis and security validation. Section IV concludes the paper highlighting the major findings of the experiment.

II. PROPOSED CASCF SCHEME

In this section, we explain the problem definition, preliminaries used for the proposed scheme, network model followed by the detailed description of the functions.

A. PROBLEM DEFINITION

In IoTs, the devices are connected over Internet. IoT communication is affected by various security issues. To safeguard the data of IoT devices in communication and to provide the required security services cryptography solutions have become integral part. Hence, the present work shows a solution for the IoTs. It ensures confidentiality, authentication, integrity and non-repudiation services. The solution objectifies the following.

- To reduce the time consumption by using signcryption method
- To reduce the overhead by the cryptographic processes by using aggregate signcryption.
- To reduce the complexity of certificates by using certificateless approach

B. PRELIMINARIES

Let G_1 and G_2 be the cyclic groups of same order q where G_1 is additive group and G_2 is multiplicative group. A bilinear map e: $G_1 \times G_2 \rightarrow G_e$ is a function such that $\forall u \in G_1$ and $\forall v \in G_2$; $a, b \in Z$ it has the following [30]:

$$e(u^a, v^b) = e(u, v)^{ab} \tag{1}$$

These maps are also called as bilinear pairings as they associate the elements of G_1 and G_2 to the elements of G_e. Assuming g_1 and g_2 be the group generators of G_1 and G_2 respectively, the admissible bilinear map is admissible

if $e(g_1, g_2)$ is able to generate the elements of G_e and e is efficiently computable. Such admissible mapping should also possess the property of non-degeneracy and computability as defined below.

1) NON-DEGENERACY

A bilinear map $e : G_1 \times G_2 \rightarrow G_e$ is non-degenerate if it satisfies the conditions:

1) $Ker(e) = 0$; $e(u, v) = 0 \; \forall \; u \in G_1$ implies $v = 0$ and vice versa
2) $\dim G_1 = \dim G_2$

2) COMPUTABILITY

There exists an efficient algorithm to compute $e(g_1, g_2)$, for $g_1 \in G_1$ and $g_2 \in G_2$.

3) COMPUTATIONAL DIFFIE-HELLMAN (CDH) PROBLEM

For a cyclic group G of order q, CDH states that: For a given (g, g^a, g^b) with any random generator $g \in G$ and random $a, b \in \mathbb{Z}_q$, it is computationally intractable to compute g^{ab}.

4) DECISIONAL BILINEAR DIFFIE-HELLMAN (DBDH) PROBLEM

Let G be cyclic group of order q and with generator g. For a given g^a and g^b with uniformly and independently chosen $a, b \in \mathbb{Z}_q$, it is to be calculated g^{ab} is random in G.

5) GAP DIFFIE-HELLMAN (GDH) PROBLEM

Let G be cyclic group of order q and with generator g. Given, $(g^a, g^b) \in G_1$ with unknown $a, b \in \mathbb{Z}_q$, then compute $g^{ab} \in G_1$ with the help of DBDH oracle.

C. SYSTEM MODEL

In the proposed scheme, two Raspberry Pi, three minicomputers, five mobile phones and one desktop are considered to develop the IoT model. One Raspberry Pi 3 is made as client model and it is connected with DHT-11 and MQ-135 sensors to collect the environmental data (experimental room). This data is signed and forwarded to another Raspberry Pi 3 model which acts as a server for the sensor network capability. Mobile phones are working as end devices. The desktop is working as a server where the sensor network server is also connected and the verification of the message is carried out here. Table-1 summarizes some important notations and symbols used in the proposed work and Figure 1 shows the system model carried out.

D. FUNCTIONAL DESCRIPTION

The proposed scheme follows the work shown in [29]. The scheme involves the prime entities: Key Generation Center (KGC), a sender u_s and receiver u_r, an aggregating set a of n users and Aggregate Signcryption Generator (ASG). KGC is responsible for generating keys. Sender and receiver are the parts of communicating nodes where $u_s, u_r \in a$. ASG creates

TABLE 1. List of important notations and symbols.

Symbol	Description
$\mathbb{Z}_q$	Finite field of integer elements
G_1, G_2	Cyclic groups
$\mathbb{Z}_q*$	Group of integers under multiplication
e	Bilinear map
g_1,g_2,	Generators of groups
msk	Master secret key
H_1, H_2	Hash functions
$param$	Public parameters
ID_{u_i}	Identity of sender (signers)
mpk	Master public key
$t, \delta t$	Time stamp with system error or delay
$\mathcal{M}$	Message
$\triangle$	State information of a system
$\{Pu_{u_i}, Pr_{u_i}\}$	Public-private key pair of senders
ID_{u_r}	Identity of receiver
$\{Pu_{u_r}, Pr_{u_r}\}$	Public-private key pair of receiver
$\overline{C}$	Aggregate signcrypted ciphertext

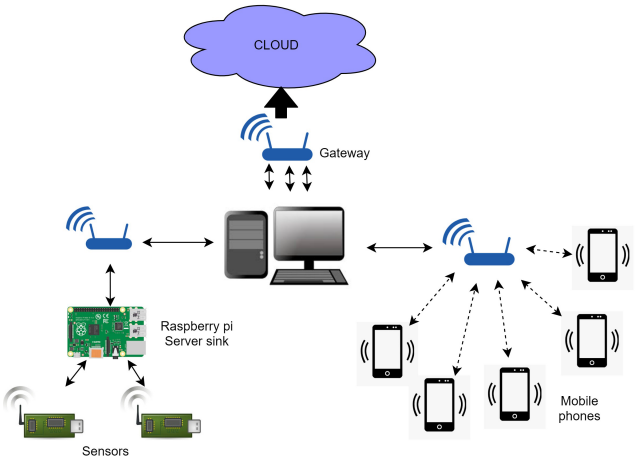

FIGURE 1. System Model for the proposed scheme showing the connection between end devices (sensor, mobiles) via router and gateway to internet.

