IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2022, accepted March 6, 2022, date of publication March 16, 2022, date of current version March 31, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3160231

Light-Weight Secure Aggregated Data Sharing in IoT-Enabled Wireless Sensor Networks

GHAWAR SAID[1], ANWAR GHANI[1], ATA ULLAH[2], MUHAMMAD AZEEM[1], MUHAMMAD BILAL[3], (Senior Member, IEEE), AND KYUNG SUP KWAK[4], (Life Senior Member, IEEE)

[1]Department of Computer Science & Software Engineering, International Islamic University, Islamabad 44000, Pakistan
[2]Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan
[3]Department of Computer Engineering, Hankuk University of Foreign Studies, Yongin-si, Gyeonggi-do 17035, South Korea
[4]Department of Information and Communication Engineering, Inha University, Incheon 22212, South Korea

Corresponding authors: Anwar Ghani (anwar.ghani@iiu.edu.pk) and Kyung Sup Kwak (kskwak@inha.ac.kr)

This work was supported by the National Research Foundation of Korea-Grant funded by the Korean Government [Ministry of Science and ICT (MSIT)] under Grant NRF-2020R1A2B5B02002478.

ABSTRACT Internet of Things (IoT) is a network of physical objects or things that can communicate and share information. In IoT-enabled Wireless Medical Sensor Network (WMSN), the smart sensing devices share remote patient monitoring data towards central repositories. During medical data aggregation and transmission, security is mandatory to guard against intruders. The main problem in existing base schemes is that complex multiplication operations are used for batch key creation. These schemes are computationally expensive and require huge memory space at the aggregator node (AN). This paper presents a lightweight Secure Aggregation and Transmission Scheme (SATS) for secure and lightweight data computation and transmission. SATS provides a lightweight XOR operation for obtaining batch keys instead of the expensive multiplication operation. Furthermore, the AN Receiving Message Algorithm (ARMA) is presented at the AN to aggregate data generated by sensor nodes. The Receiving Message Extractor (RME) algorithm is presented to decrypt the message and perform batch verification at the Fog-Server. SATS protects against several security threats such as denial of service attacks, the man in the middle attack, and reply attacks. The proposed SATS is simulated by using simulation tool NS 2.35. The results show that SATS provides lightweight data transmission by reducing computation and communication costs.The computation cost of the SATS scheme is 14%, 23% and 59% at AN, and at Fog-Node 6.5%, 21.5% and 51%, and Communication cost 6%, 3%, and 4% at Sensor Node, and at AN 6%, 9%, and 12% better than PPDAS, IDAP, and ASAS respectively. The proposed SATS is compared with relevant schemes and the results show that it provides better storage capacity, computations cost, communications cost, and energy consumption.

INDEX TERMS Data aggregation, data sharing, fog node, batch key, IoT-enabled WSN.

I. INTRODUCTION

Internet of Things (IoT) is a network of things such as machines, objects, and devices having sensors and technology to enable connectivity for the purpose of information gathering and exchange. It is an emerging new network technology with the objective and opportunity to transform human life by enhancing the technology of the Internet. Therefore, its applications in diverse paces of lives are seen to be increasing significantly [1]. IoT is a new paradigm that enables a large number of smart things to be linked with the Internet. The objects like actuators and sensors devise are capable to manage and forward the data to a system without human contribution. In IoT, Wireless Sensor Networks is an important component mostly deployed for sensing data from the surrounding devices and relay that data to a central controller for further processing. IoT can benefit from wireless sensor networks, which can contain a variety of objects for smart device computing, communication, caching, and sensing [2], [3].

IoT is applicable in medical, healthcare, industry, agriculture, security, vehicles and smart Home [4]–[7], which are shown in Fig. 1. IoT has become an elementary structure of block for smart objects, things, and items. Several wireless

The associate editor coordinating the review of this manuscript and approving it for publication was Chi-Yuan Chen.

or wired networks, short-range or long-range communication to attain interoperability. It supports a suitable information security method to deliver manageable and modified real-time online look-up [8]. Its covers a wide range of household sensing devices as well as a huge amount of data in order to make intelligent working judgments [9]. Biomedical devices are utilised by hospitals and nursing institutes to monitor the patients record.

In Wireless Sensor Networks (WSN) sensors cover a large area and can have several sensors in the same region. It may lead to the collection of repeating data patterns, resulting in high computing and communication costs [10]. Therefore, aggregation is a critical activity for removing repeating patterns from data before transmitting it over a communication channel in order to reduce communication costs and storage capacity. There are many key challenges that disturb the narration of the WSNs due to their individual appearances. The efficient energy utilization is the main issue for the survivability of the network in the IoT-enabled WSN [11].

IoT-enabled wireless sensor networks are used in several survivability applications like remote health monitoring, smart homes, intelligent transportation systems. Survivability is the capability of the WSN to provide an acceptable level of services when a failure occurs and improve the network lifetime. Therefore, an efficient and accurate algorithm is required to analyze survivability. The survivability of the network is also based on security. Security generally shows the resilience of the system against different types of security attacks to enhance the survivability of the network. In this scenario, the combination of survivability and security effectively provides necessary services. Security is also a critical concern in an IoT-enabled WSN environment to maintain data integrity, confidentiality, freshness,network availability, and accuracy in the event of internal and external attacks [12], [13]. Taking light weight operation of XOR with at private key for verification of data at Aggregator Node, and then Aggregator Node encrypt that data within own private key. After encrypted the data send securely to the FoG-Server.

A Fog assisted approach is utilized for reducing transmission delay and storage requirements. It has also been identified that most of the studies in the context of IoT enabled WSN focus on survivability, communication complexity and energy consumption. However, transmitting large amount of data requires more memory as well as increasing computational, and communication cost.

A demand for an efficient technique that delivers safe data aggregation at the network's edge while simultaneously managing heterogeneity among sensor nodes has been learned through numerous secure aggregation-based schemes. We believe that adequate lightweight and secure transmission technologies for fog-based healthcare systems are lacking. Furthermore, several data sharing schemes considering lightweight and secure data sharing but still limited work have been studied for healthcare-based mechanisms.

In this article, we present a lightweight and secure aggregated-data transmission scheme (SATS) that obtains batch keys verification via the XOR operation. In place of conventional methods' costly multiplication keys batch verification operation. To use a light-weight batch key establishment approach that relies on the XOR operation rather than multiplication. It not only reduces computational cost but also reduces parameter sizes for storing the parameters.

From the results perspective, SATS provides better communication cost and computational cost against existing schemes. We identified the gap in the recent research studies that most of the research studies enhance the communication cost and energy consumption because while transmitting a large amount of data, more memory utilization also enhances the computational cost. The motivation of this paper is to overcome the different security issues by providing a feasible method for a secure healthcare system in WMSN. Moreover, it also considers the security for secure data collection and sharing. The fog-based approach is utilized for fast access and reducing the storage overhead at the cloud server. Several existing schemes, provide secure data transmission but still have different open challenging issues that are should be overcome in future research concerns. Therefore, we present a secure and lightweight data aggregation method to overcome the recent challenging issues.

The main contributions of this article are enumerated as follows;

- To present a lightweight XOR operation for obtaining batch keys and also generate a secret key among the aggregator nodes and fog node for secure communication.
- To use a light-weight batch key establishment mechanism where XOR operation is involved instead of multiplication operation. It not only reduces computational cost but also reduces parameter sizes for storing the parameters.
- To present data transmission by local sensing devices and then receiving message at AN and extraction of message on the FoG server to extract the values of sensing devices by employing a second level delimiter. Moreover, identity of the sensing device is also maintained.
- Finally, extensive simulations are performed using NS-2.35 to validate the proposed scheme by comparing the results with the counterparts.

The remainder of this article is structured as follows. Section II discuss the literature review. The system model and identification of problem is presented in Section III. Section IV outlines the suggested strategy, which is based on A Light-weight Secure Aggregated Data Sharing Scheme using IoT-enabled WSN. The results have been discussed and analyzed in section VIII and finally section IX concludes the paper.

II. LITERATURE REVIEW

This section explores the related schemes for data aggregation in IoT assisted WSN. Moreover, Fog-assisted and healthcare-based schemes are also considered that provide a secure and privacy-preserved medical data transmission.

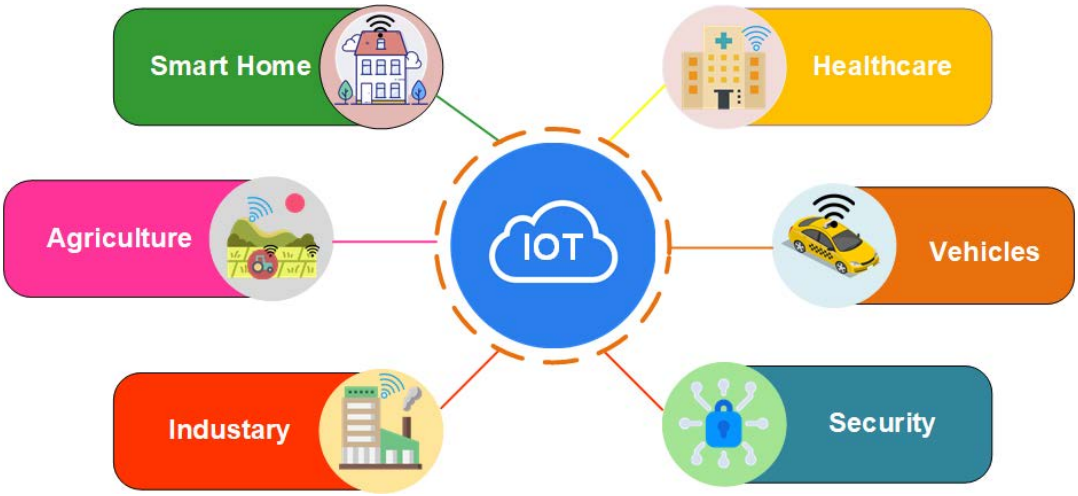

FIGURE 1. Application of IoT.

