Received December 26, 2020, accepted January 12, 2021, date of publication January 19, 2021, date of current version January 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3052850

Secure Healthcare Data Aggregation and Transmission in IoT–A Survey

ATA ULLAH[1], MUHAMMAD AZEEM[1], HUMAIRA ASHRAF[2], ABDULELLAH A. ALABOUDI[3], MAMOONA HUMAYUN[4], AND NZ JHANJHI[5]

[1]Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan
[2]Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad 44000, Pakistan
[3]College of Computer Science, Shaqra University, Shaqra 11961, Saudi Arabia
[4]Department of Information systems, College of Computer and Information Sciences, Sakaka, Saudi Arabia
[5]School of Computer Science and Engineering (SCE), Taylor's University, Subang Jaya 47500, Malaysia

Corresponding authors: NZ Jhanjhi (noorzaman.jhanjhi@taylors.edu.my) and Ata Ullah (aullah@numl.edu.pk)

ABSTRACT Internet of medical things (IoMT) is getting researchers' attention due to its wide applicability in healthcare. Smart healthcare sensors and IoT enabled medical devices exchange data and collaborate with other smart devices without human interaction to securely transmit collected sensitive healthcare data towards the server nodes. Alongside data communications, security and privacy is also quite challenging to securely aggregate and transmit healthcare data towards Fog and cloud servers. We explored the existing surveys to identify a gap in literature that a survey of fog-assisted secure healthcare data collection schemes is yet contributed in literature. This paper presents a survey of different data collection and secure transmission schemes where Fog computing based architectures are considered. A taxonomy is presented to categorize the schemes. Fog assisted smart city, smart vehicle and smart grids are also considered that achieve secure, efficient and reliable data collection with low computational cost and compression ratio. We present a summary of these scheme along with analytical discussion. Finally, a number of open research challenges are identified. Moreover, the schemes are explored to identify the challenges that are addressed in each scheme.

INDEX TERMS IoT, healthcare, smart medical devices, fog computing, data aggregation, security, compression.

I. INTRODUCTION

Internet of Things (IoT) comprise of smart devices to exchange information with each other [1]. Multiple intelligent sensory elements and wearable smart devices contribute to develop IoT [2] and play a vital role in fields like healthcare, mining, buildings, cities, agriculture, transportation, Industries and automated systems [3]. In healthcare, smart medical devices connect peoples and smart objects which makes life easy and simple [4]. Internet of Medical Things (IoMT) is becoming an essential element in healthcare. It provides smart services for healthcare by collecting various types of information and transmitting it to cloud repositories [5], [6]. IoMT joins everything in smart healthcare. Therefore, a green [7] solution is required to overcome the several challenging issues in recent strategies of IoT based smart healthcare [8]. Medical devices provide remote monitoring of patient to improve the quality and efficiency of patient medical treatment [9]. Patient sensor devices transmit health information to nearby smart collector devices or servers. Medical networks ensure patient safety, organize patient information and provide timely critical health information in emergency situations [10]. In the application of healthcare, many miniaturized devices are exploited for healthcare data collection. Hence, their secure transmissions should be also discussed. For example, [11] proposes secure transmission protocols in wearable devices. Reference [12] develops an effective authentication scheme for promising battery-free implanted devices on human bodies. In this Context, cyber physical systems (CPS) are also used in social services, especially in healthcare-based applications. It enhances the quality of medical care and extensively reduces the healthcare cost [13]. In health monitoring, patients' health related data is transmitted towards the cyber world to process and analyze huge amounts of data in real time [14]. In this situation, an improved computing frameworks are required to dynamically integrate both real and cyber aspects of medical cyber physical systems (MCPS) [15]. Real time monitoring

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

and feedback control services based systems in healthcare scenarios are considered as MCPS. Thus, it develops a need for the IoT enabled medical network capable of managing challenging communication requirements and handling processing of large number of users [16]. Fog computing architectures provide data computation, storage services and networking as a middle layer among cloud server and end user.

Fog based system escorts cloud computing model to the edge of the network thus enabling low latency, interoperability and local analysis as few basic attributes of Fog computing. The term "FoG server" was invented by Cisco [17]. Smart healthcare architecture [18] allows monitoring devices to interact with the patient and remotely share data to the server [19], [20]. At the edge of the network, it processes huge amount of data generated by numerous devices to reduce the bandwidth and energy consumption. It reduces the overhead at the cloud server and also balancing the load among multiple local fog nodes. It also provides local processing and storage to attain better quality and response as compared with cloud. Integration of fog and IoT provide more reliable, secure and efficient services for users [21]. Fog node locally processes data and predict intelligent decisions in emergency situation to efficiently handle the critical situation of patient health [22]. In smart healthcare systems, fog nodes with smart collector nodes at the edge of the network can be applicable because healthcare systems have attributes of low power, energy and bandwidth [23]. Fog computing and cloud computing can be an appropriate combination to overcome challenges in IoT and healthcare system [24], [25].

In IoMT, data aggregation is a requisite technique to abolish redundant health parameters of patient data and diminishing transmission cost. In data aggregation, numerous medical sensing devices collect patient data. Edge devices aggregate data from the medical sensor nodes and then send the aggregated data to the cloud server [26]. The collection of data can be categorized into two types of devices Homogeneous and Hybrid devices. Both types of devices separately transmit data to the Fog node. Moreover, mobile devices are introduced as a collector node for efficient data aggregation [27]. It is a challenging task in remote health monitoring systems because nodes are mostly located in hostile surroundings with insecure transmission medium. In such scenario, there is a possibility of malicious attacks like data modification and data forgery. There is a need for secure data aggregation while preserving the data integrity and privacy of the patient [28]. In IoT, security and privacy for sensitive data of patients is essential [29] and quite challenging in IoMT.

Secure and privacy preserved aggregated data is the main and compulsory part at both end node device and fog node [30]. Authentication [31] of edge devices is also important task to preserve the integrity of data because these devices aggregate data from sensor nodes and send it to cloud server. Security schemes in data aggregation is categorized in two types of cryptography. Firstly, asymmetric cryptography provides secure data aggregation using public and private keys for encryption and decryption. Secondly, symmetric cryptography provides secure data aggregation using single key for encrypt and decrypt data. Privacy preservation and encryption-based security plays a vital role in preserving the integrity of sensitive healthcare information [32]. Alongside security and privacy, data compression is played a significant role in healthcare data collection. The compression size of data depends upon the compression ratio. It reduces the communication, computation cost and also reduces delay while sending collected data over the edge node or cloud.

Figure 1 illustrates data aggregation in fog enabled smart healthcare and device interaction scenarios. A number of sensing devices are attached to the patient's body to collect patient's healthcare data. Sensing devices send this data to the data aggregator node like smartphones, tabs, and wearable smart devices. Smart collector nodes transmit sensitive healthcare data towards the Fog server. Compression and authentication are performed on patient data and stored locally at edge nodes. Fog node processes the data in the required format of the cloud. The cloud server acquires data from fog node and stores in cloud repositories. In the case of non-delay tolerant data, fog server transmits real-time healthcare data on a priority basis towards the cloud. Compression applies to aggregated data after that it stored at cloud repositories. Healthcare data are available at cloud servers for authenticated medical professionals or users to access specific health information. A request of authenticated user firstly received at the edge node for the required information. In case of data availability, edge nodes send necessary information to the requested device. Else, edge devices acquire requisite data from cloud repositories.

Existing surveys contribute to the literature for healthcare data aggregation in IoT based sensing devices. In survey papers [21] and [33], healthcare devices, architectures, and technologies are discussed whereas applications of fog computing are explored in [19] and [34]. These surveys do not consider security schemes during the transmission of aggregated data. In [32], [24], security was considered but IoT scenarios were not extensively explored. In case of [35] and [36], the secure data collection and aggregation scenarios were discussed but fog-assisted approached were not considered. In [37] and [38], secure data sharing with fog computing support but the limitations and challenges were not explicitly explored. Most of the healthcare-based fog approaches are considered for appropriate functionality and usability. In this context, the security of fog based healthcare systems often ignore. The motivation of this paper is to consider the IoMT security threads, feasible solutions, and future concerns. Moreover, it also considers the influence of security while aggregating and transmitting healthcare information. Recently, the fog assisted approached are taking growing interest of researchers due to its benefits for reducing transmission delays while accessing or storing data at cloud repositories. We have identified the gap that fog assisted schemes for secure data collection, aggregation, and transmission are still needed in literature where the limitations

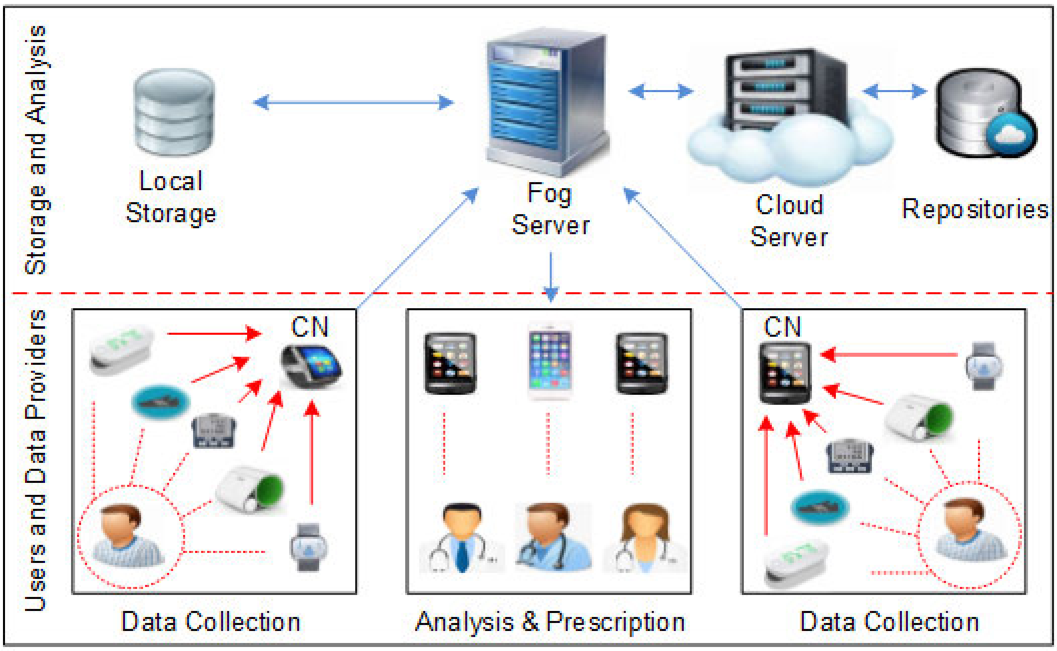

FIGURE 1. Data aggregation in smart healthcare devices.

and open research challenges are also explored. The main contributions of our work are as follows.

1) An extensive review is performed to evaluate secure and efficient data aggregation schemes in IoT.
2) Highlighting the healthcare scenarios with IoT. A summary of existing surveys is explored in Table 1 to identify the gap for our work.
3) Furthermore, we provide analytical review of secure aggregation schemes in the literature.
4) A taxonomy is presented to explore the flow and categorization of the literature.
5) Finally, we identified numerous open research challenges and then verified that how many schemes in literature have addressed these challenges.