the final signcryption and validates the incoming signcryptions. The modifications in the existing algorithm [29] deals with the changes in the key generation process and master key creation. Subsequently, we obtain an improved framework for IoT signcryption. However, we have followed the same stages of execution as shown in the above mentioned process. The proposed framework modules are shown in Figure 2. The functioning of the scheme is sub categorized as: Setup, Partial private key extract, User key generate, Signcrypt, Aggregate, Aggregate verify and Aggregate unsigncrypt. Some of the assumptions made for the scheme are:

- KGC is secure and trusted.
- Aggregation of signcryptions are done by a special module ASG linking to a set of users separately.
- Aggregate unsigncryption is done by the receiver.

The detailed functioning of the scheme in the IoT framework is shown below.

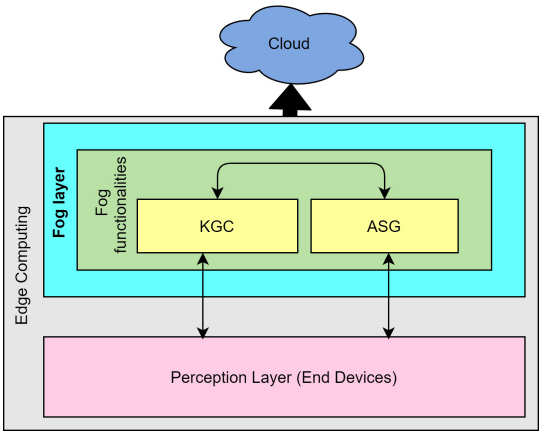

FIGURE 2. The framework for the proposed scheme showing the viability of KGC and ASG in fog layer for better computation aspect.

1) SETUP

This function is processed by KGC. It inputs a random point on an elliptic curve E over a finite field $\mathbb{Z}_q$ with an order $o = q^k$ where, random prime number q and k is an integer, and the other two integer elements a, b such that: $y^2 = x^3 + ax + b, (a, b) < q$. It then stores the master secret key (msk) with itself and publishes system parameters (param) as shown in Algorithm 1.

Algorithm 1 Set Up

1: **Input:** $y^2 = x^3 + ax + b$
2: **Output:** msk, $param$
3: Obtain a cyclic additive group G_1 from $\mathbb{Z}_q$ of prime order q with generator g_1
4: Obtain the non-zero elements of $\mathbb{Z}_q$ to generate the cyclic multiplicative group G_2. The order of this group should be q and generator is g_2.
5: e: $G_1 \times G_1 \rightarrow G_2$
6: Select a random number $r \in \mathbb{Z}_q^* \rightarrow msk, G_1 \subseteq \mathbb{Z}_q^*$
7: Master public key $(mpk) = r.g_1.g_2$
8: Initialize the hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$ and $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^k$
9: Store r and publish $param : \{G_1, G_2, e, g_1, g_2, mpk, H_1, H_2\}$

2) PARTIAL PRIVATE KEY GENERATION

Once the system parameters are set up, KGC initializes the process of key generation for the users registering for the network. KGC takes input $param$,msk, the identity of the user ID_{u_i} registering for the network and timestamp t of 128 bits. Timestamp helps for preventing stale or revocation of keys. Note that, the proposed scheme uses ICMetrics to generate the identity of the users and converted them into 128-bit binary representation: $ID_{u_i} = \{0, 1\}^{128}$ [31]. This identity is generated by an individual user. KGC returns a partial private key $\widehat{Pr_{u_i}}$ for the user u_i through an assumed secure channel. The process is shown in Algorithm-2.

Algorithm 2 Partial Private Key Generation

1: **Input:** $param$, msk, ID_{u_i}
2: **Output:** $\widehat{Pr_{u_i}}$
3: Compute $Q_i = H_1(ID_{u_i})$
4: $\widehat{Pr_{u_i}} = H_1[(msk.Q_i)||(t + \delta t)]$
5: Return $\widehat{Pr_{u_i}}$

3) USER KEY PAIR GENERATION

After getting the partial private key from KGC, each user executes a process to generate public-private key pair. The process inputs $param$ and user's identity ID_{u_i}. It outputs a private key Pr_{u_i} and a corresponding public key Pu_{u_i} for the user u_i. The private key is kept secret with the user and the public key is shared without any certification. The process is summarized in Algorithm 3. Signcrypt: Whenever

Algorithm 3 User Key Pair Generation

1: **Input:** $param$, $\widehat{Pr_{u_i}}$
2: **Output:** $\{\widehat{Pu_{u_i}}, \widehat{Pr_{u_i}}\}$
3: Choose a random number $r_u \in \mathbb{Z}_q^*$
4: $Pr_{u_i} = \widehat{Pr_{u_i}}.r_u$
5: $Pu_{u_i} = r_u.g_1.g_2$
6: return $\{Pr_{u_i}, Pu_{u_i}\}$

a registered user u_i wants to communicate, it executes the process of signcryption. The process takes inputs of $param$, some state information $\triangle$, message $\mathcal{M}$, identity of the its own ID_{u_i}, public key Pu_{u_i}, private key Pr_{u_i}, the identity of the receiver ID_{u_r} and its corresponding public key Pu_{u_r}. The process outputs a signcrypted message $\mathcal{C}$. The process is shown in Algorithm 4.