A. DATA AGGREGATION SCHEMES FOR IoT ENABLED WSN

In this subsection, we shall explore the data aggregation schemes that consider the smart sensing devices to collect the data and share with the collectors. These schemes transmit the aggregated data from different nearby sensing devices linked to a certain user instead of sending data for individual devices separately. For comparative analysis of the proposed scheme, different light-weight schemes have been identified, for example, D. Qin *et al.* introduces a secure aggregation scheme based on state-full Public Key Cryptography using state-full public key namely SPKC. Moreover, an additional homomorphic encryption and aggregated MAC to provide confidentiality and honesty from beginning to end [14]. Jingwei et al presents ''Verifiable Data Aggregation Scheme (VDAS) for Internet of Things [15] that contains three types of entities such as a Key-Generation-Center (KGC), IoT terminals, and IoT data center where KGC can generate the cryptographic keys. The aggregator nodes aggregates the data from the terminal nodes and use the batch key method to appended its own signature to send data. The use of batch key method for concatenation on the aggregated data and then appending signature increases the size of the data leading to increase in computation and communication cost.

S. O. Ogundoy *et al.* [16] presents a EDAS scheme to preserved the user identity and also hide the physical location of devices. Moreover, the strategy protects against several security attacks and reduces both computation and communication costs. Moreover, EDAS generates a signature from the message M_i and then send that data in the form of (M_i, π_i, T_i). The signature generation procedure from the message that clearly increases the data size, leading to an increase in communication cost. In [17] an anonymous and secure aggregated scheme (ASAS) that provide data anonymity and node authentication to ensure data integrity. The terminal nodes forwards the query to the PCS for authentication. After the authentication,FN receives all the encrypted messages of the TDs and aggregates it using batch key method. After that, the aggregated data is sent to PCS. However, the communication cost is still high at the PCS. IDAP protocol provides data aggregation scheme that provide batch key based verification. The batch key method is employed at the collector node. All the smart devices In batch all the data multiplying to one after the other and so on and then send then send it to PCS. However, the transmission cost of the presented scheme still need improvements. [18]. In PPDA [19] authors preserved the privacy of the data in both aggregation and transmission phases. Moreover, a batch key method is utilized to aggregate data from the sensor nodes. The complex multiplication operations enhance the computational cost.

In [20] T. Wang *et al.* presented a time scheduling algorithm that provides effective data gathering by employing mobile sink nodes. Although, each mobile sink node moving on its trajectory and minimum spanning tree is employed to reduce the transmission cost.However, when the number of sensor nodes is increased the energy consumption of the scheme is enhanced and also enhances the transmission delay. Ning *et al.* presented an efficient task offloading scheme based on that supports mobility. A ball and bins theory is adopted for constructing a sustainable scheme that provides task offloading from the highly utilized cloud to the less utilized one. Furthermore, it provides resistance against DDoS attacks and provides data computation only for authenticated users. [21].

CMIP scheme provides secure agrees to the cloning model of the mobile agent to decrease the job interval when the MA's visit has a maximum number of Soner-Nodes to visit. The CMIP addresses this issue by breaking down the circuit into sub-itineraries and assigning a different MA to each. However, when the number of sensing nodes increases, the CMIP starts to consume more energy. Moreover, it lowers

the throughput when a large number of source nodes use CMIP as the size of the data increases [22]. Tabinda *et al.* introduce a scheme that provides secure and intelligent data collection from many user equipment and transmitted it to the sink node via joint machine type communication. It provides an effective selection of authenticated relays to cooperatively aggregate data. The presented scheme suffers from high costs in terms of hardware and its maintenance [23].

In [24] Changlun *et al.* presented a secure and privacy-preserved data aggregation scheme to protect the integrity of data during data aggregation and transmission. Symmetric key-based data encryption is utilized to protect the data and also shield against several security attacks. Therefore, in [25] PPM-HDA scheme presents a privacy preserving data aggregation for WBANs and provide fault tolerance. In this context, the cloud server can calculate multiple arithmetical functions of client's health data to offer a variety of services.

To provide effective data aggregation and maintain data confidentiality, the SPPDA approach based on bilinear pairing is described for the remote health sensing systems. The bilinear El Gamal cryptosystem's homomorphic property is employed to obtain privacy-preserving safe computing and combines it with aggregate signature to enable data authenticity and integrity in the WBAN [26]. Due to increase communication and computation overhead, it consumes more energy.

M. Naghibi *et al.* [27] in this article authors suggest a secure data aggregation structure based on a grouping of the star and tree structure. Physically, the network is separated into four equal halves. Each portion recognises a regular and consistent star structure in order to convey data.

In [28] the authors aims to develop a dual resource attentive and security framework for IoMT based distant healthcare systems. To offer constancy in IoMT, a biometrics-keys generation method is employed to encrypt medical data that is useful for reducing resource requirements of the system.

In wireless sensor networks, E. Hasheminejad *et al.* [29] describe a viable data aggregation approach based on a tree topology. The scheme intends to lower energy usage, improve network dependability, and extend the life of the network. Building a three-part binary tree, authentication, and dependable data aggregation are all part of the approach.

In [30] the RDDI scheme optimizes the data distribution and finding routes method.Furthermore, a fuzzy hierarchical model is adopted for secure data transmission. In [10] EHDA scheme provides secure and lightweight data aggregation. The sensor nodes share compressed healthcare data with the collector node. Symmetric key based data encryption is employed to provide secure and lightweight healthcare data transmission. Moreover, compress healthcare data forwarding reduces the communication and storage costs.

In [31] Tian et al, introduce a binary tree assisted model for fog based approaches. The presented approach forward a pre-processed data to the edge node. In this scenario, the computational cost at the edge server is reduced and also improve the efficiency of system.

WSNs have various uses in the IoT and Industrial IoT IIoT, according to M. S. Yousefpoora *et al.* [32] in this study the data aggregation algorithms are well-known in WSNs for their ability to reduce energy consumption. Furthermore, because of their wireless connectivity, these networks are vulnerable to a variety of threats. As a result, ensuring data security during the data aggregation process is critical.

In the article [33] the authors present a novel method that is supported by mobile-edge nodes, and that is responsible for the uniformity of sensor devices in the IoT-enabled wireless sensor networks.

In the literature review, we conclude that a number of schemes provide solutions for secure data aggregation. However, efficient and secure data aggregation and transmission are quite challenging for resources constrained environments. In IoT enabled-WSN, intelligent devices have limited resource constraints such as energy, available memory storage, communication bandwidth, and transmission speed. Therefore, a green computing mechanism is required that provides secure data transmission and aggregation while efficiently utilizing the limited resources.

III. SYSTEM MODEL AND PROBLEM STATEMENT

During data exchange from sender to sink via intermediate nodes, an intruder at the intermediate node can falsify the data. Therefore, security is a primary concern while transmitting sensitive healthcare data. In this context, we introduce a secure data aggregation and transmission model for IoT-enabled wireless sensor networks. Fig 2 illustrates that a group of smart sensor devices is attached to the patient body. Sensor nodes provide secure data forwarding to a designated aggregator node for peer-to-peer communication. We assume that smart sensor nodes periodically forward data and aggregator nodes share data in response to a request from the FoG-Server. Moreover, medical professionals request patient health parameters from the fog server to provide remote data analysis and prediction.

In our system model, various smart medical sensor nodes are attached with body of the patient. The wearable sensor nodes collect the healthcare information of the patient. The collected information is shared with the aggregator node (AN) for secure data aggregation. In Figure 2, we explain the simple idea of sensors devices-to-AN interaction. Moreover, The AN node receives healthcare information from the sensor nodes and provides secure data aggregation. In this context, ANs share aggregated data directly or indirectly to the fog server. The AN_3 and AN_4 can directly share an aggregated message to the fog server. The AN2 and AN1 are unable to directly interact with the fog server. Therefore, AN_2 share aggregated data to the intermediate node AN_4. The AN_4 aggregates data from sensor nodes and also aggregates the data received from the AN_2 and shares the aggregated message with the Fog node. Similarly, the AN_1 also interacts with AN_2 and AN_3 for sharing the data with the fog server. We provide data aggregation as a result of the AN-to-AN