The rest of the paper is organized as follows; Section 2 explores the literature review of data collection, aggregation and transmission schemes that also consider security. In Section 3, we present the analytical discussion of dominating studies where a summary of these scheme is also presented in a tabular format. Section 4 presents open research challenges and Section 6 conclude our work.

II. LITERATURE REVIEW

This section, we formulate a taxonomy for different secure aggregation schemes shown in Figure 2. Presented taxonomy of secure schemes divided into three sections like secure Fog based data aggregation schemes, secure data aggregation schemes in healthcare and secure data aggregation schemes using fog computing in healthcare. In this section, we have also focused on the different basic issues of secure data aggregation and data dissemination while using fog node. Fog computing support mobility for providing efficient and smooth communication at remote locations.

A. SECURE FOG BASED DATA AGGREGATION

IoT security from a data perspective is categorized security in three different aspects like One-stop, Multi-stop, and End-stop aspects [32]. In the one-stop dimension data aggregated by one endpoint node and send it over the internet and received from the internet [43]. In this perspective, lightweight crypto is a need for a security perspective and a trusted environment for the data transition to the internet. In the multi-stop aspect, multiple groups of devices remain connected with the internet or a local network. This situation leads to the need for secure communication among several nodes. In the end-stop aspect, the applications are based on different aspects like smart home and smart healthcare [44]. These aspects provide privacy, forensics, and social or legal challenges for a researcher to formulate an effective solution for these issues. An anonymous and secure aggregation scheme (ASAS) presents a model not only for data aggregation from terminal nodes but also protect the identity of end nodes. It implements pseudonyms and homomorphic encryption techniques to assure the privacy of data. While preserving the integrity of data, end node devices anonymously transmit data to the fog node and assist the end node data over the cloud server. The presented scheme saves the bandwidth from Fog to cloud while applying data aggregation techniques [45]. A lightweight privacy-preserving data aggregation (LPDA) Scheme combines the Homomorphic Paillier encryption and the Chinese Remainder Theorem. Moreover, it aggregates

TABLE 1. Summary of surveys on secure data aggregation based scheme.

Main focus of Survey	Description
Systematic review on enabling technologies of personalized healthcare system in IoT.	Jun et al. [39] explore evolving technologies that move healthcare towards personalized health care system. A systematic review of IoT based personal health care system. It categorizes healthcare devices on four different layers and provides future research challenges and trends. However, requirements and future research directions not highlighted clearly.
Enabling technologies and application of healthcare architecture in IoT.	Hossein et al. [33] conduct a systematic literature review on main healthcare application like elements of healthcare architectures, IoT based technologies, and cloud-based architectures. In IoT enable smart healthcare, explored the issues, challenges but not properly discussed problem faced while aggregating healthcare data.
Comprehensive survey on Fog Computing which includes multiple architectures.	Carla et al. [19] conducted an extensive survey to highlight the importance of Fog computing in different scenarios. It is a real contribution in Fog computing and opens research questions for the researcher but not properly considering the security of fog while aggregating data.
Coherent approach with respect to Fog computing in healthcare	Frank et al. [34] present fog computing in healthcare while focuses on related case studies. It highlights the challenges and advantages of Fog. However, the limitations not explicitly highlighted.
Multi-dimensional secure data aggregation.	Jianwei et al. [32] explore IoT security in terms of three different aspects. One-stop, Multi-stop, and End-stop security aspects. Key points and limitations are not clearly explored. It also provides different challenges and how these challenges are useful for IoT are not properly highlighted.
Elaborates security, privacy and communication requirements with security threats and challenges.	Samaher et al. [40] present the WBANs, with the highly secure and privacy-preserving requirements and protocols in WBAN. In this way, it points out the communication architecture, security challenges, threats, research direction to find out different security issues. It explores solutions based on secure WBAN schemes but did not highlight the key opportunities and requirements.
Protocols for security aspects in IoT enabled healthcare.	Ramadhan et al. [35] focus on security in healthcare and addressed future work. In this way, it highlights the need for new projects or research for improving healthcare. A comparative analysis of the studies did not discuss clearly.
Security measures for data collection in terms of collector nodes and network collector nodes.	Huaqing et al. [36] discuss the security-related issue and application related to the data collection. Categorizes the objectives for the secure data aggregation only and not targeting the fog. Moreover, it provides open research directions and future work for the researchers. It does not explicitly present the limitations and future research directions.
Transition of clinic centric to patient centric treatment in medicine and healthcare.	Bahar et al. [37] discussed challenges faced while aggregating data from healthcare devices and transmit via Fog and cloud servers. It presents case study of smart glasses and Fog driven gloves to point out essential needs for healthcare in terms of scalability, security, and privacy. Future research directions and limitations are not properly explored.
Elaborates security and privacy issues with multiple healthcare techniques	Riazul et al. [38] present the IoT as a platform that work as a backbone in different healthcare techniques. The Healthcare industry trends and techniques elaborated in multi perspectives. The e-health based security and privacy risks are discussed but not considering the fog. Future research directions and open issues based on healthcare discussed but Key features, requirements, and limitations not considered.
A comprehensive study of developing IoT communication standards and technologies suitable for healthcare.	Gordana et al. [41] introduced emerging technologies for IoT-enabled healthcare applications. Several issues related to security and privacy are considered and also considered open challenging tasks for future research studies. Moreover, it emphasizes on energy-efficient wireless technologies for IoMT. However, the limitations and requirements are not explicitly highlighted.
An extensive review of IoT-enabled healthcare schemes from the perspective of security and privacy.	Jigna et al. [42] explored several blockchain-based schemes and also exploring different security and privacy concerns of IoMT by analyzing them in tabular form. Although, the advantages and limitations of presenting schemes are explored. However, challenges and issues related to data aggregation are not properly discussed.

data at a single device. Likewise, a one-way hash chain technique utilizes to avoid bad data injection threat. Edge nodes report aggregation based on C_{is} to directly obtain device D_i individual data and receiving total number of $c_{1s}, c_{2s} \dots, c_{Ns}$ from all IoT devices in time slot T_S. Fog devices utilize secret key S_{N+1} to compute hash $H\left(T_S\right)^{n.S_{N+1}}$ and executes data aggregation procedure shown in equation (1). In this scenario, Fog devices process data locally to upload filter data at the cloud storage and also perform division of devices into subgroups according to its sensing functionality. From an efficiency perspective, it minimizes the computational and communication costs up to some extent [46].

$$\begin{cases} C_s = \left(\prod_{i=1}^{N} C_{is}\right).H\left(T_S\right)^{n.S_{N+1}} \\ mac_s = h\left(C_s\,||TS||\,sk\right) \end{cases} \tag{1}$$

APPA is an anonymity and privacy based aggregation scheme. It provides an anonymous update of certificate and also preserves the integrity of data aggregated from smart devices. On the edge of the system, data is aggregated from smart sensing devices SD_s and upload this data using a transmission network towards the Fog node FN_s. It acts as a middle layer that temporarily stores data to apply local computation on the received data as per selected format of the cloud server before sending this data towards the public cloud server PCS. In equation 7, data is collected by smart devices at Fog $d_1, d_2 \dots, d_n$ at time $t\epsilon\mathbf{T}$ given in equation (2). Therefore, SD_i is the i^{th} smart device and it picks random number $r_s\epsilon Z_N^*$, C_i is comprised of $SD_i's$ pseudonym and perform computation on encrypted data where (σ_i) message digest computes smart devices SD_i, taking hash of received ciphertext in in equation above $(H_3\left(C_i\right))\,mod\ n$ and SD_i send data packet to the FN_K node given in equation (3) [47].

$$\begin{aligned} C_i &= (Pseu_{SD_i})^{d_i}.r_s^n mod\ n^2 \\ &= (g^{r_i r_j})^{d_i}.r_s^n mod\ n^2 \end{aligned} \tag{2}$$

$$SD_i \rightarrow FN_K : \{C_i\,||\sigma_i||\,Crep_{SD_i}||TS\} \tag{3}$$

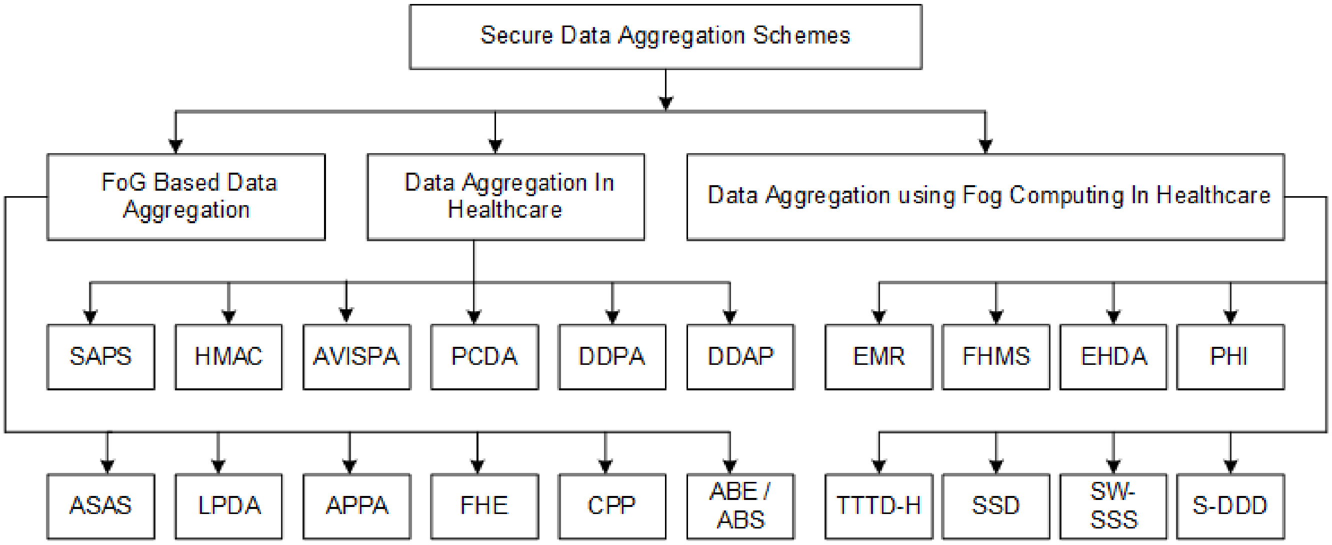
Secure Data Aggregation Schemes
FoG Based Data Aggregation
Data Aggregation In Healthcare
Data Aggregation using Fog Computing In Healthcare
SAPS
HMAC
AVISPA
PCDA
DDPA
DDAP
EMR
FHMS
EHDA
PHI
ASAS
LPDA
APPA
FHE
CPP
ABE / ABS
TTTD-H
SSD
SW-SSS
S-DDD

FIGURE 2. Taxonomy for secure data aggregation schemes.

In equation (4) and (5), data is aggregated at the Fog node, FN_K verify $(H_3 (C_i))\ mod\ n$ holds or not. If holds then it starts aggregating data with SDs using pseudonym certificate.

