SECURE DATA AGGREGATION AND DISSEMINATION USING BATCH KEYING IN INTERNET OF MEDICAL THINGS

By

JAVERIA RASHEED

NATIONAL UNIVERSITY OF MODERN LANGUAGES

ISLAMABAD

August, 2024

Secure Data Aggregation and Dissemination using Batch Keying in the Internet of Medical Things

By

JAVERIA RASHEED

BSCS, Air University, 2021

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

Computer Science

To

FACULTY OF ENGINEERING & COMPUTER SCIENCE

NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD

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 Computing for acceptance

Thesis Title: Secure Data Aggregation and Dissemination using Batch Keying in the Internet of Medical Things

Submitted By: Javeria Rasheed **Registration #:** 66 MS/CS/S22

Master of Science in Computer Science (MSCS)
Degree Name in Full

Computer Science
Name of Discipline

Dr. Ata Ullah
Research Supervisor

Signature of Research Supervisor

Research Co-Supervisor

Signature of Research Co-Supervisor

Dr. Sajjad Haider
Head of Department (CS)

Signature of HoD (CS)

Dr. M. Noman Malik
Name of Dean (FEC)

Signature of Dean (FEC)

August 26th, 2024

AUTHOR'S DECLARATION

I Javeria Rasheed

Daughter of Abdul Rasheed

Registration # 66 MS/CS/S22

Discipline Computer Science

Candidate of **Master of Science in Computer Science (MSCS)** at the National University of Modern Languages do hereby declare that the thesis **Secure Data Aggregation and Dissemination using Batch Keying in the Internet of Medical Things** submitted by me in partial fulfillment of MSCS degree, is my original work, and has not been submitted or published earlier. I also solemnly declare that it shall not, in the future, be submitted by me for obtaining any other degree from this or any other university or institution. I also understand that if evidence of plagiarism is found in my thesis/dissertation at any stage, even after the award of a degree, the work may be canceled and the degree revoked.

Signature of Candidate

Javeria Rasheed

Name of Candidate

26 Aug, 2024

Date

ABSTRACT

Title: Secure Data Aggregation and Dissemination using Batch Keying in Internet of Medical Things.

The Internet of Medical Things (IoMT) is a new fastest growing technology that consist of wearable medical sensors to collect patient's medical data and transmit it to the cloud repository for storage. It enables real time analysis of patient data and allow doctors to take preventive measures accordingly. The security of sensitive medical data is mandatory while transferring it via the Internet. The existing base scheme emphasizes on reducing the transmission costs and maintains the security of IoMT system. The value of the secret key is null at the initial phase while sending data from sensor node (SN) to head node (HN). Due to the null value, the risks of security attacks by intruders are increased. The Proposed Batch Key based Secure Data Aggregation (BK-SDA) scheme focus on minimizing the risks of security attacks and reducing the transmission cost by improving the algorithms. In Batch Key based Secure Data Aggregation at Head Node (BKSDA-HN) algorithm, it chooses a random number for secret key rather than null value at the initial phase. It also applies batch verification on received data to ensure its authenticity and then performs aggregation at HN. On the other Batch Key based Secure Data Extraction at Fog Server (BKSDE-FS) algorithm, the batch verification is also applied on received data before starting the process of data extraction. The BK-SDA scheme is implemented on NS 2.35 simulation tool to check the performance of proposed algorithms. In NS 2.35, the TCL files is used for nodes placement and C++ language to control the functionality of nodes and AWK files to extract results. The performance of BK-SDA is evaluated under three performance evaluation metrics like communication cost, computational cost, and energy consumption cost. The experimental result show that the performance of BK-SDA scheme is better than other existing schemes to reduce communication cost and energy consumption cost but it consumes more computational cost as compare to others. The proposed BK-SDA scheme reduce the data transmission costs in terms of communication and energy consumption cost and improve the security algorithm to make the system more efficient and secure for data communication.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IoT	-	Internet of Things
IoMT	-	Internet of Medical Things
DC	-	Data Center
MO	-	Medical Organization
KGC	-	Key Generation Center
CSP	-	Cloud Service Provider
TPA	-	Third-Party Auditor
DO	-	Data Owner
CRT	-	Chinese Remainder Theorem
DMK	-	Distributed Multiparty Key
GH	-	Group Head
HN	-	Head Node
MN	-	Mobile Node
SN	-	Sensor Node
HN	-	Head Node
CS	-	Cloud Server
MEC	-	Mobile Edge Computing
FS	-	Fog Server
PCC	-	Public Cloud Center
ES	-	Edge Server
TD	-	Terminal Device
BS	-	Base Station
CH	-	Cluster Head
WN	-	Wireless Node
SKG	-	Secure Key Generator
SK	-	Secret Key
CA	-	Certificate Authority
TCL	-	Tool Command Language

LIST OF SYMBOLS

SN_{ij}	-	Sensor Node ID
CS_{ij}	-	Cipher Message at Sensor Node
Em_{ij}	-	Encrypted Message at Sensor Node
ts_{ij}	-	Timestamp of Sensor Node
TS_{ij}	-	Timestamp of Head Node
A_m	-	Aggregated Message
S_K	-	Secret Key
$\oplus$	-	XOR Operation
σs_{ij}	-	Hash Function of Sensor Node
σa_{ij}	-	Hash Function of Head Node
HN_{ij}	-	Head Node ID
BK_{ij}	-	Batch Key between Sensor Node and Fog Server
OM_{ij}	-	Original Message extracted at the Fog Server

ACKNOWLEDGMENT

First of all, I 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 was extended from several sources for which I would like to express my sincere thankfulness and gratitude. Yet, there were significant contributors to 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 administration of the Department of Computer Sciences who supported me throughout 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.

DEDICATION

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.

