FOG-ORIENTED SECURE AND LIGHTWEIGHT HEALTHCARE DATA AGGREGATION IN INTERNET OF THINGS

MUHAMMAD AZEEM

NATIONAL UNIVERSITY OF MODERN LANGUAGES

THESIS AND DEFENSE APPROVAL FORM

The undersigned certify that they have read the following thesis, examined the defense, are satisfied with overall exam performance, and recommend the thesis to the Faculty of Engineering and Computer Sciences.

THESIS TITLE: FOG-ORIENTED SECURE AND LIGHTWEIGHT HEALTHCARE DATA AGGREGATION IN INTERNET OF THINGS

Submitted By: Muhammad Azeem   Registration #: 25/MS/CS/S19(Feb)

Master in Computer Science (MSCS)   Computer Science
Title of the Degree   Name of Discipline

________________________ Signature:________________________
Name of External Examiner

________________________ Signature:________________________
Name of Internal Examiner

Dr. Ata Ullah________________ Signature:________________________
Name of Research Supervisor

________________________ Signature:________________________
Name of Co-Supervisor

Dr. Sajjad Haider______________ Signature:________________________
Name of HoD (CS)

Dr. Basit Shahzad______________ Signature:________________________
Name of Dean (FE&CS)

Prof. Dr. Muhammad Safeer_______ Signature:________________________
Name of Pro-Rector Academics

July 13th, 2021

"I hereby declare that I have read this thesis and in my opinion this thesis is sufficient in terms of scope and quality for the award of the degree of Master of Science in (*Computer Science*)"

Signature : ______________________________

Name : Assoc. Prof. Dr. Ata Ullah

Date : July 13th, 2021

FOG-ORIENTED SECURE AND LIGHTWEIGHT HEALTHCARE DATA AGGREGATION IN INTERNET OF THINGS

MUHAMMAD AZEEM

A thesis submitted in fulfillment of the
requirements for the award of the degree of
Master of Science (Computer Science)

Department of Computer Sciences
National University of Modern Languages

July 2021

DECLARATION

I declare that this thesis entitled "*Fog-oriented Secure and Lightweight Healthcare Data Aggregation in Internet of Things*" is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ________________________

Name : Muhammad Azeem

Date : July 13th, 2021

This thesis work is dedicated to my parents and my teachers throughout my education career who have not only loved me unconditionally but whose good examples have taught me to work hard for the things that I aspire to achieve.

ACKNOWLEGEMENT

First of all, I wish to express my gratitude and deep appreciation to Almighty Allah, who made this study possible and successful. This study would not be accomplished unless the honest espousal that was extended from several sources for which I would like to express my sincere thankfulness and gratitude. Yet, there were significant contributors for my attained success and I cannot forget their input, especially my research supervisor, Dr. Ata Ullah, who did not leave any stone unturned to guide me during my research journey.

I shall also acknowledge the extended assistance from the administrations of Department of Computer Sciences who supported me all through my research experience and simplified the challenges I faced. For all whom I did not mention but I shall not neglect their significant contribution, thanks for everything.

ABSTRACT

Internet of things (IoT) is becoming an essential research concern because of its broad applicability in the real world. IoT-enabled wireless sensors are deployed to collect the information of patient health. In a healthcare scenario, sensor devices are placed on the body of the patient. Smart healthcare devices securely aggregate healthcare information and forward healthcare data to the base station. Sensor nodes have limited energy, computational, and storage capabilities for communication. Although, several aggregation techniques are utilized to reduce communication costs in healthcare data transmission. However, secure and lightweight data transmission of healthcare data is the main concern. This thesis explored the existing secure data aggregation schemes and presents an appropriate solution for challenging issues of existing schemes. This thesis presents an Efficient and Secure Data Transmission and Aggregation (ESDTA) scheme that provides secure and lightweight data transmission. A secure message aggregation (SMA) algorithm is employed to aggregate data at Mobile nodes (MN). Healthcare parameter values are aggregated by using the colon as a delimiter. Moreover, a secure message decryption (SMD) algorithm is employed at the fog node (FN). The proposed algorithm provides lightweight and secure data transmission by applying symmetric key-based data encryption and removing redundant healthcare parameter values from transmitted data. The simulation scenario for ESDTA proposed scheme is implemented through simulation tool NS2.35. We have compared ESDTA with existing related studies EHDA, SPPDA, APPA, and ASAS. The proposed scheme is compared with the related research studies and provide 23% better communication cost in terms of bytes exchange, 19% better computational cost, 15% better energy utilization, 57% better storage, and 32% less number of compromised bytes. Hence, results prove the sovereignty of the proposed work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ABE/ABS	-	Attribute Based Encryption / Attribute Based Signature
APPA	-	Anonymous and Privacy Preserved Data Aggregation
ASAS	-	Anonymous and Secure Aggregation Scheme
AVISPA	-	Automated Validation of Internet Security Protocols and Applications
CPP	-	Cooperative privacy preservation
CPS	-	Cyber Physical Systems
DDPA	-	Data Decentralization and Privacy based Algorithm
DDAP	-	Dynamic Distributed Architecture for Privacy
EMR	-	Electronic Medical Records
EHDA	-	Efficient Healthcare Data Aggregation
FHE	-	Fully Homomorphic Encryption
FHMS	-	Fog Based Health Monitoring System
HMAC	-	Hash message authentication
IoT	-	Internet of Things
IoMT	-	Internet of Medical Things
LPDA	-	Lightweight Privacy-preserving Data Aggregation
MCPS	-	Medical Cyber Physical Systems
PCDA	-	Priority-based Compressed Data Aggregation (PCDA)
PHI	-	Personal Health Information
SAPS	-	Secure Authentication and Prescription Safety
SDDD	-	Secure De-duplicated Data Dissemination
SSD	-	Secure and Scalable Deduplication
SW-SSS	-	Slepian-Wolf-coding-based Secret Sharing Scheme
TTTD	-	Two Thresholds Two Divisors
WBANs	-	Wireless Body Area Networks

LIST OF SYMBOLS

CD_i	-	Compressed data at sensor nodes
SK_{Fi}	-	Key among SN and FN
C_i	-	Cipher text at sensor nodes
SN_{id}	-	Sensor nodes ID
TS	-	Time stamp
N	-	Nonce value
H''	-	Hash function
RV_{MN}	-	Received data at Mobile node
E_m	-	Encrypted and compressed message at mobile node
C_m	-	Aggregated message at MN
HPV_{Ri}	-	Currently received healthcare values
HPV_{Oi}	-	Last received healthcare values
$H'(C_{i_{SD}})$	-	One-way hash function
C_{is}	-	Cipher text received from sensor node
D_i	-	Device id
S_{N+1}	-	Secure Key
$H(T_S)^{n.S_{N+1}}$	-	Secure hash function
σ_i	-	Digest Message
r_k	-	Random number generated in pseudonym
c	-	Output of the encryption
m	-	Plaintext output
op	-	The number of computations
$D \in R^m$	-	Personal data of a patient
K	-	Symmetric key
X_i	-	Secret Key

CHAPTER 1

INTRODUCTION

1.1 Overview

Internet of things (IoT) plays an essential part in different fields such as medical, construction, agriculture, industry, smart transport, and smart cities [1]. IoT is based on the number of smart devices that collaborate to forward information toward the remote servers. Remote servers store the received information in the server repositories [2]. Several smart sensor nodes play a vital part in the development of IoT. In recent research studies, researchers gaining interest in IoT-enabled wireless sensor networks [3]. In the real world, IoT works as a bridge to connect humans and smart devices to automate the several concerns of the different fields. In the healthcare domain, medical devices help to remotely observe the health condition of the patient. In this context, the health condition of the patient is continuously monitored to make health analysis and prescription procedures simple and easy [4]. Internet of medical things (IoMT) is a primary concern in recent days. Smart healthcare devices aggregate healthcare-sensitive data and forward this aggregated data toward the cloud server by using intermediate smart nodes [5],[6]. IoMT automates the healthcare domain and remotely controls the health of patients [7]. In this context, an efficient scheme is required to cover the recent aggregation-based research studies in IoMT [8]. Medical applications provide remote data access for process of real-time patient health analysis and remote prescription [9]. Smart devices are placed on the body of the patient to gather real-time health information of the patient. The collected healthcare data is forward toward the collector nodes or medical servers.

IoT-based healthcare applications provide privacy of patient data and patient identity. In an emergency scenario, IoMT applications efficiently forward sensitive health data on a priority basis [10]. Several healthcare intelligent devices are used for secure and effective data aggregation and transmission. The scheme [11] ensures the secure transmission of data from wearable healthcare sensor devices. The scheme [12] provides an authentication-based protocol for battery-less fixed devices on the patient body. In this scenario, the cyber-physical system (CPS) is mostly used in healthcare applications. Hence, CPS help to maximize the quality of medical care and minimizes the cost of health services [13]. In remote health, monitoring edge devices provide real-time data analysis, processing, and storage of large healthcare data and transmit processed data to the medical servers. [14]. In this context, a green computing protocol is required to overcome several issues of medical cyber-physical systems (MCPS) like effective real-time data analysis in critical situations [15]. MCPS is providing real-time surveillance and response-based services in the healthcare domain. Therefore, it is an essential requirement to develop an IoT Based healthcare system. To handle the communication needs in emergencies and also handle the number of requests in real-time [16]. Fog computing also plays an essential role in healthcare. Fog provides data computation and data storage at the edge of the network. It mostly acts as an intermediate layer sensor nodes and base station

The fog computing concept was introduced by Cisco [17]. The concept of fog computing provides data computation and analysis at the edge of the network. In this context, it provides low latency, less communication cost, and minimum energy consumption [18]. Fog-based intelligent healthcare architectures devices collect and analyze data at the edge of the network and forward toward the remote server for further processing and storage [19][20]. A huge amount of data generated by the number of devices at network edge fog computing provides data processing and analysis to minimize transmission cost and energy utilization. In this scenario, a load of data at the cloud server for computation and storage is balanced by the number of fog nodes that provide local storage and analysis. In Figure 1.1, smart health sensors send the healthcare parameters of the patient to the collector node. The fog node provides local data analysis and forwards processed data to the medical server for storage.

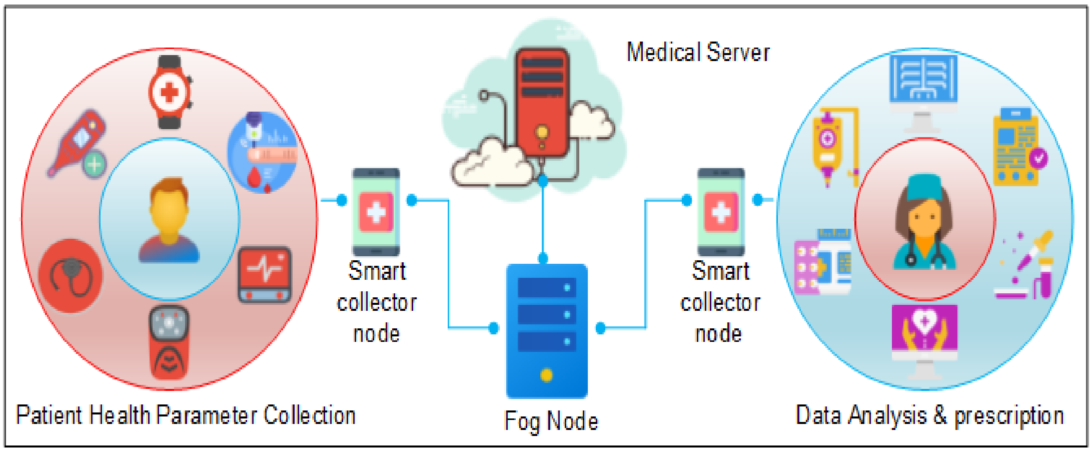

Medical Server
Smart collector node
Smart collector node
Patient Health Parameter Collection
Fog Node
Data Analysis & prescription

Figure 1.1: Healthcare data collection and analysis

A combination of IoT and fog in healthcare-based schemes provide more effective and secure services. [21]. Edge node plays an essential part in emergencies by providing real-time data analysis and predicts decisions according to the situation to effectively handle the critical health condition of the patient [22]. In most healthcare systems a mobile collector node is placed between the sensor node and fog node because healthcare-based systems have a limited number of resources [23]. The integration of fog computing and cloud computing helps to minimize several challenging issues of IoT-enabled healthcare [24][25].

In IoT-enabled healthcare systems, data aggregation is an essential technique to reduce redundant healthcare values. In this way, the size of transmitted information is reduced and transmission cost is also reduced. In the aggregation scenario, several sensor nodes collect healthcare data of the patient. Mobile nodes at the edge of the network aggregate healthcare information from the sensor nodes. After that, aggregated information forward to the medical server after processing data at the fog node as per the requirement of the medical server [26]. Smart mobile nodes are introduced as aggregator nodes for effective data collection at the edge of the network [27]. In IoMT, sensor nodes are mostly placed in a secure environment and used insecure medium for data forwarding. In this context, a chance of node capturing and data tempering is enhanced. Therefore, a secure and effective aggregation scheme is required to protect the data integrity of data and also provide handle real-time critical health information of the patient [28]. Security of data while transmitting and privacy of patient identity both are essential and the main challenging tasks in IoT-enabled healthcare. [29].

Data security is an essential aspect in the data gathering at sensor nodes, data aggregation at the mobile node, and local computation and analysis at the fog node [30]. At the Fog node, data authentication is a primary concern because these devices received aggregated information from the mobile aggregator node and further upload the data at the cloud server after local data processing [31]. Most of the security schemes used two types of data encryption like asymmetric and symmetric. In asymmetric-based encryption, data is encrypted using the public key for data encryption and the private key for data decryption. on the other hand, symmetric key-based encryption using a single key for both data encryption and decryption. Data encryption, authentication, and anonymity are the main concerns to preserve the integrity of sensitive healthcare information while transmitting in open network [32]. In healthcare-based data aggregation, data compression plays a vital role. It is as important as security and privacy while forwarding data in the network. However, the compressed size of the data is based on the compression ratio. Although, compressed data transmission minimizes the transmission cost, latency, and energy consumption.

The fog-assisted IOMT system for a secure and lightweight data aggregation is illustrated in Figure 1.2. Several wearable sensor nodes and battery-less sensor nodes are placed on the body of the patient to collect the health parameters in real-time. sensor nodes forward the collected information to the mobile aggregator node like intelligent mobile phones and wearable intelligent devices. Smart mobile nodes received the collected health parameters from the medical sensor nodes. Mobile aggregator nodes locally processed received data and send data toward the fog node.

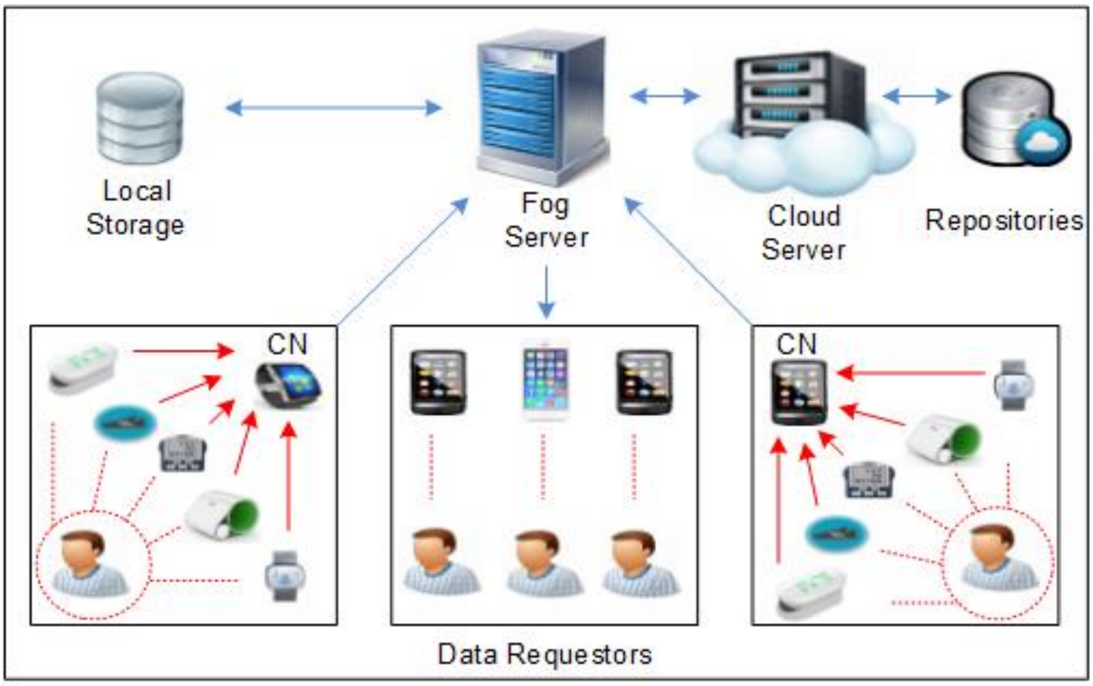


Figure 1.2: Aggregation Scenario

The fog node received the aggregated data from the mobile node and performs data compression and authentication and after that locally stores the processed information. Moreover, the fog server provide local data computation and send data to the cloud server for storage and future access. After that, forward the processed information to the cloud server for storage. In the case of critical healthcare data, fog servers predict decisions on a priority basis on real-time data and forward th is information to the cloud server on a priority to proceed further. In the case of normal data, fog nodes apply compression on the received data and forward this information to the medical server. The medical professional can access the patient information from the medical server by using a fog node after completing the authentication procedure. If the requested information is available at the fog node medical professionals can access the information directly from the fog node. Otherwise, fog nodes request the required info from the medical or cloud server then the medical. professional received the required data.