The term r_k represents random number selected in pseudonym generation, $(Crep_{SD_i})$ is a pseudonym certificate at smart devices as given in (6) where TS is a timestamp, message digest is calculated by $\sigma_{C_a} H_3 (C_a)\ mod\ n$ and further transmit report packet to the public cloud server [47].

$$\begin{aligned}\sum_{i=1}^{n}(C_i.Crep_{SD_i}) &= \sum_{i=1}^{n}[\left(g^{r_i r_j}\right)^{d_i}.g^{r'_i r_z})]mod\ n^2\\ &= g^{(d_1,d_2\ldots,d_n)r_j r_z}mod\ n^2 \qquad (4)\\ C_a &= \sum_{i=1}^{n}\left(C_i.Crep_{SD_i}\right).Crep_{FN_j}.g^{r'_k}\\ &= g^{(d_1,d_2\ldots,d_n)r_j r_z}.g^{r'_i r'_z r_k}.g^{r'_k}mod\ n^2\\ &= g^{\sum_{1=1}^{n} d_i}mod\ n^2 \qquad (5)\end{aligned}$$

PCS also applies computation on received data to analyze data in the context of the required format. Trusted TCA and local LCA certification authority authorities are independent agencies that preserve the integrity of data and also provide secure data transmission.

$$FN_K \rightarrow PCS : \{\sigma_{C_a}||C_a||TS||Crep_{SD_i}\} \qquad (6)$$

Although, that provides multilevel security and authentication of smart devices. However, it is a reasonable choice for the performance in limited devices scenario. In case of large no of devices, performance of APPA scheme is affected. To overcome this issue, a scalable and efficient scheme is required. It demands a real-time healthcare data transmission scheme with improved performance [47]. Abdulatif *et al.* present a secure edge of things (EoT) framework in smart healthcare. It uses fully homomorphic encryption (FHE) to preserve data privacy. Clustering-based techniques analyze large scale heterogeneous data for real-time computation and local storage at the EoT devices. A lot of devices generate data and transmit over the cloud server. EoT devices are the middle layer between the cloud and the end node devices to reduce the overhead at the cloud servers. Key generation is based on two BGV keys $secret_{key}$ and $public_{key}$. Homomorphic encryption generates ciphertext c for plaintext m where op is number of computations. BGV has following homomorphic properties in equation (7). FHE provides storage and analysis capability for encrypted data. This work applies clustering-based techniques like the K-means clustering(KMC) algorithm and Fuzzy C-Mean clustering (FCMC) algorithm for local processing at edge nodes [48].

$$m_1 op\ m_2 = DEC\ (Enc\ (m_1)\ op\ Enc\ (m_2)) \quad \forall m_1,\ m_2 \epsilon A_p \qquad (7)$$

In the time-aware and space-ware scenario, a cooperative privacy preserved scheme provides authentication and access control of data at wearable devices. The edge node utilizes MinHash authentication for privacy preservation of sensitive data with similarity determination of patient data in a space-aware scenario. At the cloud server, cyphertext base encryption allows access control and achieves an efficient data structure while using bloom filters in a time-aware scenario. This smart healthcare architecture elaborates security issues for edge and cloud-based hybrid computing and also solved these issues such as mutual authentication, privacy preservation, preserving the integrity of data. Security analysis was conducted on GNY logic to prove the correctness of the design. [49]. An (ABE/ABS) provides security and control data access with updated ciphertext in Fog computing. Moreover, utilize ciphertext policy attribute-based encryption (CP-ABE) and attribute-based signature (ABS). It provides secure access to data while using ciphertext updates and computation outsourcing. It presents attribute-based data encryption based on multiple policies. End nodes transmit ciphertext over the Fog node to perform encryption and decryption. Signing of data is performed at the Fog node to send data over cloud repositories. On the receiving side, only that user can decrypt the ciphertext whose attributes full fill the requirements of access policies. It also provides secure update ciphertext and data access control [50].

B. SECURE HEALTHCARE DATA AGGREGATION

Evolving technologies like wearable smart devices and smartphones lead healthcare towards a personalized healthcare system [51]. Wearable and smart sensing devices are becoming an essential part of our daily life cycle. Generally, IoT based personal healthcare systems divide personal health care devices into four different layers. These layers are such as application layer, data processing layer, network layer, and sensing layer. The security of a personalized healthcare system is an essential open research issue [39]. Moreover, High security and privacy based protocols are the basic requirements of WBAN [52], [53]. In this scenario, different security measures like TinySec [54] Biometric, ZigBee security service, wireless security protocol, Bluetooth security protocol, hardware encryption, and encryption techniques. Likewise, several communication architectures of IoMT are targeting the multiple aspects of security and privacy to preserve the integrity of patient data [40], [55]. Moreover, existing studies explore numerous issues and challenges in the healthcare domain and provide suitable solutions for IoMT based applications, technologies, and architectures in terms of security and interoperability.

Remote healthcare services are major contributions of IoT in healthcare [56]. In this context, security and privacy both are the main challenging issue for remote health monitoring systems [33], [57]. Therefore, SAPS provides a secure communication platform for patients and medical professionals without acknowledging their personal information. In session key generation, it attains the un-traceability and anonymity of members. It provides secure and anonymity based remote conversation between authenticated patient and healthcare professional. This research work provides a platform for privacy preserved and secure healthcare based data transmission [58]. In lightweight data aggregation schemes, security is an essential need for the deployment of e-healthcare applications. To solve this problem, apply keyed-hash message authentication (HMAC) to authenticate the integrity of data during data exchange. Registration of sensing devices based on masked identity $MSId_i$ as $MSId_i = h(Id_i||X_i)$. It calculates hash of device id value Id_i and secret key X_i. During authentication phase, authentication code is $HMAC = (MSId_i, Id_i, N)$ where N is an nonce value of sensor nodes and M at base station. Message is received at based station. Symmetric key K is established by concatenating nonce values and encrypted with X_i secret key of sensor node as $K = F(Enc(N||M, X_i))$. The base station calculates, decrypts, verifies the session key and stores in table. In this model, data collected from different sensing devices attached to the body of the patient to transmit over the edge node or base station. It provides secure aggregation of healthcare data by authenticating both sensors and base stations. In this situation, it reduces energy, communication, and computation cost along with security against different attacks. However, it applies to only device-level security for healthcare applications [59].

In a lightweight and centralized two-hop WBANs scheme, different sensors on the body of a patient transmit data at the edge nodes for aggregation. For security, it authenticates sensing data with local hub node or edge node. To attain the anonymity of data session keys are generating over the edge nodes. On the other hand, it authenticates the security of the presented model with (AVISPA). Only a few hash operations perform over the edge and sensor nodes to achieve low computational cost and energy consumption. In this case, there is no need to store any information related to the security of sensitive data over the public cloud server. Therefore, the computation of data from a security perspective performs over the edge or hub device [60]. A lightweight and priority-based compressed data aggregation scheme (PCDA) improves the efficiency of sensitive patient data transmission. It considers the efficient data aggregation over the central servers is a critical task. Thus, compression and encryption can resolve this issue at the central servers. It is using a cryptographic hash algorithm to preserve healthcare data. It contributes to the medical wireless sensor network (WSN) to compress the data for reducing communication costs. It encrypts the data for the security of collected healthcare information [61].

Ashutosh *et al.* present decentralized privacy preserved scheme in healthcare (DDPA). It highlights the security and privacy concerns related to the remote monitoring of patients. The model ensures the identity verification. Formatted data transmit to smart contracts with threshold values. These threshold values decide the patient's condition like normal or abnormal. The alert message of abnormality is transmitted to the patient and stored at cloud server as well. It presents a blockchain mechanism to manage and analyze sensitive healthcare data. Security and privacy system models are based on cryptographic primitives to make transactions of data anonymous and secure. The model utilizes both asymmetric and symmetric approaches for securing the transaction of the data [62]. DDAP scheme provides privacy preservation and dynamically distributed storage in the healthcare monitoring system. It introduces a pseudonymized architecture for dynamically distributed data storage and a dynamic query analyzer to preserve the integrity of healthcare data. The pseudonymization and anonymization methods are utilized for the privacy preservation of healthcare data. It formulates a design of a query analyzer for anonymization. Privacy constraint, using prior information $D \in R^m$ mean single data record, P probability density based set of possible joint functions p *on* R^m and A be a strategy. Moreover, P generates m-dimensional D and D' independent data records. ε mean

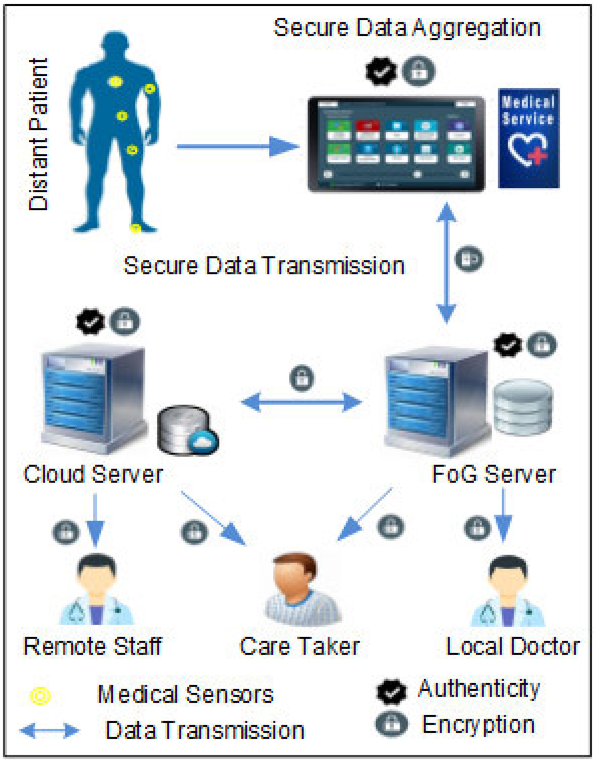

FIGURE 3. Secure data transmission and storage at FoG and cloud.

privacy budget for a differential privacy constraints are shown in equation (8) where $q \leq m$ is total number of queries, $K_1, \ldots, K_1. \varepsilon_k$ is an information available after first K queries for disclosure. Privacy constraint further divided into steps in equation (9). It provides the privacy of healthcare data while storing and data analyzers utilize for healthcare data analysis [63]. Multiple studies point out the communication architecture, privacy, security challenges and threats. Open research directions are also explored.

$$\forall Pp : Prob_P \left\{A\left(D\right) = A\left(D'\right)\right\} = \int_{D \in R^m} P\left(dD\right) \geq e^{-\varepsilon} \tag{8}$$

$$Prob_P \left\{A\left(d_{q1}, \ldots, d_{qk}\right) = A\left(d'_{q1}, \ldots, d'_{qk}\right) |A \times \left(d_{q1}, \ldots, d_{qk-1}\right) = A\left(d'_{q1}, \ldots, d'_{qk-1}\right)\right\} \geq e^{-(\varepsilon_k - \varepsilon_{k-1})} \tag{9}$$

C. SECURE DATA AGGREGATION USING FOG COMPUTING IN HEALTHCARE

Fog computing in healthcare focuses on the secure data collection and data aggregation for the local and remote patients. Security and privacy are essential to ensure confidentiality and integrity of data while transmitting sensitive medical data toward the cloud server [64] as shown in Figure 3. Patient-centric healthcare system helps in reducing clinic-centric treatment by remotely monitoring by local/remote medical staff [65]. Generally, The patient-centric healthcare system consists of a multi-layer structure [37]. In this context, fog computing faces different challenges like reducing latency, privacy, energy efficiency, bandwidth, scalability, and dependability. It is a challenging task to efficiently aggregate data from healthcare devices and locally processed data at the fog then transmitted towards the cloud server [34]. Rahul *et al.* introduce privacy preserved healthcare framework for electronic medical records (EMRs) using Fog. EMR considers privacy as a main challenging issue and focuses on preserving privacy with fast response time in the Fog assisted healthcare scenario. Edge devices, aggregate patient data then transmit it towards Fog accumulators. The identity manager uses pseudo identity for the individual identity of patient records and starts the cryptographic exchange for the security of the devices. The fog layer is a middle layer between the sensor nodes and the public cloud server. Therefore, the Fog layer has required any services from the public cloud server. In this situation, a key center provides a security key for authentication [66].