CHAPTER 1

INTRODUCTION

1.1 Overview

The Internet of Things (IoT) is a network of interconnected devices equipped with sensors to communicate and exchange data over the Internet. The key concept of IoT is to allow embedded sensors in computing devices to collect and share data with minimal human intervention. This data is used for decision-making, data automation, and remote monitoring [1]. In IoT-based systems, sensors detect objects in their surrounding and convert them into electrical signals. These signals are then used for processing, data transmission, data analysis, remote monitoring, and initiating actions within the IoT ecosystem [2].

IoT devices have many innovative applications in various fields of life such as healthcare systems, transportation, agriculture, industrial settings, security systems, and many more as shown in Figure 1.1. In the healthcare system, wearable sensor devices remotely monitor patient data to provide immediate treatment if needed. For transportation, real-time vehicle tracking and traffic management sensors are useful for tracking vehicle location and movement and monitoring traffic flows to make decisions accordingly. In an agricultural IoT setting, the soil sensors and trackers monitor the conditions of the soil to improve the production of food and vegetables. In Industrial systems, IoT devices monitor the working of heavy machines, optimize their operations, and detect their maintenance issues easily. To maintain the system's security, the IoT devices provide smart security cameras, smart locks, and motion sensors to enable remote surveillance [3].

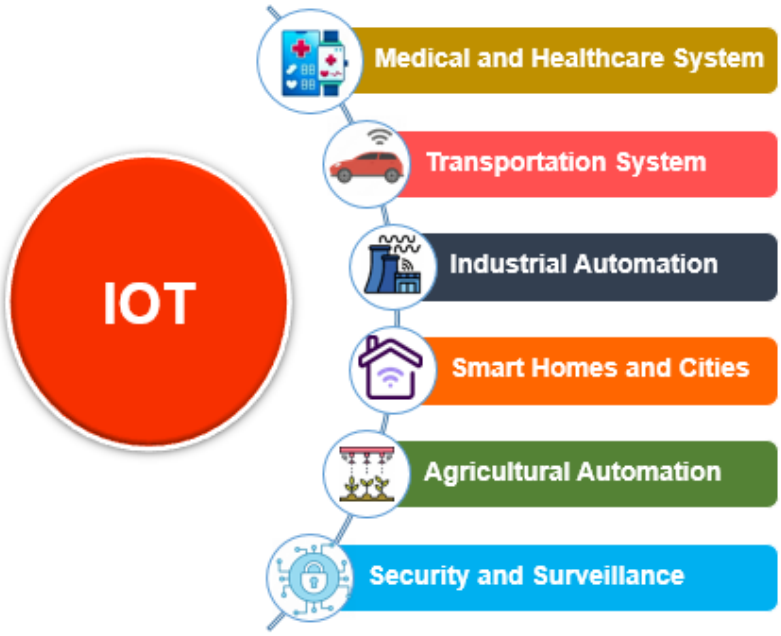

Figure 1.1: Applications of IoT

The Wireless Body Area Network (WBAN) is a network of wearable sensors placed on or around the human body to monitor a patient's psychological data or other health-related metrics. These sensors collect data such as heart rate, body temperature, blood pressure, and movement, which can then be transmitted wirelessly to a central device, like a smartphone or a dedicated hub. In IoT, WBAN's play a significant role in the healthcare sector because they enable continuous, real-time health monitoring and provide valuable data for various e-health applications. This data can be further transmitted to cloud-based systems for analysis, storage, and access by healthcare professionals. The integration of WBAN with IoT facilitates the creation of smart healthcare solutions, enabling remote monitoring, early detection of health issues, and timely medical interventions [4].

Due to the massive growth of IoT applications, there is a need to analyze and remove redundancies in data before transmitting it to the cloud repository. Data Aggregation is a powerful technique to eliminate redundant data and improve the transmission cost [5]. The Internet of Medical Things (IoMT) based on WBAN plays a crucial role in collecting data from multiple sensing devices. During the data aggregation, the sensing devices collect and aggregate

the patient's data from the medical sensor nodes and then forward it to the fog server for extraction and the cloud server for storage [6].

However, IoT also exposes numerous threats to our daily lives, the main security threats are data breaches and service disruptions. The security threats in the IoT environment are related to our practical lives and indirectly influence our personal lives. Without reliable and secure IoT devices, these IoT applications can fail to meet the required demands of the systems [7]. In Wireless Sensor Networks (WSNs), IoT-based systems always worked to encounter security challenges, authentication problems, privacy issues, and storage complexities to maintain and improve the confidentiality, integrity, freshness, and accuracy of data [8].

Alongside data communications, security, and privacy are also quite challenging to securely aggregate and transmit healthcare data to Fog and cloud servers. There are several batch verification schemes have already been used to ensure secure data transmission across the network. However, these schemes are not sufficient to fulfill the requirements of a secure and privacy-protected system in the IoT paradigm [9].

1.2 Motivation

IoT is the biggest innovation in the field of information technology. IoT provides an interface to connect physical objects to the internet and make them smart objects. IoT is applicable in numerous fields of life like healthcare, grid systems, industries, agriculture, and many more [3]. While data transmission, security plays a significant role in preventing the network from unauthorized access and misuse of data. IoT applications offer valuable benefits during data communication via the Internet. However, it is also necessary for IoT-based systems to protect user privacy and ensure system security against vulnerabilities and attacks.

1.2.1 Architecture of Internet of Medical Things

In the past, the healthcare system relied only on physicians' decisions based on their expertise, patients' symptoms, and diagnostic reports. But now it is aided by the Internet of Medical Things (IoMT), doctors can monitor their patients or even their surroundings by using sensors via the Internet. The IoMT enables remote detection and control of objects across existing network infrastructures [10], [11]. The architecture of IoMT consists of three layers shown in Figure 1.2 such as IoMT Wearable devices, the Edge computing layer, and the Cloud Computing layer.