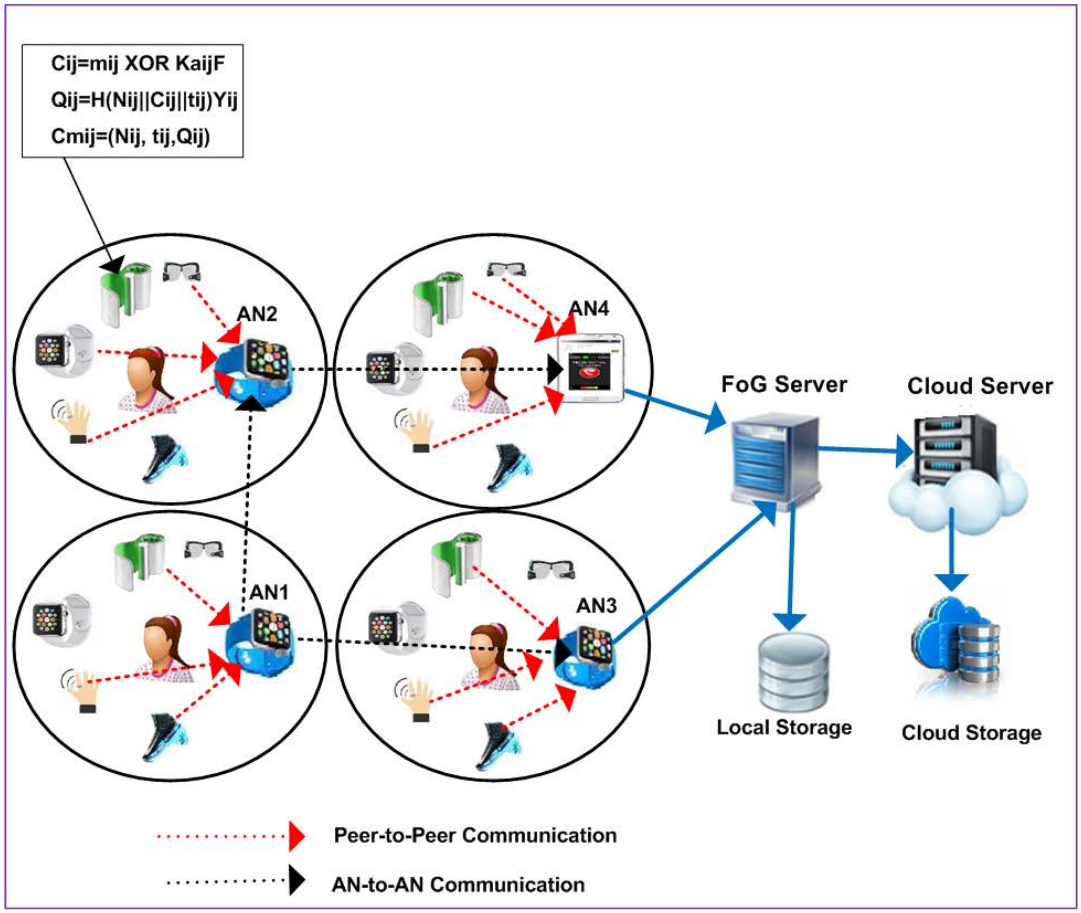

FIGURE 2. System model for peer-to-peer communication for aggregated-data exchange to FoG-Server.

interaction. Furthermore, the fog node provides secure data extraction and computation then forwards data to the cloud server for storage and access.

The main problem in the existing schemes is that the complex multiplication operations for extensive calculations cause computational overhead. In case of multiplying very large values, the resultant value exceeds the maximum size of storage for a certain variable. For the large amount of data transmission to base station, it causes additional overhead due to extensive computations. Large values also cause storage and transmission costs. In this scenario, a cyclic transmission of a predetermined amount of data is a viable option. To avoid a sensing bottleneck, an efficient and green sensing technique is necessary. Therefore, we present a secure and lightweight data aggregation scheme in section IV.

In these approaches [17], [18], and [19], the batch technique was employed for key verification and transfer data to a public cloud server. As batch technique used for verification of keys, in this method first all keys of the sensor devices multiplying to each other's and then send for further transmission. In batch verification, extensive multiplication increases communication and computational cost and also utilizes extra storage space at AN and fog nodes.

IV. SECURE AGGREGATED-DATA TRANSMISSION SCHEME (SATS)

In this section, the proposed Secure Aggregated-data Transmission Scheme (SATS) is presented. The scheme focuses on reducing the computation and communication complexity, therefore, it used Exclusive OR (XOR) operations instead of large multiplications during cryptography operations. We also focused on ensuring the security strength while reducing the computational cost. Symmetric key encryption is utilized for secure data transmission. SATS ensures different security factors like integrity protection, data authentication, availability, and message freshness. Moreover, hierarchical data aggregation is used to provide a lightweight and secure data sharing. Fig 3 describes the three different phases of the proposed scheme like data collection and transmission in local sensing devices, Message receiving and data aggregation at the AN, and message description and data extraction at the Fog node. A second-level delimiter is also employed to retrieve the sensing data of the sensor nodes and store it at the local storage of the fog server. After collecting the data from various regions over a set period, FoG-Server refines the data and uploads it in the required format to the cloud storage.

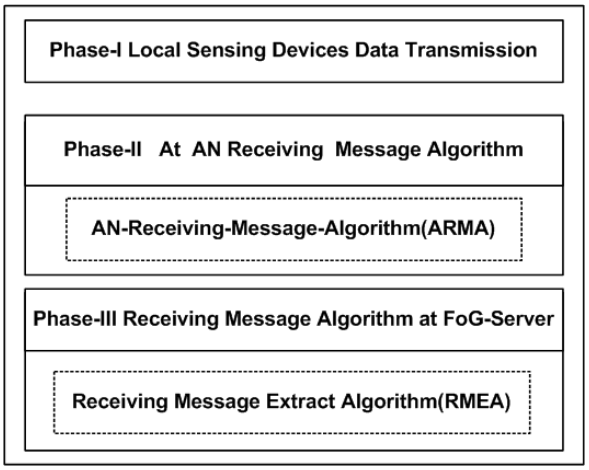

FIGURE 3. Phases of proposed scheme.

List of notation is shown in Table 1.

TABLE 1. List of notations.

S.N	Notation	Description
1	N_{ij}	Sensor node ID
2	t_{ij}	Timestamp at sensor node
3	C_{ij}	Cipher text at sensor node
4	σ_{ij}	Hash function at sensor Node
5	Cm_{ij}	Encrypted message received at AN
6	A_{cm}	Aggregated message at AN
7	$\oplus$	XOR operation
8	X_c	Secret key between fog server and AN
9	IDA_i	Aggregator node ID
10	Ka_{ij}F	Batch key at fog server
11	m_{ij}	Extracted message at the fog server

In the first phase, the sensing devices (SD) collect the healthcare data of the patient. The sensor nodes (N_{ij}) forwards the collected information to AN. The SDs collect the healthcare values of the patient.In case of normal temperature sensing node cannot send the data to the AN. Only those SDs forward the patient data to the AN that contains patient values other than normal values. For example, a node that have a body temperature of more than 39°C or 100.6°F that can send the temperature value to the AN The SD creates a ciphertext C_{ij} message by taking the XOR with the secret key (X_c). The σ_{ij} signature is set for hash-function value of the N_{ij}, C_{ij}, and timestamp t_{ij}. The SDs forward the encrypted message $Cm_{ij} = X_c\ (N_{ij}, t_{ij}, C_{ij}, \sigma_{ij})$ to AN. In the second phase, the proposed scheme present a receiving message algorithm at AN that receives messages Cm_{ij}. At AN the message receiving algorithm is shown in the algorithm 1.

In algorithm 1, the article present AN Receiving Message Algorithm (ARMA) at AN. Initially, it receives an encrypted message Cm_{ij} from the SDs. Algorithm1 elucidates that the AN collects the data Cm_{ij} from all the sensing devices where i is the node ID. Intially, AN node has empty data so the value of A_{cm} is nil. Each encrypted message received from the SD that contains Cm_{ij} the node ID (N_{ij}), Time-stamp (t_{ij}),

Algorithm 1 AN Receiving Message Algorithm (ARMA)

Require: $A_{cm} = null, X_c = null$, MSG($Cm_ij$)
Ensure: performs aggregation on received data from sensor nodes

```
Receive Cm_ij = (N_ij, t_ij, C_ij, σ_ij) from SD_ij
if T(t_ij)' − T(t_ij) < δt then
    σ_ij ← H(N_ij‖C_ij‖t_ij)
    if σ_ij ← σ'_ij then
        A_cm ← A_cm‖Cm_ij
    else
        Discard Message
    end if
    X_c ← X_c ⊕ Cm_ij
else
    Discard Message
end if
Performs Batch Verification At Aggregator Node
X_c ← X_c ⊕ Cm_ij
σ_i ← H(IDA_i‖X_c‖t_i)
Send (IDA_i, X_ci, σ_i, t_i) to FoG-server
```

signature σ_{ij}. Moreover, the AN receives $Cm_{ij} = (N_{ij}, t_{ij}, C_{ij}, \sigma_{ij})$ from N_{ij}. After receiving the message the AN node checks the time-stamp $T(t_{ij})$ of the received message. In case $T(t_{ij})' - T(t_{ij}) < \Delta t$ is true then the received message is fresh otherwise discard the outdated message. Next, AN calculates signature like this $\sigma_{ij} = H(N_{ij}\|C_{ij}\|t_{ij})$ for received Cm_{ij} and if σ_{ij} equals to σ'_{ij} is true mean it ensures the message integrity otherwise discard the message due to integrity violation. All received messages are concatenated by AN as the $A_{cm} = A_{cm}\|Cm_{ij}$ that the results as $A_{cm} = (Cm_{ij}\left\|Cm_{ij+1}\right\| \ldots \|Cm_q)$ for the q messages collected at AN. Then, perform batch verification at the AN. The $X_c = X_c \oplus Cm_{ij}$ which is determined by taking the XOR of Cm_{ij} with the secret key which generated between FoG-Server and AN. The hash of the message is calculated $\sigma_i = H(IDA_i||X_{ci}||t_i)$ and add this hash in the encrypted message $(IDA_i, X_{ci}, \sigma_i, t_i)$ and forward this message to the FoG-Server.

In the third phase, the proposed scheme introduces a Receiving Message Extraction (RME) algorithm at FoG-Server. The encrypted message is collected from the ANs sequentially. FoG-Server after receiving the aggregated messages from all the AN then separately decrypt the data of each AN. After that, a delimiter is used to extract the node-level data of each SD. Algorithm 2 illustrates the message description procedure at the FoG-Server. An encrypted message is received from the AN. RME provides batch verification on the received message. Initially, received a ciphertext $X_c = X_c \oplus Cm_{ij}$ then extract the encrypted message A_{cm} by taking the XOR with the batch key $A_{cm} = Cm_{ij} \oplus Ka_{ij}F$. Then, comparing the hash of the received message with the calculated hash of the message at the fog server. If σ_{ij} equals to σ'_{ij} is true. Then compute $Cm_{ij} = A_{cm} \oplus Ka_{ij}F$ taking for loop as

For count = 1 to q, and extract the $Cm_{ij} = (N_{ij}, t_{ij}, C_{ij}, \sigma_{ij})$. Next, check the timestamp of the received message. In the case $T(t_{ij})' - T(t_{ij}) < \Delta t$ is not true discarded the outdated message otherwise, Calculate $\sigma_{ij} = H(N_{ij} \| C_{ij} \| t_{ij})$. If σ_{ij} equals to σ'_{ij} then get the required message like as $m_{ij} = C_{ij} \oplus Ka_{ij}F$ otherwise discard message.The flow of operations for the data sharing are depicted in the scheme model as shown in Fig 4.