Algorithm 4 Signcryption

1: **Input:** $param$, $\triangle$, $\mathcal{M}$, ID_{u_i}, Pu_{u_i}, Pr_{u_i}, ID_{u_r}, Pu_{u_r}
2: **Output:** $\mathcal{C}$
3: Choose a random number $r_i \in \mathbb{Z}_q^*$
4: Compute $U_i = r_2.g_1.g_2$
5: Compute $Q_{u_r} = H_1(ID_{u_r}||t)$
6: Compute $T_i = e(mpk, Q_{u_r})^{r_2}$
7: Compute $h_i = H_2(U_i, T_i, r_i, Pu_{u_r}, \triangle)$
8: Compute $V_i = h_i \oplus \mathcal{M}$
9: Compute $H_i = H_1(U_i, V_i, ID_{u_i}, Pu_{u_i}, ID_{u_r}, Pu_{u_r})$
10: Compute $H_\triangle = H_1(\triangle)$
11: Compute $W_i = r_i H_i + r_u H_\triangle$
12: return $\mathcal{C} : \{U_i, V_i, W_i\}$

4) AGGREGATE

Aggregate Signcryption Generator (ASG) follows the process of aggregation. It inputs an aggregating set a of n users, some

state information $\triangle$, the identity of senders ID_{u_i} and their public keys Pu_{u_i}, signcrypted ciphertexts $\mathcal{C}_i$. It outputs an aggregate ciphertext $\overline{\mathcal{C}}$. The process is shown in Algorithm 5.

Algorithm 5 Aggregation

1: **Input:** $a, \triangle, ID_{u_i}, Pu_{u_i}, \mathcal{C}_i, ID_{u_r}$
2: **Output:** $\overline{\mathcal{C}}$
3: $\overline{W} = \sum_{i=1}^{n} W_i, i = 1, 2, .., n \in a$
4: Combine U_i
5: Combine V_i
6: $\overline{\mathcal{C}} = \{U_1, .., U_n, V_1, .., V_n, \overline{W}\}$
7: Transmit $\overline{\mathcal{C}}$

5) AGGREGATE VERIFY

Any receiver who is receiving $\overline{\mathcal{C}}$ is able to verify the aggregated signcryption. For this, the inputs the receiver needs appropriate public keys of the receivers for which that $\overline{\mathcal{C}}$ is generated. The adversaries are unable to verify because the lack of key components availability. It compares the outputs and process further to unsigncryption if the comparison is valid else connection is aborted. The process is shown in Algorithm 6.

Algorithm 6 Aggregate Verification

1: **Input:** $a, ID_{u_i}, Pu_{u_i}, ID_{u_r}, Pu_{u_r}, \triangle, \overline{\mathcal{C}}$
2: **Output:** Accept or Discard
3: For $i = 1$ to n do
Compute $H_i = H_1(U_i, V_i, ID_{u_i}, Pu_{u_i}, ID_{u_r}, Pu_{u_r})$ End do
4: Compute $H'_{\triangle} = H_1(\triangle)$
5: Compute $I_1 = e(\overline{W}, Pu_{u_i})$
6: Compute
$I_2 = e(\sum_{i=1}^{n} Q_i, mpk) \prod_{i=1}^{n} e(H_i, U_i) e(H'_{\triangle}, \sum_{i=1}^{n} Pu_{u_i})$
7: if $(I_1 = I_2)$
then accept $\overline{\mathcal{C}}$
else
discard and abort
8: return NULL

6) AGGREGATE UNSIGNCRYPT

Once the verification is done for $\overline{\mathcal{C}}$, the receiver executes the unsigncryption process. The receiver uses $\overline{\mathcal{C}}$, the state information $\triangle$, identity ID_{u_r} and its public-private key pair $\{Pu_{u_r}, Pr_{u_r}\}$, all the senders' identities ID_{u_i} and their corresponding public keys Pu_{u_i} and outputs n number of plaintexts. The unsigncryption process is shown in Algorithm 7.

The overall scheme is summarized in Figure 3. It shows the connection between KGC, users (sender and receiver) and ASG. The numbers in the figure represents the sequence of operation in the presented work.

Algorithm 7 Aggregate Unsigncryption

1: **Input:** : $\overline{\mathcal{C}}, \triangle, ID_{u_r}, Pu_{u_r}, Pr_{u_r}, ID_{u_i}, Pu_{u_i}$
2: **Output:** $\{\mathcal{M}_1, \mathcal{M}_2, .., \mathcal{M}_n\}$
3: For $i = 1$ to n do
4: Compute $T_i = e(U_i, \widehat{Pr_{u_r}})$
5: Compute $h_i = H_2(U_i, T_i, r_{u_r} U_i, ID_{u_r}, Pr_{u_r}, \triangle)$
6: Compute $\mathcal{M}_i = V_i \oplus h_i$
7: return $\{\mathcal{M}_1, \mathcal{M}_2, .., \mathcal{M}_n\}$
8: End do

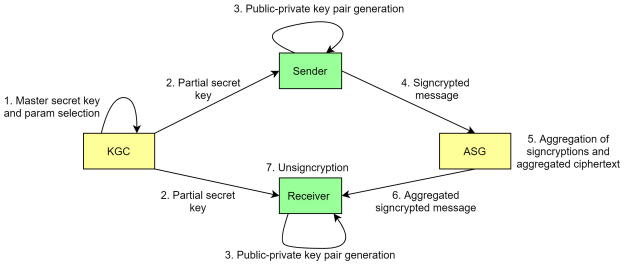

FIGURE 3. Sequence of operations among the framework modules: sender, receiver, KGC and ASG.