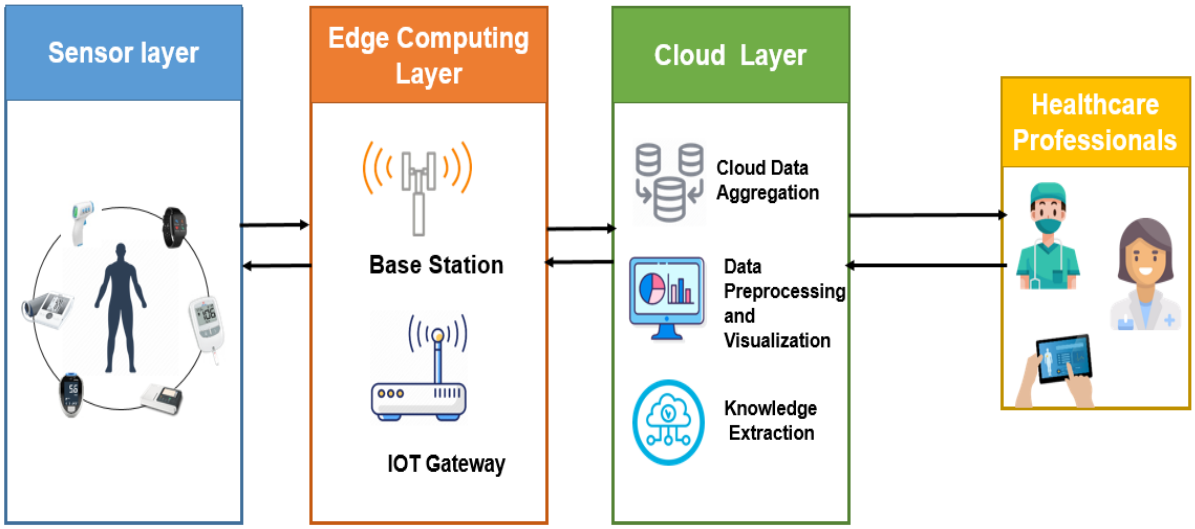

Figure 1.2: Architecture of Internet of Medical Things

In the first layer, the medical sensor devices are attached to the patient's body to gather the required data. These sensors are transformed into wearable devices like watches, shoes, or necklaces that measure the pulse rate, heartbeat, body temperature, glucose level, and other health-related parameters. The second layer also known as the Fog Layer acts as a middle layer between the cloud server and the IoMT device layer, which consists of local servers and gateway devices. This layer securely extracts and processes the data from sensing devices and then sends it to the cloud server for storage. The third layer is a cloud server layer that stores

the data in the cloud database, and healthcare professionals can access the patient's data anytime from the cloud server. This helps them to actively track the patient's data, which can be viewed on a smartphone, laptop, tablet, etc. The doctor then analyzes this data and provides feedback if any unusual or worse health condition is observed in the patient record [12]. The architecture shows how the patient's data is transmitted from sensing devices to the fog server and then stored on the cloud database. While designing an IoT-based healthcare system for real-time patient monitoring, it is essential to outline all the activities associated with the health application [13], [14].

1.2.2 Applications of the Internet of Medical Things

The development in the field of IoMT improves the quality of medical treatment by enabling remote monitoring and analysis of patient data. Wireless sensor devices collect and send real-time data to the doctors for examining patient's condition to detect potential healthcare issues and provide necessary medication or treatment on time. The major applications and benefits of the IoMT system are early disease prediction and diagnosis, remote access to healthcare records, human behavior recognition, telemedicine, and less resource utilization [15], [16].

The use of IoMT is increasing daily, so the privacy and security of data are also becoming an important factor in the healthcare system. In remote treatment, patient's data is stored in the hospital database and accessible to different stakeholders such as doctors, nurses, laboratory staff, etc. The security of sensitive medical data is mandatory to increase the efficiency and usefulness of the IoMT system [17], [18].

1.2.3 Constraints in the Internet of Medical Things

Although various techniques have existed to build a secure healthcare system, but few constraints still require attention are shown below:

i. Key Management:

Managing the secret keys that keep medical networks secure is a problem that needs to be solved. While there are multiple ways to fix some of these problems there isn't a single method that works well for wireless devices and ad-honc connections and establishing the healthcare network [19],[20].

ii. Device Management:

Effective device management is required to enhance asset utilization, increase throughput, and minimize maintenance expenses. Addressing this constraint ensures a thoughtful approach to optimizing device usage and improving operational efficiency while reducing all the disruptions in the IoMT ecosystem [21].

iii. Data Security and Privacy:

Smart wearable medical devices quickly gather and send information to the network, but many don't have reliable ways to send data securely. Also, it's not easy to control, update, and keep these devices safe from one central place. Because of this, important medical information can be at risk from intruders who could break the system and steal patients' sensitive healthcare data [22],[23].

iv. Computational Power:

Smart wearable devices have significantly expanded their systems in the remote healthcare monitoring domain. With a vast number of interconnected devices, handling and executing computational tasks within the IoT framework is still a challenge that needs to be overcome [24].

v. Security Threats:

Due to some outdated and inadequate healthcare defense systems, hackers may exploit the system by launching attacks to gain profits as much as they can. They employ attacks to destroy systems, hack hospital databases to sell patient data, threaten to expose private information, and even disrupt the power supply connection. It highlights the importance of taking enhanced security measures to establish a secure network for the transmission of sensitive medical information [25], [26].

1.3 Problem Background

While exchanging the data from sender to destination nodes through intermediate nodes, the intruders can manipulate the data at any of the intermediary nodes. It increases the risk of security attacks during the transmission of sensitive healthcare data in a network. To establish a wireless network, there are very limited resources such as memory, energy, computing power, and communication capabilities available. So, the risk of security attacks becomes more significant when smart devices consistently establish their connection with the Internet and they contain very limited resources. So, there is a need to build a system that fulfills the security requirements and consumes fewer resources during data transmission.