Algorithm 2 Receiving Message Extraction (RME) Algorithm at FoG-Server

Require: Procedure Receive AN-MSG-(A_{cm})

Ensure: Perform Batch Verification form the Message Received of AN

```
Receive X_c ← X_c ⊕ Cm_ij
After Verification of message
Extract A_cm ← Cmj ⊕ Ka_ijF
if σ_ij ← σ'_ij then
    Cm_ij ← A_cm ⊕ Ka_ijF
    for count ← 1 → q do
        Extract Cm_ij ← (N_ij, t_ij, C_ij, σ_ij)
        if T(t_ij)' − T(t_ij) < δt then
            Calculate σ_ij ← H(N_ij‖C_ij‖t_ij)
            if σ_ij ← σ'_ij then
                m_ij ← C_ijoplusKa_ijF
                Save to local Storage of FoG-Server
            else
                Discard the Message due to Violation of Integrity
            end if
        else
            Discard the Message due to Failure of Freshness
        end if
    end for
else
    Discard Message due to Violation of Integrity in Cm_ij
end if
Send Acknowledge-Message to AN
```

Figure 4 shows the flow of the proposed scheme, a set of medical sensing devices that can be utilized for peer-to-peer data transmission to a given AN. After collections of all the sensing devices, the AN aggregates the collected data. Then, AN sends the aggregated message to the FoG-Server for further processes. At the end of the process extract the data and get the required message.

V. SECURITY ANALYSIS

The proposed security model is suitable for secure and lightweight data remote health monitoring. Therefore, the formally security analysis of the proposed scheme is conducted to prove that it protects against several security attacks. Some security attacks are discussed as follows.

A. NODE IMPERSONATION ATTACK

Data integrity protection ensures that the data during transmission must not be changed in an unauthorized manner. Mostly, in unreliable communication networks, malicious nodes change the data during transmission. Data in transmission may sometimes be changed or lost due to a device failure or malfunction. Therefore, effective mechanisms are essential to ensures survivability and protect the data integrity in the IoT based sensor networks. Thus, the proposed scheme provides secure communication by performing different security operations like Hash, XOR, and secret key to encrypt and transmit the messages over the network. The proposed approach computes hash of the message and attaches a timestamp to protect the message integrity. In this system model, some basic properties of the nodes are used to provide access to other nodes. A batch key based encryption is utilized to protect data integrity and provide secure data transmission.

B. REPLAY ATTACK

In a replay attack, an attacker delays and resend the intercept messages to the destination. To prevent this attack, a timestamp is employed on all the messages. The proposed scheme drops the outdated messages to avoid resent or delayed messages. In this context, the proposed scheme discards those messages that are received after pre-established time limit to shrink the opportunity window for the replay attacks.

C. MAN-IN-THE-MIDDLE ATTACK

An attacker can intercept the communication of two nodes by injecting an adversary node in the middle. To provide resistance against man-in-the-middle attack, the proposed scheme utilizes batch key-based encryption. The sensitive information of nodes is protected by taking the hash of collected data and other security credentials. The proposed algorithms provide secure data encryption and decryption to protect from a man-in-the-middle attack.

D. DENIAL OF SERVICES ATTACK

In a DOS attack, malicious nodes first accurately provide the information after that denied to produce accurate results. In the proposed scheme, only authenticated nodes (ANs) can take part in the communication process. The ANs are mobile nodes that provide data aggregation and message authentication. Received messages are authenticated using hash functions and the timestamp of the message is also checked. Therefore, the proposed scheme resists against denial of service attack as well as protects the data integrity during communication. The proposed lightweight and secure data aggregation and message authentication-based scheme provide effective resistance against denial of services and enhances the network survivability.

VI. THEORETICAL ANALYSIS

The theoretical analysis is conducted based on time complexity, communication cost, computational cost and

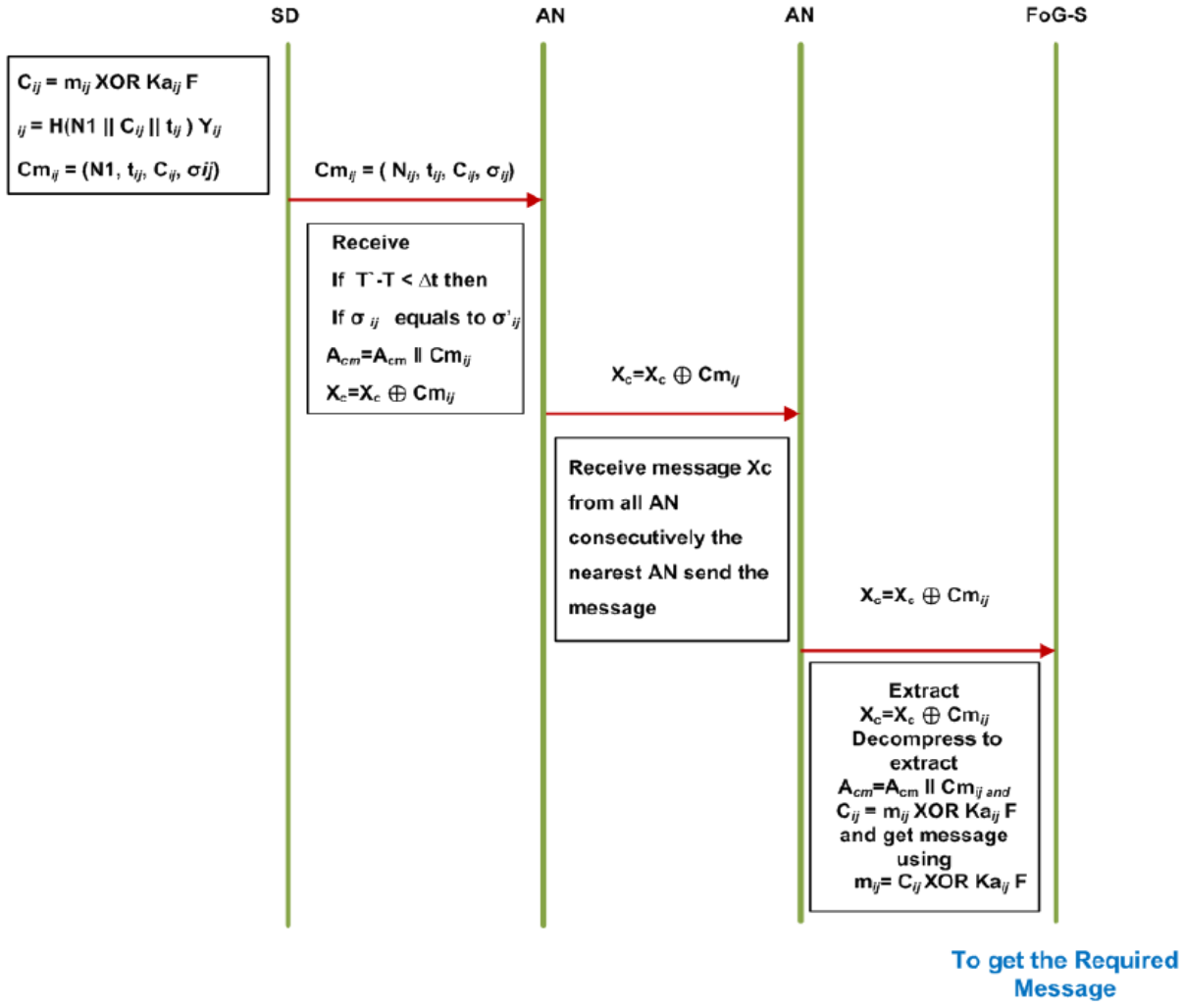

FIGURE 4. Flow operation of the scheme model.

energy consumption. In our presented scheme SATS, algorithm 1 provides secure data aggregation at the AN and algorithm 2 provides data encryption and local computation at the Fog node.

In the case of computational time, algorithm 1 provides received message verification in constant time complexity. Moreover, the number of sensor nodes forward the aggregated data to the AN. The aggregated messages are based on the number of sensor nodes that are n. Therefore, the time complexity of algorithm 1 during data aggregation is O(n). In algorithm 2, provide message verification and decryption in constant time. The collected information of each node is extracted in O(n) time. The overall time complexity of both algorithms is O(n). Thus, the time complexity of SATS is better than ASAS, IDAP, and PPDAS. The energy consumption during communication is calculated as $E_c = (E_s \times T_m) + (R_m \times E_{rs}) + (M_d \times E_s)$ where E_s denotes energy utilized during single message transmission, T_m denotes the total number of messages are forwarded, R_m denotes the total number of messages are received, E_{rs} energy utilized during single message receiving procedure and M_d denotes the total count of drop messages.In this context, the E_s and E_{rs} are considered as 0.1815μJoules and 0.045μJules based on the sensor nodes configuration in the simulation setup. To analyze the energy consumption a number of messages $50 - 200$ are forward to analyze the energy utilization during communication. In this context, SATS provide efficient energy consumption because SATS reduces the packet drop ratio and also utilized less energy while communication as compared with the related aggregation scheme. In the transmission of aggregated data number of sensor nodes respond and there is a probability that a node can be a malicious node. In this context, the probability of malicious nodes is calculated as

$$\mathrm{P_CN} = 1 - \left(\frac{R_n - 3}{C_n}\right) \Big/ \left(\frac{R - n}{C_n}\right) = \frac{C_n}{R_n - 2} \qquad (1)$$

where R_n denotes the receiving nodes and C_n denotes the probability of compromised node. In this scenario, we are considering sender and receiver both are excluded from the number of compromised nodes. Moreover, one neighbor node

can also be excluded to measure the probability.To measure the probability of the responding a number of responding nodes that are varied from $50-150$ nodes to calculate the number of compromised nodes. Moreover, a node is compromised then the messages are received on that node are also compromised. In this context, the probability of compromised bytes can also be calculated as

$$\mathrm{P_{CB}} = 1 - \left(\frac{T_b - 1}{C_b - 1}\right) \Big/ \left(\frac{T_b}{C_b}\right) = \frac{C_b}{R_b} \tag{2}$$

where C_b represents the number of compromised bytes and T_b represents the total number of bytes are transmitted. In this case, the total number of responding nodes are varied from $50-150$ to measure the probability of compromised bytes. In the SATS only those nodes can respond that can fulfill the query conditions thus less number of responding nodes are compromised nodes. On the other hand, the number of compromised bytes are also reduced because SATS no forwarding the redundant data and also provide compressed data transmission. Thus, in both cases SATS provide less number of compromised bytes and compromised nodes in contrast with other existing schemes. Moreover, the simulation results are analyzed in the section VIII.