Data aggregation technique plays a vital role to reduce redundant values and energy utilization. The sensor nodes forwards collected information towards the

Mobile node. Thus, mobile node gathers healthcare parameters from several medical sensors. The transmission of gathered information to the fog server is a main issue in medical applications like remote patient monitoring and ambulance monitoring. Moreover, security of patient sensitive data is also a main concerns in IoMT. Mostly, the insecure transmission paths lead toward the different malicious attacks. Therefore, data must remain encrypted at the fog server and also in the transmission phase. In this context, effectively aggregate data while preserving the integrity of healthcare parameters and patient identity anonymity is a challenging task in IoMT. To overcome the issues discussed above for privacy and security while transmitting and aggregating the healthcare data in IoMT, we proposed an efficient and secure data transmission and aggregation (ESDTA) scheme for secure data analysis of patient health at remote location. In our proposed work data aggregated at the mobile nodes and decrypted at the fog node. In Table 1.1, discuss the healthcare scenario in the context of IoT. A summary of recent healthcare enabled data aggregation surveys are considered to identified the gap for our presented scheme [33].

Table 1.1: Review of Data Aggregation Based Surveys

Main focus of Survey	Description
Systematic review on enabling technologies of personalized healthcare system in IoT.	Jun et al. [34] 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. [35] 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. [36] 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. [37] 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. [38] 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. [39] 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. [40] 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. [41] 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. [42] 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. [43] 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.

In Table 1.1, several recent surveys discuss several aggregations-based research studies in IOMT. The [23] and [35], elaborate different techniques for remote health monitoring. Although, [19] and [36] consider the recent fog-assisted healthcare applications that target the security of patient data during transmission. However, these two surveys do not properly consider the security architectures for data forwarding. The [32], not acknowledge the concerns for IoT but different aspects of security are considered. The survey [38] and [39], discussed the data gathering at the base nodes and data aggregation at the base station but the fog scenario is not addressed in these surveys. A fog-based secure data forwarding based several research studies are elaborated in [40] and [41] surveys but the vulnerabilities and challenges are not properly discussed. The fog-enabled healthcare methods are discussed to complete some appropriate concerns. Most probably healthcare-based approaches are not properly considered a security. Therefore, the main concern of the thesis is to consider the IoT-based healthcare security concerns, effective solutions for future research studies. Moreover, also acknowledge the impact of security during data aggregation and data forwarding in the network. In the past few years, secure fog-assisted healthcare applications gaining the attention of researchers for secure data transmission of data, low latency, effective data access, and monitoring at remote locations.

1.2 Application Areas

This section includes three different application areas based on smart healthcare such as data aggregation of IoT enable healthcare data of patients in hospitals, Mobile patient monitoring, Ambulance monitoring and IoV. Discussed areas are those areas where our presented work can be applicable in future technologies.

1.2.1 IoT based data aggregation is applicable in Healthcare data for patients in hospitals

In hospitals, multiple wearables, gadgets and sensing devices are placed on the body of a patient to collect the health parameters (glucose level, blood pressure, temperature, oxygen level, heartbeat) values of the patient and edge devices are aggregate parameter values of the patient and these values further upload to the Cloud server using FoG server or directly upload to the Cloud server. In this scenario, services are utilized to develop applications and these healthcare applications are used by patient and healthcare professionals. Using Cloud and FoG approaches enable medical consultants to remotely access the health information of the patients on their smart phones and tab [37].

1.2.2 Mobile patients Monitoring

In IoT enable healthcare scenario, a patient wearable sensing devices and available at remote locations (home, market, office and somewhere else) and this data updated at the servers using collector nodes like smart phones devices or vehicles. Therefore, in many situations patients require long term monitoring required and availability of patient at hospital is not possible. In this way, smart healthcare systems provide continuous remote monitoring of patient health conditions. Using cloud services, healthcare professionals remotely access the health care records of the patients and prescribe medicines using IoT healthcare applications [34].

1.2.3 Ambulance Monitoring and IoV

In IoV, a vehicle aggregates data from the wearable healthcare device of the patient while driving. Vehicle analyzes the health condition of the patient and in case of emergency like critical condition of patient or accident occurs, vehicle can communicate with the nearby medical center and ambulance and update the healthcare condition of the patient until ambulance arrived. Ambulance also communicate with the hospital and after picking deriver ambulance also update the healthcare parameters with the hospital smart healthcare system to arrange the required equipment and medical staffs before the arrival of the patient to the hospital [44].

1.3 Research Motivation

The problem in existing schemes is the main motivation to select this research area because the transmission of the data from one cell phone/collector to other is not secure. Moreover, IoT enable smart healthcare, attain lots of attention from past few years. Personalized healthcare technologies provides a lot of benefits in personal health perspective. In present prevailing conditions, patient prefer remotely consult the medical professionals except emergency conditions. In this scenario, security of healthcare information is a significant feature of IoMT. Therefore, hiding the identity of sensing devices and preserving the integrity of the data are primary challenges in smart healthcare. Light weight and efficient transmission of sensitive healthcare data also have challenging issues. In emergency scenario, continuous connectivity and efficient communication are also challenging tasks. In this thesis the main motivation is to resolve these issues by providing reliable solutions [45].

1.4 Problems Statement

The main problem is that relaying the data from one cell phone/collector to other is unsecured. In the case of non-collaborative collectors in [46], the nearby neighbor may be the malicious node. Although, the data is encrypted using the secret key with the FoG server and the neighboring malicious node cannot directly decrypt the data but it can discard the packet instead of sharing it with the FoG server and causing a denial of service attack. Moreover, the average compression rate of the existing scheme compressed data up to only 8 bits. It transmits the redundant values that also enhances the communication and storage cost.

1.5 Research Objectives

Our research objectives are based on security of aggregated data listed as follows.

1) Provide data security for sharing of sensitive healthcare data using FoG based scheme.
2) Ensure compressed and lightweight data transmission from sensor nodes to fog node by reducing redundancy and energy consumption.
3) Protecting the healthcare data against several security threats while transmitting.
4) Reduce communication cost, computational cost, energy consumption, storage cost and enhance the resilience against node capture attacks.

1.6 Research Questions

Research questions for this research work are listed a follows;

1) RQ1: What are the key factors for securing the existing mechanism for FoG-assisted healthcare data sharing?
2) RQ2: What are the security issues and constraints for low power smart devices for aggregating and sharing the healthcare data towards FoG servers?
3) RQ3: How the message size can be reduced by excluding redundant values?
4) RQ4: What type of hash functions are used for ensuring the integrity of data during transmission?
5) RQ5: How recent studies reduce communication cost by ensuring resilience as well?

1.7 Scope of the Research Work

This study aims to provide secure data transmission and aggregation of healthcare data from end nodes to the fog server. The scope of the study is limited to medical information of patients both at the hospitals and remote locations. Moreover, this study only considers the secure data transmission of healthcare data but does not properly consider any priority-based data transmission mechanism in emergencies.

1.8 Thesis Organization

The rest of the thesis is organized as follows, an Efficient and Secure Data transmission and Aggregation (ESDTA) scheme for IoMT. ESDTA scheme provides secure and lightweight healthcare data collection and forwarding. The scheme provides Lightweight data transmission by employing data compression and removing redundant values from the data. A lightweight symmetric key-based encryption is utilized to reduce the consumption of resources. The massage compression algorithm is utilized at sensor nodes to reduce energy consumption, communication cost, and storage. Moreover, the data aggregation technique is used at mobile nodes to reduce the transmission cost.

Chapter II discusses the literature review. Chapter III illustrates the system model and objectives of the proposed scheme. Different phases of the proposed scheme are discussed in chapter IV. The performance and security analysis of the proposed solution with other existing dominating schemes is Highlighted in chapter V. Finally, Chapter VI of the thesis concludes our work and provides future research directions.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

In this section, a taxonomy is presented for security and data aggregation-based schemes as considered in Figure 2.1. In our taxonomy, we classified several secure data aggregation schemes into three sections. (i) Fog-assisted data aggregation-based research studies, (ii) Security-based research studies in healthcare, (iii) Fog-assisted data aggregation-based research works in healthcare. Furthermore, we elaborate the several concerns for secure data aggregation and transmission in fog-enabled healthcare. Taxonomy is presented to describe or classify the different data aggregation schemes. The classification of schemes helps the researchers to understand and found the diversities in considered aggregation schemes. Moreover, most of these studies consider remote monitoring. This taxonomy also targets many schemes that support the mobility of healthcare devices for effective communication among the intelligent nodes throughout the network.

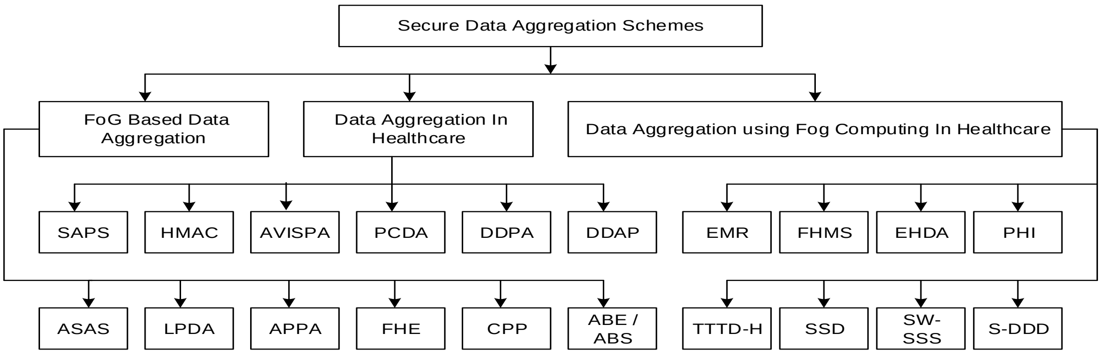

Secure Data Aggregation Schemes
FoG Based Data Aggregation
Data Aggregation In Healthcare
Data Aggregation using Fog Computing In Healthcare
SAPS
HMAC
AVISPA
PCDA
DDPA
DDAP
EMR
FHMS
EHDA
PHI
ASAS
LPDA
APPA
FHE
CPP
ABE / ABS
TTTD-H
SSD
SW-SSS
S-DDD

Figure 2.1: Taxonomy for secure data aggregation schemes

2.1.1 Secure Fog Based Data Aggregation

IoT security on the basis of data is divided into several concerns [32]. In the first concern, collection of data from one end node and upload the collected information to the server and this information can forward and access through the internet [47]. Lightweight crypto provides security and also provides secure transmission of information to the cloud server by using the internet. In the second concern, the collection of devices continuously connected with the internet and also connected with the local network. In this context, it is an essential requirement to provide secure transmission of information between the group of nodes and within a group. The third concern is based on several research studies that target intelligent healthcare architectures for the secure transmission of information. [48]. These three concerns, provide several challenges to formulate an efficient solution to overcome the challenges of the recent research studies. The (ASAS) scheme provides an anonymity-based aggregation scheme. The secure data aggregation is conducted at terminal devices. Anonymity is used to hide the identity of the end node. Pseudonyms encryption and homomorphic encryption both are utilized for the privacy of data. End nodes securely collect the data and provide data anonymity and further transmit the required data at the remote server for data storage. Moreover, it preserves the bandwidth by utilizing data aggregation techniques. [49]. The (LPDA) is a privacy-based data aggregation system to protect the transmitted information. It preserves the integrity of data by joining two encryption methods and data aggregation is conducted at a single node. A hashing technique is used to avoid the threats of malicious data injection. At edge devices the aggregation of data is based on C_{is} to get the device id D_i of a single data and the number of information received from $c_{1s}, c_{2s} \dots, c_{Ns}$ the IoT enabled nodes in time stamp T_S. Fog nodes used a secure key S_{N+1} to conduct a hash function $H(T_S)^{n.S_{N+1}}$ and performs data aggregation process as given in the equation (2.1). In this context, edge nodes analyze and process the data and purified data is uploaded at the remote servers. The devices are classified based on their purposes like data collection, data aggregation, and data analysis. It effectively reduces transmission cost, storage cost, computational cost, and energy consumption [50].

$$\begin{cases} C_s = (\prod_{i=1}^{N} C_{is}) \,.\, H(T_S)^{n.S_{N+1}} \\ \quad mac_s = h(C_s||TS||sk) \end{cases} \tag{2.1}$$

An anonymity-based data aggregation architecture (APPA) protects the information while forwarding in the network. The integrity of data is preserved and also update the security certificate anonymously. At the aggregator node, collected data of sensor nodes SD_s is received and aggregated at the aggregator node and forward the aggregated data Fog node FN_s by using secure transmission medium. Fog node is an intermediate node between the cloud server and aggregator nodes. It provide local data processing and storage and process data before forwarding the healthcare information to the public cloud server PCS. At the fog node aggregated data received from the sensor devices $d_1, d_2 \ldots, d_n$ at time $t \epsilon \boldsymbol{T}$ as shown in equation (2.2). Moreover, SD_i is the i^{th} intelligent node and select the random number $r_s \epsilon Z_N{}^*$, C_i is based on $SD_i{}'s$ and apply data computation on received encrypted information where (σ_i) digest message is conducted at the smart nodes SD_i, applying the hash on the received cyphertext $(H_3(C_i))mod\ n$ and SD_i forward data toward the fog node FN_K as given in equation (2.3) [51].

$$\begin{aligned} C_i &= (Pseu_{SD_i})^{d_i} \,.\, r_s{}^n \ mod\ n^2 \\ &= (g^{r_i r_j})^{d_i} \,.\, r_s{}^n \ mod\ n^2 \end{aligned} \tag{2.2}$$

$$SD_i \rightarrow FN_K\colon \{C_i||\sigma_i||Crep_{SD_i}||TS\} \tag{2.3}$$

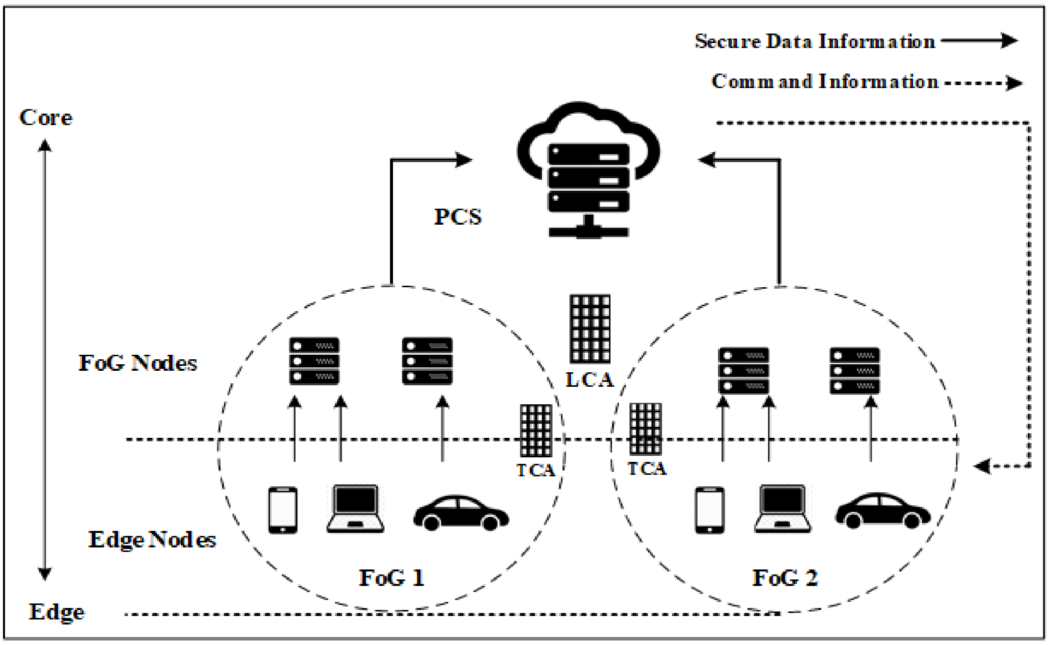


Figure 2.2: Fog based data aggregation

In equation (2.4) and (2.5), aggregation of data is computed at the fog node, FN_K prove $(H_3(C_i))mod\ n$ holds or not. If holds then, pseudonym is used to start data aggregation at the sensor node. r_k is a random number generated in the generation of pseudonym, $(Crep_{SD_i})$ is a sensor nodes certificate as shown in (2.6) . Moreover, TS denotes timestamp, digest message is collected by σ_{C_a} $H_3(C_a)$ $mod\ n$ and forward the information packet toward the public cloud server [51].

$$\sum_{i=1}^{n}(C_i\,.\,Crep_{SD_i})$$

$$= \sum_{i=1}^{n}[(g^{r_i r_j})^{d_i}\,.\,g^{r_i{}' r_z})]\ mod\ n^2$$

$$= g^{(d_1\,, d_2\ \dots, d_n\,)r_j r_z}\ mod\ n^2 \tag{2.4}$$

$$C_a = \sum_{i=1}^{n}(C_i\,.\,Crep_{SD_i})\,.\,Crep_{FN_j}\,.\,g^{r_k{}'}$$

$$= g^{(d_1\,, d_2\ \dots, d_n\,)r_j r_z}.\,g^{r_i{}' r_z{}' r_k}.\,g^{r_k{}'}\ mod\ n^2$$

$$= g^{\sum_{1=1}^{n} d_i}\ mod\ n^2 \tag{2.5}$$

At the PCS, computation is performed on the received information to examine the data in terms of a demanding format. The trusted certification authority and LCA are self-governing companies that provide data transmission while protecting the sensitive information.

$$FN_K \rightarrow\ PCS: \{\sigma_{C_a}||C_a||TS|\big|Crep_{SD_i}\big\} \tag{2.6}$$

APPA provides authentication of devices at multi-levels. In the case of limited devices, it is a wise selection for in the case of a limited number of devices. In this context, when the number of smart devices is increased the performance of APPA is a little bit reduced. A secure and efficient scheme is required to overcome the vulnerabilities of this scheme. It can be applied in the case of a large number of devices after some modifications in the scheme. [51]. The EoT is a secure architecture at the edge devices. FHE algorithm is applied to protect the patient data. It applies clustering base systems to examine the huge amount of data to provide data analysis, data processing, and data storage by the devices that on the edge of the system. The data generated by the smart devices is uploaded to the cloud server for computation and storage. The keys generation process is based on the BGV keys $secret_{key}$ and $public_{key}$. Ciphertext c is the output of the encryption, the plaintext output is denoted by m, and the number of computations are denoted by op. The properties of GGV algorithm are shown in equation (2.7). FHE algorithm received the encrypted information and perform data analysis on the data and also provide storage ability for processed data. At the edge of the network, a clustering-based procedure and FCMC algorithm provide local processing of data. [52].

$$m_1\ op\ m_2 = DEC\big(Enc(m_1)\ op\ Enc(m_2)\big)\ \forall\ m_1, m_2\ \epsilon\ A_p \tag{2.7}$$

A cooperative privacy-based scheme is discussed in both time and space-aware situations. It provides data authentication at the sensor node and also provides secure data access at the wearable devices. A MinHash authentication algorithm is employed at the edge nodes to protect sensitive healthcare data from several malicious security threads. In space aware situation, a similarity measurement of healthcare parameters of the patient. Cyphertext-supported encryption provides access control. The bloom filters are applied to obtain effective data construction in the time-aware situation. The Intelligent medical frameworks discuss security concerns both in fog and cloud computing. A solution for these concerns is provided by the healthcare architectures and these concerns are authentication, anonymity, and privacy preservation. GNY logic is used for security examination to verify the efficiency of the scheme. [53]. The ABE/ABS scheme utilized an updated ciphertext-based approach to provide fog-enabled secure data access and control. Ciphertext update is utilized to securely access the data and forwarding by preserving data integrity. The computation overhead is balance by utilizing computation outsourcing to outsource some computations. Attribute-based data encryption is conducted to encrypt and decrypt data on the basis of several policies. The ciphertext is forwarded from the sensor node to the fog node. At the fog node received data is decrypted and authentication of data and some local process are conducted and encrypt the data before forwarding it to the cloud server. In the case of attribute-based authentication, after receiving the data only authenticated can decrypt the information. Authenticated users are those users their attributes are verified the attribute requirements or complete the terms of data access methods. Therefore, it provides secure data transmission and authentication-based data access. [54].