1.4 Problem Statement

Many batch verification methods have already been used to provide secure and efficient data aggregation during data transmission over the network. These methods also play a major role in reducing the complexity of communication and energy consumption costs and making the system more efficient. During Cryptographic operations, the Exclusive OR (XOR) operations are used for batch key creation rather than big multiplications to reduce the data transmission costs. The value of the secret key is null at the initial stage to reduce computational cost but it compromises security during data transmission. The intruders can recover the secret

key after some attempts. If the attacker has successfully found the secret key. So, he can easily find out the batch keys and once it is exposed the original message will also be recovered.

1.5 Research Questions

The research study will provide the answer to the following questions:

i. How does the XOR method secure the security strengths during data transmission?
ii. How does the Batch Keying Method reduce Computational, Communication, and Energy Consumption costs in IoMT-based systems?

1.6 Aim of the Research

The research aims to securely share the patients' healthcare aggregated data to the fog server and then save it in the central repositories in the cloud. There are many ways to securely transfer data to the cloud server but still, there is a need to establish a network that requires less computation, communication, and energy consumption costs.

1.7 Research Objectives

The objectives of this research study are:

i. To provide a secure data aggregated solution while ensuring the security strengths
ii. To reduce the communication and energy consumption cost as compared to existing schemes

1.8 Scope of Research Work

The research is focused on reducing the data transmission cost and making the system more secure and efficient for the healthcare environment. The transmission path and communication nodes are not completely secure while transmitting data from one place to another through the Internet. The efficient batch verification method is introduced in this research work to ensure data security. It also modifies the existing algorithms to minimize data transmission costs as well.

1.9 Thesis Organization

The rest of the thesis is organized as follows:

Chapter 2 provides background information on batch authentication and data aggregation schemes in the IoMT system to identify the research gaps, security challenges, system vulnerabilities, and transmission costs.

Chapter 3 presents the methodology of proposed schemes that consist of the analysis phase, design phase ,development phase, and the performance evaluation phase to understand the purpose, requirements, and solution of the proposed research work.

Chapter 4 offers a detailed description of batch key-based secure data aggregation protocol and the complete working of both algorithms for data aggregation and extraction presented in the section.

Chapter 5 will provide information on the simulation environment, system requirements, and tools for implementing the proposed algorithms. This section also presented the comparison results of the proposed scheme with three other existing schemes under the performance evaluation metrics of computational cost, communication cost, and energy consumption cost.

Chapter 6 will provide a complete summary of the proposed research work, and also include the key points for future work that should be considered in upcoming research.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

This chapter addresses the issues related to security while establishing a network in a healthcare system. These issues arise to make the system secure from security attacks. To protect the system, different batch verification and data aggregation schemes are introduced that have some benefits as well as some limitations that are going to be discussed in this chapter.

2.2 Batch key-based schemes in IoMT systems

In IoMT systems, the attackers consistently tried to retrieve patient's sensitive information and alter it, to jeopardize the privacy and security of data. The batch auditing and verification techniques identify the loopholes in the system and propose a solution to resolve them.

Said *et al*. [27] introduced the Secure Aggregated-Data Transmission Scheme (SATS) to ensure secure and light-weighted data transmission in IoT-enabled wireless sensor networks. In the existing schemes, the computational overhead at aggregator nodes is increased by the usage of complex multiplication operations for batch key generation. The current secure data aggregation algorithms used in healthcare systems also require a huge amount of memory space at the aggregator node. SATS resolves this problem by using an XOR operation for batch key verification as compared to multiplication, which reduces computational costs. SATS works in three phases: data gathering by sensor nodes and performing encryption, receiving encrypted

messages and aggregating them at the aggregator node, and finally message extraction at the fog node. The sensor nodes encrypt the data and send it to the aggregator node. Using XOR and secret keys, the node aggregates the data it has received and after that transmits the encrypted aggregated data to the fog server. The secret keys are used between the aggregate node and the fog node to make sure the communication between the nodes is safe. Secret keys are used by the fog node to decrypt data, while delimiters are used to extract the values of each sensor node. The Simulation results using NS 2 demonstrate that SATS offers better communication and computational cost as compared to existing schemes. The computational overhead is reduced by 14-59% at the head node, and 6% -51% at the FS, and communication cost is reduced by 6-12% for all nodes. In a resource-constrained wireless healthcare environment, SATS offers an effective method for secure data transfer with minimal computational and communication overhead.

The external cloud service providers cannot be reliable enough to ensure the integrity and security of information obtained from the cloud. Due to various technical and management challenges, the integrity verification process of cloud-based data is costly and difficult to implement on resource-constrained IoT devices. Hussein *et al*. [28] propose a secure and lightweight integrity-preserving data exchange (SL-IPDE) scheme in IoT cloud systems.SL-IPDE uses cryptographic hashing with cost-efficient mathematical operations and key chain method for dynamic integrity checking of data stored in cloud-based IoT systems. The cryptographic hash function with lightweight XOR operations generates a proof of minimizing integrity checking time. A key chain method implements a one-time key usage method to address security threats. A semi-trusted server is also utilized by SL-PDE to conduct batch integrity audits on the data exchanged and stored in the cloud environment on behalf of smart device users. It also ensures audits without local data replication. The experimental results of SL-PDE provide better integrity protection, key management, and privacy preservation systems for IoT-based cloud environments. Compared to existing solutions based on bilinear map-based pairing operations, it also significantly reduces computational overhead, communication, and storage costs. The SL-IPDE scheme with a semi-trusted third-party server efficiently manages the integrity verification process for resource-constrained IoT devices and enhances the performance by reducing the transmission cost making it reliable for cloud-based environments.