VII. FORMAL VERIFICATION

To verify our work, we performed the Rubin logic [34] based formal analysis to verify the functionality as per the standard flow of steps for the security scheme. It verifies the mandatory requirements demanded by a certain security protocol and its related operations for encryption, decryption, and hashing. These steps are considered to be near to the actual implementation of the protocol and cover all the essential steps to verify the functionality of the protocol as per standardized flow. The formal method also verifies against the possible security attacks that are guarded if a certain flow of mandatory steps is followed. A global set ensures the use of main entities and related variables accessible to the entire functionality of tasks in a global manner. In a similar vein, possession set and belief set are also managed along with a behavior list tilted BL as shown in Table 2.

We explore the stepwise description for the message sharing among the *Nij*, *ANj*, and *FS*. In each step, we show the cryptographic operations including encryption, decryption, hashing, *XOR*, message newness, and concatenation. After sending the message, the update operation stores the local values to sustain the required values. On receiving side, it checks the message freshness or newness by taking the difference of timestamp sent by the node and the current timestamp at the AN_j. Moreover, the hash is also matched to ensure the message's integrity. In the end, the forget operation is used to remove the extra variables.

VIII. RESULTS AND ANALYSIS

Extensive simulations is performed to validate the proposed technique considering that devises are Installed in a 1500×1500 cm area. Also it involves the Edge-Server and Public Cloud Center. The proposed scheme is compared to the existing schemes computations cost, storage capacity at edge server and communication cost. For simulation NS-2.35 on Fedora Core 16 is used to mimic message initiation and trace annotation, and the TCL file contains the arrangement of nodes, the placement of node, message initiation, and trace annotation. A separate class in C is constructed to implement the transmit and receive operations for sensing devices and the edge server. Following that, using AWK script for files to retrieve the values of the trace files. After that the proposed approach is compared to what's already out there base schemes including ASAS [17], IDAP [18], and PPDAS [19]. Table 3 shows a list of simulation parameters.

TABLE 2. Local set at sender, CH_j and *FS*.

1. Sender (N_i)
POSS(N_i) = ID_{N_i}, K_M, $K_{N_i-AN_i}$
BEL(N_i) = {# (ID_{N_i}), # (K_M), # ($K_{N_i-AN_i}$)}
$BL(N_i)$ = Concatenate$(ID_{N_{ij}}, t_{ij}, C_{ij}) \rightarrow Con_{N_{ij}}$
$Hash(h(.); Con_{N_{ij}}) \rightarrow \sigma_{ij}$
Encrypt$(\{ID_{N_{ij}}, Add_{NODE}, Con_{N_i}, \sigma_{ij}\}K_{N_{ij-AN_j}}) \rightarrow C_1$
Send$(AN_j, \{ID_{N_{ij}}, C_1\}) \rightarrow M_1$, Update $(M_{ID=1})$
2. Group Head (AN_j)
$POSS(AN_j) = \{ID_{AN_j}, K_{AN_j-N_{ij}}, K_{ANj-FS}\}$
$BEL(AN_j) = \{\#(ID_{AN_j}), \#(K_{AN_j-N_{ij}}), \#(K_{AN_j-FS})\}$
$BL(AN_j) = Get(M_1)$ from N_{ij} and extract C_1
$Dec(\{C_1\}K_{AN_{i-N_{ij}}})$ to get $[\{ID_{N_{ij}}, Add_{NODE}, Con_{N_i}, \sigma_{ij}\}]$
Message-Newness $(t'_{ij}) - t_{ij}) \geq \Delta t$ if true then Msg is aborted
Concatenate $(ID_{N_{ij}}, t_{ij}, C_{ij}) \rightarrow Con'_{N_{ij}}$
$Hash(h(.); Con'_{N_{ij}}) \rightarrow \sigma^*_{ij}$
Integrity $(\sigma_{ij} = \sigma^*_{ij}$ if mismatch, then abort
Concatenate $(A_{cm}, M_1) \rightarrow Agg\_Msg_{AN}$
$XOR(Agg\_Msg_{AN}, K_{AN_j-FS}) \rightarrow X_c$
Concatenate $(ID_{AN_j}, X_c, t_i) \rightarrow Con_{AN_j}$
$Hash(h(.); Con_{AN_j}) \rightarrow \sigma^*_i$
Encrypt $(\{ID_{AN_j}, Con_{AN_j}, \sigma^*_i\}K_{AN_j-FS}) \rightarrow C_2$
Send $(ID_{FS}, \{ID_{AN_j}), C_2\}) \rightarrow M_2$
Update $(M_{ID=2})$
3. Fog Server (FS)
$POSS(FS) = \{ID_{FS}, K_{FS-AN_j}\}$
$BEL(FS) = \{\#(ID_{FS}), \#(K_{FS} - AN_j)\}$
$BL(FS) = Get(M_2)$ from AN_j and extract C_2
Dec$(\{C_2\}K_{FS-AN_j})$ to get $[\{ID_{AN_j}, Con_{AN_j}, \sigma^*_i\}]$
Concatenate $(ID_{AN_j}, X_c, t_i) \rightarrow Con'_{AN_j})$
$Hash(h(.); Con'_{AN_j}) \rightarrow \sigma^{\sim}_i$
Integrity $(\sigma_i = \sigma^{\sim}_i)$ if mismatch, then abort
Extract Data from message Agg_Msg_{AN}

A. COMPUTATIONAL COST

The SATS scheme is compared with IDAP, PPDAS, and ASAS for computational cost both at the fog and aggregator nodes (AN). At the AN node in Fig. 5, when the number of aggregator nodes is 10, the computational cost of PPDAS 157.4184 ms, ASAS is 314.3232 ms, IDAP is 188.2813 ms, and that of the proposed SATS is 105.214 ms. From these

TABLE 3. Simulation parameters.

Parameters	Values
Network Field	1500×1500 meters
Node of numbers	15-to-80
Radius of Cluster	500 m
Power of transmission at Node	0.1815μ J
Sensing radius	130 m
Initial energy	1000 J
Receiving Power	0.045μ J
Channel Type	Wireless
Propagation Model	Two Ray
Power of transmission at AN	0.5819 J
Receiving Power	0.045 J
Physical Type	Wireless Physical
Mac Protocol Type	MAC/802-11
Queue Type	DropTail/PriQue
Antenna Type	Omni Antenna
Max Packet in Queue	60
Router Trace	ON
Mac Trace	OFF
Agent Trace	ON
Number of SDs and ANs	$1 - -10$
Time Slots	$0.1 - -1.0$ seconds
Probability	$0 - -1$

results, it can be clearly observed that the proposed SATS scheme performs better than its counterparts and is suitable for mobile patient. The figure also shows that the growth in computation cost of the proposed scheme is slow and linear in nature. It means if the number of nodes are increase the proposed scheme may perform even better than the competing schemes.

If the computation cost is observed from a percentage point of view, the computational cost of the proposed SATS scheme is 14%, 23%, and 59% better than PPDAS, IDAP, and ASAS respectively. Therefore, the less computational complexity of the proposed scheme makes it more efficient at the fog node as shown in Fig. 6. It can be observed from the figure that When the number of ANs $=$ 10, the computational cost of PPDAS is 157.0747, ASAS is 283.437, ms,IDAP is 482.782, ms respectively and that of the proposed SATS is 151.0747, ms. So it is clear that the proposed scheme has the lowest computation cost as compared to its counterparts.

In terms of percentages, the computational cost of SATS at the fog node is 6.5%, 21.5%, and 51% better than PPDAS, ASAS, and IDAS respectively. Therefore, based on these results it can be concluded that the proposed SATS is more efficient than its competitors in terms of computation cost considering both the aggregator node as well as the fog node.

A comparison of the computation cost at aggregator node is presented in Table 4. The data presented in Table 4 shows a comparative analysis of the proposed SATS with the counterparts schemes for different number of nodes in terms of computation cost. It can be seen from the table that the proposed scheme performs better than its counterparts in case of single as well any number up to 10 nodes. It can also be observed that the growth in computation cost is almost linear showing that increasing the number of node can keep the cost growth steady.