2.1.2 Secure Healthcare Data Aggregation

Emerging IoT applications like wearable intelligent devices directed healthcare toward automated personalized healthcare systems [55]. IoT-enabled wearable smart sensors are getting a lot of attention and becoming a part of our routine life. Mostly, in the healthcare-based system security is an essential requirement, and designing efficient and secure remote health monitoring systems is a challenging task. [34]. Privacy and security both are the primary concerns for IoT-based healthcare systems [56][57]. In this context, several security protocols are utilized for the security of data while transmitting such as biometric, tiny Sec [58], encryption techniques, and security algorithms. IoMT architectures are mostly considered the various aspects of security and privacy for effective data transmission of sensitive healthcare information in the network [59][37]. The recent healthcare studies examine several challenging issues in the healthcare field. There is a need to overcome these challenging issues by providing an effective system that provides the solution for exciting issues in the IoMT based architectures. Moreover, suitable healthcare applications are design based on security and privacy requirements.

The remote monitoring of patient health conditions is a primary concern in IoMT. Healthcare applications provide continuous health monitoring and a prescription of a patient at a remote location [60]. In this scenario, both security and privacy are the essential concerns to provide effective health monitoring in remote regions [35][61]. The SAPS introduces a secure and anonymity-based communication model that provides secure health monitoring by hiding the identity of both patient and medical experts. Therefore, it provides anonymity while generating the session keys to hide the identity of the participants. Moreover, a secure anonymity-based remote communication by hiding the identity of both patient and the medical expert. Only authenticated patients and doctors can take a part in the remote health monitoring session. It preserves the integrity of and identity of the patient and doctor while transmitting data to the medical servers [62]. In healthcare applications, security is an essential need. Hence, a secure and lightweight aggregation protocol is discussed. It employs a key and hash-based authentication algorithm that is utilized to validate the data during the transmission of data. The registration phase of sensor node is depend on the masked identities such as $MSId_i$ as $MSId_i = h\ (Id_i||\ X_i)$. The hash of both id value Id_i and secret key X_i are first calculated. A authentication code is $HMAC = (MSId_i, Id_i, N)$ is used to authenticate the sensor nodes and only authenticated nodes forward the collected information to the base station. Moreover, N is an nonce value and M is the received message at the BS. A symmetric key K is constructed by concatenating nonce values and encrypted these values with X_i. The secret key generation for smart sensor node is defined as $K = F(Enc(N\ ||\ M,\ X_i))$. The encrypted message is received at the base station. It decrypts the received message using the symmetric key and performs computations on the data and after that stores this information into the table. An authentication base data aggregation for healthcare data is conducted. Authentication is conducted both at the sensor nodes and BS.

Although, it provides protection against several existing security threats. However, only provide device-level security for IOMT. Moreover, It provides effective data transmission and less energy consumption [63].

A two-hop-based scheme is discussed for WBANs. It introduces lightweight data transmission and provides a centralized approach. Generally, in WBANs intelligent sensor nodes are placed on the body of the patient to collect the healthcare values of the patient. Next, sensor nodes forward the collected data to the edge node for secure data aggregation. The edge node authenticates the sensor nodes by creating session keys and only authenticated nodes forward the collected data to the edge node. Otherwise, the security algorithm AVISPA is used for secure healthcare data forwarding. At the edge node, it provides less transmission cost. In this context, security-related data is not gathered at the cloud server because security-related data processing and computation is conducted at the edge of the network [64]. PCDA is a compression-based scheme that provides a lightweight and aggregation-based effective transmission of sensitive healthcare data. At the edge node, it is an essential task to efficiently aggregate the values of the patient health condition. Hence, data compression and data encryption help to provide efficient data collection at the central servers. A hashing-based cryptographic algorithm is employed to protect healthcare data. In the case of medical sensor nodes, data compression minimizes the communication cost. It encrypts the data before transmitting the data to the server for secure data transmission [65].

DDAP is a decentralized privacy-based scheme. It considers the security and privacy aspects of remote health monitoring. It improves security and performance by reducing the delay in different security concerns to provide efficient monitoring and prescription of patient health. it also provides an authentication model that allows only authenticated patients. transmission of data is based on the threshold values. Moreover, the condition of the patient is also analyzed on the basis of these threshold values. Introduced scheme forward a reminder message toward the patient and store at the cloud server. It also stores the hash of the data at the network overlay. A blockchain mechanism is employed to maintain and examine the collected health parameter values of the patients. A cryptographic approach is employed to provide secure data transmission and provide privacy by applying anonymity. For secure data transmission, it utilizes both symmetric and asymmetric data encryption [66]. DDAP scheme introduces dynamic and shared data storage in healthcare monitoring and also preserves the integrity of the data. A pseudonymized design is employed for dynamic sharing base data storage. A dynamic query analyzer is utilized for anonymization to protect sensitive healthcare data. For privacy preservation, earlier knowledge is utilized $D \in R^m$ denote a personal data of a patient, P possibility of density-based collection of feasible shared $p\ on\ R^m$ and A is a approach. Furthermore, P create m-dimensional D and D' autonomous data records ε denote the privacy estimation given in the equation (2.8) where $q \leq m$ denote the w , $K_1, \dots, K_1$. ε_k denotes the data that have K question for acknowledgement. Several steps for privacy are shown in equation (2.9). The integrity of the data is preserved while forwarding and storage of data. The data analyzer is utilized for secure data analysis [67]. Several research studies discuss the security and privacy concerns and future research concerns are also discussed.

$$\forall Pp\colon Prob_P\{A(D) = A(D')\} = \int_{D \in R^m} P(dD) \geq e^{-\varepsilon} \tag{2.8}$$

$$\begin{gathered} Prob_P\left\{A\left(d_{q1}, \dots, d_{qk}\right) = \right. \\ A\left(d'_{q1}, \dots, d'_{qk}\right) \mid A\left(d_{q1}, \dots, d_{qk-1}\right) = \\ \left. A\left(d'_{q1}, \dots, d'_{qk-1}\right)\right\} \geq e^{-(\varepsilon_k - \varepsilon_{k-1})} \end{gathered} \tag{2.9}$$

2.1.3 Secure Data Aggregation Using Fog Computing in Healthcare

The fog node is the intermediate layer that provides local data computation and data processing for healthcare data. Healthcare data is collected at the edge of the network and in terms of security preserve the data from several security threats while transmitting to the cloud server. The healthcare-sensitive information is stored at the cloud repositories [68] as illustrated in Figure 2.3.

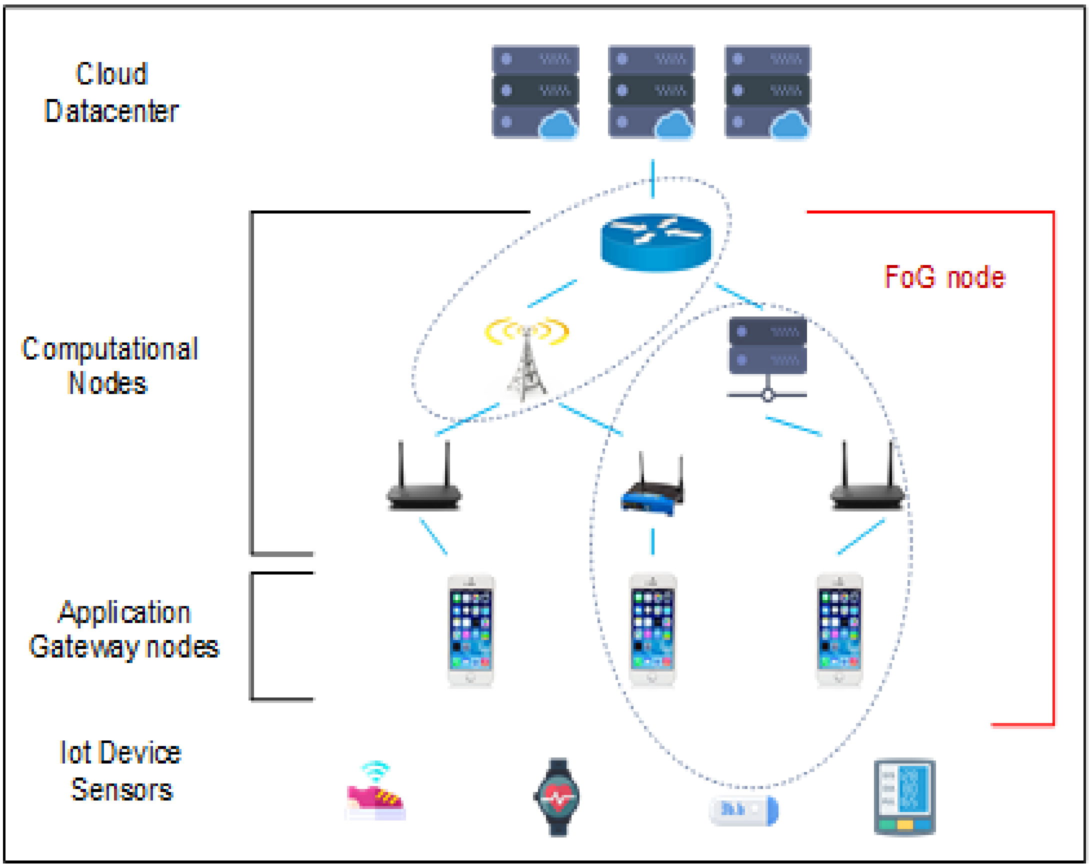


Figure 2.3: Generalized Fog Scenario

In the past few years, the patient-centric approach in healthcare systems is gaining interest day by day. Therefore, clinic centric approach is replaced with remote health monitoring to observe the health condition of the patients in a remote area [69].

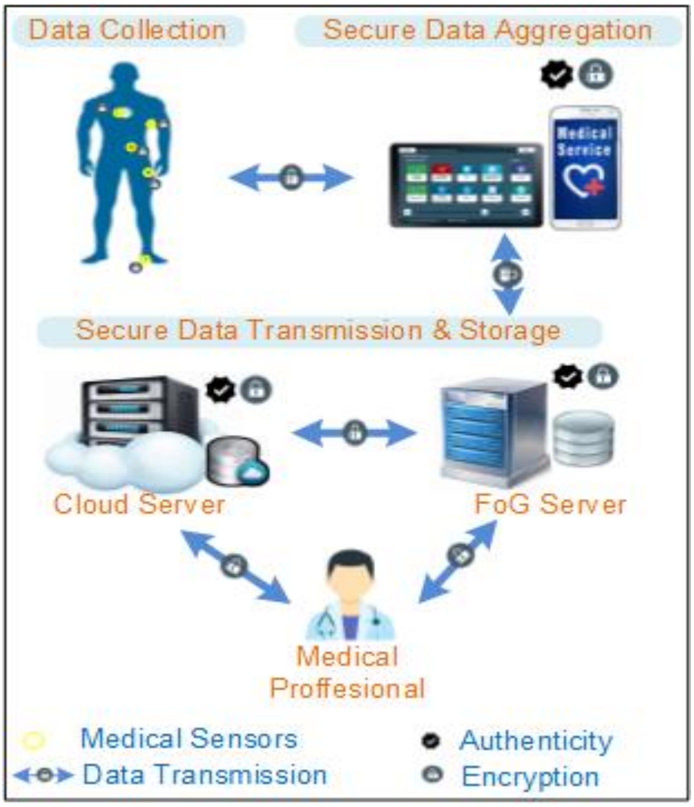


Figure 2.4: Generalized Concept of Secure Healthcare Data Forwarding

The patient-centric approach is based on several layers for secure monitoring of patient health [40]. In this scenario, the frog node plays an important role in the patient-centric healthcare systems. Hence, the fog node faces many security and performance issues while taking part in several processes of the medical architectures. In the medical system, it is a challenging issue to provide effective data computation and analysis of received data and at the fog node. It provides secure and efficient data access at the edge of the network [36]. The EMR scheme is a privacy-based healthcare framework. It provides secure data transmission electronic healthcare values using fog computing. Privacy is a main challenging task in the EMR. It provides privacy along with effective response time while using fog. In this scenario, the edge node aggregates the healthcare data and transmits it to the fog node. It utilizes pseudo-identity to identify the single patient record. Security of devices are is implemented by using the cryptographic method for secure data exchange. A key center provides secure key creation authentication for secure communicating among the fog node and cloud server as illustrated in Figure 2.4 [70].

In fog-enabled healthcare systems, sensitive healthcare information of patients is computed at the fog node to predict prescriptions for the different diseases of the patients. In FHMS, sensor nodes have battery-less fixed devices, Healthcare applications are deployed at the edge of the network. Health information data-id is classified into two types extrinsic and intrinsic. Extrinsic sensors collect the information related to the surrounding of the patient and intrinsic data is gathered through biosensors. it provides local data processing and storage for fast response and further stores information in the remote medical servers. Although, a key based security method is utilized. However, there is no peculiar security model is design for the security of medical health parameters. Moreover, no encryption method is introduced for the security of data. [71]. EHDA provides a secure data aggregation scheme. Sensor nodes collect the health values of the patient and forward encrypted values to the aggregator node to aggregate the data at the aggregator node. A message aggregation protocol is utilized at the mobile collector node to aggregate the received healthcare data and forward the aggregated data to the fog node to decrypt the received data using symmetric and check the integrity of the data and also extract the device-level data of the individual sensor node. It processes the data as per the requirement of the cloud server at the edge of the network and further uploads the data to the cloud server for data storage. Along with security, a heterogeneous based data compression mechanism is also utilized to reduce the data size to minimizes the communication cost and energy consumption during forwarding the healthcare data [46].

Data compression is becoming an essential part of IoMT because of the limited resources of healthcare devices. Wearable sensor nodes are attached to the body of the patient have limited battery power. Recent data compression-based schemes are introduced to minimizing communication cost, energy consumption, and storage cost. TTTDH algorithm is introduced for smart healthcare systems. it utilized the data compression method by merging different algorithms sequentially. The comparison of Huffman and LZW performance of Huffman proves that it is better than LZW. Although LZW provides a better compression ratio. However, it consumes more time for data compression. on the other hand, LZW is also compared with the TTTD. In this comparison, TTTD provides better performance than LZW but the data LZW provides a high compression ratio. Hence a hybrid method is introducing by merging two algorithms TTTD and Huffman algorithm respectively. TTTD-H provides better performance and data compression. In the case of huge data compression time of TTTD-H is also increased [72]. SSD scheme is introduced for secure data deduplication. It helps in the statistical calculation by utilizing scalable data deduplication. record linking protocol is utilized for the deduplication of patient healthcare values. The main focus of SSD is based on three main aspects like security, performance, and scalability. The semi-honest method is applied for secure data forwarding also provides id-based identification of healthcare values of single-patient data. SSD performance-wise is an effective scheme and also suitable enough for scalability. It also provide privacy for the health values of the patient [73].