Wehao Wang *et al.* [29] proposed a Certificate-Based Remote Data Integrity Batch Auditing (CBRDIBA) protocol in cloud-based IoMT devices that are capable to resist collusion attacks. The CBRDIBA protocol generates two keys: a public key and a private key. The data owner forwards the public key to the cloud server to generate signatures for each data block using the provided public key. Both the signatures and blocks are then stored in the cloud. The data owner asked the cloud server for a block signature for sending a batch auditing request to the cloud server. In response, the cloud server will send the corresponding block signatures to the data owner. Using the private key, the data owner then validates the signatures. If the signatures are correct, it indicates that the data is safe and untampered. The CBRDIBA protocol security has been implemented by utilizing the Java Pairing-Based Cryptography (JPBC) Library within the framework of the random oracle model. Its performance is evaluated by comparing it with several other data integrity audition protocols under metrics like batch auditing, resistance against collusion attacks, absence of key escrow, anonymity, and Luca's error search. While employing a certificate-based cryptosystem, the protocol effectively resolves issues related to certificate management. The CBRDIBA protocol deploys efficient error search techniques such as Luca's search to address batch auditing failures instead of binary search and introduced timestamps integrated into the Hash Value Tags (HVTs) to prevent the system from expiring proofs. This evaluation encompasses its efficiency in both theoretical and experimental analysis of the protocol against a single data owner. It tackles the challenges of key escrow and secure channels. The evaluation process highlights the CBRDIBA protocol provides better security and resistance against the integrity issue to protect the system against the advanced level of collusion attacks. The protocol's efficiency is further underscored by its communication and computational proficiency in implementing advanced security measures in the current system.

To address the new issues brought by the enormous scale of IoT devices, dynamic membership of users, and changes in the number of devices, the paper examines effective group key management techniques. Maintaining access control of IoT data without the help of reliable online entities is essential for its security. Kung *et al.* [30] propose GROUPIT, a lightweight group key management scheme for dynamic IoT environment systems that can effectively handle dynamic membership changes and changes in device numbers for IoT environments. In the two-tier architecture of GROUP IT, the key management is carried out both within and

between groups that consist of users and devices. Users and devices are grouped based on the combinations of subscribed device groups and similar functionalities. A master key encryption system based on the Chinese Remainder Theorem is used to encrypt updates between user groups, while logical key hierarchy is used for key management within groups. The decentralized and batch-based methods reduce the key update overhead by dividing time into small intervals. The key distribution center smoothly updates keys to provide secrecy when memberships change. According to analysis, GROUPIT saves users' storage costs as compared to previous schemes that manage each device individually. It also performs well as compared to other competing schemes in terms of reducing computational overhead by switching it from linear to constant time when membership changes.

Digital signatures are one of the important security components for authenticating data shared over wireless sensor networks (WSNs). The Data sent over WSNs needs to be authenticated by ensuring its confidentiality and integrity through digital signatures. The paper empirically compares various batch verification techniques for digital signatures in wireless sensor networks (WSNs) based on elliptic curve cryptography (ECC). Verifying individual signatures for WSNs with limited resources takes a lot of time in verification. By validating several signatures concurrently in a single computation, batch verification approaches can speed up the verification process. To reduce per-signature verification costs, batch verification makes groups and verifies multiple signatures at once. Kumar *et al.* [31] examine and analyze various Elliptic Curve Cryptography using Batch Verification (ECCBV) algorithms is the aim of the paper. The ECCBV algorithm is identical to the standard Elliptic Curve Digital Signature Algorithm (ECDSA) verification algorithm concerning security. These algorithms gain popularity due to the small batch size that is essential for resource-constrained devices. To evaluate the performance metrics in terms of verification time and throughput show the effectiveness of each algorithm presented in the paper. The effectiveness of each algorithm is examined experimentally by considering factors like batch size, key size, and the number of verifiers and finding out how these factors affect the performance of different ECCBV algorithms. Based on the resource-limited WSNs, the comparison of various algorithms helps the researchers choose the appropriate batch verification technique based on network size.

An enhanced anonymous batch verification method based on Certificate -less Aggregate Signature (CL-AS) is presented by Liu et al. for mobile healthcare crowd sensing (MHCS) applications. Due to individual verification, existing signature schemes are ineffective for MHCS. The CL-AS scheme was first conducted with crypt-analysis to show that an adversary could forge legal signatures without using the secret key value which poses serious concerns about the Random Oracle Model regarding forgery attacks, identity traceability, and many other security risks. The CL-AS scheme for MHCS consists of four entities: Clients, a data center (DC), medical organizations (MO), and a key generation center (KGC). According to tasks given by the MO, clients use mobile sensors to collect health data and send it to the DC. The DC plays an essential role in this process because it assigns MO tasks to clients and aggregates and verifies large amounts of user data through effective batch verification. The MO analyzes DC results and then defines relevant tasks to facilitate diagnoses as shown in Fig 2.1.

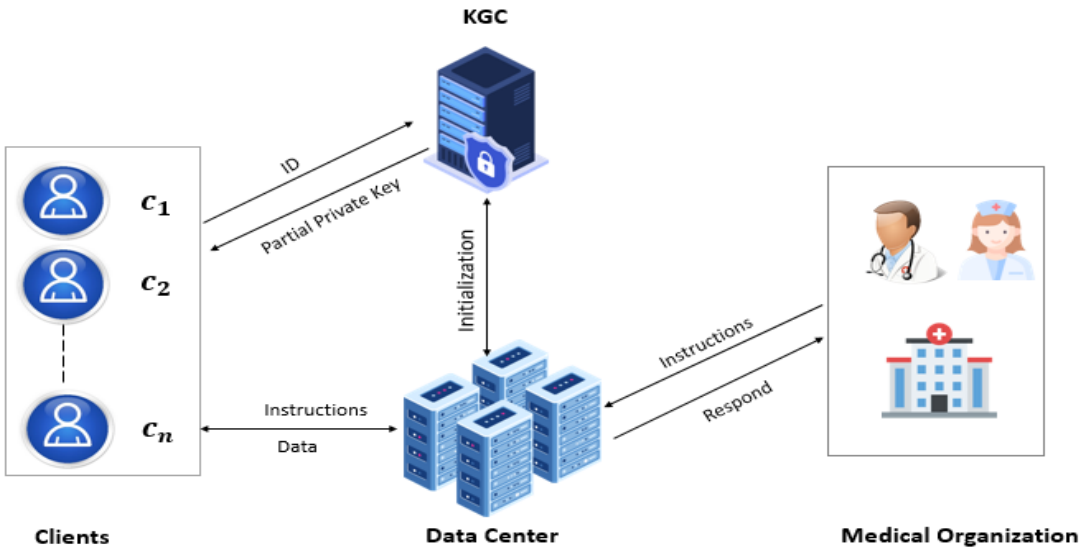

Fig 2.1: CL-AS model for MHCS system

The KGC is a semi-trusted entity that manages the system by generating and distributing private and public keys and registering clients, and it may also access private user data for financial gain. In this scheme, each entity in the MHCS system works independently to achieve the security goal of establishing a certificate-less mobile healthcare crowd-sensing system. The