III. EXPERIMENTAL RESULTS

In this section, performance of the proposed scheme has been measured. The scheme is also compared with the existing schemes shown in [27][28] and [29]. Performance metrics, comparative analysis and security analysis are shown in the following subsections.

A. PERFORMANCE METRICS

Performance of the schemes are measured based on the following metrics.

1) THROUGHPUT

Throughput is defined as the number of messages successfully delivered per unit time. In this case, we have assumed that, the network throughput is fixed and measurement is done only for the message signcryption functions. It has been measured in bits/seconds.

2) DELAY

It is defined as the round-trip time in the network. Generally, delay is comprised of processing delay, queuing delay,transmission delay and propagation delay. Assuming that all the other delays are static, only processing delay has been measured and compared.

3) ENERGY CONSUMPTION

IoT is comprised of devices which are resource constrained. Therefore, the schemes developed for IoT security should provide less energy consumption. This metric is measured with residual energy parameter and represented in percentage.

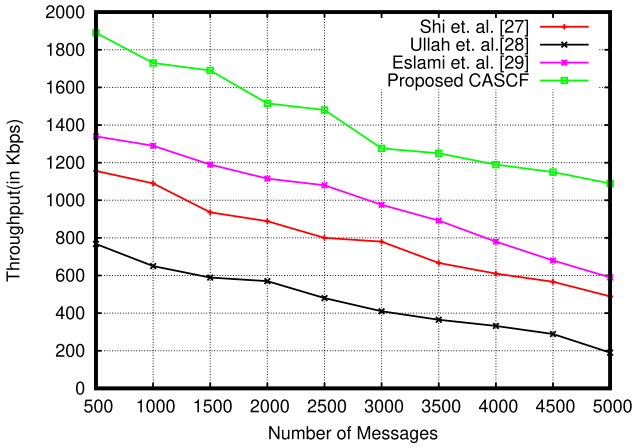

FIGURE 4. Throughput comparison among CASCF and other approaches.

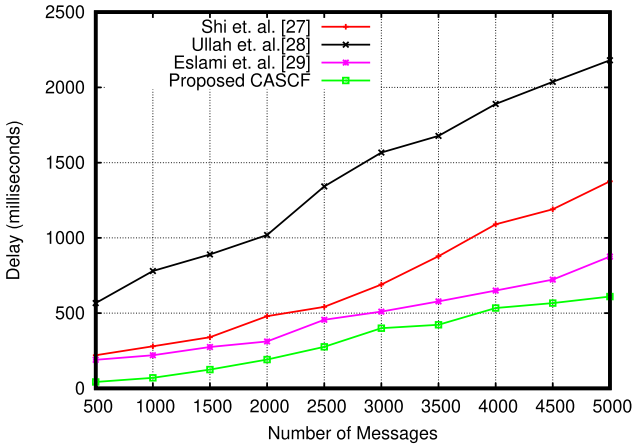

FIGURE 5. Delay comparison among CASCF and other approaches.

4) MEMORY CONSUMPTION

This metric is measured in terms of kilobytes required for overall storage of keys, intermediate values and certificates (wherever the comparison approaches use certificates)

5) COMPLEXITY

The complexity of the schemes is measured in their individual operation complexity basis. The less complex algorithms are more suitable for IoT framework.

B. EXPERIMENTAL RESULTS

For the experimentation, we have used overall 5000 messages in the network setup as shown in Figure-1. Memory in KGC is maintained with 8GB RAM configuration and 1GB ROM separately only for aggregate signcryption process. Message size has been varied from 10 KB to 2MB with average size of 1000KB. The comparative result is shown in Figure-4. The result shows that with the increasing number of messages (number of bits), the performance of the schemes degrades. However, in comparison the degradation in the proposed scheme is less. It shows that CASCF is able to produce 28.3%, 43.6%, and 17.9% better throughput as compared to the schemes in [27],[28] and [29] respectively. The reason behind this throughput behaviour of CASCF is the use of certificate-less approach and reducing the number steps involved in the processing as shown in the exiting schemes. In the next experiment we have measured the processing delay of the schemes. The size of the message does not affect the cryptographic schemes. So, the delay is the overall processing of the signcrypted message, aggregation and receiver's aggregate unsigncryption. This has been measured by subtracting the queuing delay, transmission delay and propagation delay from the roundtrip time where those delays are assumed to be constant and the transmission channel is congestion free. The delay output is shown in Figure-5. Figure-5 shows that CASCF possess the reduced delay as compared to other schemes. The certificateless signcryption creates an effect on this as the delays for creating certificates and verifying certificate are avoided here. The approach in [29] uses similar

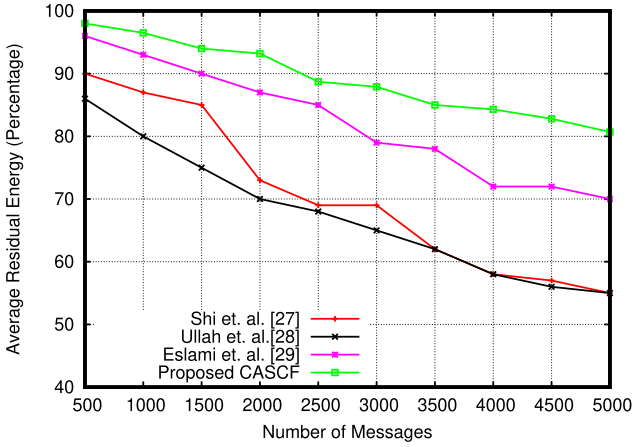

FIGURE 6. Residual energy comparison among CASCF and other approaches.

kind of certificateless approach and therefore having similar kind of output. However, the reduction steps in CASCF produces less delay. Overall, CASCF is able to obtain 25% less delay as compared to other algorithms.