The privacy protector scheme provides a data aggregation-based scheme for medical data. It protects against several security threats during data aggregation and transmission. A privacy protector protocol is used to protect the medical data of a patient. A secret distribution of data at several public cloud servers. It preserves the integrity of medical data and also provides data forwarding in the case when the data packet is lost. the multi-cloud server approach is utilized by the scheme to provide continuous data access without any issue. in this scenario, if any server is down then the required information can be access from the other servers. [74]. S-DDD scheme provides secure data deduplication. ACA algorithm is used to find out the cut point between the two windows. It utilized a fog-based approach. data deduplication is conducted on the fog node to remove the redundant healthcare parameter values at the edge node before forwarding data to the cloud server for storage. The symmetric key-based encryption is utilized to provide effective data exchange among intelligent healthcare devices. It provides efficient utilization of energy and less communication cost. It also provides variety in the chunk sizes of healthcare data [75]. PHI scheme provides secure data deduplication for healthcare. encryption-based secure data transmission and collection is provided by the PHI scheme. Real-time data collection and prediction mechanisms are introduced for remote health monitoring of the patient. Medical professionals can access the collected information from cloud server prescription. An attribute-based encryption method is utilized to secure data transmission and storage. Deduplicated data is forwarded to the cloud repositories for storage to minimum bandwidth utilization and less storage cost [76].

2.2 Comparative Analysis

This section provides a comparative analysis of different secure aggregation-based schemes. These schemes are considered based on the main concern, the contribution of the scheme, weak and strong points. These schemes are categorized in our proposed taxonomy as shown in Figure 2.1. we analyzed the reviewed schemes of the literature and illustrated these schemes using the tabular form. According to the taxonomy, these schemes are categorized into three subdivisions. In subdivision 1, secure and fog-assisted data aggregation schemes are considered for healthcare. LPDA [50], APPA [51], ABE / ABS [54] schemes conduct analysis for the computational cost. [50][51] schemes conduct analysis for the computational cost. Moreover, FHE [52] CPP [53] analyzes the execution of the scheme. Analysis proves that these schemes can be applied in real-world healthcare systems with some improvements in the performance of the schemes. In subdivision 2, secure aggregation schemes are considered for healthcare. SAPS [62], HMAC [63], AVISPA [64], PCDA [65] are present the graphical analysis in terms of communication, computation, and storage cost. Low computation and storage costs are explored in [62], provide less computational cost while [63][64], minimum energy consumption with high computation cost in [65], provide low energy consumption along with the low computational cost [66][67] provide security during data transmission. In subsection 3, secure fog assisted data aggregation schemes for healthcare. FHMS [71] EHDA analyzed for energy consumption. provide analysis for secure data compression ratio and compression time. Moreover, TTTD [72], SSD [73] provide analysis for secure data compression ratio and compression time. [72], PHI [76] is analyzed based on compression ratio. Most of the security schemes are can be implemented for secure health monitoring of the patient. These schemes required some improvement to implement in the healthcare domain.

Table 2.1: Summary of Secure Data Aggregation based Schemes for Healthcare

Scheme	Basic Idea	Methods	Metrics	Limitations	Strength
Secure Fog Based Data Aggregation Schemes					

ASAS [49]	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 [50]	LPDA 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. Communication overhead 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 [51]	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	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.

	are privacy and security.				
FHE [52]	Clustering to analyze large scale heterogeneous data at network edge. 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 [53]	This scheme secure data access and control in time aware and space aware scenario. 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 [54]	This scheme provides security and control data access to encrypt	CP-ABE and ABS encrypt data with access and	Metrics presented for comparison	Introduced architecture have high communicatio	Security provided by encrypting sensitive

	sensitive data and attribute-based signature (ABS) allows authenticated users to decrypt the ciphertext.	update policies. Encryption, description, and signing at FOG node.	of computational overhead with encryption decryption and signing.	n cost and high computational cost at the Fog node.	data, provide secure attribute-based control data access to update ciphertext and signing computations.
Secure Data Aggregation Schemes In Healthcare					
SAPS [62]	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 [63]	An authentication based secure data access is considered. In this way, it provide less energy utilization and secure data transmission.	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 [64]	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 scheme provides low computational, communication costs, and less energy consumption.
PCDA [65]	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.
DDPA [66]	This scheme formulates a block-chain mechanism to control and predict healthcare information. 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 [67]	A prototype of pseudonymization and anonymization method for protecting the healthcare data. It	A distributed storage architecture with query analyzer for anonymization.	De-pseudonymiz-ation service provided by differential	Difficult to implement.	Pseudonymization and anonymization methods are merged for data aggregation

	also provide anonymization.		privacy analyzer		in healthcare.
Secure Data Aggregation Schemes Using Fog Computing in Healthcare					
EMR [70]	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.
FHMS [71]	Healthcare based data aggregation applications are provide secure data monitoring at the edge of the network.	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 in the Fog-cloud scenario.
EHDA [46]	Sensor nodes forward health data to the aggregator node for the compression and transmits it to the Fog node. This work uses symmetric keys for encryption and	Message receiving algorithm at aggregator, message extraction algorithm at the fog, and NS-2.35	Message size with communication cost. Energy consumption with sensing-	Inter-communication between edge node enhancing communication cost.	Scheme consumed less storage and energy consumption, less communication cost. Better resilience

	decryption and also utilizes static edge nodes, non-static aggregated nodes.	simulation tool.	aggregated nodes.		and transmission ratio.
TTTD [72]	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 [73]	A record linking algorithm is introduced for deduplication of healthcare data.	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 [74]	It introduces secret sharing of data with the several remote 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 [75]	ACA uses to find out the point of identification among the windows and reduces transmission cost of healthcare data.	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 [76]	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.

From Table 2.1, we conclude that most of the schemes not considering data compression only 25 % of schemes considering data compression. In healthcare scenario, 1 scheme considering data compression. In the discussed schemes 75% of research studies considering fog computing. Moreover, most of the schemes transmit redundant values. Therefore, we are trying to cover the research gap of these studies.

Table 2.2 illustrated the comparative analysis of recent data aggregation based schemes against several performance criteria. The values of the schemes are denoted with H (High), A (Average) and L (Low) with different factors.

Table 2.2: Summary for the Comparative Analysis of Schemes

Schemes	Communication Overhead	Computational Cost	Energy Consumption	Storage	Delay	Security Level
ASAS [49]	H	A	H	A	H	A
LPDA [50]	L	A	A	A	L	H
APPA [51]	A	A	A	A	A	H
FHE [52]	L	A	A	A	L	H
CPP [53]	L	A	A	L	A	H
ABE / ABS [54]	A	L	L	L	A	H
SAPS [62]	L	H	A	A	A	H
HMAC [63]	A	A	A	L	A	H
AVISPA [64]	H	H	H	L	A	H
PCDA [65]	L	L	A	A	L	A
DDPA [66]	H	A	H	L	A	H
EMR [70]	A	L	A	A	L	A
FHMS [71]	H	L	H	A	L	L
EHDA [46]	A	A	A	L	H	H
TTTD [72]	L	L	L	L	A	L
SSD [73]	L	A	A	L	L	H
SW-SSS [74]	H	A	A	L	A	A
S-DDD [75]	A	H	L	L	A	H
PHI [76]	A	H	A	L	L	H

From Table 2.2, we conclude that data aggregation research studies are evaluated against several research concerns. Most of the schemes provide a high level of security. Moreover, 25 % of schemes provide high communication cost, 20% of schemes provide high computational cost and energy consumption. Most of the considered schemes provide aggregation-based secure data transmission. Therefore, most protocols provide better security, less storage, and minimum delay.

2.3 Open Research Challenges

IoMT technologies gain interest in terms of remote patient health monitoring but many challenges still need to overcome. This section discusses several challenging issues of recent studies. To design an effective data aggregation mechanism these challenging issues need to be resolved. In IoMT, several challenging tasks still need to be resolved. In this context, only relevant challenging issues are considered. It is necessary to resolve these challenging tasks of recent research studies that are identified from reviewed schemes. In this thesis, we are resolved different important challenging concerns of healthcare-based research studies like security, storage, communication cost and etc.

2.3.1 Security for Data Aggregation

Security IoT-enabled healthcare data is an essential research concern for the protection of healthcare data [21]. In IoMT based applications, a secure network and hardware both are key features for data protection and network scalability [77]. In healthcare, authentication is an essential criterion because authenticated devices are considered to be secure and effective for secure data exchange among smart healthcare devices [40]. In a hostile environment, security is a prime concern for secure data transmission among the smart healthcare devices and transmission toward the remote server. It is quite difficult to protect against several security threats. Mostly these threats are not detectable and capture sensitive healthcare information or capture any smart device for conduct malicious activities [64][74][78]. In this context, attackers can access the data of the patient while aggregating the healthcare data. Node capturing opens the way for several security attacks [75]. Several challenges and security concerns are kept under consideration before constructing a secure mechanism for patient health monitoring [65]. t is a challenging task to design a scheme that protects against several security attacks [30]. Effectively detect the security attacks and protect against these threats is the main concern in terms of secure data aggregation and transmission [76]. In the healthcare scenario, malware detection and shielding against these attacks is a challenging research concern for future research works [79]. In fog-assisted healthcare systems, it is a challenging task to design a framework that detects malicious attacks and provides protection against several malicious attacks [80][81]. In fog-based architectures, the number of edge devices present. In case an edge device is captured and this node can open a path for several security attacks. Malicious nodes working of the whole system. In IoMT, smart devices mobile devices act as aggregator nodes and using the open network for data exchange. Therefore, these devices are easily becoming malicious nodes. therefore it is an essential need to design a green architecture that detects and protects against several security attacks [82][83]. Mostly the middle layers of the system are under attacked to disturb the whole system by malicious data injection. therefore the security of healthcare-based systems is a primary concern and securing the edge devices for several security threats [84]. In WBAN [85], medical data is encrypted with the ciphertext for data transmission and store in repositories [86]. Moreover, the construction of a secure data aggregation mechanism that utilizes fewer resources is a challenging task in the medical field. IoT based healthcare system faces several challenges while aggregating the sensitive information from the smart sensor nodes [87]. Hence, in the open network, the healthcare values of the patient's health are not secured while transmitting and an attacker can access this information and affect the analysis and prescription procedure of patient health.

2.3.2 Privacy of Data for Information Exchange

Privacy is also an essential factor to protect healthcare information and also hide the identity of the patients [88]. Privacy and security are like two sides of coins so both are important in several concerns in healthcare like secure and privacy preserved data gathering, aggregation, and storage [32]. In healthcare systems, privacy is a challenging concern for protecting sensitive information while exchanging data among the devices [53][22][89]. The implementation of fog in healthcare-based systems enhancing the performance of the system but also raises new challenging concerns related to security and privacy [70][90]. Mostly, healthcare-based architecture first gathers the health values of a patient by using intelligent sensor nodes, smart mobile collector nodes aggregate the collected information, and the fog node received data analyzed and processed locally. Therefore, the privacy of data at three different stages is an essential and challenging research concern Therefore, it is an essential requirement to design protocol that protects the data and identity of individuals from any malicious attacks. then, the attacker cannot access the protected information of the patient [91]. In recent privacy preservation schemes encryption and anonymity-based privacy preservation, both are essential methods for the privacy of the healthcare data [49], [92]. Hence, the construction of privacy preserved and thread protector scheme is a challenging task for future research works [93].

2.3.3 Privacy of Quality of Services for Healthcare Data Exchange

Privacy for the quality of services depends on the requirement of the services. it varies from one application to another and it maintains the performance of healthcare applications up to a certain level. In fog-assisted healthcare, quality of services plays an essential role for load balancing by sharing the one task at multiple nodes to properly utilize the resources of the system [94]. Maintaining the data integrity during data exchange from the edge node to the cloud server and also provide quality of services is an essential challenging concern [71]. For the quality of services, latency plays a main role in the healthcare domain. QoS and latency both are inversely proportional to each other in the case of maintaining the quality of services then the latency of the transmitted data should be minimum. latency is a time that a device can take for data forwarding and receiving. In, system waiting time. Therefore, the quality of services is based on latency and bandwidth. In simple words, QoS is fast response time and less energy utilization. In this context QOS the main concern in IOMT.

2.3.4 Scalability for Massive Data Sharing

Scalability of the network is an essential task for effective data transmission and collection in healthcare based data aggregation schemes [95]. Resource management is a main challenging concern in IoMT based healthcare schemes [96]. Network scale can be enhanced by increasing the network bandwidth band latency. Most of the time some architecture provides efficient performance at a small scale but on the large scale performance of the system is also affected [45]. Fog-enabled healthcare systems provide remote access to patients through medical experts. In this context aggregation processes are scalable for remote access. In emergencies, the scalability of healthcare services is a challenging research topic because the demand for services is abruptly increased. High demand for services affects the server performance or sometimes the server or networks are collapsed [44]. Thus, an effective and scalable healthcare architecture is required to support the rising need for healthcare services in critical situations.

2.3.5 Resource Management for Massive Data

Data management of critical healthcare data depends upon the aggregation of healthcare data effective manners. Data management is a main challenging concern and also more effective in IoMT scenario. Edge data processing provides a solution for data management by applying local data processing and analysis of healthcare data and data is further uploaded at the cloud server [40]. In IOMT, heterogeneity allows communication among the several types of devices using some appropriate algorithms. In the healthcare scenario, various devices of various development companies are attached to the body of the patient. Sensor nodes forward its collected information to the respected server. Therefore, the heterogeneity of devices is a challenging need to overcome for future research studies [97]. Transmission of data from the sensor node to the edge node for local data processing to overcome the heterogeneity issue [98] Heterogeneity is an essential factor between the sensor node and the fog node because it provides an effective data exchange among heterogeneous devices. In the case of multiple users that are utilizing the same resources. Along with heterogeneity, the management of resources performs an essential role by providing fast response to the requestors. Data offloading is also a challenging task and it can be useful in fog assisted healthcare scenario because fog nodes analyze which smart nodes provide low latency then the data is offloaded to those devices.

2.3.6 Fog Assisted Storage Repositories

The fog server provide local data computation and the cloud server provides permanent data storage at the cloud server [99]. Fog server support to store the latest data in the local storage to provide data analysis and real-time data forwarding. Moreover, data is processed locally and predict intelligent decision according to the received healthcare information before collaborating with or forwarding the aggregated information to the cloud server [100][101] Most of the organization provide services to store big data for data storage and this data can be access in future whenever it required. Store data can be access to predict the decision and also used for data analysis [102]. The fog-based healthcare architectures are based on multiple huge numbers of a smart sensor node to collect the health values of the patient and these devices share the real-time information with the fog node. It applied data processed the data at the fog node for removal of redundant data at the edge of the network before forwarding the data toward the medical servers [103]. Medical professionals can access the information of the particular patient from the fog nodes for p[atient health analysis and prescription [104]. Hence, effective data processing and storage both are essential research topics. Thus, there is a need for an effective storage technique for future research studies that can manage the storage issues at all layers of IoT-based healthcare systems.

2.3.7 Deduplication for Healthcare Data

The data deduplication method removes the redundant values from the set of data to reduces its size up to some extent and also reducing the data forwarding cost. In security-based data deduplication, data ownership is also a challenging task that needs to be overcome in future research works [105]. In a multi-user scenario, if the ownership of the user is removed from the data they can't access the specific data. and the system prevents these users to access the data after canceling the access to some particular data. Data deduplication filters the redundant data before forwarding the healthcare values to the cloud server [103]. In this context, data compression reduces the size of the data bits to reduce the size of the data packet forward at the open network [106]. Therefore, compressed data consume less space at the storage repositories [107]. It is a challenging task to design an effective scheme that provides a high compression ratio with minimum compression time [108]**.** In this scenario, this architecture helps to reduce data size for transmission and also preserve the storage cost [72]**.** Secure data deduplication is a challenging task. A secure solution that can provide secure data deduplication. in this context data encryption is conducted at the end nodes and data deduplication is applied to the data at the edge nodes. The contrast of security and deduplication is a primary research concern for secure and effective data deduplication [76].

2.3.8 Deduplication Continuous Connectivity Support During Mobility

Continuous connectivity is an essential research topic for monitoring mobile patients at remote locations. In this context, a patient is Therefore, it can use other networks or nearby devices that are connected with the network. It can use these devices for the transmission of data unless it is again connected with its network. This situation leads to security and privacy concerns for patient-sensitive information [109][110]. In the fog paradigm, healthcare-based aggregator nodes like mobile phones and vehicles act as a aggregator nodes to provide support for mobility to effectively forward the collected information to the fog node from any remote location using the open network [111] [112][113]. In this context, a smart and intelligent devices act as a aggregator node to gather information from intelligent sensor nodes of patients that are placed on the body of the patient, and mobile collector nodes provide secure data transmission over the network [114]. Smart healthcare devices are placed at the healthcare center are forward collected data to the medical server and the devices are at the remote location are also forward the collected information to the medical server [44]. Continuous connectivity with mobile devices at remote regions is a challenging task. Therefore, in the case of end node mobility, it is a critical task to provide continuous support for moving sensor nodes across the number of fog servers [115]. Mobility management is required to ensure the continuous connectivity of the mobile devices. Although, effectively handle mobility is a challenging task. However, limited research studies are conducted from a mobility perspective. Thus, continuous mobility support providing architecture is required and still a challenging research topic [116].

2.3.9 Reduce Communication & Computational Cost to Improve Efficiency

In healthcare scenario, while aggregating the healthcare parameters so it is essentially important to reduce the communication cost [65]. In smart healthcare, sensor devices have limited resources and there is a need to effectively utilize these resources. Therefore, an effective healthcare design that provides less cost while forwarding the healthcare values [36]. There is a need to employ intelligent protocols to reduce the cost of both sensor and edge nodes while forwarding data among the smart devices and the cloud server [4][117]. Efficiency in the case of healthcare scenario is that the aggregation of data in less time and less utilization of resources. In the case of secure data transmission, both security and scalability are the main challenging task [73]. The integration of intelligent data computation and prediction toward the intelligent data aggregation techniques for future research studies. Therefore, it will improve the effectiveness of the data aggregation process [39][118]. The reduction of transmission costs during the data transmission process from sensor nodes to the cloud server while using intermediate node fog server [119]. Efficiency is an essential requirement for fast response time and efficiently forward the data to the cloud server. Moreover, limited research studies are conducted for real-time data transmission, forwarding, analysis, and prediction decisions according to the health condition of the patient. In emergencies, an efficient data aggregation protocol is required to forward the non-delay tolerant data to overcome the critical condition of the patient [120]. Therefore, it is an essential need in future research studies to construct a protocol that can effectively handle both types of data delay-tolerant and non-delay tolerant data.