improved (CL-AS) scheme does not require certificates to achieve privacy preservation, batch verification, and security requirements for mobile healthcare crowd sensing. The algorithms for creating, verifying, and aggregating signatures make use of random numbers, hash functions, and bi-linear pairing maps. The security of CL-AS against chosen message attacks in the random oracle model is evaluated by using the Diffie-Hellman method. The Performance evaluation proves that the scheme can meet security requirements without increasing the computational overhead. In comparison to previous works, the scheme provides anonymity, unforgeability, non-repudiation, and resistance against the attack while also improving certificate management showing that it is both secure and effective for the mobile healthcare crowd-sensing application [32].

Jing Han *et al.* [33] proposed an efficient batch auditing scheme based on the Lucas sequence (BA-LS) method to tackle the issues related to data integrity, confidentiality, and security of medical information in IoMT systems. Securing sensitive medical data owned by data owners (DOs) is very crucial, there are some methods like encryption and batch auditing used in the existing schemes. However, the approaches used in the existing schemes have some limitations like they only work to protect the system from specific kinds of attacks but there is no mechanism to reduce communication overhead and provide an efficient method to identify damaged data files. The scheme uses Lucas sequences related to the Fibonacci series for batch auditing. In the auditing process, DO creates Lucas sequences from the original medical data divides it into multiple data blocks, and encrypts each block for cloud storage. Batch keys are generated for each data block by choosing any unique random number as a secret key. The third-party auditor (TPA) sends each data block to the cloud and by using the self-query operation for data authentication, the cloud service provider (CSP) processes the encrypted blocks and forwards the outcomes to the TPA. The TPA then employs the polynomial commitment method to authenticate the cloud's results. When the verification succeeds, it shows that the data is reliable. If there's any failure occurs, the auditor can easily find which data files are corrupted. The successful verification confirms data integrity, while any failure allows the auditor to identify corrupted data files. The scheme also ensures that TPA and CSP are unable to view the actual content of data files to maintain their security shown in Fig 2.2.

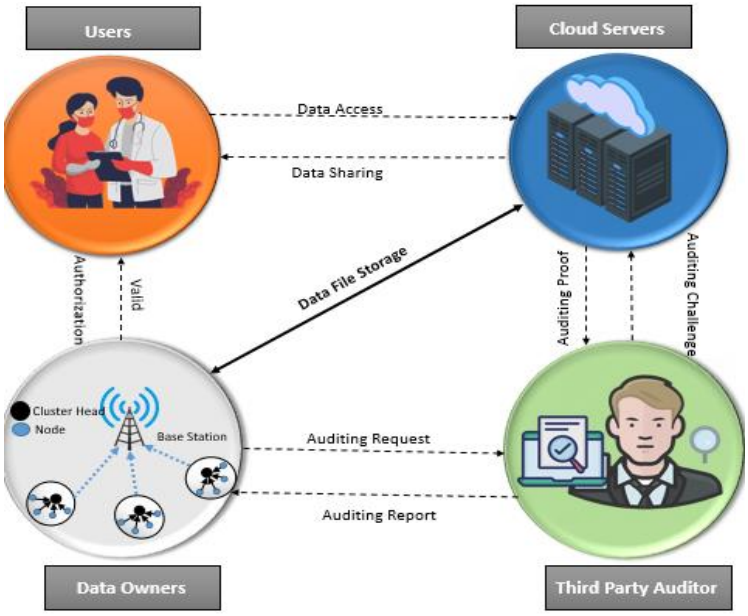

Fig 2.2: Batch Auditing System

The results show that the Lucas search method used in the scheme performed better than previously used binary search methods. In the scheme, the communication overhead complexity is reduced in the auditing phase by moving it from a linear scale to a constant scale, unlike other previous existing schemes which grow linearly. The experiment shows a low error file ratio of 0.1% and a high prior probability of 90% for checking corrupted files and also reduced workload for TPA and CSP by sending the specific amount of data to the Lucas search method for authentication. The scheme successfully detects unauthorized data modifications and maintains a low false-positive rate. Furthermore, the computational overhead is reduced when auditing large data batches that highlight the capabilities of the scheme for real-world IoMT applications.

Jubin Kang *et al.* [34] proposed a Radio Frequency Identification batch authentication (RFIDBA) scheme in IoMT systems. The scheme provides a lightweight and secure solution that is used to efficiently authenticate RFID tags and minimize the workload during data transmission. The main problem in the existing scheme is that they cannot be lightweight enough to correctly detect unauthorized tags and reduce the workload on RFID tags. The

existing RFID authentication methods only verify one tag in each single authentication session but for a large number of tags relying on the old single-tag authentication protocol cannot be enough and that may cause long delays in patient treatment. To tackle these issues, the author introduces a low-cost RFID batch authentication protocol to authenticate multiple RFID tags and reduce the workload during data transmission. For this purpose, the scheme employs homogeneous linear equations to authenticate multiple RFID tags and make it lightweight by performing batch keying XOR method. In homogeneous linear equations, a group of multiple tags is encrypted with a secret key and sent to the reader. The reader decrypts the tags with its public key and validates it. There is no need to store a key for each tag because the tags can regenerate an unlimited combination of solutions for a key to preserve its uniqueness for each tag. To minimize the tag's overload, the simple XOR operation is used to reduce the amount of time and speed during the authentication phase. The scheme also plays a role in protecting the medical system against different attacks by allowing only legitimate entities to authenticate tags, correctly identify illegal tags, and not allow authentication of replaying messages. Compared to other existing authentication methods, the scheme not only reduces the authentication time and costs but also enhances its security, so a secure and lightweight RFID system can be easily applicable in any healthcare scenario.