In Fog based patient health monitoring systems, data of different diseases is processed and aggregated at the edge of the network. In FHMS, sensing devices consist of wearable and non-wearable sensing devices and applications for personal health monitoring running on the edge devices. Sensitive data of the patient divides into two types of sensing data extrinsic and intrinsic. In extrinsic data of patients need the environmental sensors and intrinsic data collected by biosensors. After the local processing of data at the Fog, server data transmit towards the cloud server and store in cloud repositories. Moreover, it provides a basic level security using an encryption key but it lacks in providing proper security model [67]. The EHDA efficient healthcare data aggregation scheme provides peer to peer-based data communication of sensing devices and node to node-based data communication of collector nodes. Message receiving algorithm is used at the aggregator node to create a secure aggregated message. Aggregator nodes compress data size to reduce energy consumption and communication cost while transmitting data to fog node. At the edge node, the message extraction algorithm is utilized to extract device-level data [68].

Data compression gains a lot of attention in healthcare because of sensing devices on the body of a patient who has limited resources. Existing studies provide several compression mechanisms to reduce communication and storage costs. Robinson *et al.* present the scheme for wearable sensor networks and provide compression by combining different algorithms in sequence. It combines Huffman with LZW and analysis shows that the Huffman algorithm is stable. Moreover, LZW is better in terms of compression ratio and consumes more time. It also combines TTTD with LZW and analysis shows that TTTD has a lower compression ratio than LZW but still faster from LZW. Therefore, a new hybrid algorithm introduces by combining TTTD and Huffman algorithms in a sequence. TTTD-H improves compression and performance. It enhances performance while reducing the compression file size by utilizing the TTTD-H algorithm.

In this context, it also enhances the compression time [69]. SSD provides secure and scalable deduplication of healthcare data for statistical computations. Thus, a deterministic record linking algorithm is used to de-duplicate the horizontally partitioned healthcare data. The presented scheme targeting three main issues are efficiency, scalability, and security. From a security perspective, a semi-honest model applies to protect the identity of individuals and the integrity of data. The presented scheme is a fast and scalable scheme that protects the privacy of patient healthcare sensitive data [70].

A privacy-protecting scheme for healthcare data aggregation introduces a privacy-protection which is Slepian-Wolf-coding-based algorithm(SW-SSS). It shares data in association of multiple public cloud servers while ensuring data integrity and retransmission occurs in case of data loss. Patient data stores on multiple cloud servers in case any cloud server is compromised but the data still protected [71]. A secure deduplication and data dissemination (S-DDD) scheme introduces an adaptive chunking algorithm (ACA) to show the cut point between two windows. It reduces the communication and storage costs while using the Fog layer as a collector node and receiving duplicated values to remove redundancy on the collector node. It provides secure data exchange between smart devices and the collector nodes while using symmetric encryption [72]. Personal health information (PHI) is an encryption and deduplication based scheme for real-time data. The health physicians are authorized for treatment through a public cloud server. It utilizes Attribute-Based Encryption (ABE) along with deduplication to reduce bandwidth and storage space while sending data over the cloud server [73].

III. COMPARATIVE ANALYSIS

In this section, we present the comparative analysis of data in the tabular form. It explores basic idea, method, metrics, limitations, and strong points of the schemes. In Table 2, we provide an analytical review of those schemes discussed in the literature review in detail and elaborate them in a tabular form. In this table, we present the summary of data aggregation based schemes for healthcare. These schemes categorize into three sections. Section-I elaborates six different schemes based on secure Fog based data aggregation in healthcare. In these schemes, LPDA [46], APPA [47], ABE/ABS [50] formulate metrics for computational costs. [46], [47] also presents metrics for communication cost and FHE [48] CPP [49] construct metrics for execution time with the number of edge devices. Analysis of this section provides that those schemes are applicable in the healthcare scenario, with further minimizing the computation and computational costs with a minimum storage cost. Section-II elaborates six different schemes based on secure data aggregation schemes in healthcare. In these schemes, only SAPS [58], HMAC [59], AVISPA [60], PCDA [61] analyzed metrics while comparing with other schemes, four of them present metrics for communication costs. Low computation and storage costs are explored in [58], low computational cost and energy consumption in [59], [60], minimum energy consumption with high computation cost in [61], anonymous and secure transaction of healthcare data in [62], [63]. Section-III elaborates eight different schemes based on secure data aggregation schemes using Fog computing in healthcare. In these schemes, FHMS [67] EHDA provides metrics for energy consumption. The analysis provides that efficiency and energy consumption need to be improved to implement in the smart healthcare-based systems. Moreover, TTTD [69], SSD [70] presents metrics for compression time by taking compression time under consideration, low compression time provides efficient transmission and low latency rate. Reference [69], PHI [73] introduce metrics for file size compression. The analysis proves that if we reduce the size of data, then it also reduces the computational and storage costs.

Table 3 presents the comparative analysis of scheme where different matrices are explored in terms of low, average and high. Data aggregation schemes are studied to evaluate the security concerns in Fog assisted healthcare. We have examined the metrics of these studies in terms of High, Average, and Low, respectively. In the presenting schemes, AVISPA [60], DDPA [62], ASAS [45], and FHMS [67] provide high values in terms of communication cost and energy consumption. The main target of this paper is the security of data while aggregating. Therefore, most of the schemes provide a high level of security with minimum delay and storage cost.

IV. OPEN RESEARCH CHALLENGES

IoT enables healthcare technologies to provide a lot of benefits from a personal health perspective but many challenges still ahead like cost-effective sensing devices, advanced algorithms for lifelogging data, privacy, and security. This section explores numerous research challenges to construct efficient and secure data aggregation schemes for fog assisted IoMT. In the Healthcare domain, multiple challenging issues need to consider. However, we only target the relevant ones. In the future, there is an essential need to overcome these challenges. The COVID-19 arises the need for secure data collection and remotely monitoring the patients. Our work highlights the key challenges in the healthcare domain to provide future research direction in IoT enabled healthcare. These open research challenges are considered as follows;

A. SECURITY FOR DATA AGGREGATION

In IoMT, security is the prime technical concern for protecting connected devices and connected networks [21]. Secure network and hardware lead to secure and enhanced IoMT [74]. Trust management is a criterion in which a device considered to be secure and reliable while interacting with other devices [37]. In open networks, security is an essential need while exchanging data between the sensors and servers. It is quite difficult to avoid criminal activities who attain valuable information about the patients or perform undetectable physical attacks in open networks [60], [71], [75]. In data aggregation, third parties access the sensitive information of

TABLE 2. Summary of secure data aggregation based schemes for healthcare.

Scheme	Basic Idea	Methods	Metrics	Limitations	Strength
Secure Fog Based Data Aggregation Schemes					
ASAS [45]	Aggregates data from terminal nodes and protects the identity of end nodes using pseudonyms and using homomorphic encryption to assure the privacy of data.	It uses pseudonyms and homomorphic techniques for secure data aggregation.	Comparative analysis for time overhead with no of ciphertexts in one aggregation.	Identification and authentication enhance Computational cost at Fog node.	This novel approach provides security and anonymity efficiently.
LPDA [46]	Aggregate data at one, it filters false injected data at network edge locally before sent this data to the control center. Devices divided into a subset to take the mean and variance of each subdivision. It uses non-homogeneous (hybrid) IoT devices with security.	Homomorphic Paillier encryption, Chinese Remainder Theorem, and one-way hash chain techniques.	Communication overhead from IoT devices to Fog devices. and from Fog devices to the control center.	LPDA is time consuming.	Better Fault tolerance, efficiency, Less communication and computational cost. Comparative analysis shows the supremacy of this scheme on others.
APPA [47]	APPA supports the autonomous update of the certificate and pseudonym. It also provides privacy for aggregated data of smart devices. It applied Asymmetric keys for encryption and decryption. The essential features are privacy and security.	Paillier algorithm utilizes for generation, encryption, and decryption. Pseudonym certificate to calculate data.	Computation cost between the number of SD in Fog. Communication overhead among the number of SD in Fog node.	It provide real time communication with limited devices.	Security and privacy are implemented by local authentication at Fog nodes. Efficiently provide anonymity to preserve the integrity of the data.
FHE [48]	Clustering to analyze large scale heterogeneous data at the EoT devices. Although a lot of devices generating data and send it over the cloud. EoT is the middle layer between the cloud server and the end node devices.	KMC, FCMC Algorithms and fully homomorphic encryption are applied to store and analyze data.	Execution time with several edge devices and patients. Types of chest pain with patient age.	It increases homomorphic computational overheads and Capabilities need to be improved.	Ensures security of bio-signal data over edge devices and privacy of outsourced data from its source. Also, store or analyze encrypted data.
CPP [49]	This paper provides authentication and access control of data in time aware and space aware scenario. MinHash authentication for privacy preservation of sensitive data with similarity determination of different patients while preserving the integrity of the data in the space-aware scenario.	MinHash authentication to identify the redundant data and cyphertext base encryption for remote data excess control.	Metrics formulated for comparative analysis of different schemes for the execution time of edge computing nodes.	Computational cost increased because of local data authentication.	Strong contributions are privacy and security both at the edge node and also at cloud servers. It checks for redundant data of different patients and also ensures data integrity.
ABE / ABS [50]	This paper provides security and controls data access with an update ciphertext in Fog computing. Ciphertext policy attribute-based encryption (CP-ABE) to encrypt sensitive data and attribute-based signature (ABS) allows authenticated users to decrypt the ciphertext.	CP-ABE and ABS encrypt data with access and update policies. Encryption, description, and signing at FOG node.	Metrics presented for comparison of computational overhead with encryption decryption and signing.	Introduced architecture have high communication cost and high computational cost at the Fog node.	Security provided by encrypting sensitive data, provide secure attribute-based control data access to update ciphertext and signing computations outsourced from edge devices to Fog node.
Secure Data Aggregation Schemes In Healthcare					
SAPS [58]	Secure communication among patients and healthcare professionals with anonymity. It also provides the un-traceability of members while generating a session key.	Rubin logic for presented work & validation through simulation in NS2.35.	For storage, communication in the authentication, computational cost at user and server.	Computational overhead owing to complex operations and High transmission delays.	Security and anonymity for information sharing between healthcare consultants and patients.
HMAC [59]	It provides a secure aggregation of healthcare data by authenticating both sensors and base stations. In this way, their work reduces energy and less communication and computation costs with security against different attacks.	It uses Keyed-Hash for message integrity and authentication.	Cost analysis of energy with exchange techniques and also comparing with other protocols.	This work provides only device-level security and also applicable to a limited number of devices.	Security with less energy consumption, less communication, and computational cost as compared to AES & AES-HMAC.
AVISPA [60]	For data anonymity, session keys are generating over edge nodes. For security, it provides authentication at a local server and other devices using AVISPA.	Provides security and authentication with the local server and establishes session keys.	Comparison of energy, communication cost, and computational time.	Does not preserve the integrity of data due to the fragility of the open wireless channels.	This paper provides low computational, communication costs, and less energy consumption.
PCDA [61]	It contributes to the medical wireless sensor networks. A PCDA considers compression to reduce communication costs and utilizes encryption for the security of sensing data.	The integrity of encrypted data preserved by a cryptographic hash algorithm.	It provides less compression time, communication overhead, and energy consumption.	Average compression rate enhances cost for computations and communication.	Efficient data collection with less compression time, computational cost, and energy consumption.