Table 2.3: Summary of Addressing Challenging Issues in Schemes

Schemes	Scalability	Quality of Service	Data Aggregation	Mobility	Load balancing	Heterogeneity
ASAS [49]	No	No	Yes	No	Yes	No
LPDA [50]	No	Yes	Yes	No	Yes	Yes
APPA [51]	No	Yes	Yes	Yes	Yes	Yes
FHE [52]	Yes	No	Yes	No	Yes	Yes
CPP [53]	No	No	Yes	No	Yes	No
ABE / ABS [54]	Yes	No	Yes	Yes	Yes	Yes
SAPS [62]	Yes	No	Yes	Yes	Yes	Yes
HMAC [63]	Yes	No	Yes	Yes	No	Yes
AVISPA [64]	Yes	No	Yes	Yes	No	Yes
PCDA [65]	Yes	Yes	Yes	No	No	No
DDPA [66]	Yes	No	Yes	Yes	Yes	Yes
DDAP [67]	No	No	Yes	No	No	Yes
EMR [70]	No	No	Yes	Yes	Yes	Yes
FHMS [71]	No	Yes	Yes	No	Yes	No

EHDA [46]	No	No	Yes	Yes	Yes	Yes
TTTD [72]	No	No	Yes	No	No	Yes
SSD [73]	Yes	Yes	No	No	No	Yes
SW-SSS [74]	Yes	Yes	Yes	Yes	Yes	Yes
S-DDD [75]	No	No	Yes	Yes	No	No
PHI [76]	No	Yes	Yes	No	No	No

Table 2.3 consider several healthcare based data aggregation schemes and observe that these schemes are overcome which challenging tasks. The two main challenges are not properly focuses by several research studies and these research topics are scalability and quality of services. Moreover, other considered challenges are considered by the most of the schemes.

From Table 2.3, we conclude that there is a need to manage the heterogeneity of the node in future research studies to enhance the performance of the remote health monitoring of the patients. The next lesson is learned that lots of vulnerabilities in existing research studies in terms of real-time data analysis and perdition according to the present health condition of the patient.

2.6 Summary

Different security concepts based on data transmission and aggregation schemes have been reviewed and issues have been identified. We conduct a critical review of discussed schemes in taxonomy. Next, analyze these schemes by utilizing the tabular method. Furthermore, several open challenging issues of secure data aggregation and transmission also consider.

CHAPTER 3

METHODOLOGY

3.1 Overview

This section presents a summary of our proposed approach and system model. This section also provides an overview of the security requirements and design objectives of the proposed approach. The main aim of the work is to provide secure and lightweight data aggregation and transmission. Furthermore, the main objectives of the thesis are secure data transmission, minimum storage utilization, less communication, computational costs, and energy consumption.

3.2 Operational Framework

In this section, a secure data gathering model is presented to remotely monitor the health condition of a patient. Different security requirements and threads are considered for proposed approach. Next, we discuss the communication model and design concerns of our proposed work. Our proposed model considers an IoMT based system to monitor the patient's health conditions in remote areas. We concentrate on secure data aggregation and transmission data to the fog and cloud server as illustrated in Figure. 3.1. Sensor nodes are denoted by (SN) = { $SN_1, SN_{i+1}, \dots SN_n$} and n is the total number of sensor nodes are placed on the body of a patient to gather different healthcare parameters like blood pressure, temperature, and heart rate. The sensor nodes forward collected data to the mobile node. Next, mobile nodes are denoted by MN and wirelessly connected with sensor nodes. These nodes gather healthcare data of each sensor node and perform aggregation on the collected data. Thus, the aggregated healthcare parameters are forwarded towards the Fog node. Finally, Fog node (FN) received aggregated data from mobile nodes. The aggregated values are locally stored and processed at the fog node. Further, it processed data according to the format then transmit to the cloud server. The network model describes a secure data aggregation and transmission method for remote health monitoring. The transmission of healthcare data from sensor nodes to the server is completed in 3 different steps. In our proposed model, we assume that SNs are attached with the body of a patient. SNs compresses the data before transmitting toward the MN. Moreover, SNs and MNs are communicate by using secret key and MN also use secret key to communicate with fog node. We also assume that the FN transmits the processed data to the cloud server for storage and future access.

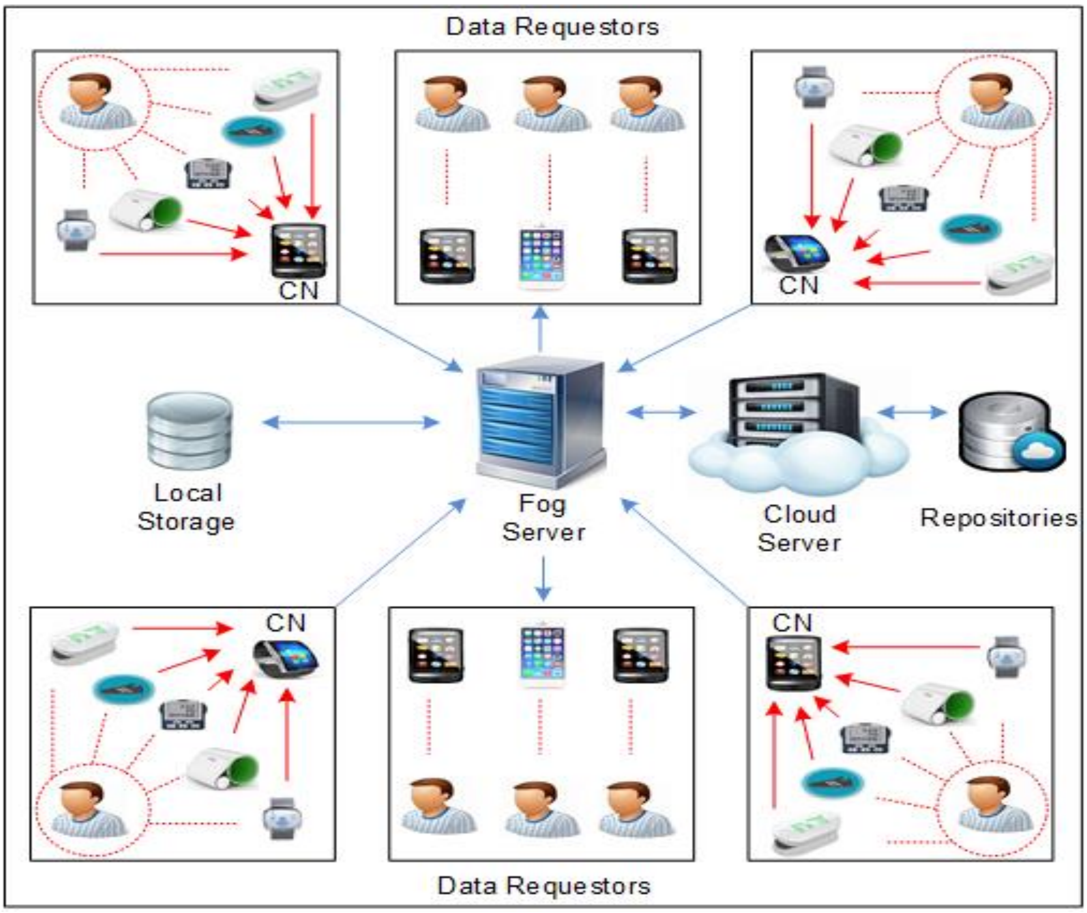


Figure 3.1: System Model for Remote Health Monitoring

3.2.1 Communication Model

In the network communication model, SNs, MNs, and FNs are communicated by using WiFi technology. Sensor nodes directly communicate with the available mobile node. The distance between fog nodes and mobile nodes is long, and the nodes communicate through the internet. Our communication model is based on the following points: (i) we assume that the communication among the nodes is secure by using a symmetric key (ii) Every SN can communicate with a single MN at a time. (iii) MN aggregates the collected data and forwards it to the FN. (iv) Each FN conducts computational operation and provides local storage. (V) we consider only one cloud server for secure data storage and access.

3.2.2 Security Essentials

Security is an essential requirement for the detection and protection of sensitive healthcare information from several malicious attacks. Therefore, the communication between the SN and MN is secure. In case an attacker can access the wireless communication of the nodes but cannot access the information in the forwarded data packet. Moreover, to preserve the integrity of data no unauthorized user can access the specific healthcare information. The authentication based encrypted data is transmitted to ensure the integrity of data. In this context, anonymity also considers for hiding the identity of users.

3.2.3 Design Objectives

Our main objective is to construct a secure data transmission and gathering system for IoMT. The main objective of our work is secure data aggregation and transmission of healthcare values within a network. We also preserve the integrity of data by using key-based data encryption to protect against several security attacks. In this context, the freshness of data is the main key for proper analysis and prescription of the patient current health condition.

3.3 Research Design and Development

This section presents the solution for identified challenging issues of data aggregation schemes. Our proposed work is divided into Three phases data collection and computation at SN, data aggregation at CN, data decryption at fog node. Moreover, message compression algorithm is utilized after the collection of the data in phase 1 and removal of redundant data after the decryption of received data in phase 3 as shown in Figure 3.2.

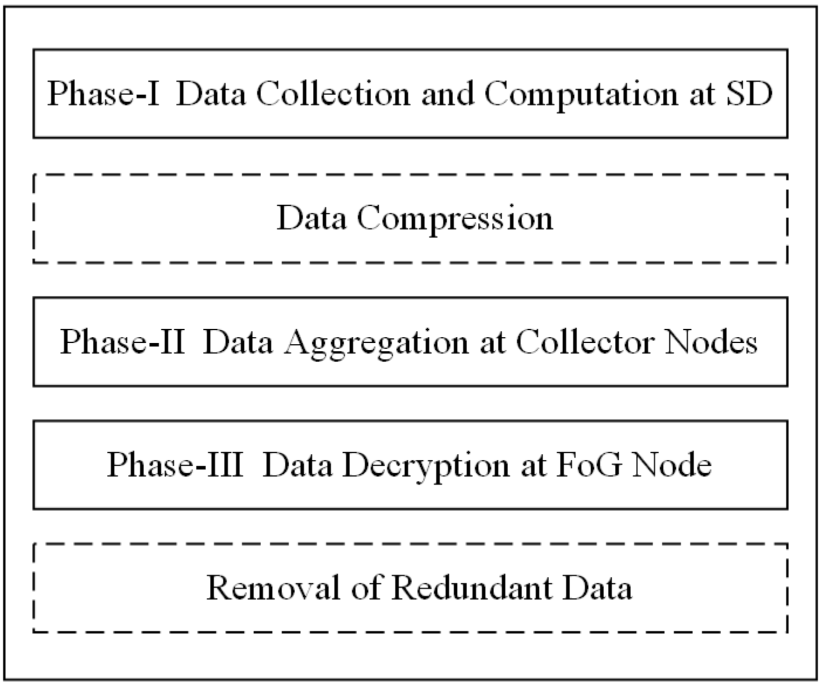
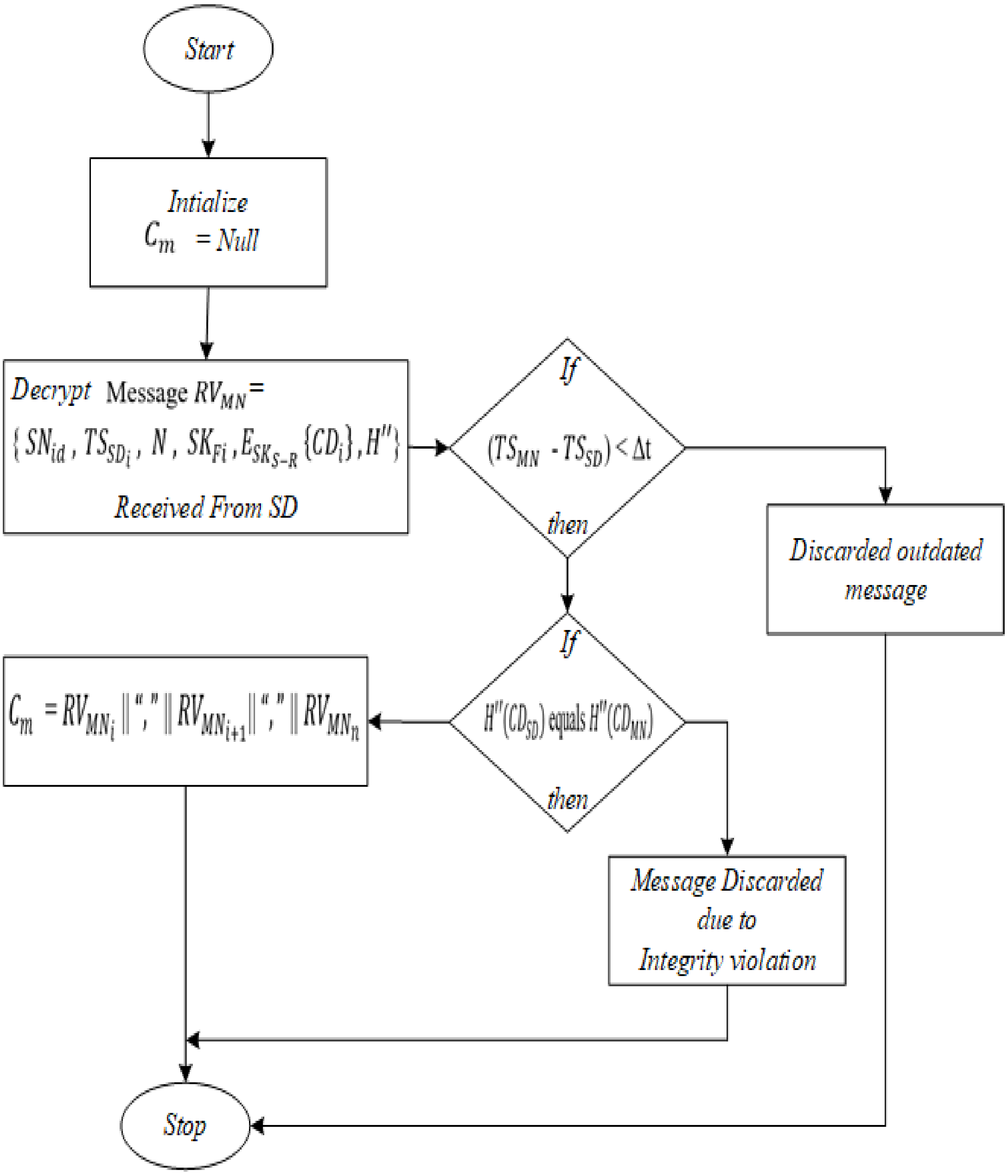

Phase-I Data Collection and Computation at SD
Data Compression
Phase-II Data Aggregation at Collector Nodes
Phase-III Data Decryption at FoG Node
Removal of Redundant Data

Figure 3.2: Different phases of ESTDA

3.3.1 Secure Data Aggregation at MN

In Figure 3.3, an encrypted and compressed message is received from the sensor node. First of all, check the timestamp of the message to check the message's freshness. Then, check the integrity violations in the message by comparing the hash with the hash of the received message. Finally, the messages received from the sensor nodes are aggregated by using the colon as a delimiter. Further, aggregated data send at the FN.



Start
Intialize
C_m = Null
Decrypt Message RV_{MN} =
$\{SN_{id}, TS_{SD_i}, N, SK_{Fi}, E_{SK_{S-R}}\{CD_i\}, H''\}$
Received From SD
If
$(TS_{MN} - TS_{SD}) < \Delta t$
then
Discarded outdated message
If
$H''(CD_{SD})$ equals $H''(CD_{MN})$
then
$C_m = RV_{MN_i} \| "," \| RV_{MN_{i+1}} \| "," \| RV_{MN_n}$
Message Discarded due to Integrity violation
Stop

Figure 3.3: Flow Chart for Algorithm 1

3.3.2 Secure Data Decryption at FN

In Figure 3.4, an encrypted and compressed message is received from the MN. First of all, check the timestamp of the message to check the message's freshness. Then, check the integrity violations in the message by comparing the hash with the hash of the received message. Furthermore, decrypt the received message and extract the healthcare parameter values from the received message. Then, again check the message integrity violation by comparing the hash. Finally, replace the redundant values with a boolean value. Further, FN send processed data to the cloud server for storage.