Mahmood Z *et al*. [35] proposed a distributed multiparty key (DMK) establishment scheme for a secure and authenticated key management system for IoT devices. The goal of DMK is to ensure secure and efficient communication during information exchange between smart devices. For IoT devices with limited resources, the existing password-based authentication schemes are limited to interacting with only three parties to minimize high computational and communication costs. DMK addresses these issues in two phases using chaotic maps to provide one-way hashing and Chebyshev polynomials for common multiparty key generation. In Phase I, the group heads (GH's) after authenticating themselves by a trusted server establish an intra-group session key. In Phase II, this intra-group session key starts communication between GH's and member nodes, and the inter-group session key establishment is used for communication between nodes in the neighboring groups shown in Fig 2.3. Rubin Logic is utilized for security analysis and formal modeling for the inter-group key establishment scenario.

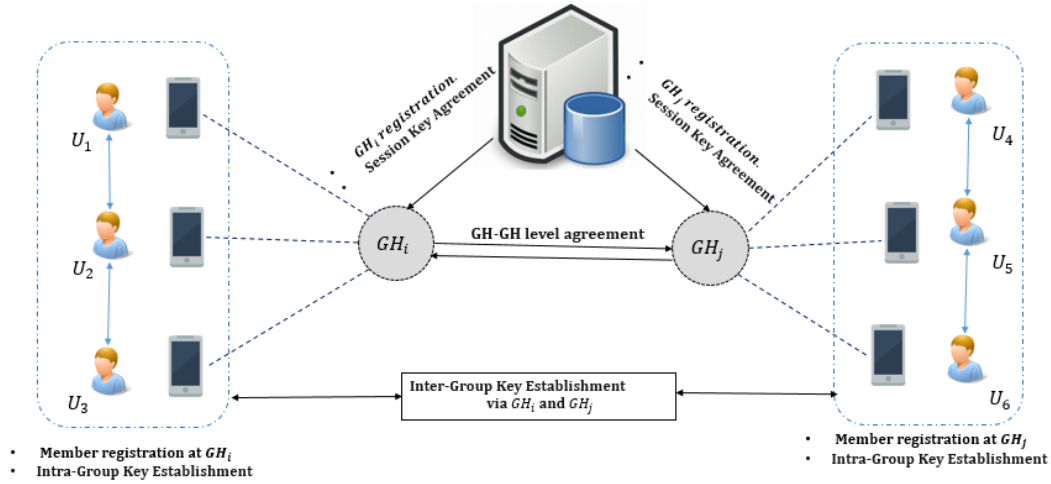

Fig 2.3: DMK architecture

To evaluate the performance of DMK in terms of computation cost, communication cost, and security by using the simulation tool NS 2.35. The simulation results show that it performs well in terms of computation cost and communication cost reduced by 60% and 58% as compared to existing PAKE schemes. It also provides resilience against security attacks making it suitable for resource-constrained IoT environments.

Hu Xiong *et al*. [36] present a secure certificate-less signature batch verification scheme (CLSBV) in IoT systems to address the issues of data authenticity, network congestion, and service delay. The existing certificate-less schemes (CLS) verify individual signatures at once so it cannot be appropriate for the actual implementation of the IoT system that can deal with massive amounts of requests. The scheme handles multiple signatures using an efficient and secure batch verification mechanism while ensuring data authenticity. It employs elliptic curve and symmetric polynomial algorithms in the random oracle model to enhance the performance of multiple signature verification and make it secure and efficient. However, it also solves the issues of batch failures, invalid signature verification, and accepting valid signatures in inaccurate batches which can increase the importance of batch verification under the CLSBV random oracle model. The comparative analysis shows that the scheme performs better in terms of communication cost and communication overhead. It also demonstrates the importance of the scheme for identifying invalid signatures and batch verification as compared to previous

ones. In the future, this scheme can be implemented to provide a secure and efficient CLSBV system for the random Oracle model in IoT devices.

In IoT environments, smart sensor devices provide cost-effective data gathering and sharing services but due to continuous online availability they are becoming more vulnerable to security threats. Therefore, an efficient key generation method is required to protect sensor nodes, edge nodes, and cloud servers from security attacks during data communication. The existing key generation schemes are computationally expensive due to the complex multiplication operations required when the number of parties is increased within a network. Altowaijri *et al*. [37] proposed a Secure Multiparty Key Distribution (SMKD) scheme to protect the network from security attacks and reduce the computational overhead during data communication.SMD scheme consists of three phases. In the first phase, head nodes register and authenticate the mobile nodes in their group, and generate a session key to enable secure communication between them without distributing the entire key over the network. In the second phase, head nodes generate the same session key and share it with other head nodes to ensure secure communication between different groups. In the last phase, the trusted server authenticates all the connected head nodes and generates multi-party session keys to enable secure communication between the nodes. The simulation results show that SMKD performs better than other existing schemes regarding communication, computational, and energy consumption costs. SMKD provides an efficient node authentication and multiparty key generation mechanism to enable secure communication among nodes and reduce computational overhead, especially for large networks.