TABLE 2. *(Continued.)* Summary of secure data aggregation based schemes for healthcare.

DDPA [62]	This paper formulates a block-chain mechanism to manage and analyze sensitive healthcare data. For privacy, it provides an anonymous data distribution.	Uses hashing, cryptographic mechanisms, and both types of encryption keys.	No graphs but security attacks are formulated and finds security margins.	Communication cost due to Rebroadcasting. Overlay operation rise computations.	Mitigating security & privacy risks along with limited resources.
DDAP [63]	A prototype of pseudonymization and anonymization method for privacy preservation of healthcare data. It constructed the design of a query analyzer for anonymization.	A distributed storage architecture with query analyzer for anonymization.	De-pseudonymization service provided by differential privacy analyzer	Difficult to implement.	Pseudonymization and anonymization methods are merged for data aggregation in healthcare.
Secure Data Aggregation Schemes Using Fog Computing in Healthcare					
EMR [66]	Presented work provides privacy with fast response time and less delay while comparing with other studies. This framework consists of edge devices to aggregate data of a patient and transmits it to the cloud server.	Identity token generation, token decryption algorithm, and elliptic cryptographic for confidentiality.	Transmission delay with several EMR's. Query view ratios with several EMR's.	High transmission delay and communication cost.	Framework efficiently provides privacy and security. Experimental and comparative analysis proves its efficiency in the Fog-Cloud network.
FHMS [67]	Sensing devices like wearable and non-wearable devices. Applications for personal health monitoring running on the edge devices. Sensitive data of the patient classified into two types of sensing data extrinsic and intrinsic.	In the simulation, iFogSim toolkit used for Both Fog-cloud and CloudSim toolkit only used for the cloud.	For average latency, network usage comparison, and energy consumption of fog computing versus cloud.	Dynamic changes in system topologies enhance computational cost in task distribution.	It provides minimum latency rate, low communication cost, and minimum energy consumption in the Fog-cloud scenario.
EHDA [68]	Sensing devices send data to the collector node for the compression and transmits it to the Fog node. This work uses symmetric keys for encryption and decryption and also utilizes static edge nodes, non-static aggregated nodes.	Message receiving algorithm at aggregator, message extraction algorithm at the fog, and NS-2.35 simulation tool.	Message size with communication cost. Energy consumption with sensing-aggregated nodes.	Inter-communication between edge node enhancing communication cost.	Scheme consumed less storage and energy consumption, less communication cost. Better resilience and transmission ratio.
TTTD [69]	TTTD-H algorithm combining TTTD and Huffman algorithm in sequence based on the results of TTTD and other compression algorithms. It improves compression and performance.	TTTD and Huffman algorithms execute sequentially.	Compression factor, file size, compression time, and compression with TTTD-H.	High compression time.	Presented scheme enhanced performance by reducing compressed file size and also reduce communication cost.
SSD [70]	Deterministic record linking algorithm used to deduplicate the horizontally partitioned healthcare data. Main issues are efficiency, scalability, and security.	Record linking algorithm for horizontal partition of dataset.	Analysis of time with the number of custodians and total number of records.	Enhance computational cost in partitioning.	Efficiently provides security and scalable to implement in a wide range.
SW-SSS [71]	It introduces secret sharing of data with the association of multiple public cloud servers while protecting the integrity of patient's data. Provide retransmission of data in terms of data loss.	Slepian-Wolf-coding-based algorithm for secret sharing and share repairing for the privacy of data.	No comparative analysis conducted, a collection based privacy preserved schemes.	Data storage to several cloud servers enhances the storage cost.	Provides security, access control, and reliable data transmission at cloud servers.
S-DDD [72]	ACA uses cut-point identification between two windows. It reduces communication and storage overheads at the fog layer.	Adaptive chunking Algorithm for the cut point identification.	Average chunk size to analyze the change in fixed and VLC sizes.	Complex computations at the fog node.	Less redundant data due to local processing and storage at fog for secure data sharing.
PHI [73]	A collection of real-time data as a piece of PHI and transmit that data to the authorized health physicians for treatment through the public cloud server. Security using an asymmetric approach and ABE.	ABE provides secure sharing of healthcare data from sensing devices to the cloud.	Comparative analysis of deduplication for storage cost and file uploading time at cloud.	Data integrity is not preserved in channels, more communication due to dynamic topologies.	Efficient and secure data transmission. Eliminates redundant data to decrease the storage cost and upload bandwidth.

a patient and open a gateway for different security threats [72]. Many different challenges are faced while designing security solutions in MWSNs [61]. To formulate an efficient and secure mechanism against several security threats is a challenging task [30]. Securely detect and protect data from several threats is a hot topic while transmitting sensitive data towards Fog and cloud server [73]. Malware detection and protection at Fog node in healthcare domain is an open research challenge [76]. Fog assisted systems still need to formulate suitable schemes which provide continuous protection and computation of resources to protect against malware attacks [77], [78]. A large number of edge devices are part of fog based system where any malicious device can inject malware for denial of service. Smartphones or smart devices are installed as a fog node owing to these devices easily affected by malware infection. Thus, there is a need to formulate artificial intelligent schemes or deployed malware detection devices at edge nodes to avoid these security attacks [79], [80]. Attackers target the middle layer to change the data or affect the communication of the central layer with

TABLE 3. Summary comparative analysis of schemes.

Schemes	Communication Overhead	Computational Cost	Energy Consumption	Storage	Delay	Security Level
ASAS [45]	High	Average	High	Average	High	Average
LPDA [46]	Low	Average	Average	Average	Low	High
APPA [47]	Average	Average	Average	Average	Average	High
FHE [48]	Low	Average	Average	Average	Low	High
CPP [49]	Low	Average	Average	Low	Average	High
ABE / ABS [50]	Average	Low	Low	Low	Average	High
SAPS [58]	Low	High	Average	Average	Average	High
HMAC [59]	Average	Average	Average	Low	Average	High
AVISPA [60]	High	High	High	Low	Average	High
PCDA [61]	Low	Low	Average	Average	Low	Average
DDPA [62]	High	Average	High	Low	Average	High
EMR [66]	Average	Low	Average	Average	Low	Average
FHMS [67]	High	Low	High	Average	Low	Low
EHDA [68]	Average	Average	Average	Low	High	High
TTTD [69]	Low	Low	Low	Low	Average	Low
SSD [70]	Low	Average	Average	Low	Low	High
SW-SSS [71]	High	Average	Average	Low	Average	Average
S-DDD [72]	Average	High	Low	Low	Average	High
PHI [73]	Average	High	Average	Low	Low	High

other layers. Security is a salient research problem in computing devices that are located at the edge of the network [81]. In WBAN [82], sensitive data encrypts with the ciphertext to maintaining minimal storage space and other resources [83]. However, it is a challenging task to formulate a secure system consuming fewer medical resources. IoT faces multiple challenges while aggregating data from smart devices like the availability of resources, security, and privacy concerns [84]. In this situation, sensitive medical information related to the patient can be changed. Thus, fog nodes face those security threats which do not exist in cloud architecture.

B. PRIVACY OF DATA FOR INFORMATION EXCHANGE

Privacy is a prime concern to protect the sensitive data of individuals and also protect the identity of individuals [85]. In privacy, there is a need for a standard to attain privacy of data storage, sharing, transmission, and applications in e-health [32]. Privacy preservation is a significant challenge in the communication of sensitive data and open access data for edge and cloud computing-based healthcare system [22], [49], [86]. The deployment of the Fog layer boosts the potential of IoM. In this context, these deployments introduce multiple security and privacy issues [66], [87]. Smart healthcare based IoT enabled systems mostly follow three basic steps like data collection at the sensory layer, data aggregation at the collector layer, and data analysis or processing at the Fog or cloud layer. Privacy in three basic scenarios is a necessary open research topic in healthcare [88]. In the present situation, there is a need to implement a privacy preservation mechanism to preserve the integrity of data and ensure that third parties cannot access the healthcare sensitive data [89]. In IoT, several existing privacy preservation mechanisms of data aggregation fall in different categories like anonymity based privacy preservation [45], encryption based privacy preservation [90]. The design of IoMT based privacy preserved scheme with significant data utility still a critical challenge for future research [91].

C. PRIVACY QUALITY OF SERVICES FOR HEALTHCARE DATA EXCHANGE

Quality of service(QoS) is different types of priorities for multiple application according to the requirement and ensure a certain level of performance for data transmission. In Fog based healthcare paradigm, quality of services is a major concern while transferring tasks from one node to another node with less load as compared to the first one [92]. In exchange for data from the end node to the server node, the main challenging task is to preserve the integrity of sensitive patient data [67]. In IoT, latency is the time required to send a data packet from one node device to another. Latency is known as round trip time, the total time to send and receive data from the device. Waiting time is also called latency, like a system waiting for another element to complete its processing. The quality of service depends on different aspects of performance, such as latency and bandwidth. In other words, QoS means low processing time and power consumption at the Fog node. QoS is a prime challenging issue in Fog based healthcare system.

D. SCALABILITY FOR MASSIVE DATA SHARING

Scalability represents the capability of system, network, and software application to enhance and manage the increasing demand. IoMT based network systems growing in size and network complexity can lead to scalability issues [93]. The management of resources is also a main challenging problem in Fog and cloud-based healthcare systems [94]. Scalability in networks involves increase in bandwidth and number of users. Generally, a formulated algorithm running efficiently on a small scale whereas it is challenging in large scale by ensuring reliability and efficiency [95]. Integration of a healthcare system allows professionals to remotely access the patient and also enhances the scalability and flexibility of data aggregation from remote areas. Scalability is a challenging task to provide health care services in emergency scenarios because the requirement for healthcare services is increased that leads towards the server and network breakdown [96]. An efficient and scalable healthcare system is required to overcome the increasing demand for healthcare services.

E. RESOURCE MANAGEMENT FOR MASSIVE DATA

Data management of sensitive data depends on data type, size, velocity, and a collection of a large amount of data in less possible time. Data management is itself a challenging issue and also in the smart healthcare domain. Therefore, fog computing provides a solution by managing and processing data locally at the middle layer between the smart sensing devices and the cloud storage repositories [37]. In IoT, heterogeneity belongs to a platform that permits communication and multiple types of devices using multiple protocols. Heterogeneity is also a challenging topic in Fog computing. In the healthcare paradigm, different sensing devices of multiple companies are attached to the patient's body. Moreover, every device sends separately patient data to the medical server. Implementation of heterogeneity is a challenging issue in this healthcare framework [97]. Data transmit from sensing devices to the edge node for local processing for this communication heterogeneity [98] plays a significant role because it permits this communication between end and edge nodes. In a multiuser-scenario, multiple users interact with the same resource. Accordingly, the management of resources plays a significant role in providing a minimum delay to the device user. A challenging task data offloading is overcome by using fog computing because the fog node decides which node provides minimum delay while offloading data to another server node.