Energy is another parameter which is very much important in IoT framework. The measurement has been calculated as the average residual energy of all the end devices cumulatively. The result is shown in Figure-6. The energy comparison shown in the Figure-6 depicts that the algorithms of [27] and [28] have an average energy consumption 45% of the total energy; however, at the beginning energy consumption is more for [28] and after 3000 messages [27] degrades more rapidly in residual energy. On the other hand, CASCF and algorithm in [29] are better than the other two algorithms due to the avoidance of certificates. Further, CASCF is more efficient by changing the key generation mechanism by reducing the energy consumption by 48%, 49.7% and 15.6% as compared to [27]–[29] respectively. Memories are important for any cryptographic process. With the increasing number of messages, it is obvious that individual memory consumption increases but in comparison results show that CASCF is more advantageous in term of memory as the consuming memory amount is less in the work. The other three algorithms show

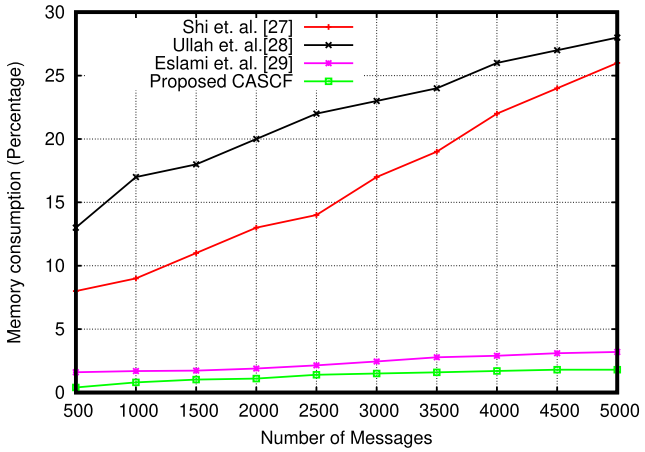

FIGURE 7. Residual energy comparison among CASCF and other approaches.

TABLE 2. Parameters for measuring complexity.

Parameter	Description
T_G^+	Time for scalar addition for cyclic group
T_G^*	Time for scalar multiplication for cyclic group
T_p	Time for pairing
T_H	Time for hash
T_{op}	Time for bitwise operator (Assumed to be constant)

memory usage of 25%, 36% and 18% more than the CASCF. Therefore, in view of memory utilization CASCF proves its efficiency. The comparison result is shown in Figure-7.

The measurement of the complexity has been done in two parts: receiver side computational complexity and communication complexity. We have followed the similar parameters and notation for this metric as mentioned in [29]. The notations are summarized in Table-2 and the comparison is shown in Table-3.

Table-3 shows that the communication complexity is less as compared to the schemes describe in [27] and [28]; however, [29] and CASCF show the similar kind of communication complexity. On the other hand, for sender side complexity is more for CASCF but receiver side computation complexity and aggregator computation complexity are the least among the all. As an overall, CASCF is efficient in terms of complexity of computation and communication cost.

C. SECURITY VALIDATION

The security analysis of CASCF with IoT infrastructure is explained here. The analysis consists of discussion about the Diffie-Hellman problems and other security features as required. CASCF uses the same attacker adversary model with challenge response game to validate the Diffie-Hellman assumptions [29]. However, we have provided an intuitive discussion to validate the work. As before the aggregation, the base is signcryption, we have not included any explicit discussion of signcryption security as it is mentioned in [32].

1) DIFFIE-HELLMAN PROBLEMS

We have analysed a reduction for CDH as if g^{an} is solvable from a given g^a, then CDH problem is solvable. Let $\mathcal{A}$ be an adversary that uses g^a for random a and outputs g^{a2} with a probability P. A construction is made as $\mathcal{A}'$who receives $u = g^a$ and $v = g^b$ and works as follows. $\mathcal{A}'$ runs A for n times on input u, v and $u.v$. If $\mathcal{A}$ returns correct answer every time then $\mathcal{A}'$ have $\mathcal{A} = g^{an}$, $B = g^{b^n}$ and $C = g^{(a+b)^n}$. Thus, $\mathcal{A}'$ gives output as $n\sqrt{\frac{C}{\mathcal{A}.B}}$ where, $n\sqrt{}$ is the prime modulo q. The probability of this calculation if it is correct for a random generator g and unknown a, b becomes: P^n,where $P = \frac{\prod_{(i=1)}^{n} P(g)}{\sum_{(i=1)}^{n} \prod a. \prod b} \rightarrow 0$. It validates that the proposed scheme is intractable under CDH problem.