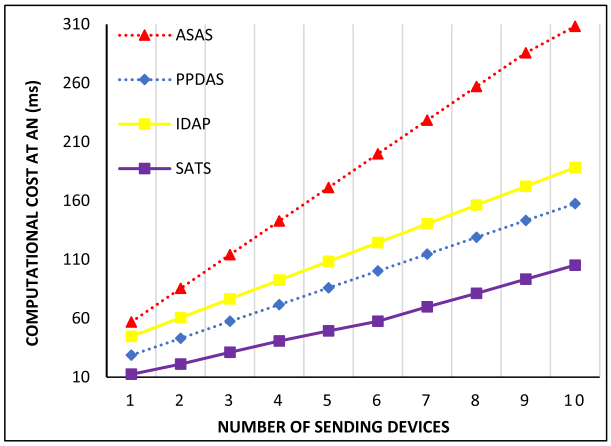

FIGURE 5. Computational cost for SDs.

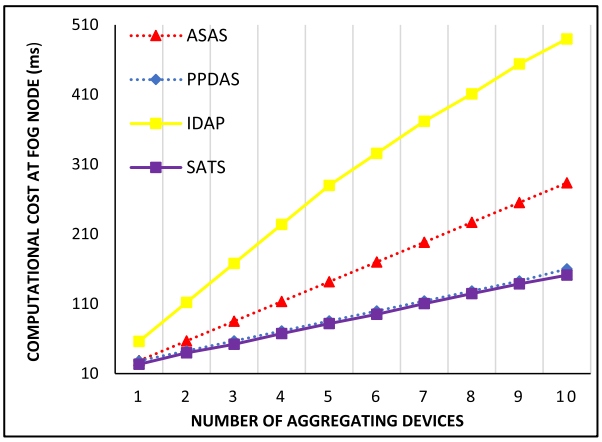

FIGURE 6. Computational cost for ANs.

TABLE 4. Comparative analysis of the proposed SATS with the existing schemes in terms of computation cost at AN(ms).

Nodes	SATS	PPDAS [19]	ASAS[17]	IDAP[18]
1	12.432	28.6599	56.8740	44.6157
2	21.168	42.9664	85.4812	60.5781
3	31.1424	57.4484	114.0854	76.5410
4	40.714	71.5799	142.6908	92.5039
5	49.339	85.8839	171.2962	108.4668
6	57.432	100.1834	199.9016	124.4297
7	69.682	114.4989	228.5071	140.3926
8	81.281	128.8054	257.1124	156.3555
9	93.293	143.119	285.7178	172.3184
10	105.214	157.4184	314.3232	188.2813

Similarly, a comparative analysis of the proposed SATS at the fog is presented in Table 5. The data presented in the table shows that the proposed scheme has the tendency towards lower computation cost, however, this tendency is very insignificant and show almost the same behavior as that of the computation cost at the ANs presented in Table 4. However, it can be seen that the proposed SATS scheme outperforms its competitors no matter what the number of nodes is.

TABLE 5. Comparative analysis of the proposed SATS with the existing schemes in terms of computation cost at FoG-Server.

No of AN	SATS	PPDAS [19]	ASAS[17]	IDAP[18]
1	23.3162	28.3162	28.3437	55.782
2	39.6227	42.6227	56.6874	111.9564
3	51.9292	56.9292	85.0311	167.9346
4	67.2357	71.2357	113.3798	223.9128
5	81.5422	85.3422	141.7185	279.891
6	94.8487	99.8487	170.0622	335.8692
7	110.1552	114.1552	198.4059	381.8474
8	124.4617	128.9617	226.7496	397.8256
9	138.7682	142.768	255.0933	403.8038
10	151.0747	157.0747	283.437	459.782

B. ENERGY CONSUMPTION

Simulation is performed to gauge the energy consumption of the proposed scheme at the SN nodes in the aggregation process. Trace files are used to pattern the residual elasticity of all nodes. The AWK files are applied to extract values for the amount of energy consumed. In Fig. 7 the energy consumption of the sensor nodes is considered during the transmission of data. Initially, the energy level of every sensor node is set to 1000 joules. The energy consumption of the sensor nodes at 0.7 seconds is considered to be 0.00033μJoules for ASAS, 0.00045μJoules for PPDAS, 0.00042μJoules for IDAP, and 0.00031μ Joules for SATS, respectively.

In Fig. 8 the energy consumption at the aggregator node is demonstrated. Here again, the initial energy of every node is set to 10000 joules. It can be clearly observed from the results that at the time of 0.8 seconds the aggregator nodes consume 0.0058μ Joules in case of ASAS, 0.0082μ Joules in case PPDAS, 0.0075μ Joules in case of IDAP, and 0.0054μ Joules in case of the proposed SATS scheme respectively. Results elucidate that SATS is energy efficient as compared to its counterpart schemes.

Table 6 presents the comparative data of the proposed SATS with other competitors in case of ANs. From the table it can be clearly seen that at the start when at a time of 0.1s there is not a significant difference in energy consumption of the proposed scheme and at least the two other schemes namely ASAS and IDAP. However, as the time passes the difference in the energy consumption of the proposed scheme and the others increases. It can also be observed that the growth in energy consumption of the proposed scheme seems to slow down as the time passes. It can be concluded that the proposed scheme performs well in comparison to its competitors in terms of energy consumption at SNs.

Similarly, Table 7 presents the comparative energy consumption of the proposed SATS scheme in comparison with the existing schemes at SDs. Here the difference in the beginning is more evident than the previous Table 6. however, the overall growth of the scheme is not too fast. Therefore, it can deducted the the energy depletion rate at SDs is slower overall and in particular in case of the proposed scheme. At individual level, however, the proposed the SATS performs better than its competitors at all times. Therefore, it can be concluded that the proposed scheme is energy efficient in comparison to its counterparts and also enhance the network survivability.

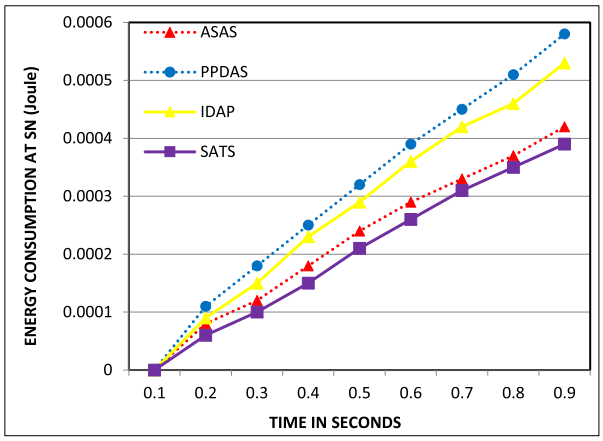

FIGURE 7. Energy consumption for for different number of nodes SNs.

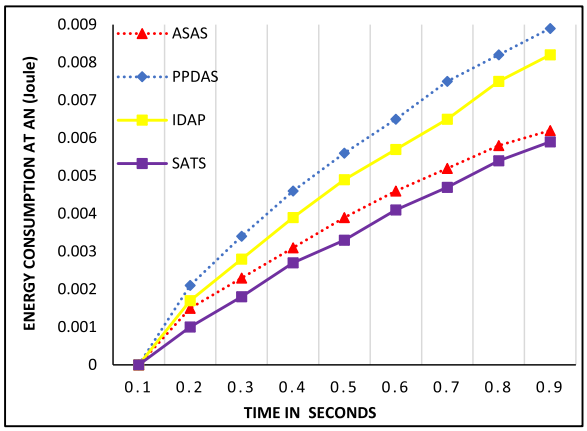

FIGURE 8. Energy consumption for for different number of nodes ANs.

C. COMMUNICATION COST

Fig 9 elucidates the communication cost based on the number of smart devices on fog. When the number of sensor nodes is 54, then PPDAS, IDAP, ASAS, and SATS have 23.3193 ms, 22.2561 ms, 22.7877 ms, and 21.2561 ms respectively. Fig 10 illustrates the communication cost based on the number of aggregator node in the fog. When the aggregator nodes are 12 then the communication cost is 28.3193 ms, 27.2561 ms, 26.7877 ms, and 24.2561 ms for PPDAS, IDAP, ASAS, and SATS, respectively. Aggregator nodes forward data towards the fog node. In case the fog node is not in the communication range of the aggregator node.

Then, the message is forwarded to the next aggregator node. For sensor nodes, SATS attains 6%, 3%, and 4% less communication cost. In the case of aggregator nodes, SATS attains 6%, 9%, and 12% less communication cost as compared with PPDAS, IDAS, and ASAS, respectively.

TABLE 6. Comparative analysis of the proposed SATS with the existing schemes in terms of energy consumption at AN (Joule).

Time	SATS	PPDAS [19]	ASAS[17]	IDAP[18]
0.1	0.004	0.009	0.005	0.006
0.2	0.001	0.0021	0.0015	0.0017
0.3	0.0018	0.0034	0.0023	0.0028
0.4	0.0027	0.0046	0.0031	0.0039
0.5	0.0033	0.0056	0.0039	0.0049
0.6	0.0041	0.0065	0.0046	0.0057
0.7	0.0047	0.0075	0.0052	0.0065
0.8	0.0054	0.0082	0.0058	0.0075
0.9	0.0059	0.0089	0.0062	0.0082

TABLE 7. Comparative analysis of the proposed SATS with the existing schemes in terms of energy consumption at SD (Joule).

Time	SATS	PPDAS [19]	ASAS[17]	IDAP[18]
0.1	0.0002	0.0009	0.0004	0.0006
0.2	0.00006	0.00011	0.00008	0.00009
0.3	0.0001	0.00018	0.00012	0.00015
0.4	0.00015	0.00025	0.00018	0.00023
0.5	0.00021	0.00032	0.00024	0.00029
0.6	0.00026	0.00039	0.00029	0.00036
0.7	0.00031	0.00045	0.00033	0.00042
0.8	0.00035	0.00051	0.00037	0.00046
0.9	0.00039	0.00058	0.00042	0.00053

Table 8 presents the Comparative Analysis of the proposed SATS with the existing schemes in terms of Communication cost, at SD on Fog. The data presented in the Table 8 shows that the proposed scheme has the tendency towards lower computation cost. It is important for the Sensor Devices (SD) to consumes less communication cost, as the low level communications cost is good for the users.