F. FOG ASSISTED STORAGE REPOSITORIES

Fog server consists of sufficient storage as local repositories and large data storage as cloud repositories at the cloud server. Cloud repositories store a large amount of data [99]. Fog server helps in maintaining the most recent data in local repositories to provide real-time data transmission and local processing for decision making at the Fog node before interacting with the cloud server. Big data [100], [101] storage provides a platform for record-keeping to maintain a history of record and processed data for decision making so it can be accessed in the future [102]. The fog-enabled medical systems consist of multiple large numbers of sensing devices across the network to send real-time patient data towards the Fog node. It locally processes data and further uploads de-duplicated data over the cloud server [103]. On the other hand, medical staff requests a Fog server using smart mobile devices to access patient data [104]. Therefore, efficient data processing and storage have become a challenging issue. However, new algorithms or techniques will be needed in the future to manage the storage among the nodes.

G. DEDUPLICATION FOR HEALTHCARE DATA

Data deduplication is a procedure that removes redundant data and lowering storage costs. Data ownership management and abortion is an open research issue for secure data deduplication [105]. In a multi-user scenario, if ownership of some users removes from the ownership member list so prevent these users from accessing data after removal of their ownership to some specific data and also filter redundant data before sending it over cloud [103]. Data compression is known as bit coding [106]. In this way, the convergence of data bits in those manners consumes less space on the server [107]. A high rate of data compression ratio is a challenge to implement during data exchange between the sensor node and the edge devices [108]. In this perspective, it reduces the communication cost because of the reduced size of transmitting data [69]. Encryption based security and privacy of de-duplicated data is also a challenging research issue. One related solution to attain secure duplication is to encrypt data at the smart collector node and deduplication of data performed on the Fog server. Efficient and effective deduplication with security is a crucial open research challenge in secure deduplication [73].

H. DEDUPLICATION CONTINUOUS CONNECTIVITY SUPPORT DURING MOBILITY

It becomes a more challenging issue in the mobility of a patient. Thus, a patient is present at a location where it could not find the connectivity of the network [109]. Then, he can use the other network or other smart devices nearby for data transmission. In this case, there is an issue of security and privacy of the patient's sensitive data [110], [111]. In Fog architecture, healthcare-based sensors and data collector devices such as mobile phone devices [112] or vehicles [113], [114] act as a collector node to provide continuous connectivity support to efficiently send data from sensor nodes to Fog node while using collector node. In this scenario, a patient using a mobile device as a collector node that collects the data of different wearable sensing devices attached to the patient's body and performs multiple communications over the network [115]. Smart devices in the healthcare centre are available in remote locations. Smartphones and vehicles communication is also an open research issue in IoMT [96]. In IoT enabled healthcare systems, mobility of devices or patients is also challenging. It demands continued support of services while moving across multiple Fog nodes [116]. In the Fog node, mobility management issues require a guarantee of no interruption from provided services. There is a need for suitable techniques and schemes for efficiently handling mobility but scarce research conducted on mobility [117] and still an open research topic for future research studies.

TABLE 4. Summary of addressing challenging issues in schemes.

Schemes	Scalability	Quality of Service	Data Aggregation	Mobility	Load balancing	Heterogeneity
ASAS [45]	No	No	Yes	No	Yes	No
LPDA [46]	No	Yes	Yes	No	Yes	Yes
APPA [47]	No	Yes	Yes	Yes	Yes	Yes
FHE [48]	Yes	No	Yes	No	Yes	Yes
CPP [49]	No	No	Yes	No	Yes	No
ABE / ABS [50]	Yes	No	Yes	Yes	Yes	Yes
SAPS [58]	Yes	No	Yes	Yes	Yes	Yes
HMAC [59]	Yes	No	Yes	Yes	No	Yes
AVISPA [60]	Yes	No	Yes	Yes	No	Yes
PCDA [61]	Yes	Yes	Yes	No	No	No
DDPA [62]	Yes	No	Yes	Yes	Yes	Yes
DDAP [63]	No	No	Yes	No	No	Yes
EMR [66]	No	No	Yes	Yes	Yes	Yes
FHMS [67]	No	Yes	Yes	No	Yes	No
EHDA [68]	No	No	Yes	Yes	Yes	Yes
TTTD [69]	No	No	Yes	No	No	Yes
SSD [70]	Yes	Yes	No	No	No	Yes
SW-SSS [71]	Yes	Yes	Yes	Yes	Yes	Yes
S-DDD [72]	No	No	Yes	Yes	No	No
PHI [73]	No	Yes	Yes	No	No	No

I. REDUCE COMMUNICATION AND COMPUTATIONAL COST TO IMPROVE EFFICIENCY

In data aggregating, there is a need to overcome these challenges like reducing communication costs, energy consumption [61]. In smart healthcare, there is a pivotal requirement of cost-effective wearable sensing devices. In this perspective, smart devices must be rich in quality and less in cost [34]. It is a challenging issue to introduce intelligent services with the sensor node and the edge nodes during data exchange to reduce the communication cost [4], [118]. In the IoT scenario, efficiency means real-time data aggregation in minimum time with less consumption of resources. In practical use of secure multiparty computations, the main challenging issues are efficiency and scalability [70]. In the combination of intelligent processing and data-aggregation takes us toward the intelligent data collection techniques in the future. In this context, systems improve the efficiency and effectiveness of data aggregation [36], [119]. Cost reduction in terms of communication and computation while aggregating data at the Fog server is a demanding issue in the context of Fog computing [120]. Moreover, efficiency is a challenging topic for real-time data aggregation over the cloud server while using the Fog node. We observed that scarce research conducting on priority based non-delay tolerant data aggregation. In this way, there is a need to research efficient priority based data aggregation from sensor nodes to the Fog node and further upload non-delay tolerant data to cloud servers on priority bases [121]. In future work, research demands to explore new Fog based techniques and algorithms to aggregate real-time data efficiently. Table 4 explores whether the schemes have considered the identified challenges or not. It has been observed that scalability and quality of service are not considered by most of the schemes in literature. On the contrary, data aggregation, mobility, load balancing and heterogeneity are considered by most of the schemes.

J. LESSONS LEARNED

The lesson learned from reviewed schemes and research challenges are explored as follows. From the aspect of design, there is a need for effective technologies to manage the heterogeneity among the IoMT nodes, fog cloud. Another lesson is learned concerns the deficiency of suitable tracking and restructuring techniques in fog enabled healthcare systems. These mechanisms play a critical role while considering mobility and scalability but still scarce research has been considered for these mechanisms.

V. CONCLUSION

IoT is essentially important to improve the quality of human life by the interconnection of different technologies, smart devices, and applications. Healthcare schemes consider the medical architecture and its role in the physical world. In this context, smart medical devices aggregate patient data and transmit towards server nodes for analysis. It is quite challenging to securely and efficiently transmit data towards the Fog/cloud server. In this paper, we have conducted a survey of secure healthcare data collection, aggregation and transmission approaches that are categorized as per taxonomy. We have categorically presented the comparative analysis for the dominating schemes in the literature. We have focused on secure data aggregation based schemes, secure fog-assisted data collection, and healthcare schemes. By involving fog computing for healthcare data sharing, the transmission delays are reduced as compared to the only cloud approach. It can be beneficial for non-delay tolerant emergency applications in healthcare. Moreover, the compressed data collection based schemes are also explored that reduce the data size and sharing cost. Furthermore, open research challenges are identified and then verified that whether the schemes in literature addressed these challenges or not. It opens a new horizon for the researchers to resolve these issues by proposing dependable novel solutions. In the future, we shall explore the impact of software-defined networking to analyze the data before its transmission to reduce data traffic and communication costs.

REFERENCES

[1] A. K. Das, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Future Gener. Comput. Syst.*, vol. 89, pp. 110–125, Dec. 2018.

[2] B. Pourghebleh and N. J. Navimipour, "Data aggregation mechanisms in the Internet of Things: A systematic review of the literature and recommendations for future research," *J. Netw. Comput. Appl.*, vol. 97, pp. 23–34, Nov. 2017.

[3] M. Aazam, S. Zeadally, and K. A. Harras, "Fog computing architecture, evaluation, and future research directions," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 46–52, May 2018.

[4] R. Mahmud, F. L. Koch, and R. Buyya, "Cloud-fog interoperability in IoT-enabled healthcare solutions," in *Proc. 19th Int. Conf. Distrib. Comput. Netw.*, Jan. 2018, pp. 1–10.

[5] J. N. S. Rubí and P. R. L. Gondim, "IoMT platform for pervasive healthcare data aggregation, processing, and sharing based on OneM2M and OpenEHR," *Sensors*, vol. 19, no. 19, p. 4283, 2019.

[6] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdic, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, vol. 5, no. 5, pp. 3810–3822, Oct. 2018.

[7] T. Nazir and M. T. Banday, "Green Internet of Things: A survey of enabling techniques," in *Proc. Int. Conf. Automat. Comput. Eng. (ICACE)*, Oct. 2018, pp. 197–202.

[8] C. Zhu, V. C. M. Leung, L. Shu, and E. C.-H. Ngai, "Green Internet of Things for smart world," *IEEE Access*, vol. 3, pp. 2151–2162, 2015.

[9] S. Khezr, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, vol. 9, no. 9, p. 1736, 2019.

[10] M. Usak, M. Kubiatko, M. S. Shabbir, O. V. Dudnik, K. Jermsittiparsert, and L. Rajabion, "Health care service delivery based on the Internet of Things: A systematic and comprehensive study," *Int. J. Commun. Syst.*, vol. 33, no. 2, p. e4179, 2020.

[11] W. Wang, L. Yang, Q. Zhang, and T. Jiang, "Securing on-body IoT devices by exploiting creeping wave propagation," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 696–703, Apr. 2018.

[12] Z. Luo, W. Wang, J. Xiao, Q. Huang, T. Jiang, and Q. Zhang, "Authenticating on-body backscatter by exploiting propagation signatures," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 1–22, Sep. 2018.

[13] H. Dubey, A. Monteiro, N. Constant, and M. Abtahi, "Fog computing in medical Internet-of-Things: Architecture, implementation, and applications," in *Handbook of Large-Scale Distributed Computing in Smart Healthcare* (Scalable Computing and Communications). Cham, Switzerland: Springer, 2017, pp. 281–321.

[14] K. Takleef, K. Ali, M. A. Salim, and M. Wadi, "An overview of patient's health status monitoring system based on Internet of Things (IoT)," *Wireless Pers. Commun.*, vol. 114, no. 3, pp. 2235–2262, 2020.

[15] N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. S. Tavares, "Medical cyber-physical systems: A survey," *J. Med. Syst.*, vol. 42, p. 74, Mar. 2018.