Similarly, for DBDH, we first try to calculate the advantage for the adversary $\mathcal{A}$. It takes a quadruple input as: (g, g^a, g^b, g^{ab}) and attempts to get the advantage of getting a random g^{abc} in G. If a, b are chosen uniformly with a random c in G, the correlation to make g^{abc} will be difficult. The probability of such advantage for $\mathcal{A}$ is given as:

$$Adv(\mathcal{A}) = |P(Adv(g, g^a, g^b, g^{ab}) - P(Adv(g, g^a, g^b, g^c)|; \\ g \leftarrow e : \{G^n \times G^n\}; \{a, b, c\} \leftarrow \mathbb{Z}_q^* \quad (2)$$

For, the polynomial time-based systems like the proposed scheme, the advantage becomes zero. This infers that the CASCF is unable to solve DBDH, and hence it is safe. Now, extending the CDH problem with a random oracle, the GDH validation is conducted as mentioned in [29]. For an attacker Å, it uses the proposed scheme with a master public key mpk with a generator g^a and a random number $l \leqslant q_{H_1}$, where H_1 is the oracle and q is the maximum number of iterations in oracle and receives a GDH tuple (g, g^a, g^b) in G_1 from an adversary $\mathcal{A}$. Å sends $A : G_1, G_2, e, g, mpk$. As the queries allowed for Å is only H_1 therefore, for H_2 queries it checks if DBDH is true and checks if $e(U, Pu) = e(U, g)$; if it is true and the tuple exist with a value of h, Å returns it or chooses a random h, updates itself and sends to $\mathcal{A}$. $\mathcal{A}$ then sends identities of the uses, public keys, and the messages, a forged ciphertext $\mathcal{C}^*$ and some state information. Each identity to be chosen from the set of n identities having the same probability. Moreover, the aggregate verification process should also return true on the forged aggregated signcrypted message which leads for Å to calculate g^{ab}. This ensures that the proposed scheme is secure against GDH assumption.

2) OTHER SECURITY REQUIREMENTS

a: CORRECTNESS

The following equality proves the verifiable correctness of the proposed work.

$$e(\overline{W}, g) \\ = e(\sum_{i=1}^{n} W_i, g) \\ = e\Big(\sum_{i=1}^{n} (\widehat{Pr_{u_i}} + r_i H_i + r_u H_\triangle), g\Big)$$

TABLE 3. Comparison of complexity.

	Sender side computation complexity	Receiver side computation complexity	Aggregation computation complexity	Communication complexity
Shi et. al. [27]	$6T_G^* + 4T_H + 2T_p + T_G^+ + T_{op}$	$(2n+1)T_H T_G^+ + (n+3) T_p T_H + nT_G^* T_{op}$	$n(3T_H + T_p + 2T_G^*)$	$(n+1)\|G_1\|.(n+1)\|G_2\|$
Ullah et. al. [28]	$8T_G^* + 4T_H + 3T_p + 2T_G^+ + T_{op}$	$(4n+1)T_H T_G^+ + (2n+3) T_p T_H + nT_G^* T_{op}$	$3(n+1)T_H + (n+1)T_p + 2T_G^*)$	$(n+1)^2\|G_1\|.(n+1)^2\|G_2\|$
Eslami et. al. [29]	$5T_G^* + 3T_H + T_p + T_G^+ + T_o p$	$(2n+1)T_H + (2n+3)T_p + n(T_G^* + T_{op})$	$(n+2)T_H + 4T_p$	$(n+1)\|G_1\|$
Proposed CASCF	$6T_G^* + 4T_H + T_p + T_G^+ + T_{op}$	$n(T_p + T_H + T_G^* + T_{op})$	$(n+1)T_H + 3T_p$	$(n+1)\|G_1\|$
n is the number of the message. The complexity is calculated on the technical specification of the system as: 4GB RAM, 16GB storage based mobile devices including laptop and mobile phone and then taken as average.				

$$= e\Big(\big(\sum_{i=1}^{n} H_1(msk.Q_i) \uparrow Extract(t+\delta t) + r_i H_i + r_u H_\triangle\big), g\Big)$$
$$= e\Big(\sum_{i=1}^{n} Q_i, mpk\Big) \prod_{i=1}^{n} e(H_i, U_i) e(H'_\triangle, \sum_{i=1}^{n} Pu_{u_i}) \quad (3)$$

b: UNFORGEABILITY

The proposed CASCF in signcryption mode is unforgeable against adaptive chosen message attacks. Two cases are considered here. A challenge-response game is initiated as mentioned in [33]. A challenger $\mathfrak{C}$ generates the public parameters *param* and *msk* by executing the setup algorithm. It sends *param* to an adversary $\mathcal{A}'$. $\mathcal{A}'$ then performs series of queries and outputs $(ID'_{u_s}, ID'_{u_r}, \delta')$. In this, it is to be assured that $\mathcal{A}'$ has not extracted the partial private key as it uses a random number and timestamp with hash. Another assumption is that for the chosen message, $\mathcal{A}'$ is unable to use set keys or private key queries on ID'_{u_s}. As a result, The output of aggregation verification is false and $\mathcal{A}'$ is unable to proceed further. In an extensive scenario, if $\mathcal{A}'$ is able to input a forged ciphertext $\overline{\mathcal{C}}$ in the aggregation, it cannot retract the key pairs as the challenger $\mathfrak{C}$ wins the game by prohibiting $\mathcal{A}'$ from getting the partial private key or replacing the public keys.

c: INTRACTABILITY

Intractability of the proposed CASCF is discussed through CDH and GDH assumptions.

d: FORWARD SECRECY

CASCF ensures the property of forward secrecy. In our scheme, if the master secret key *msk* of a KGC is compromised, the attacker is able to get the partial secret key but unable to obtain the private key of the user as it is generated with *msk* and a random number. This random number is user specific and secret too. Therefore, to generate the private key, the attacker needs the random number r_u, which is private to the user only. Thus, generation of private key is infeasible. Furthermore, timestamp is added to generate the keys which preserves the freshness of the secret key. The above discussion clearly says that the proposed scheme is secure.