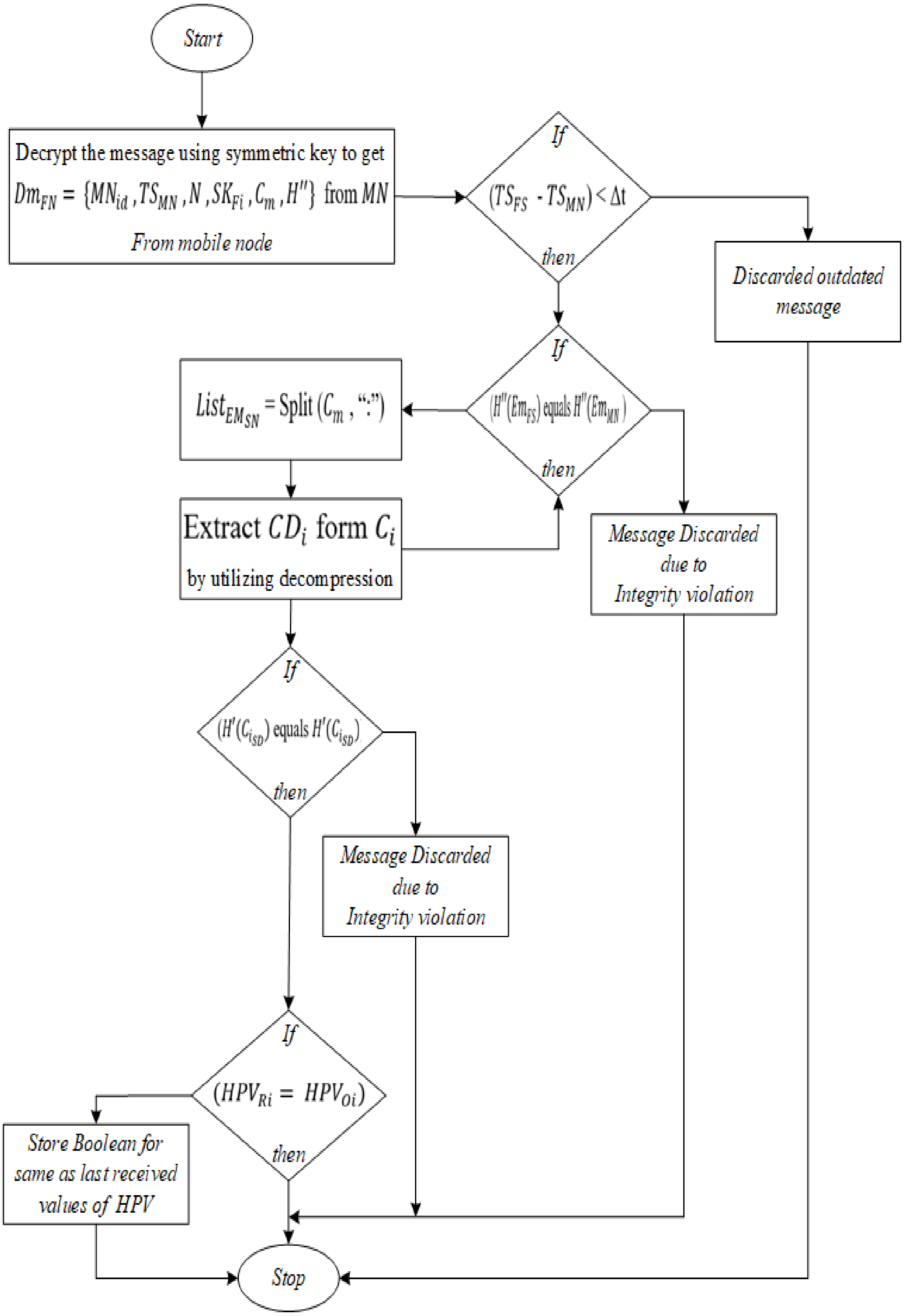

Start
Decrypt the message using symmetric key to get
$Dm_{FN} = \{MN_{id}, TS_{MN}, N, SK_{Fi}, C_m, H''\}$ from MN
From mobile node
If
$(TS_{FS} - TS_{MN}) < \Delta t$
then
Discarded outdated message
If
$(H''(Em_{FS})$ equals $H''(Em_{MN}))$
then
$List_{EM_{SN}} = \text{Split}(C_m, \text{“:”})$
Extract CD_i form C_i
by utilizing decompression
Message Discarded due to Integrity violation
If
$(H'(C_{i_{SD}})$ equals $H'(C_{i_{SD}}))$
then
Message Discarded due to Integrity violation
If
$(HPV_{Ri} = HPV_{Oi})$
then
Store Boolean for same as last received values of HPV
Stop

Figure 3.4: Flow Chart for Algorithm 2

3.4 Parameters

Table 3.1, presents the simulation parameters values that are employed for our proposed simulation scenario.

Table 3.1: List of Simulation parameters

Parameters	**Values**
Network Field	1600 × 1600 m
Node numbers	20~200
Cluster radius	500 m
Sensing radius	160 m
Initial energy	1200 J
Transmission Power at Node	0.928 µJ
Receiving Power	0.052 µJ
Channel Type	Wireless
Propagation Model	Two Ray
Transmission Power at AN	0.6143 µJ
Receiving Power	0.052 µJ
Physical Type	Wireless Physical
Mac Protocol Type	Mac/802–11
Queue type	DropTail/PriQue
Antenna Type	Omni Antenna
Max Packet in Queue	60
Router Trace	ON
Mac Trace	OFF
Agent Trace	ON
Nodes per Group	8–40 nodes
Original Unit Data Size	50–500 bytes
Number of Messages	64–128 messages
Given Time Slot	0.1–1.0 s
Responding Node Count	50–200 nodes

3.5 Performance evaluation

In this section, evaluation parameters are discussed to evaluate the performance of the proposed scheme while comparing it with related schemes. The simulation scenario is discussed to provide an overview of our proposed simulation scenario. Moreover, the proposed model is elaborated and different simulation tools are also considered which are employed for simulation.

3.5.1 Evaluation parameters

Our proposed scheme is compared with 4 related schemes based on several evaluation parameters. The ESDTA is analyzed against several parameters such as (i) communication cost in terms of bytes exchange and communication cost in terms of energy consumption, (ii) computation cost in terms of a number of nodes, (iii) energy consumption at SN, and energy consumption at MN, (iv) Number of compromised bytes and the number of compromised nodes, and (v) storage cost. In chapter 5, results show that ESDTA provides better results based on evaluation parameters discussed above.

3.5.2 Modeling and simulation

We have validated our work using a simulation tool NS 2.35. A hierarchical model is employed for node deployment. In this scenario, SNs are placed in the area of 1600 × 1600 meters. We also consider the MN and Fog nodes for the appropriate type of computations like data Anonymity, encryption, decryption, hashing, and secure transmission of data. Simulation is conducted using NS 2.35 on Fedora Core 16, Where TCL files provide node arrangement, node placement, and commence of a message. We create separate classes by utilizing the C language to achieve the functionality of data forwarding and receiving. Moreover, AWK script files are utilized to obtain results from trace files.

3.6 Summary

The system model of the proposed efficient and secure data transmission and aggregation scheme is discussed in this chapter. A communication model is elaborated in this chapter. The security essentials and design goals of our proposed approach are discussed. We also discuss the flow of proposed data aggregation algorithm at the MN and data decryption algorithm at the fog node. Moreover, we consider the performance evaluation of proposed model. The evaluation parameters also consider based on these parameters performance of our scheme is analyzed. Finally, the simulation scenario and model is discussed.

CHAPTER 4

PROPOSED EFFICIENT AND SECURE DATA TRANSMISSION AND AGGREGATION (ESDTA) SCHEME

4.1 Overview of Proposed Scheme

In this section, we present an Efficient and Secure Data Transmission and Aggregation ESDTA scheme. In healthcare scenario, secure data generation, aggregation, and transmission are challenging issues. Security of data is an essential requirement for data sharing based applications in IoMT. Our proposed scheme provides a solution for discussed problems by providing secure data aggregation, lightweight data transmission and data compression and removal or redundant data. Moreover, the list of notations is shown in Table 4.1.

Table 4.1: List of Notations

Notation	Description
$\boldsymbol{CD_i}$	Compressed data at sensor nodes
$\boldsymbol{SK_{Fi}}$	Key among SN and FN
$\boldsymbol{C_i}$	Cipher text at sensor nodes
$\boldsymbol{SN_{id}}$	Sensor nodes ID
$\boldsymbol{TS}$	Time stamp
$\boldsymbol{N}$	Nonce value
$\boldsymbol{H''}$	Hash function
$\boldsymbol{RV_{MN}}$	Received data at Mobile node

$\boldsymbol{E_m}$	Encrypted and compressed message at mobile node
$\boldsymbol{C_m}$	Aggregated message at MN
$\boldsymbol{HPV_{Ri}}$	Currently received healthcare values
$\boldsymbol{HPV_{Oi}}$	Last received healthcare values
$\boldsymbol{H'(C_{i_{SD}})}$	One-way hash function

4.2 Data Collection and Computation at SD

In phase I, Smart sensor nodes generate different health parameter values and securely transmit collected data to the MN. In this context, our solution utilizes a compression scheme and symmetric key based encryption for lightweight and secure data exchange.

In the initial phase, sensor nodes gather healthcare parameter values (HP_V) and values are collected as $G_{SD} = \{HPV_i : HPV_{i+1} \ldots : HPV_n\}$. Collected healthcare values are compressed by utilizing the compression method $CD_i = \{ G_{SD} \{(H'(HPV_i : HPV_{i+1} \ldots : HPV_n))\}$ and apply symmetric key-based encryption for secure data transmission toward the MN.

4.2.1 Message compression and message formation at SD

The message compression algorithm stores 16-bits in the memory to reduce the size while transmitting to preserve per bit energy utilization. Mostly, the healthcare parameter values of the patient are in numeric form. The small values of temperature, pressure, and humidity are scaled to represent in BITSET as shown in steps 6 and 7. Suppose a temperature value is '35' and a size of 16-bits. First of all, these two values are divide into two 8 bit characters by taking 3 and 5 separately. The bit-set adds the lower 4 bits of 3 (0011) and 5 (0101). Moreover, both values are concatenated in the char-set of 8-bits. For the values with more number values loop is applied to add the bits in the bit-set. The delimiter is also employed in the bit-set.

The healthcare values are compressed (CD_i) and encryption of cipher text is obtained by using symmetric key (SK_{Fi}). Cipher text (C_i) includes (SN_{id}) ID of sensing devices, (TS_{SD_i}) sensing devices time stamp and N is a nonce value as shown in equation (4.1). Symmetric key base encryption is utilized for secure data exchange. The encrypted message includes the hash of the whole message to check message integrity on the receiving side. Sensor nodes forward lightweight and secure data to the mobile node which performs aggregation on the received message.

$$S \rightarrow R: E_{K_{S-R}} \{SN_{id} \text{ , } TS_{SD_i} \text{ , } N \text{ , } SK_{Fi} \text{ , } E_{SK_{S-R}} \{CD_i\} \text{ , }$$

$$H''(SN_{id} || \, TS_{SD_i} \, || \, N \, || \, SK_{Fi} \, || \, E_{SK_{S-R}} \{CD_i\})\} \qquad (4.1)$$

C_i is the message forward by the sensor nodes to the mobile node as given in (4.2).

$$C_i = (SN_{id} \text{ , } TS_{SD_i} \text{ , } N \text{ , } SK_{Fi} \text{ , } E_{SK_{S-R}} \{CD_i\} \text{ , } H'') \qquad (4.2)$$

4.3 Message Receiving and Aggregation at MN

In phase II, we introduce a secure data aggregation (SMA) algorithm at MN in Table 4.2. A compressed and encrypted message is received from the sensor nodes. In this context, only those nodes forward the healthcare parameters to the MN that meet the pre-installed query requirements like sensor nodes only forward those values that are greater than the normal range. SMA algorithm explains the functionality of secure data receiving and aggregation procedures. MN receives the encrypted and compressed data packet RV_{MN} from sensor nodes. Each RV_{MN} includes a node ID (SN_{id}), Timestamp (TS_{SD_i}), nonce value (N), Symmetric key (SK_{Fi}), compressed data (CD_i) and hash of message. For example, a message received from SN_i = $S \rightarrow R: E_{K_{S-R}} \left\{SN_{id} \text{ , } TS_{SD_i} \text{ , } N \text{ , } SK_{Fi} \text{ , } E_{SK_{S-R}} \{CD_i\} \text{ , } H''\right\}$ is received at MN. Secondly, SN_{i+1} = $S \rightarrow R: E_{K_{S-R}} \left\{SN_{id} \text{ , } TS_{SD_{i+1}} \text{ , } N \text{ , } SK_{Fi+1} \text{ , } E_{SK_{S-R}} \{CD_{i+1}\} \text{ , } H''\right\}$ message received and likewise other sensor nodes forward data packets. Finally, a message received from the SN_n = $S \rightarrow R: E_{K_{S-R}} \{SN_{id} \text{ , } TS_{SD} \text{ , } N \text{ , } SK_{Fi} \text{ , } E_{SK_{S-R}}$

$\{CD_i\} , H''\}$. All received message are aggregated at mobile node by using colon as a delimiter. In the SDA algorithm, MN receives the Ci from the sensor nodes depicts in (4.2). The MN calculates the timestamp TS_{MN} - TS_{SD} < Δt. Hence, accepts the RV_{MN} received message when the condition is true else drops an outdated message. Next, MN computes the hash $H''(CD_{SD})$ equals $H''(CD_{MN})$ for the received message and compares it with the already computed hash given in the RV_{MN} to guarantee the message integrity. The hash of the received message is equal to the provided hash then; MN concatenates all received messages by using the colon as a delimiter. Subsequently, MN transmits an aggregated healthcare values to the FN and preserve the privacy of sensitive healthcare information by transmitting symmetric key based encrypted message to the fog node. Encrypted message (E_m) is formulated by using SDA algorithm as given in equation (4.3).

$$E_m = \{MN_{id} , TS_{MN} , N, SK_{Fi} , C_m , H''\} \tag{4.3}$$

Moreover, in the case of integrity violation discarded the received message and the functionality of SDA algorithm is presented in Table 4.2.

Table 4.2: Algorithm 1 (*Message Receiving & Aggregation Algorithm at MN*)

```
Initialize $C_m$ = null
Message $RV_{MN} = \{ SN_{id} , TS_{SD_i} , N , SK_{Fi} , E_{SK_{S-R}} \{CD_i\} , H''\}$ received from SD
If ($TS_{MN}$ - $TS_{SD}$) < Δt then
    If $H''(CD_{SD})$ equals $H''(CD_{MN})$ then
        $C_m = RV_{MN_i} \| \text{“,”} \| RV_{MN_{i+1}} \| \text{“,”} \| RV_{MN_n}$
    Else
        Received message dropped owing to integrity violation
    End if
Else
    Drop outdated message
End if
```

4.4 Message Extraction at FN

In phase III, we introduce the secure message decryption (SMD) algorithm at the fog node (FN) that receives compress and encrypted messages $Dm_{FN} = \{MN_{id}, TS_{MN}, N, SK_{Fi}, C_m, H''\}$ from all MNs. Initially, the SMD algorithm examines the message freshness and integrity violation at the fog node.

Table 4.3: Algorithm 2 (*Message Extraction Algorithm at FN*)

```
Decrypt the message using symmetric key to get
$Dm_{FN} = \{MN_{id}, TS_{MN}, N, SK_{Fi}, C_m, H^{\prime\prime}\}$ from $MN$
If ($TS_{FS}$ - $TS_{MN}$) < Δt then
    If ($H^{\prime\prime}$ ($Em_{FS}$) equals $H^{\prime\prime}$ ($Em_{MN}$ ) then
        For count 1 to n
            $List_{EM_{SN}}$ = Split ($C_m$ , “:”) // Colon used as delimiter
            Extract $CD_i$ form $C_i$ by utilizing decompression
            if ($H^{\prime}$ ($C_{i_{SD}}$) equals $H^{\prime}$ ($C_{i_{SD}}$) then
                Extract $HPV$ from $List_{EM_{SN}}$
                If ($HPV_{Ri} = HPV_{Oi}$) $then$
                    Insert Boolean for same values
                Else
                    Store values without change in local repositories
                End if
            Else
                Received message dropped owing to integrity violation
            End if
    Else
        Received message dropped owing to integrity violation
    End if
Else
    Drop outdated message
End if
```

In this context, the symmetric key-based encryption is utilized to decrypt the received message. Next, check the timestamp of the received message ($\boldsymbol{TS_{FS}}$ - $\boldsymbol{TS_{MN}}$) < Δt. In case the condition is true, then calculate the hash function $\boldsymbol{H''(Em_{FS})}$ of received message and compare with the pre-computed hash $\boldsymbol{H''(Em_{MN}}$) in the message. After calculating the hash, extract the received message. To extract the original healthcare values loop is utilized from 1 to n where n is the number of sensor nodes that forwards health parameters. The FN decompresses the healthcare information and split values $\boldsymbol{C_m}$ on the basis of colon. The list of encrypted messages $\boldsymbol{List_{EM_{SN}}}$ is extracted to individually decrypt the health parameter values. Furthermore, extract the individual sensor node messages by utilizing the decompression method. Then, calculate the hash for each Ci to extract the healthcare parameter values of each SN as given in Table 4.3.

4.4.1 Removal of Redundant Data

In phase IV, the SMD algorithm calculating the hash of extracted values $H'(C_{i_{SD}})$ after completing the encryption procedure. Then, compare the extracted health parameter values of the last received healthcare parameter values (e.g blood pressure, heart rate, and temperature) of the same sensor node. if any received values are the same as the last received values then store Boolean value instead of storing whole values again in the FoG server. Finally, FN formatting the extracted healthcare parameters. Afterward, it transmits the formatted healthcare information to the medical server. In the case of compression, coded numbers are used to convert the message into bits by applying binary values of 4-bits. For predefine values of sensor nodes (SN =9), Ciphertext at sensor nodes (Ci = 513,806), timestamp (TS = 8,311,723) of 32 bits, take into account ciphertext of 64 bits, hash method of 64 bits and 16 bits of node id. In this context, the compression ratio is equal to the compression size divide by data size. It provides message size reduction up to 80% and also reduces energy consumption and transmission cost.

4.5 Summary

In this chapter, the functionality of our proposed scheme is discussed. Firstly, we consider data collection at sensor nodes and employing a message compression algorithm to compress the received healthcare parameter values. Secondly, the SMA algorithm is employed for data aggregation at MN. Finally, the SMD algorithm is employed at the fog node for data decryption and removal of redundant data.