[16] S. Tahir, S. T. Bakhsh, M. Abulkhair, and M. O. Alassafi, "An energy-efficient fog-to-cloud Internet of Medical Things architecture," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 5, pp. 1–13, 2019.

[17] F. Y. Okay and S. Ozdemir, "A secure data aggregation protocol for fog computing based smart grids," in *Proc. IEEE 12th Int. Conf. Compat., Power Electron. Power Eng. (CPE-POWERENG)*, Apr. 2018, pp. 1–6.

[18] L. A. Tawalbeh, R. Mehmood, E. Benkhlifa, and H. Song, "Mobile cloud computing model and big data analysis for healthcare applications," *IEEE Access*, vol. 4, pp. 6171–6180, 2016.

[19] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-Art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 416–464, 1st Quart., 2018.

[20] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear ElGamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12601–12617, 2017.

[21] Y. Yin, Y. Zeng, X. Chen, and Y. Fan, "The Internet of Things in healthcare: An overview," *J. Ind. Inf. Integr.*, vol. 1, pp. 3–13, Mar. 2016.

[22] R. Dantu, I. Dissanayake, and S. Nerur, "Exploratory analysis of Internet of Things (IoT) in healthcare: A topic modelling & co-citation approaches," *Inf. Syst. Manage.*, vol. 6, pp. 5224–5232, Apr. 2019.

[23] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: Architecture, key technologies, applications and open issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 27–42, Nov. 2017.

[24] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the Internet of Things: A Survey," *ACM Trans. Internet Technol.*, vol. 19, no. 2, pp. 1–41, 2019.

[25] N. Kshetri, "Privacy and security issues in cloud computing: The role of institutions and institutional evolution," *Telecommun. Policy*, vol. 37, nos. 4–5, pp. 372–386, 2013.

[26] M. Engineer, R. Tusha, A. Shah, and D. K. Adhvaryu, "Insight into the importance of fog computing in Internet of medical Things (IoMT)," in *Proc. Int. Conf. Recent Adv. Energy-Efficient Comput. Commun. (ICRAECC)*, Mar. 2019, pp. 1–7.

[27] W. Tang, J. Ren, K. Zhang, D. Zhang, Y. Zhang, and X. Shen, "Efficient and privacy-preserving fog-assisted health data sharing scheme," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–23, Dec. 2019.

[28] C. Guo, P. Tian, and K.-K. R. Choo, "Enabling privacy-assured fog-based data aggregation in E-healthcare systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1948–1957, Mar. 2021.

[29] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, Jan. 2015.

[30] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[31] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer authentication protocol for wireless body area networks," *Future Gener. Comput. Syst.*, vol. 78, pp. 956–963, Jan. 2018.

[32] J. Hou, L. Qu, and W. Shi, "A survey on Internet of Things security from data perspectives," *Comput. Netw.*, vol. 148, pp. 295–306, Jan. 2019.

[33] H. Ahmadi, G. Arji, L. Shahmoradi, R. Safdari, M. Nilashi, and M. Alizadeh, "The application of Internet of Things in healthcare: A systematic literature review and classification," *Universal Access Inf. Soc.*, vol. 18, no. 4, pp. 837–869, Nov. 2019.

[34] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare–a review and discussion," *IEEE Access*, vol. 5, pp. 9206–9222, 2017.

[35] A. Ramadhan, "A survey of security aspects for Internet of Things in healthcare," in *Information Science and Applications (ICISA)*, vol. 376. Singapore: Springer, 2016, pp. 1237–1247.

[36] H. Lin, Z. Yan, Y. Chen, and L. Zhang, "A survey on network security-related data collection technologies," *IEEE Access*, vol. 6, pp. 18345–18365, 2018.

[37] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Gener. Comput. Syst.*, vol. 78, pp. 659–676, Jan. 2018.

[38] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[39] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, "Advanced Internet of Things for personalised healthcare systems: A survey," *Pervas. Mobile Comput.*, vol. 41, pp. 132–149, Oct. 2017.

[40] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Informat. J.*, vol. 18, no. 2, pp. 113–122, Jul. 2017.

[41] G. Gardasevic, K. Katzis, D. Bajic, and L. Berbakov, "Emerging wireless sensor networks and Internet of Things technologies—Foundations of smart healthcare," *Sensors*, vol. 20, no. 13, p. 3619, 2020.

[42] J. J. Hathaliya and S. Tanwar, "An exhaustive survey on security and privacy issues in Healthcare 4.0," *Comput. Commun.*, vol. 153, pp. 311–335, Mar. 2020.

[43] D. Kumar and S. Chauhan, "IoT based healthcare services for monitoring post injury," in *Proc. Int. Conf. Intell. Comput. Control Syst. (ICCS)*, May 2019, pp. 293–296.

[44] P. Gope and T. Hwang, "BSN-care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors J.*, vol. 16, no. 5, pp. 1368–1376, Mar. 2016.

[45] 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.

[46] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[47] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, Jan. 2019.

[48] A. Alabdulatif, I. Khalil, X. Yi, and M. Guizani, "Secure edge of things for smart healthcare surveillance framework," *IEEE Access*, vol. 7, pp. 31010–31021, 2019.

[49] H. Liu, X. Yao, T. Yang, and H. Ning, "Cooperative privacy preservation for wearable devices in hybrid computing-based smart health," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1352–1362, Apr. 2019.

[50] Q. Huang, Y. Yang, and L. Wang, "Secure data access control with ciphertext update and computation outsourcing in fog computing for Internet of Things," *IEEE Access*, vol. 5, pp. 12941–12950, 2017.

[51] R. K. Kanth and P. Liljeberg, "Information and communication system technology's impacts on personalized and pervasive healthcare: A technological survey," in *Proc. IEEE Conf. Norbert Wiener 21st Century (21CW)*, Jun. 2014, pp. 1–5.

[52] J. Shen, Z. Gui, S. Ji, J. Shen, H. Tan, and Y. Tang, "Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks," *J. Netw. Comput. Appl.*, vol. 106, pp. 117–123, Mar. 2018.

[53] R. A. Khan, "The state-of-the-art wireless body area sensor networks: A survey," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 4, pp. 1–23, 2018.

[54] B. Mbarek and A. Meddeb, "Energy efficient security protocols for wireless sensor networks: SPINS vs TinySec," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, May 2016, pp. 1–4.

[55] T. Han, L. Zhang, S. Pirbhulal, W. Wu, and V. H. C. de Albuquerque, "A novel cluster head selection technique for edge-computing based IoMT systems," *Comput. Netw.*, vol. 158, pp. 114–122, Jul. 2019.

[56] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, "Security issues on wireless body area network for remote healthcare monitoring," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput.*, 2Jun. 010, pp. 327–332.

[57] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and privacy in implantable medical devices and body area networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 524–539.

[58] Z. Mahmood, H. Ning, A. Ullah, and X. Yao, "Secure authentication and prescription safety protocol for telecare health services using ubiquitous IoT," *Appl. Sci.*, vol. 7, no. 10, p. 1069, 2017.

[59] H. Khemissa and D. Tandjaoui, "A lightweight authentication scheme for E-Health applications in the context of Internet of Things," in *Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol.*, Sep. 2015, pp. 90–95.

[60] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, and K.-K.-R. Choo, "Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks," *Comput. Netw.*, vol. 129, pp. 429–443, Dec. 2017.

[61] 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.

[62] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[63] S. Darwish, I. Nouretdinov, and S. Wolthusen, "A dynamic distributed architecture for preserving privacy of medical IoT monitoring measurements," in *Proc. Int. Conf. Smart Homes Health Telematics (ICOST)*, 2018, pp. 146–157.

[64] H. A. Al Hamid, S. M. M. Rahman, M. S. Hossain, A. Almogren, and A. Alamri, "A security model for preserving the privacy of medical big data in a healthcare cloud using a fog computing facility with pairing-based cryptography," *IEEE Access*, vol. 5, pp. 22313–22328, 2017.

[65] M. Al Ameen, J. Liu, and K. Kwak, "Security and privacy issues in wireless sensor networks for healthcare applications," *J. Med. Syst.*, vol. 36, no. 1, pp. 93–101, Feb. 2012.

[66] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S. J. Lim, "Privacy ensured e-healthcare for fog-enhanced IoT based applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019.

[67] A. Paul, H. Pinjari, W.-H. Hong, H. C. Seo, and S. Rho, "Fog computing-based IoT for health monitoring system," *J. Sensors*, vol. 2018, Oct. 2018, Art. no. 1386470.

[68] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 1, pp. 163–174, Jan. 2020.

[69] R. Raju, M. Moh, and T.-S. Moh, "Compression of wearable body sensor network data using improved Two-Threshold-Two-Divisor data chunking algorithms," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Jul. 2018, pp. 949–956.

[70] K. Y. Yigzaw, A. Michalas, and J. G. Bellika, "Secure and scalable deduplication of horizontally partitioned health data for privacy-preserving distributed statistical computation," *BMC Med. Informat. Decis. Making*, vol. 17, no. 1, pp. 1–19, Dec. 2017.

[71] E. Luo, M. Z. A. Bhuiyan, G. Wang, M. A. Rahman, J. Wu, and M. Atiquzzaman, "PrivacyProtector: Privacy-protected patient data collection in IoT-based healthcare systems," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 163–168, Feb. 2018.

[72] A. Ullah, I. Sehr, M. Akbar, and H. Ning, "FoG assisted secure deduplicated data dissemination in smart healthcare IoT," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2018, pp. 166–171.

[73] R. S. Sharon and R. J. Manoj, "E-health care data sharing into the cloud based on deduplication and file hierarchical encryption," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2017, pp. 1–6.

[74] W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight E-Healthcare IoT devices with fair incentives," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8714–8726, Oct. 2019.

[75] M. Wazid, A. K. Das, V. Odelu, N. Kumar, M. Conti, and M. Jo, "Design of secure user authenticated key management protocol for generic IoT networks," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 269–282, Feb. 2018.

[76] T. D. Dang and D. Hoang, "A data protection model for fog computing," in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, May 2017, pp. 32–38.

[77] M. Azeem and A. Ullah, "Secure healthcare data aggregation scheme for Internet of Things," in *Proc. Int. Conf. Cyber-Living, Cyber-Syndrome Cyber-Health*, 2019, pp. 175–186.

[78] Y. Winnie, U. E., and D. M. Ajay, "Enhancing data security in IoT healthcare services using fog computing," in *Proc. Int. Conf. Recent Trends Advance Comput. (ICRTAC)*, Sep. 2018, pp. 200–205.

[79] J. Demme, M. Maycock, J. Schmitz, A. Tang, A. Waksman, S. Sethumadhavan, and S. Stolfo, "On the feasibility of online malware detection with performance counters," *ACM SIGARCH Comput. Archit. News*, vol. 41, no. 3, pp. 559–570, Jun. 2013.

[80] S. Pundir, M. Wazid, and D. P. Singh, "Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges," *IEEE Access*, vol. 8, pp. 3343–3363, 2020.

[81] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst.*, Sep. 2014, pp. 1–8.

[82] N. Bradai, L. Chaari Fourati, and L. Kamoun, "WBAN data scheduling and aggregation under WBAN/WLAN healthcare network," *Ad Hoc Netw.*, vol. 25, pp. 251–262, Feb. 2015.