IV. CONCLUSION

In the present work, a solution for IoT security has been shown. It uses the aggregate signcryption to enhance the network performance. Bilinear map is used in scheme. Moreover, timestamp is used in key generation process to obtain the freshness of the keys. The framework uses a set of nodes as aggregate signature generator. Most viably, it is to be used fog layer of IoT infrastructure. Performance is measured based on throughput, delay, energy consumption, memory consumption. Results are compared with some existing schemes. The complexities of the schemes are compared. Comparative analysis infers that the proposed scheme is efficient for IoTs. Moreover, security analysis confirms the accomplishment of security objectives of the work. In the sender side, the computation complexity is more which is considered as a future objective.

ACKNOWLEDGMENT

(Tai-Hoon Kim and Gulshan Kumar contributed equally to this work.)

REFERENCES

[1] J. Y. Khan and M. R. Yuce, *Internet of Things (IoT): Systems and Applications*, 1st ed. Singapore: Jenny Stanford, 2019.
[2] E. D. Matos, R. T. Tiburski, C. R. Moratelli, S. J. Filho, L. A. Amaral, G. Ramachandran, B. Krishnamachari, and F. Hessel, "Context information sharing for the Internet of Things: A survey," *Comput. Netw.*, vol. 166, Jan. 2020, Art. no. 106988.
[3] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Comput. Netw.*, vol. 144, pp. 17–39, Oct. 2018.
[4] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, "A survey on Internet of Things security: Requirements, challenges, and solutions," *Internet of Things*, Nov. 2019, Art. no. 100129, doi: 10.1016/j.iot.2019.100129.
[5] S. Rizvi, R. Orr, A. Cox, P. Ashokkumar, and M. R. Rizvi, "Identifying the attack surface for IoT network," *Internet Things*, vol. 9, Mar. 2020, Art. no. 100162.
[6] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, "Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2702–2733, 3rd Quart., 2019.
[7] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019.
[8] S. Zeadally, A. K. Das, and N. Sklavos, "Cryptographic technologies and protocol standards for Internet of Things," *Internet of Things*, Jun. 2019, Art. no. 100075, doi: 10.1016/j.iot.2019.100075.
[9] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) ≪ cost(signature) + cost(encryption)," *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 1294. New York, NY, USA: Springer-Verlag, 1997, pp. 165–179.
[10] Y. Yuan, "Security analysis of an enhanced certificateless signcryption in the standard model," *Wireless Pers. Commun.*, vol. 112, no. 1, pp. 387–394, May 2020.

[11] D. Dharminder and D. Mishra, "Understanding signcryption security in standard model," *Secur. Privacy*, vol. 3, no. 3, pp. 1–15, May 2020.
[12] S. Ullah, X.-Y. Li, and L. Zhang, "A review of signcryption schemes based on hyper elliptic curve," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Aug. 2017, pp. 51–58.
[13] S. Belguith, N. Kaaniche, M. Hammoudeh, and T. Dargahi, "PROUD: Verifiable privacy-preserving outsourced attribute based SignCryption supporting access policy update for cloud assisted IoT applications," *Future Gener. Comput. Syst.*, Nov. 2019, doi: 10.1016/j.future.2019.11.012.
[14] A. Karati, C.-I. Fan, and R.-H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 10431–10440, Dec. 2019.
[15] J. Qiu, K. Fan, K. Zhang, Q. Pan, H. Li, and Y. Yang, "An efficient multi-message and multi-receiver signcryption scheme for heterogeneous smart mobile IoT," *IEEE Access*, vol. 7, pp. 180205–180217, 2019.
[16] V.-H. Hoang, E. Lehtihet, and Y. Ghamri-Doudane, "Password-based authenticated key exchange based on signcryption for the Internet of Things," in *Proc. Wireless Days (WD)*, Manchester, U.K., Apr. 2019, pp. 1–8.
[17] E. Ahene, Z. Qin, A. K. Adusei, and F. Li, "Efficient signcryption with proxy re-encryption and its application in smart grid," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9722–9737, Dec. 2019.
[18] C. Peng, J. Chen, M. S. Obaidat, P. Vijayakumar, and D. He, "Efficient and provably secure multi-receiver signcryption scheme for multicast communication in edge computing," *IEEE Internet Things J.*, early access, Oct. 25, 2019, doi: 10.1109/JIOT.2019.2949708.
[19] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K.-K.-R. Choo, and Y. Park, "Certificateless-Signcryption-Based three-factor user access control scheme for IoT environment," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3184–3197, Apr. 2020.
[20] X. Fan, T. Wu, Q. Zheng, Y. Chen, M. Alam, and X. Xiao, "HSE-voting: A secure high-efficiency electronic voting scheme based on homomorphic signcryption," *Future Gener. Comput. Syst.*, Oct. 2019, doi: 10.1016/j.future.2019.10.016.
[21] N. Eltayieb, R. Elhabob, A. Hassan, and F. Li, "A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud," *J. Syst. Archit.*, vol. 102, Jan. 2020, Art. no. 101653.
[22] G. Kumar, R. Saha, M. K. Rai, R. Thomas, and T.-H. Kim, "A lattice signcrypted secured localization in wireless sensor networks," *IEEE Syst. J.*, early access, Jan. 20, 2020, doi: 10.1109/JSYST.2019.2961476.
[23] D. Boneh, "Aggregate Signatures," in *Encyclopedia of Cryptography and Security*, S. Jajodia and H. C. A. Van Tilborg, Eds. Boston, MA, USA: Springer, 2011.
[24] I. A. Kamil and S. O. Ogundoyin, "An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks," *J. Inf. Secur. Appl.*, vol. 44, pp. 184–200, Feb. 2019.
[25] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Inf. Sci.*, vols. 451–452, pp. 1–15, Jul. 2018.
[26] P. Kumar, S. Kumari, V. Sharma, A. K. Sangaiah, J. Wei, and X. Li, "A certificateless aggregate signature scheme for healthcare wireless sensor network," *Sustain. Comput., Inform. Syst.*, vol. 18, pp. 80–89, Jun. 2018.
[27] Y. Shi, J. Han, X. Wang, J. Gao, and H. Fan, "An obfuscatable aggregatable signcryption scheme for unattended devices in IoT systems," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 1067–1081, Aug. 2017.
[28] S. Ullah, F. Russo, L. Marcenaro, and B. Rinner, "Aggregate-signcryption for securing smart camera IoT applications," in *Proc. Global Internet Things Summit (GIoTS)*, Bilbao, Spain, Jun. 2018, pp. 1–6.
[29] Z. Eslami and N. Pakniat, "Certificateless aggregate signcryption: Security model and a concrete construction secure in the random oracle model," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 26, no. 3, pp. 276–286, Sep. 2014.
[30] I. Ali, T. Lawrence, and F. Li, "An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs," *J. Syst. Archit.*, vol. 103, Feb. 2020, Art. no. 101692.
[31] S. Yadav and G. Howells, "Analysis of ICMetrics features/technology for wearable devices IOT sensors," in *Proc. 7th Int. Conf. Emerg. Secur. Technol. (EST)*, Canterbury, U.K., Sep. 2017, pp. 175–178.
[32] C. Zhou, "An improved lightweight certificateless generalized signcryption scheme for mobile-health system," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 1, Jan. 2019, Art. no. 155014771882446.
[33] B. Zhang, Z. Jia, and C. Zhao, "An efficient certificateless generalized signcryption scheme," *Secur. Commun. Netw.*, vol. 2018, pp. 1–11, May 2018.