The communication cost in comparison to different existing schemes for different values of SDs is presented in Table 8 and Table 9. Table 9 presents the Comparative Analysis of the proposed SATS with the existing schemes in terms of Communication cost, at AN on Fog. It can be observed from the table that the proposed SATS performs better than its counterparts at all three values of 44, 54, and 64 of SDs. It can also be seen that ASAS and IDAP perform almost the same with slight differences. Overall however, the proposed scheme performs better than the competing scheme.

Similarly the data presented in Table 9 for different number 6, 12, and 18 of AN nodes shows that the proposed scheme is Superior in comparison to the existing schemes. It can also be observed that the competing scheme also has variations in the communication cost unlike at the SDs shown in the previous Table 8.

Now it can be concluded that in terms of computation, communication costs the proposed scheme performs better than its competitors. The proposed scheme shows significant improvements in terms of network survivability and in some cases, it provides slight improvement over the competitors. It is also observed that the existing scheme among their selves has variations in their performance at different levels.

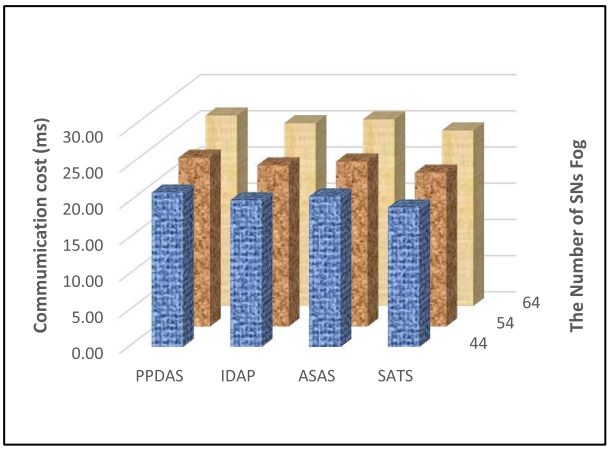

FIGURE 9. Communication cost at SNs.

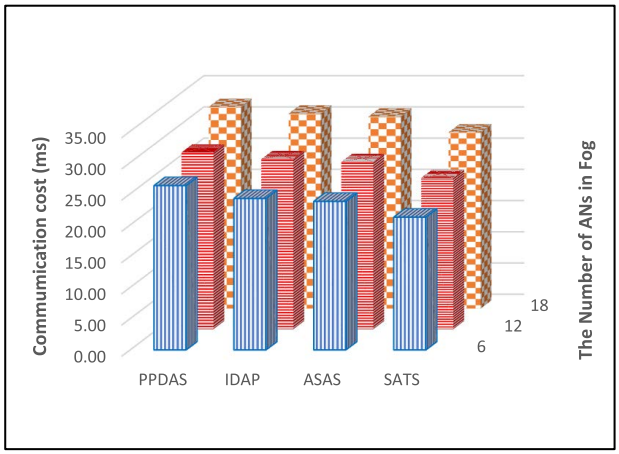

FIGURE 10. Communication cost at ANs.

TABLE 8. Comparative analysis of the proposed SATS with the existing schemes in terms of communication cost, at SD on Fog.

No of SD	SATS	PPDAS [19]	ASAS[17]	IDAP[18]
44	19.2561	21.3193	20.7877	20.2561
54	21.2561	23.3193	22.7877	22.2561
64	24.2561	26.3193	25.7877	25.2561

D. RESILIENCE

In this scenario, the probability of malicious nodes is calculated as follows.

$$\mathrm{Pr_C} = 1 - \left(\frac{N-3}{c}\right) \Big/ \left(\frac{N-3}{c}\right) = \frac{c}{N-2} \tag{3}$$

As in secure communication the number of sensor nodes reply to every query. Therefore, malicious nodes also becomes part of the communication. Fig. 11, illustrates that the number of devices varies from $40 - 120$. Simulation results elucidate that when the responding nodes are 90 the probability is 0.2081, 0.2981, 0.3981, and 0.5481 for $\mathrm{PMN} - 7$, $\mathrm{PMN} - 14$, $PMN - 21$, and $PMN - 28$ compromised nodes, respectively.

TABLE 9. Comparative analysis of the proposed SATS with the existing schemes in terms of communication cost, at AN on Fog.

No of AN	SATS	PPDAS [19]	ASAS[17]	IDAP[18]
6	21.2561	26.3193	23.7877	24.2561
12	24.2561	28.3193	26.7877	27.2561
18	28.2561	32.3193	30.7877	31.2561

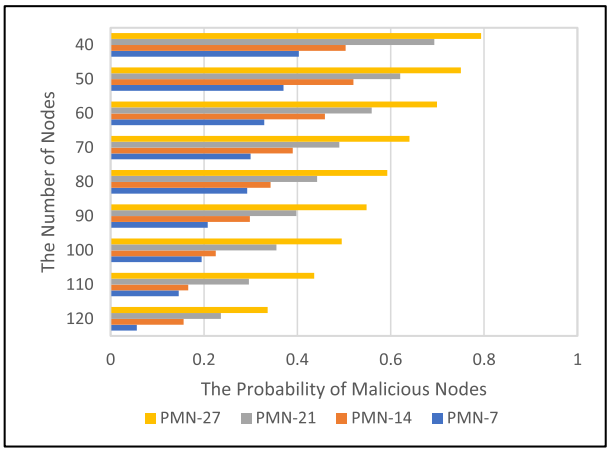

FIGURE 11. Probability of malicious nodes.

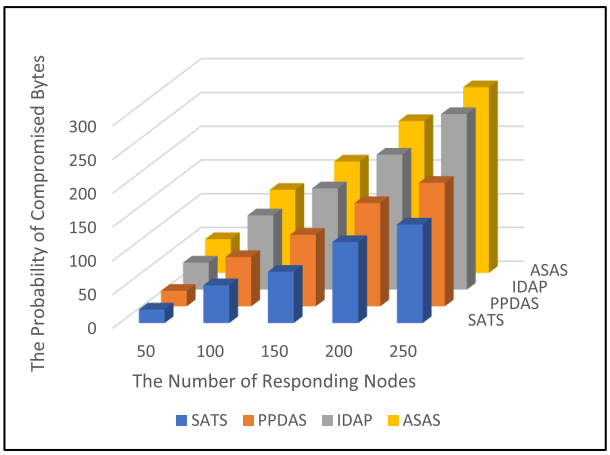

FIGURE 12. Probability of compromised bytes.

Fig. 12, illustrates the probability of compromised messages. In this context, when a single reply node is captured and data is exposed then the probability of compromised bytes can be measured as

$$Pr_{\eta} = 1 - \left(\frac{M-1}{\eta-1}\right) \Big/ \left(\frac{M}{\eta}\right) = \frac{\eta}{M} \tag{4}$$

where η shows the compromised bytes from the total number of bytes shared over the network. In the case of 200 replying nodes, the compromised bytes are 120.173, 153.869, 200.084, and 225.902 for SATS, PPDAS, IDAP, and ASAS, respectively. Simulation results elucidate that SATS attains 13%, 32%, and 42% fewer compromised bytes as compared with PPDAS, IDAP, and ASAS, respectively.

IX. CONCLUSION

The article presents the proposed SATS which comprises of three phases for data collection and transmission, message receiving and aggregation at AN, and data extraction at the Fog node. The proposed solution uses XOR and private key methods to securely transfer the data. SATS also uses a lightweight XOR operation instead of the expensive multiplication operation for obtaining batch keys. Furthermore, The ARMA is proposed to receive data at the AN and further aggregate the data of sensor nodes. The RME algorithm is presented to decrypt the message and perform batch verification at the Fog-Server. SATS protects against several security threats such as denial of service attacks, the man in the middle attack, and reply attacks. The proposed scheme is simulated using NS 2.35 where the TCL files are used for placement and message sending. The C files contain independent classes for configuring sensing devices, AN, and the FoG- Server. The experimental results show that the proposed scheme performs better than its competitors in terms of computation and communication cost as well as it has low storage requirements.The computational cost of the SATS scheme is 14%, 23% and 59% at AN, and at Fog Node 6.5%, 21.5% and 51% better than PPDAS, IDAP, and ASAS respectively. Communication cost of the SATS scheme is 6%, 3%, and 4% at Sensor Node, and at AN 6%, 9%, and 12% better than PPDAS, IDAP, and ASAS respectively.

CONFLICT OF INTERESTS

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 paper.

REFERENCES

[1] T. A. Ahanger and A. Aljumah, "Internet of Things: A comprehensive study of security issues and defense mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2018.

[2] N. C. Luong, D. T. Hoang, P. Wang, D. Niyato, and D. I. Kim, "Data collection and wireless communication in Internet of Things (IoT) using economic analysis and pricing models: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 4, pp. 2546–2590, 4th Quart., 2016.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[4] S. S. N. Ahmad, "Green computing: The overview of awareness, practices and responsibility among students in higher education institutes," *Technology*, vol. 9, no. 3, pp. 28–36, 2015.

[5] N. A. El-mawla, M. Badawy, and H. Arafat, "Security and key management challenges over WSN (a Survey)," *Int. J. Comput. Sci. Eng. Surv. (IJCSES)*, vol. 10, no. 1, pp. 15–34, 2019.

[6] A. Ghani, H. A. Naqvi, M. Sher, Z. S. Khan, I. Khan, and M. Saqlain, "Energy efficient communication in body area networks using collaborative communication in Rayleigh fading channel," *Telecommun. Syst.*, vol. 63, no. 3, pp. 357–370, 2015.

[7] A. Ghani, H. Naqvi, M. Sher, M. A. Khan, I. Khan, and A. Irshad, "Spread spectrum based energy efficient collaborative communication in wireless sensor networks," *PLoS ONE*, vol. 11, no. 7, 2016, Art. no. e0159069.