CHAPTER 5

RESULTS AND ANALYSIS

5.1 Overview

We have validated our work using a simulation tool NS 2.35. An extensive simulation is conducted based on the simulation parameters and simulation scenario discussed in chapter 3. For comparison, this thesis considers EHDA, SPPDA, APPA, and ASAS schemes from the several schemes discussed in the literature review. These schemes are selected based on 4 requirements such as data aggregation, security, healthcare, fog computing because only these 4 schemes are fulfilled all the requirements. Therefore, our proposed solution is compared with existing related studies EHDA, SPPDA, APPA, and ASAS and this comparison shows the supremacy of our scheme.

In Figure 5.1, we determine the communication cost for the transmission of aggregated data in the network. Results have shown that our proposed solution provides less communication cost while comparing with existing related schemes. Generally, a large size of data consumes more energy than smaller data. In this context, when 16000 bytes of information is transmitted from the SNs then ASAS, APPA, SPPDA, and EHDA transmit 15200 bytes, 14000 bytes, 11550 bytes, and 9300 bytes sequentially. Hence, ASAS provide maximum cost owing to the transmission of large data over the network. our proposed ESDTA scheme only transmits 8860 bytes because redundant values of healthcare parameters are replaced with I bit Boolean values. Results show that ESDTA provides 40%, 32%, 16%, and 3% less communication cost as compared with ASAS, APPA, SPPDA, and EHDA, respectively.

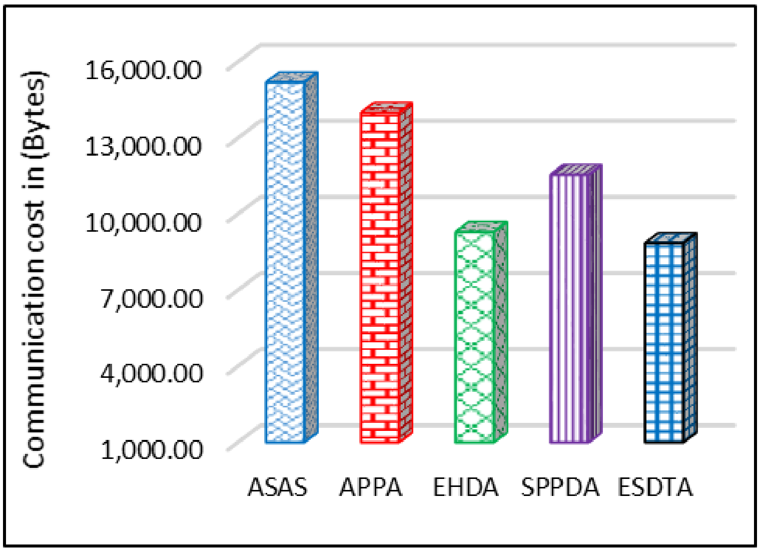


Figure 5.1: Communication Cost in Terms of Bytes Exchange

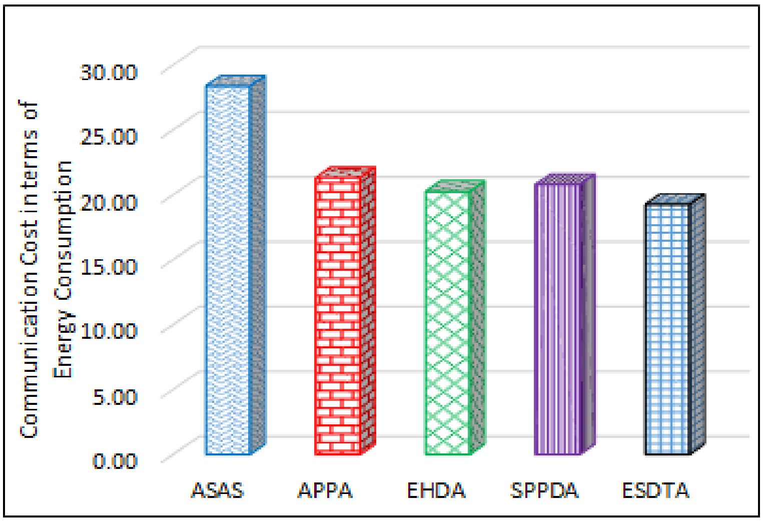


Figure 5.2: Communication Cost in Terms of Energy Consumption

The communication cost for energy can be determined by $\mathrm{C}_c = (\mathrm{E}_s * \mathrm{N}) + (\mathrm{M} * \mathrm{E}_r) + (\mathrm{D} * \mathrm{E}_s)$. Therefore, Es denotes the energy consumption for an individual message, N represents the number of forwarding messages, M denotes the number of received messages, and D represents dropped packets. In Figure 5.2, we illustrate that 96 messages are forwarded over the network. In this scenario, the consumption of energy against considered schemes like 21.7352 µJules, 22.2431 µJules, 22.6453 µJules, 22.8436 µJules, and 28.3795 µJules for ESDTA, EHDA, SPPDA, APPA, and ASAS, respectively. The transmission power E_s = 0.6143 µJules and receiving power E_r = 0.052 µJules also considered. Results illustrate that the proposed scheme archives 3%, 5%, 6%, and 23% less communication cost in term of energy in contrast with existing schemes EHDA, SPPDA, APPA, and ASAS, respectively.

In Figure 5.3, we consider the computation cost based on the number of smart devices. Hence, we analyze our proposed scheme the existing related schemes like EHDA, SPPDA, APPA, and ASAS. During data aggregation, MN aggregates the patient healthcare data. FN extracts patient data to remove redundant data. In Figure5.6, ESDTA compares with data aggregation schemes. we consider the results when the number of nodes is 40, the computational cost of ASAS, EHDA, APPA, SPPDA, ESDTA is 25.67 ms, 16.79 ms, 24.31 ms, 20.06 ms, 15.34 ms, respectively. Moreover, ESDTA provide 30%, 4%, 26%, and 14% respectively. Results of simulation prove that our proposed scheme has less computation cost as compared with other schemes.

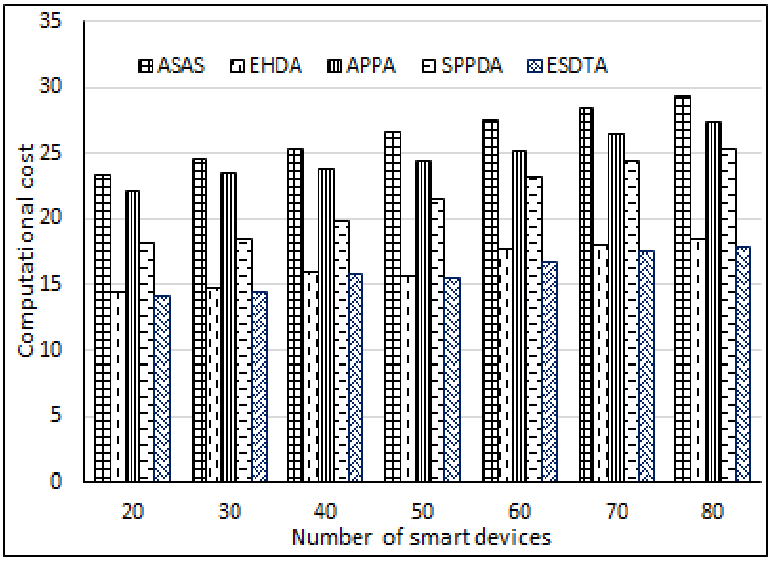


Figure 5.3: Computation Cost

We analyze the consumption of energy while aggregating data at MN nodes. Initially, we set the energy of each node is 12,000 joules. The trace files are utilized to print the remaining energy of nodes. the AWK files are employed to calculate the energy consumption by considering the difference between the currently received and last received values.

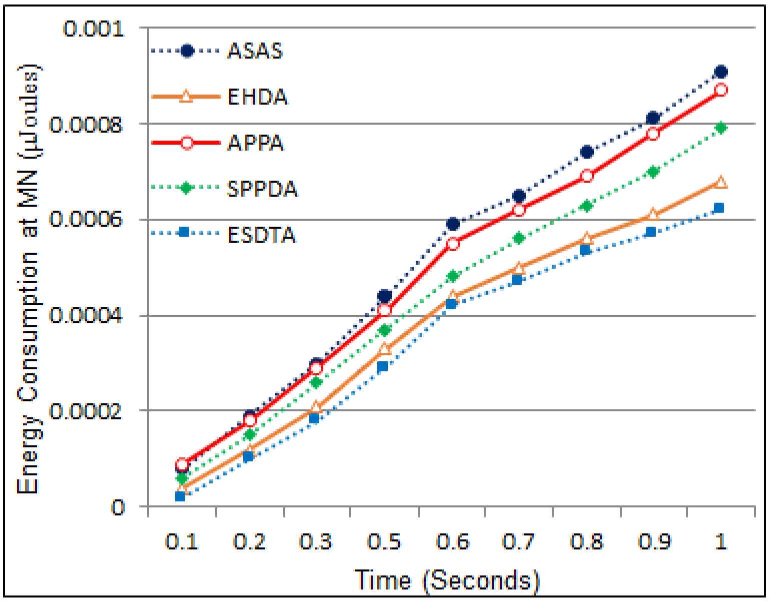


Figure 5.4: Energy Consumption at MN

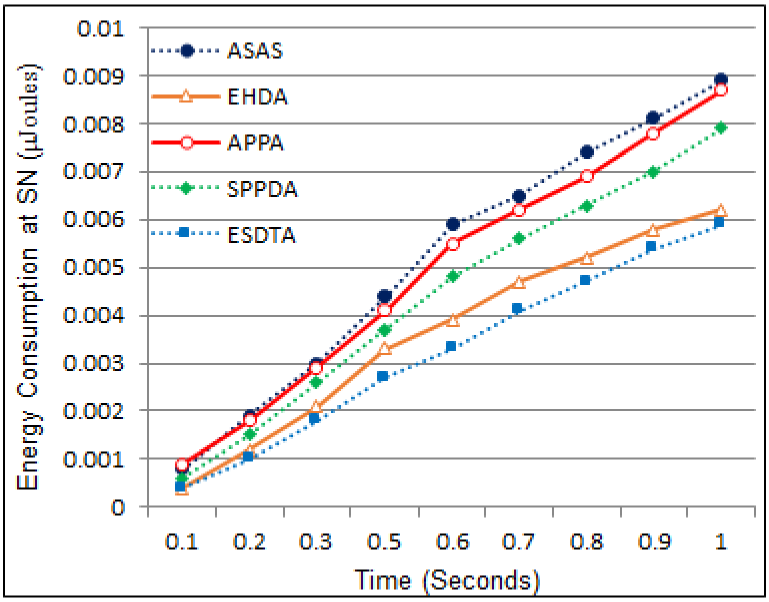


Figure 5.5: Energy Consumption at SN

Figure 5.4, demonstrates the influence of more energy utilization of MN in specific seconds while aggregating data from SNs. Results illustrate that ESDTA at MN consumes 0.00018 µJoules at 0.3 seconds because it only aggregates data from the sensor nodes. At the time of 0.6 seconds, MN consumes 0.00042 µJoules energy because data aggregated and transmitted toward the fog node simultaneously. Moreover, At the specific time of 9 seconds, ASAS, EHDA, APPA, SPPDA, ESDTA consumes energy of 0.00081 µJoules, 0.00064 µJoules, 0.00078 µJoules, 0.00073 µJoules, 0.00057 µJoules, respectively. Figure 5.5, illustrates the consumption of energy while transmitting data. The initial energy of each sensor node is 12000 joules. Sensor nodes that fulfill the query requirements then only those sensor nodes encrypting and transmitting the message. At the specific time of 6 seconds, ESDTA, EHDA, SPPDA, APPA, ASAS consumes energy of 0.00331 µJoules, 0.00396 µJoules, 0.00484 µJoules, 0.00553 µJoules, 0.00597 µJoules respectively. Results prove that the proposed approach provides 6%, 13%, 19%, and 22% better utilization of energy both at the SNs by comparing with EHDA, SPPDA, APPA, and ASAS, respectively.

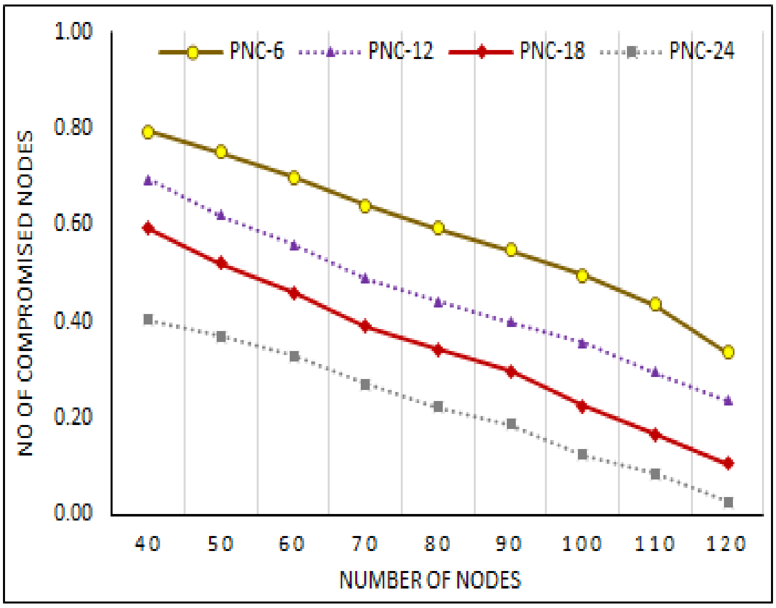


Figure 5.6: Probability of Compromised nodes

In the case of secure data communication, malicious sensor nodes can also take part in data exchange. Therefore, we calculating the flexibility for node capturing by measuring the probability of compromised nodes as $Pr_C = 1 - (\frac{N-3}{C})/(\frac{N-2}{C}) = \frac{C}{N-2}$ where N and C denote responding and compromised nodes respectively. Figure 5.6 shows that the Pr_C probability of responding nodes changes from 40 to 120 as an independent variable. we considered the results when the number of responding nodes is 120, where the probability of compromise nodes is 0.362109, 0.28219, 0.22328, 0.18438 for PCN =6,12,18,24 sequentially.

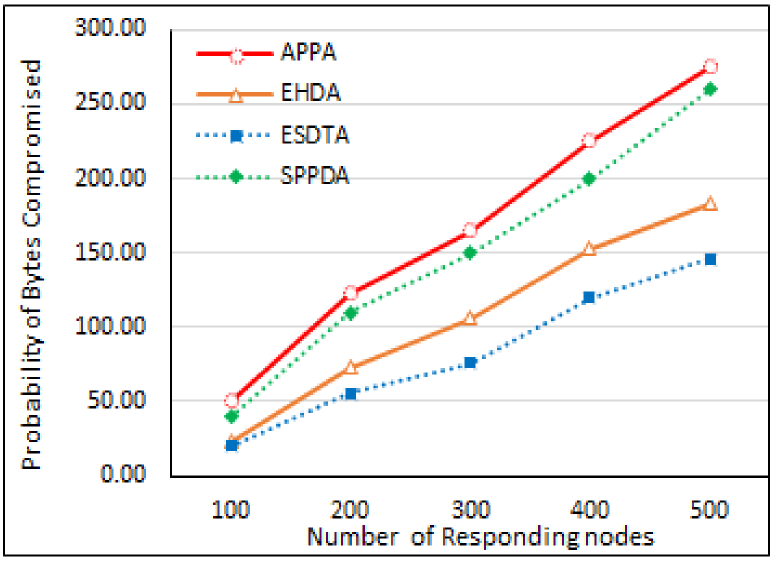


Figure 5.7: Probability of Compromised Bytes

In Figure 5.7, we consider the probability of compromised bytes while communicating. $Pr_{\eta} = 1 - (\frac{M-1}{\eta - 1})/(\frac{M}{\eta}) = \frac{\eta}{M}$ where η represents the number of compromised bytes from the whole M message bytes. We consider the 200 responding nodes where compromised bytes are 76.634 bytes, 106.903 bytes, 150.092 bytes, and 165.624 bytes for ESDTA, EHDA, SPPDA, and APPA respectively. The results show that the proposed approach provides 15%, 37%, and 44% less number of compromised nodes as compared with EHDA, SPPDA, APPA, respectively.

Figure 5.8, The original data size is selected from 100-500 bytes are forwarded for storage to observe the storage utilization of our proposed scheme with other related schemes. For example, In ESDTA the patient temperature is the same as the last received value so instead of storing the whole value a 1-bit Boolean value is stored.

Then, ESDTA, EHDA, and SPPDA compress data up to 90 bytes, 150 bytes, 175 bytes sequentially. On the other hand, APPA and ASAS provide storage of 300 bytes. Results illustrate that the ESDTA provides 20% better storage than EHDA. In case of SPPDA and APPA and ASAS, proposed scheme provide 70% better data storage as compared with other schemes.