TAI-HOON KIM (Member, IEEE) received the B.E. and M.E. degrees from Sungkyunkwan University, South Korea, and the Ph.D. degrees from the University of Bristol, U.K. and the University of Tasmania, Australia. His main research areas are security engineering for IT products, IT systems, development processes, and operational environments.

GULSHAN KUMAR received the B.Tech. degree in computer science engineering from the Amritsar College of Engineering, Amritsar, in 2009, and the M.Tech. and Ph.D. degrees from Lovely Professional University, India, with area of specialization in position and location computation in wireless sensor networks. He is currently working as an Associate Professor with Lovely Professional University. He has many publications in well renowned international journals and conferences.

RAHUL SAHA received the B.Tech. degree in computer science engineering from the Academy of Technology, West Bengal, and the M.Tech. and Ph.D. degrees from Lovely Professional University, India, with area of specialization in cryptography, position and location computation in wireless sensor networks. He is currently working as an Associate Professor with Lovely Professional University. He has many publications in well renowned international journals and conferences.

MAMOUN ALAZAB (Senior Member, IEEE) received the Ph.D. degree in computer science. He is currently an Associate Professor with the College of Engineering, IT and Environment, Charles Darwin University, Australia. He has more than 100 research articles. He is a Cyber-Security Researcher and a Practitioner with industry and academic experience. His research is multidisciplinary that focuses on cyber security and digital forensics of computer systems including current and emerging issues in the cyber environment like cyber-physical systems and the Internet of Things, by taking into consideration the unique challenges present in these environments, with a focus on cybercrime detection and prevention. He presented many invited keynotes talks and panels at conferences and venues nationally and internationally (22 events in 2018 alone). He is an Editor on multiple editorial boards, including an Associate Editor of IEEE Access and an Editor of *Security and Communication Networks* journal.

WILLIAM J. BUCHANAN is currently a Professor of cryptography. He also leads the Blockpass ID Lab, Edinburgh Napier University. He has authored 30 academic books and over 250 research articles. His main research interests include distributed ledger technology, identity systems, trust-based infrastructures, and cryptography. Along with this his work has supported the creation of a number of spin-out companies and international patents. He was awarded an OBE for his services to cybersecurity, in 2017.

MRITUNJAY KUMAR RAI received the M.Eng. degree in digital system from the Motilal Nehru National Institute of Technology, Allahabad, India, and the Ph.D. degree from the ABV Indian Institute of Information Technology and Management, Gwalior, India. He worked as an Associate Professor at Lovely Professional University, Phagwara, India. He had published more than 50 research articles in reputed international conferences and journals. His research interests include wireless networks, network security, and cognitive radio networks.

G. GEETHA is currently working as a Professor with Lovely Professional University, India. Her research interests include security and cryptography, cyber-physical systems, and software engineering.

REJI THOMAS received the Ph.D. degree from IIT Delhi. He is currently a Professor with Lovely Professional University, Phagwara, India. His research interests include logic, memory, and energy storage devices.