[8] G. Fortino, A. Guerrieri, W. Russo, and C. Savaglio, "Integration of agent-based and cloud computing for the smart objects-oriented IoT," in *Proc. IEEE 18th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2014, pp. 493–498.

[9] H. Lin and N. W. Bergmann, "IoT privacy and security challenges for smart home environments," *Information*, vol. 7, no. 3, p. 44, 2016.

[10] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer–Peer Netw. Appl.*, vol. 13, no. 1, pp. 163–174, Jan. 2020.
[11] J. Singh, R. Kaur, and D. Singh, "A survey and taxonomy on energy management schemes in wireless sensor networks," *J. Syst. Archit.*, vol. 111, Dec. 2020, Art. no. 101782.
[12] L. Bhasker, "Genetically derived secure cluster-based data aggregation in wireless sensor networks," *IET Inf. Secur.*, vol. 8, no. 1, pp. 1–7, 2014.
[13] A. Ramadhan, "A survey of security aspects for Internet of Things in healthcare," in *Information Science and Applications (ICISA)*. Singapore: Springer, 2016, pp. 1237–1247.
[14] S. Jia, S. Yang, E. Wang, and Q. Ding, "Research on stateful public key based secure data aggregation model for wireless sensor networks," *High Technol.*, vol. 23, no. 1, pp. 38–47, 2017.
[15] J. Liu, J. Han, L. Wu, R. Sun, and X. Du, "VDAS: Verifiable data aggregation scheme for Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.
[16] S. O. Ogundoyin and S. O. Awoyemi, "EDAS: Efficient data aggregation scheme for Internet of Things," *J. Appl. Secur. Res.*, vol. 13, no. 3, pp. 347–375, Jul. 2018.
[17] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 712–719, Jan. 2018.
[18] Z. Wang, "An identity-based data aggregation protocol for the smart grid," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2428–2435, Oct. 2017.
[19] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4755–4763, Jun. 2019.
[20] T. Wang, Y. Li, G. Wang, J. Cao, M. Z. A. Bhuiyan, and W. Jia, "Sustainable and efficient data collection from WSNs to cloud," *IEEE Trans. Sustain. Comput.*, vol. 4, no. 2, pp. 252–262, Apr. 2019.
[21] N. Yang, X. Fan, D. Puthal, X. He, P. Nanda, and S. Guo, "A novel collaborative task offloading scheme for secure and sustainable mobile cloudlet networks," *IEEE Access*, vol. 6, pp. 44175–44189, 2018.
[22] H. Q. Qadori, Z. A. Zukarnain, M. A. Alrshah, Z. M. Hanapi, and S. Subramaniam, "CMIP: Clone mobile-agent itinerary planning approach for enhancing event-to-sink throughput in wireless sensor networks," *IEEE Access*, vol. 6, pp. 71464–71473, 2018.
[23] T. Salam, W. U. Rehman, X. Tao, Y. Chen, and P. Zhang, "A trust framework based smart aggregation for machine type communication," *Sci. China Inf. Sci.*, vol. 60, no. 10, pp. 1–15, Oct. 2017.
[24] S. Abbasian Dehkordi, K. Farajzadeh, J. Rezazadeh, R. Farahbakhsh, K. Sandrasegaran, and M. Abbasian Dehkordi, "A survey on data aggregation techniques in IoT sensor networks," *Wireless Netw.*, vol. 26, no. 2, pp. 1243–1263, Feb. 2020.
[25] S. Han, S. Zhao, Q. Li, C.-H. Ju, and W. Zhou, "PPM-HDA: Privacy-preserving and multifunctional health data aggregation with fault tolerance," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1940–1955, Sep. 2016.
[26] B. O. Soufiene, A. A. Bahattab, A. Trad, and H. Youssef, "Lightweight and confidential data aggregation in healthcare wireless sensor networks," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 4, pp. 576–588, Apr. 2016.
[27] M. Naghibi and H. Barati, "SHSDA: Secure hybrid structure data aggregation method in wireless sensor networks," *J. Ambient Intell. Humanized Comput.*, vol. 12, no. 12, pp. 10769–10788, Dec. 2021.
[28] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Gener. Comput. Syst.*, vol. 95, pp. 382–391, Jun. 2019.
[29] E. Hasheminejad and H. Barati, "A reliable tree-based data aggregation method in wireless sensor networks," *Peer–Peer Netw. Appl.*, vol. 14, no. 2, pp. 873–887, Mar. 2021.
[30] A. Seyfollahi and A. Ghaffari, "Reliable data dissemination for the Internet of Things using Harris hawks optimization," *Peer–Peer Netw. Appl.*, vol. 13, no. 6, pp. 1886–1902, Nov. 2020.
[31] T. Wang, Y. Mei, X. Liu, J. Wang, H.-N. Dai, and Z. Wang, "Edge-based auditing method for data security in resource-constrained Internet of Things," *J. Syst. Archit.*, vol. 114, Mar. 2021, Art. no. 101971.
[32] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," *J. Netw. Comput. Appl.*, vol. 190, Sep. 2021, Art. no. 103118.
[33] T. Wang, P. Wang, S. Cai, X. Zheng, Y. Ma, W. Jia, and G. Wang, "Mobile edge-enabled trust evaluation for the Internet of Things," *Inf. Fusion*, vol. 75, pp. 90–100, Nov. 2021.
[34] A. D. Rubin and P. Honeyman, "Nonmonotonic cryptographic protocols," in *Proc. Comput. Secur. Found. Workshop VII*, Jun. 1994, pp. 100–116.

GHAWAR SAID received the B.Sc. degree from the University of Peshawar, in 2004, the M.C.S. degree from Hazara University, in 2007, and the M.S.C.S. degree from International Islamic University Islamabad, Pakistan, in 2014, where he is currently pursuing the Ph.D. degree. He is currently working as a Lecturer with the Department of Computer Science, Federal Urdu University Islamabad. His research interests include MANET, WSN, the IoT, healthcare, and security solutions.

ANWAR GHANI received the B.S. degree in computer science from the University of Malakand, Khyber Pakhtunkhwa, Pakistan, in 2007, and the M.S. and Ph.D. degrees in computer science from the Department of Computer Science and Software Engineering, International Islamic University Islamabad, in 2011 and 2016, respectively. He worked as a Software Engineer at Bioman Technologies, from 2007 to 2011. He is currently a Faculty Member of the Department of Computer Science & Software Engineering, International Islamic University Islamabad. He was selected as an Exchange Student under—EURECA Program, in 2009, with VU University Amsterdam Netherland, and the EXPERT Program, in 2011, with Masaryk University Czech Republic, funded by European Commission. His research interests include wireless sensor networks, next generation networks, information security, and energy efficient collaborative communication.

ATA ULLAH received the B.S. and M.S. degrees in computer science from COMSATS University Islamabad, Pakistan, in 2005 and 2007, respectively, and the Ph.D. degree in computer science from International Islamic University Islamabad (IIUI), Pakistan, in 2016. He has been an Assistant Professor/the Head of ITCON, National University of Modern Languages (NUML), Islamabad, Pakistan, since 2008. He was at USTB, China, from 2017 to 2018. His research interests include WSN, the IoT, IoV, and MANET.

MUHAMMAD AZEEM received the M.S. degree from the Department of Computer Science, Faculty of Engineering and Computer Science, National University of Modern Languages, Islamabad, Pakistan, in 2021. He is currently pursuing the Ph.D. degree in computer science with the Department of Computer Science, International Islamic University, Islamabad, Pakistan. He has published papers at international conferences and journals. His research interests include *ad-hoc* networks, data aggregation, data dissemination, healthcare, the Internet of Things, and fog computing.

MUHAMMAD BILAL (Senior Member, IEEE) received the B.Sc. degree in computer systems engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2008, the M.S. degree in computer engineering from Chosun University, Gwangju, South Korea, in 2012, and the Ph.D. degree in information and communication networks engineering from the School of Electronics and Telecommunications Research Institute (ETRI), Korea University of Science and Technology, in 2017. From 2017 to 2018, he was with Korea University, where he was a Postdoctoral Research Fellow with the Smart Quantum Communication Center. In 2018, he joined the Hankuk University of Foreign Studies, South Korea, where he is currently working as an Associate Professor with the Division of Computer and Electronic Systems Engineering. He is the author/coauthor of over 70 SCI(E) articles published in renowned journals, including IEEE Internet of Things Journal, IEEE Systems Journal, IEEE Transactions on Industrial Informatics, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Vehicular Technology, and IEEE Transactions on Network Science and Engineering. His research interests include cyber security, the Internet of Things, named data networking, metaverse, artificial intelligence, and edge computing. He was a Technical Program Committee Member on many international conferences, including the IEEE VTC, the IEEE ICC, and the IEEE CCNC. He serves as an Editor for the IEEE Future Directions Newsletter: Technology Policy and Ethics and the IEEE Internet Policy Newsletter.

KYUNG SUP KWAK (Life Senior Member, IEEE) received the Ph.D. degree from the University of California. He worked at Hughes Network Systems and the IBM Network Analysis Center, USA. Since then, he has been a Professor with Inha University, South Korea. He worked as the Dean of the Graduate School of Information Technology and Telecommunications and the Director of the UWB Wireless Communications Research Center. In 2006, he served as the President of the Korean Institute of Communication Sciences (KICS), and in 2009, the President of the Korea Institute of Intelligent Transport Systems (KITS). He received official commendations for achievements of UWB Radio Technology Research and Development from the Korean President, in 2009. In 2008, he was appointed as an Inha Fellow Professor (IFP). He is currently an Inha Hanlim Fellow Professor. His research interests include UWB radio systems, wireless body area network/u-health networks, nano, and molecular communications.