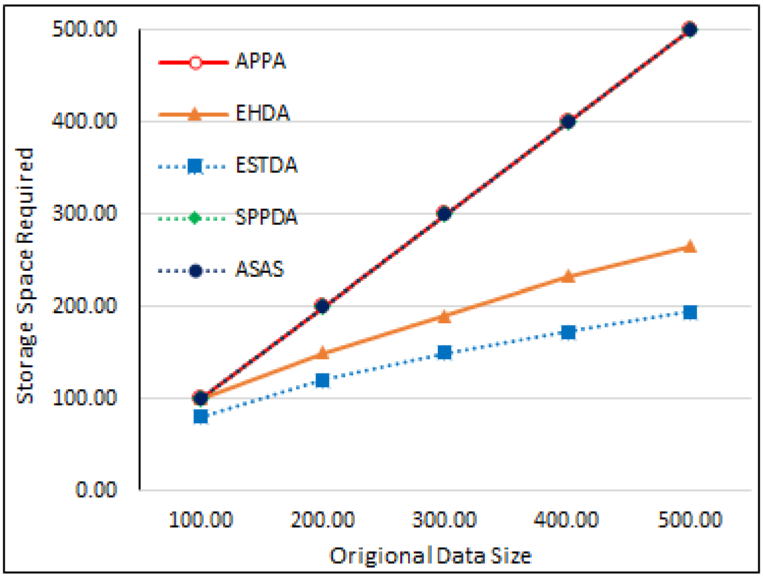


Figure 5.8: Storage Cost

5.2 Summary

In this chapter, the ESDTA scheme is compared with the other 4 related schemes. In presenting graphs, ESDTA provides 23% better communication cost in terms of bytes exchange and energy consumption, 19% better computational cost in terms of no of nodes, 15% better energy consumption in terms of node, 57% better storage in terms of data size, 32% less number of compromised in terms of bytes and nodes.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Overview

Internet of things (IoT) plays an essential role in digital transformation. IoT is revolutionizing our daily life concerns, particularly smart healthcare-based applications. IoT-enabled wireless sensors are deployed to collect the information. Sensor nodes forward the collected information to the base station by collaborating with intermediate nodes. Smart healthcare devices securely aggregate healthcare information and forward healthcare data to the base station. However, existing studies still facing communication, storage, and energy overhead issues. The main problem that relaying the data from one cell phone/collector to another is not secure. In the case of non-collaborative collectors in the nearby neighbor may be the malicious node and causing a denial of service attack. This thesis proposed an Efficient and Secure Data Transmission and Aggregation (ESDTA) scheme for lightweight and secure data transmission. A secure message aggregation (SMA) algorithm is employed to aggregate data at Mobile nodes (MN). Healthcare parameter values are aggregated by using the colon as a delimiter. Moreover, a secure message decryption (SMD) algorithm is employed at the fog node (FN). The proposed algorithm provides lightweight and secure data transmission by applying symmetric key-based data encryption and removing redundant healthcare parameter values from transmitted data. The simulation scenario for ESDTA proposed scheme is implemented through simulation tool NS2.35. We have compared ESDTA with existing related studies EHDA, SPPDA, APPA, and ASAS. The proposed scheme is compared with the related

research studies and provide 23% better communication cost in terms of bytes exchange, 19% better computational cost, 15% better energy utilization, 57% better storage, and 32% less number of compromised bytes. Hence, results prove the sovereignty of the proposed work.

6.2 Summary of your contribution

In this thesis, we present the list of simulation parameters that are implemented in the simulation scenario. First, we proposed the secure data aggregation algorithm at the mobile node to aggregate the received info of SNs. A message extraction algorithm is implemented at the fog node. It extracts healthcare parameter values and also removes redundant values. Second, the flow charts are presented to understand the flow of both algorithms at MN and FN. Finally, a comparative analysis is conducted for energy consumption, computational cost, communication cost, probability of compromised nodes, and data storage. Hence, we provide the results of our proposed scheme by comparing it with other existing schemes.

6.3 Future Work

In the future, we will consider data anonymity and authentication for hiding the identity of the patient to preserve the integrity of the data. Moreover, emergencies are also properly handled at remote locations by considering any smart and priority-based healthcare data transmission mechanism in emergencies. In the future, we will consider the security and storage perspective at the cloud server. Moreover, these challenges are explored to open a path for future research studies.

REFERENCES

[1] M. Aazam, S. Zeadally, and K. A. Harras, "Fog Computing Architecture, Evaluation, and Future Research Directions," *IEEE Communications Magazine*, vol. 56, no. 5, pp. 46–52, 2018.

[2] A. Kumar, S. Zeadally, and D. He, "Taxonomy and analysis of security protocols for Internet of Things," *Futur. Gener. Comput. Syst.*, vol. 89, pp. 110–125, 2018.

[3] 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, 2017.

[4] R. Mahmud, F. L. Koch, and R. Buyya, "Cloud-Fog Interoperability in IoT-enabled Healthcare Solutions," in *19th International Conference on Distributed Computing and Networking*, 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 (Switzerland)*, vol. 19, no. 19, pp. 1–25, 2019.

[6] A. Gatouillat *et al.*, "Internet of Medical Things: A Review of Recent Contributions Dealing with Cyber-Physical Systems in Medicine," *IEEE Internet Things*, vol. 5, no. 5, pp. 3810–3822, 2019.

[7] T. Nazir and M. T. Banday, "Green Internet of Things : A Survey Of Enabling Techniques," in *International Conference on Automation and Computational Engineering (ICACE)*, 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, pp. 1–28, 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, pp. 1–17, 2020.

[11] W. Wang, L. Yang, Q. Zhang, T. Jiang, and S. Member, “Securing On-Body IoT Devices By Exploiting Creeping Wave Propagation,” *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 696–703, 2018.

[12] Z. Luo, W. E. I. Wang, J. Xiao, Q. Huang, T. A. O. Jiang, and Q. Zhang, “Authenticating On-Body Backscatter by Exploiting Propagation Signatures,” *Proc. ACM Interactive, Mobile, Wearable Ubiquitous Technol.*, vol. 2, no. 3, pp. 1–22, 2018.

[13] H. Dubey *et al.*, “Fog computing in medical internet-of-things: architecture, implementation, and applications,” *Scalable Comput. Commun.*, pp. 281–321, 2017.

[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),” *Wirel. 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, pp. 1–16, 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. Sens. Networks*, 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 *IEEE 12th International Conference on Compatibility, Power Electronics and Power Engineering, CPE-POWERENG*, 2018, pp. 1–6.

[18] L. O. A. I. A. Tawalbeh, S. Member, R. Mehmood, and S. Member, “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. Surv. Tutorials*, vol. 20, no. 1, pp. 416–464, 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, 2016.

[22] R. Dantu, I. Dissanayake, and S. Nerur, "Exploratory Analysis of Internet of Things (IoT) in Healthcare : A Topic Modeling Approach," vol. 6, pp. 5224–5232, 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, 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," *Telecomm. Policy*, vol. 37, no. 4–5, pp. 372–386, 2013.

[26] M. Engineer, R. Tusha, A. Shah, and K. Adhvaryu, "Insight into the Importance of Fog Computing in Internet of Medical Things (IoMT)," in *International Conference on Recent Advances in Energy-Efficient Computing and Communication, (ICRAECC)*, 2019, pp. 1–7.

[27] W. Tang, J. U. Ren, K. Zhang, D. Zhang, and Y. Zhang, "Efficient and privacy-preserving fog-assisted health data sharing scheme," *ACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–23, 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. Informatics*, pp. 1–10, 2020.

[29] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Comput. Networks*, vol. 76, pp. 146–164, 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, 2017.

[31] J. Shen, S. Chang, J. Shen, Q. Liu, and X. Sun, "A lightweight multi-layer

authentication protocol for wireless body area networks," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 956–963, 2018.

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

[33] M. Humayun and N. Z. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT — A Survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[34] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, "Advanced internet of things for personalised healthcare systems: A survey," *Pervasive Mob. Comput.*, vol. 41, pp. 132–149, 2017.

[35] 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," *Univers. Access Inf. Soc.*, vol. 18, pp. 837–869, 2018.

[36] 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.

[37] 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," *Egypt. Informatics J.*, vol. 18, no. 2, pp. 113–122, 2017.

[38] A. Ramadhan, "A Survey of Security Aspects for Internet of Things in Healthcare," vol. 376, pp. 1237–1247, 2016.

[39] 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.

[40] V. Chang, F. Firouzi, N. Constant, K. Mankodiya, M. Badaroglu, and B. Farahani, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2017.

[41] S. M. R. Islam, D. Kwak, M. H. 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.

[42] 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, pp. 1–30, 2020.

[43] 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, 2020.

[44] 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, 2018.

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

[46] 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, pp. 163–174, 2019.

[47] D. Kumar and S. Chauhan, "IoT based healthcare services for monitoring post injury," in *International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2019, pp. 293–296.

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

[49] H. Wang, Z. Wang, and J. Domingo-Ferrer, "Anonymous and secure aggregation scheme in fog-based public cloud computing," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 712–719, 2018.

[50] R. Lu, S. Member, and K. Heung, "A Lightweight Privacy-Preserving Data Aggregation Scheme for Fog Computing-Enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[51] Z. Guan *et al.*, "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT," *J. Netw. Comput. Appl.*, vol. 125, pp. 82–92, 2019.

[52] 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.

[53] 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, 2018.

[54] 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.

[55] R. K. Kanth and P. Liljeberg, “Information and Communication System Technology ’ s Impacts on Personalized and Pervasive Healthcare : A Technological Survey,” in *IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, 2014, pp. 1–5.

[56] 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, 2018.

[57] R. A. Khan, “The state-of-the-art wireless body area sensor networks : A survey,” vol. 14, no. 04, pp. 1–23, 2018.

[58] B. Mbarek and A. Meddeb, “Energy efficient security protocols for wireless sensor networks : SPINS vs TinySec,” in *International Symposium on Networks, Computers and Communications, ISNCC*, 2016, pp. 1–4.

[59] T. Han, L. Zhang, S. Pirbhulal, W. Wu, V. Hugo, and C. De Albuquerque, “A novel cluster head selection technique for edge-computing based IoMT systems,” vol. 158, pp. 114–122, 2019.

[60] S. Lim, T. H. Oh, Y. B. Choi, and T. Lakshman, “Security Issues on Wireless Body Area Network for Remote Healthcare Monitoring,” in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 2010, pp. 327–332.

[61] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, “SoK : Security and Privacy in Implantable Medical Devices and Body Area Networks,” *IEEE Symp. Secur. Priv.*, pp. 524–539, 2014.

[62] 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, pp. 1–22, 2017.

[63] H. Khemissa and D. Tandjaoui, “A Lightweight Authentication Scheme for E-health applications in the context of Internet of Things,” in *9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015, pp. 90–95.

[64] 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. Networks*, vol. 129, pp. 429–443, 2017.

[65] A. B. B. Soufiene and A. T. and H. Youssef, "Lightweight and confidential data aggregation in healthcare wireless sensor networks," *Emerg. Telecommun. Technol.*, vol. 27, no. 4, pp. 576–588, 2017.

[66] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, pp. 1–17, 2019.

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

[68] H. Abdulaziz *et al.*, "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.

[69] M. Al Ameen and J. Liu, "Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications," *J. Med. Syst.*, vol. 36, pp. 93–101, 2012.

[70] 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.

[71] A. Paul, H. Pinjari, W.-H. Hong, H. C. Seo, and S. Rho, "Fog Computing-Based IoT for Health Monitoring System," *J. Sensors*, pp. 1–7, 2018.

[72] 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 *International Conference on High Performance Computing and Simulation, HPCS,* 2018, pp. 949–956.

[73] 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. Inform. Decis. Mak.*, vol. 17, no. 1, pp. 1–19, 2017.

[74] 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, 2018.

[75] A. Ullah, I. Sehr, M. Akbar, and H. Ning, “FoG assisted secure De-duplicated data dissemination in smart healthcare IoT,” in *IEEE International Conference on Smart Internet of Things, SmartIoT*, 2018, pp. 166–171.

[76] R. S. Sharon and R. Joseph Manoj, “E-health care data sharing into the cloud based on deduplication and file hierarchical encryption,” in *International Conference on Information Communication and Embedded Systems (ICICES)*, 2017, pp. 1–6.

[77] 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, 2019.

[78] 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, 2018.

[79] T. D. Dang and D. Hoang, “A data protection model for fog computing,” in *Second International Conference on Fog and Mobile Edge Computing (FMEC)*, 2017, pp. 32–38.

[80] M. Azeem and A. Ullah, “Secure Healthcare Data Aggregation Scheme for Internet of Things,” in *International Conference on Cyber-Living, Cyber-Syndrome and Cyber-Health.*, 2019, pp. 175–186.

[81] Y. Winnie, “Enhancing Data Security in IoT Healthcare Services Using Fog Computing,” in *International Conference on Recent Trends in Advance Computing (ICRTAC)*, 2018, pp. 200–205.

[82] J. Demme *et al.*, “On the feasibility of online malware detection with performance counters,” *Int. Symp. Comput. Archit.*, vol. 41, no. 3, pp. 559–570, 2013.

[83] 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.

[84] I. Stojmenovic and S. Wen, “The Fog computing paradigm: Scenarios and security issues,” in *Federated Conference on Computer Science and Information Systems*, 2014, pp. 1–8.

[85] N. Bradai, L. Chaari Fourati, and L. Kamoun, “WBAN data scheduling and aggregation under WBAN/WLAN healthcare network,” *Ad Hoc Networks*, vol.

25, pp. 251–262, 2015.

[86] M. Li, L. Wenjing, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEE Wirel. Commun.*, vol. 7, no. 1, pp. 51–58, 2010.

[87] 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, 2017.

[88] 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, 2019.

[89] 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, 2015.

[90] P. Kumar and H. Lee, “Security Issues in Healthcare Applications Using Wireless Medical Sensor Networks: A Survey,” *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[91] 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, 2016.

[92] 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. Informatics*, vol. 13, no. 3, pp. 1227–1237, 2017.

[93] I. Ali, E. Khan, and S. Sabir, “Privacy-preserving data aggregation in resource-constrained sensor nodes in Internet of Things: A review,” *Futur. Comput. Informatics J.*, vol. 3, no. 1, pp. 41–50, 2018.

[94] K. Zhang, K. Yang, X. Liang, and X. S. Shen, “Security and privacy for mobile healthcare networks: from a quality of protection perspective,” *IEEE Wirel. Commun.*, vol. 22, no. 4, pp. 104–112, 2015.

[95] D. Wu, B. Yang, and R. Wang, “Scalable privacy-preserving big data aggregation mechanism,” *Digit. Commun. Networks*, vol. 2, no. 3, pp. 122–129, 2016.

[96] M. Al-Khafajiy, L. Webster, T. Baker, and A. Waraich, “Towards fog driven IoT healthcare: Challenges and framework of fog computing in healthcare,” in *ACM 2nd International Conference on Future Networks and Distributed Systems*, 2018, pp. 1–7.

[97] S. Macwan, N. Gondaliya, and N. Raja, “Survey on Wireless Body Area Network,” 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, 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, 2017.

[100] M. Wazid, A. K. Das, and R. Hussain, “Authentication in cloud-driven IoT-based big data environment: survey and outlook,” *J. Syst. Archit.*, vol. 97, pp. 185–196, 2018.

[101] U. Ahsan and A. Bais, “A Review on Big Data Analysis and Internet of Things,” in *IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 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. Surv.*, vol. 49, no. 4, pp. 1–38, 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. Networks*, pp. 1–9, 2018.

[105] A. Ullah, K. Hamza, M. Azeem, and F. Farha, “Secure Healthcare Data Aggregation and De- duplication Scheme for FoG-orineted IoT,” in *IEEE International Conference on Smart Internet of Things (SmartIoT)*, 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, 2018.

[107] L. Xiang, J. Luo, and A. Vasilakos, “Compressed data aggregation for energy efficient wireless sensor networks,” in *8th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, (SECON)*, 2011, pp. 46–54.

[108] Y. Zhang *et al.*, “HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems,” *IEEE Trans. Ind. Informatics*, vol. 14, no. 9, pp. 4101–4112, 2018.

[109] A. Al-Fuqaha, “AL-FA-Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” *IEEE Commun. Surv. Tutorials (Accepted Publ.*, vol. 1, no. 2, pp. 78–95, 2013.

[110] E. Bertino, “Data security and privacy Concepts, approaches, and research directions,” in *IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, 2016, pp. 400–407.

[111] Y. Zhang, Q. Chen, and S. Zhong, “Privacy-Preserving Data Aggregation in Mobile Phone Sensing,” *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 5, pp. 980–992, 2016.

[112] 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.

[113] 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, pp. 1–18, 2017.

[114] 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. Networks*, pp. 1–12, 2017.

[115] X. Wang, L. E. I. 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.

[116] 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, 2012.

[117] M. Wazid and S. Member, “A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things,” *IEEE Access*, vol. 8, no. 1, pp. 88700–88716, 2020.

[118] Y. Gai, L. Zhang, and X. Shan, “Energy efficiency of cooperative MIMO with data aggregation in wireless sensor networks,” in *IEEE Wireless Communications and Networking Conference, (WCNC)*, 2007, pp. 792–797.

[119] S. Sarkar, S. Member, S. Chatterjee, and S. Member, “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, 2018.

[120] 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, 2016.

APPENDIX A

LIST OF PUBLICATIONS

i. A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT—A Survey," in *IEEE Access*, vol. 9, pp. 16849-16865, 2021

ii. M. Shafiq, H. Ashraf, A. Ullah, M. Masud, M. Azeem et al., "Robust Cluster-Based Routing Protocol for IoT-assisted Smart Devices in WSN," *Computers, Materials & Continua*, vol. 67, no.3, pp. 3505–3521, 2021.

iii. A. Ullah, K. Hamza, M. Azeem and F. Farha, "Secure Healthcare Data Aggregation and Deduplication Scheme for FoG-Orineted IoT," *2019 IEEE International Conference on Smart Internet of Things (SmartIoT),* Tianjin, China, 2019, pp. 314-319

iv. M.Azeem, A. Ullah "Secure Healthcare Data Aggregation Scheme for Internet of Things. In: Ning H. (eds) Cyberspace Data and Intelligence, and Cyber-Living, Syndrome, and Health. CyberDI, CyberLife. Communications in Computer and Information Science, vol 1137, Springer, Singapore, 2019, pp. 1-13.