[83] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, Feb. 2010.

[84] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[85] W. Ding, X. Jing, Z. Yan, and L. T. Yang, "A survey on data fusion in Internet of Things: Towards secure and privacy-preserving fusion," *Inf. Fusion*, vol. 51, pp. 129–144, Nov. 2019.

[86] V. K. Sehgal, A. Patrick, A. Soni, and L. Rajput, "Smart human security framework using Internet of Things, cloud and fog computing," *Intell. Distrib. Comput.*, vol. 321, pp. 251–263, Mar. 2015.

[87] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, Dec. 2011.

[88] X. Jia, D. He, N. Kumar, and K.-K.-R. Choo, "Authenticated key agreement scheme for fog-driven IoT healthcare system," *Wireless Netw.*, vol. 25, no. 8, pp. 4737–4750, Nov. 2019.

[89] X. Yang, X. Ren, J. Lin, and W. Yu, "On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 10, pp. 2967–2983, Oct. 2016.

[90] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system," *IEEE Trans. Ind. Informat.*, vol. 13, no. 3, pp. 1227–1237, Jun. 2017.

[91] I. Ali, E. Khan, and S. Sabir, "Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: A review," *Future Comput. Informat. J.*, vol. 3, no. 1, pp. 41–50, Jun. 2018.

[92] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, and H. H. Luo, "Security and privacy for mobile healthcare networks: From a quality of protection perspective," *IEEE Wireless Commun.*, vol. 22, no. 4, pp. 104–112, Aug. 2015.

[93] D. Wu, B. Yang, and R. Wang, "Scalable privacy-preserving big data aggregation mechanism," *Digit. Commun. Netw.*, vol. 2, no. 3, pp. 122–129, Aug. 2016.

[94] M. Al-Khafajiy, L. Webster, T. Baker, and A. Waraich, "Towards fog driven IoT healthcare: Challenges and framework of fog computing in healthcare," in *Proc. 2nd Int. Conf. Future Netw. Distrib. Syst.*, 2018, pp. 1–7.

[95] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Netw.*, vol. 153, pp. 113–131, Apr. 2019.

[96] A. S. Albahri, A. A. Zaidan, O. S. Albahri, B. B. Zaidan, and M. A. Alsalem, "Real-time fault-tolerant mHealth system: Comprehensive review of healthcare services, opens issues, challenges and methodological aspects," *J. Med. Syst.*, vol. 42, no. 8, pp. 1–56, Aug. 2018.

[97] S. Macwan, N. Gondaliya, and N. Raja, "A survey on wireless body area networks," *Wireless Netw.*, vol. 5, no. 2, pp. 107–110, 2016.

[98] H. Zhong, L. Shao, J. Cui, and Y. Xu, "An efficient and secure recoverable data aggregation scheme for heterogeneous wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 111, pp. 1–12, Jan. 2018.

[99] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: Perspectives and challenges," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 75–87, Feb. 2017.

[100] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, pp. 185–196, Aug. 2019.

[101] U. Ahsan and A. Bais, "A review on big data analysis and Internet of Things," in *Proc. IEEE 13th Int. Conf. Mobile Ad Hoc Sensor Syst. (MASS)*, Oct. 2016, pp. 325–330.

[102] S. Boubiche, D. E. Boubiche, A. Bilami, and H. Toral-Cruz, "Big data challenges and data aggregation strategies in wireless sensor networks," *IEEE Access*, vol. 6, pp. 20558–20571, 2018.

[103] Y. Shin, D. Koo, and J. Hur, "A survey of secure data deduplication schemes for cloud storage systems," *ACM Comput. Surveys*, vol. 49, no. 4, pp. 1–38, Feb. 2017.

[104] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and privacy in the medical Internet of Things: A review," *Secur. Commun. Netw.*, vol. 108, Mar. 2018, Art. no. 5978636.

[105] A. Ullah, K. Hamza, M. Azeem, and F. Farha, "Secure Healthcare data aggregation and deduplication scheme for FoG-orineted IoT," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2019, pp. 314–319.

[106] M. Amarlingam, P. K. Mishra, P. Rajalakshmi, S. S. Channappayya, and C. S. Sastry, "Novel light weight compressed data aggregation using sparse measurements for IoT networks," *J. Netw. Comput. Appl.*, vol. 121, pp. 119–134, Nov. 2018.

[107] L. Xiang, J. Luo, and A. Vasilakos, "Compressed data aggregation for energy efficient wireless sensor networks," in *Proc. 8th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2011, pp. 46–54.

[108] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "HealthDep: An efficient and secure deduplication scheme for cloud-assisted eHealth systems," *IEEE Trans. Ind. Informat.*, vol. 14, no. 9, pp. 4101–4112, Sep. 2018.

[109] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016.

[110] A. Al-Fuqaha, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[111] E. Bertino, "Data security and privacy: Concepts, approaches, and research directions," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jun. 2016, pp. 400–407.

[112] Y. Zhang, Q. Chen, and S. Zhong, "Privacy-preserving data aggregation in mobile phone sensing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 980–992, May 2016.

[113] P. Bagga, A. K. Das, S. Member, and Y. Park, "Authentication protocols in Internet of vehicles: Taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[114] C. Xu, R. Lu, H. Wang, L. Zhu, and C. Huang, "PAVS: A new privacy-preserving data aggregation scheme for vehicle sensing systems," *Sensors*, vol. 17, no. 3, p. 500, 2017.

[115] Q. Huang, L. Wang, and Y. Yang, "Secure and privacy-preserving data sharing and collaboration in mobile healthcare social networks of smart cities," *Secur. Commun. Netw.*, vol. 2017, Aug. 2017, Art. no. 6426495.

[116] X. Wang, L. Wang, Y. Li, and K. Gai, "Privacy-aware efficient fine-grained data access control in Internet of medical things based fog computing," *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[117] Q. Ren, L. Guo, J. Zhu, M. Ren, and J. Zhu, "Distributed aggregation algorithms for mobile sensor networks with group mobility model," *Tsinghua Sci. Technol.*, vol. 17, no. 5, pp. 512–520, Oct. 2012.

[118] M. Wazid, A. K. Das, S. Shetty, and M. Jo, "A tutorial and future research for building a blockchain-based secure communication scheme for Internet of intelligent things," *IEEE Access*, vol. 8, pp. 88700–88716, 2020.

[119] Y. Gai, L. Zhang, and X. Shan, "Energy efficiency of cooperative MIMO with data aggregation in wireless sensor networks," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2007, pp. 792–797.

[120] S. Sarkar, S. Chatterjee, and S. Misra, "Assessment of the suitability of fog computing in the context of Internet of Things," *IEEE Trans. Cloud Comput.*, vol. 6, no. 1, pp. 46–59, Jan. 2018.

[121] M. M. Rathore, A. Ahmad, A. Paul, J. Wan, and D. Zhang, "Real-time medical emergency response system: Exploiting IoT and big data for public health," *J. Med. Syst.*, vol. 40, no. 12, pp. 1–10, Dec. 2016.

ATA ULLAH is serving as Associate Professor at National University of Modern Languages (NUML), Islamabad, Pakistan. He received the B.S.(CS) and M.S.(CS) degrees from COMSATS Islamabad, Pakistan, in 2005 and 2007, respectively, and the Ph.D. degree in computer science from IIUI, Pakistan, in 2016. From 2007 to 2008, he was a Software Engineer with Streaming Networks, Islamabad. In 2008, he joined NUML, where he worked as an Assistant Professor and the Head of Project Committee at the Department of Computer Science until October 2017. From November 2017 to 2018, he worked as a Research Fellow with the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. In September 2018, he has rejoined NUML as an Assistant Professor/the Head ITCON. He has supervised 122 projects at undergraduate level and won one international and 45 national-level software competitions. He is awarded ICT funding for the development of projects. He has published 50 papers in ISI indexed impact factor journals and international conferences. He is also a Reviewer and a Guest Editor for journal and conference publications. His research interests include wireless sensor networks (WSNs), the Internet of Things (IoT), cyber-physical social thinking (CPST) space, health services, NGN, VoIP, and their security solutions.

MUHAMMAD AZEEM received the Master of Computer Science degree from Virtual University, Pakistan, in 2018. He is currently pursuing the M.S. degree in computer science from the Department of Computer Science, Faculty of Engineering and Computer Science, National University of Modern Languages, 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.

HUMAIRA ASHRAF received the B.S.(CS) degree from Balochistan University, Quetta, Pakistan, in 2005, the M.S.(CS) degree from BUITEMS, Quetta, in 2008, and the Ph.D. degree in computer science (with majors in cellular mobile networks and wireless networks) from International Islamic University Islamabad, Pakistan, in 2017. In 2005, she joined Sardar Bahadur Khan Women University, Quetta, as a Lecturer, where she was an Assistant Professor, from 2013 to 2016. She has been working as an Assistant Professor with the Department of Computer Science and Software Engineering, International Islamic University Islamabad, since 2017. She has published several papers in impact factor journals and international conferences. She is also a Reviewer of many ISI-indexed and impact factor journals. Her research interests include wireless sensor networks, next-generation networks, the Internet of Things, network security, IP multimedia sub-system, voice over LTE, and voice over IP.

ABDULELLAH A. ALABOUDI received the master's degree and the Ph.D. degree in computer sciences from the University of Staffordshire, U.K. He is currently working at Shaqra University, Saudi Arabia, as an Assistant Professor. He has vast experience as a Business Process Reengineer. An ample number of peer-reviewed articles are in his credit. His research interests include the Internet of Things, cybersecurity, software engineering, wireless networks, and machine learning.

MAMOONA HUMAYUN received the PhD. degree in computer architecture from the Harbin Institute of Technology, China. She has 12 years of teaching and administrative experience internationally. She has supervised various master's and Ph.D. thesis. Her research interests include global software development, requirement engineering, knowledge management, cybersecurity, and wireless sensor networks. She is an active Reviewer for a series of journals.

NZ JHANJHI is currently working as an Associate Professor with Taylor's University Malaysia. He has great international exposure in academia, research, administration, and academic quality accreditation. He worked with ILMA University and King Faisal University (KFU) for a decade. He has 20 years of teaching and administrative experience. He has an intensive background of academic quality accreditation in higher education besides scientific research activities. He had worked a decade for academic accreditation and earned ABET accreditation twice for three programs at CCSIT, King Faisal University, Saudi Arabia. He also worked for the National Commission for Academic Accreditation and Assessment (NCAAA), Education Evaluation Commission Higher Education Sector (EECHES) formerly NCAAA Saudi Arabia, for institutional-level accreditation. He also worked for the National Computing Education Accreditation Council (NCEAC). He has supervised several postgraduate students, including master's and Ph.D. students. He has edited or authored more than 20 research books with international reputed publishers, earned several research grants, and a great number of indexed research articles on his credit.

Dr. Jhanjhi has awarded as a top reviewer 1% globally by WoS/ISI (Publons) recently for the year 2019. He is an Associate Editor of IEEE Access, a moderator of IEEE TechRxiv, a keynote speaker for several IEEE international conferences globally, an External Examiner/Evaluator for Ph.D. and master's degrees for several universities, a Guest Editor of several reputed journals, a member of the editorial board of several research journals, and an active TPC Member of reputed conferences around the globe.