In IOMT systems, the traditional aggregate signature schemes failed due to the dynamic nature of group membership, while the static group of token signatures raises security concerns. To address these challenges, the Aggregate Signature with Group Rekeying (ASW-GR) scheme was proposed by Zhang *et.al* [38] that leverages the Chinese remainder theorem (CRT) and Fermat's little theorem to enable aggregate signatures with dynamic group token updates. It ensures authentication, conditional privacy, and forward/backward secrecy. In ASW-GR, the medical server constructs a broadcast message using CRT, to decrypt by smart terminals to obtain tokens. The implementation is demonstrated using the Java Pairing-Based Cryptography

(JPBC) library to show that ASW-GR is computationally efficient and existentially unforgeable under the aggregated chosen-key security model. Thus, ASW-GR allows the medical server to update tokens periodically and authenticate aggregate signatures dynamically. It provides a robust, secure, and efficient solution for data aggregation in IoMT's variable environments through conditional anonymity and forward/backward secrecy.

To revolutionize the healthcare system, IoT devices were equipped with sensors to collect real-time patient data and transmit it to cloud repositories for storage. This allows doctors to monitor patient data remotely and provide treatment accordingly. However, efficiently verifying the correctness of each patient's healthcare data in bulk is challenging for the doctors. Existing aggregated signature verification methods access all messages in an aggregated form, making it difficult for systems to efficiently verify the correctness of each individual message. To address this problem, Mao *et al.* [39] proposed a Identity based Locally Verifiable Batch Authentication (IDLBVA) scheme consisting of two identity based locally verifiable signature verification techniques. The identity-based locally verifiable aggregated signature (ID-LVEAS) enables efficient local verification of patient data using a hybrid hash function within IoMT systems. The security of the ID-LVEAS scheme is proven using the EU-CMA security model. The other identity-based locally verifiable signcryption (ID-LVASC) technique ensures both the confidentiality and integrity of healthcare data. Experimental results demonstrate that ID-LVEAS and ID-LVASC require only 0.01 seconds for verification, regardless of the number of messages. This shows that this solution is computationally efficient for practical IoMT applications.

2.3 Data Aggregation and Authentication Schemes in IoMT Systems

Muhammad Azeem *et al.* [40] proposed an “Efficient and Secure Data Transmission and Aggregation (ESDTA)” scheme to deal with the issues related to data security and privacy that arise during data aggregation in the IoMT system. The existing scheme did not efficiently

manage a large amount of data for resource constraints on healthcare devices. The author aims to design a system for a lightweight data transmission scheme that is going to transmit data securely from one end to another without any interruption. The scheme also protects the network from multiple attacks such as replay attacks, denial of service attacks, and many others. For this purpose, the authors introduced the Secure Message Aggregation (SMA) algorithm and Secure Message Decryption (SMD) algorithm to ensure secure data aggregation between Mobile Node (MN) and Fog Server (FS) and also reduce communication and computational overhead at both ends. The SMA algorithm collects data from Sensor Nodes (SNs) and aggregates it after evaluating the message freshness through timestamp verification at the MN. Then, MN encrypts the data with a secret key and sends it to the FN. At FN, the SMD employs symmetric key-based decryption methods to decrypt the received message after the timestamp and hash key values verification to ensure the message's freshness and integrity. If the timestamp condition (TS_{fs} - TS_{mn}) < 1 is true means that data is not modified during transmission and then calculates hash values of received messages. The schemes also remove redundant values by comparing the new hash values (HPV_{ri}) with previous hash values (HPV_{ro}) and put zero if the hash values are the same instead of storing the same hash values again. To evaluate the performance of the scheme in terms of communication cost, computation cost, energy consumption, resilience, and resource utilization by using the NS-2.35 simulation tool. The results show that the scheme is more secure and lightweight because it removes redundancy and improves its performance in other factors as well.

The Efficient HealthCare Data Aggregation (EHDA) scheme employs a hierarchical data aggregation method to address the issues of high communication costs energy consumption costs and storage overhead in IoT-enabled wireless sensor networks (WSNs). The existing data aggregation schemes use asymmetric key cryptography which increases these costs because of transmitting uncompressed raw data files over resource-constrained IoT devices. The EHDA scheme utilizes a hierarchical data aggregation method that consists of three phases: local transfer of compressed data, message receiving at the aggregator node, and message extraction at the fog server. In the first phase, sensing devices first compress the data, encrypt it, and then transmit it to the aggregator nodes using symmetric key cryptography. In the next phase, the aggregator nodes receive compressed data from sensor devices and perform aggregation on it before transmitting it to the fog server. In the last phase, the fog server uses a delimiter to extract

individual sensor node data. To evaluate the performance of the EHDA scheme using the simulation tool NS 2.35 shows that the EHDA performs better than other existing schemes in terms of storage cost, communication cost, and energy consumption cost. These terms are reduced by compressing data files that decrease the communication costs by 30-50% and minimize energy consumption by measuring the number of exchanged bytes and also almost achieve over 90% transmission ratio in data delivery. These results demonstrate that utilizing compression, hierarchical architecture, and fog computing makes it more efficient than other existing aggregation techniques [41].

H. Wang *et al.* [42] propose the Anonymous and Secure Aggregation Scheme (ASAS) that allows anonymized terminal devices (TDs) to securely upload encrypted aggregated data from fog nodes (FNs) to public cloud servers (PCSs). The previous schemes did not provide anonymity for TD while uploading data in PCS. The ASAS consists of six phases: setup phase, registration phase, TD data processing phase, secure data aggregation phase, Data decryption phase, and Node's revocation phase. In the setup phase, the public and private keys are calculated for communication and generate system parameters. During the registration phase, the PCS authorized both TDs and FNs by using hash signatures. In the TD data processing phase, the TDs encrypt their data before uploading it to FNs. In the secure data aggregation phase, the FNs authenticate TDs and then aggregate their encrypted data into a cipher text through homomorphic encryption techniques before uploading on PCS. In the last phase, PCS verifies the FN signature before decrypting the cipher text to retrieve the actual aggregated message. In the last phase, TDs, FNs, and PCs can revoked by each other when needed. The ASAS scheme successfully achieves anonymity, the indistinguishability of cipher texts, and efficient revocation techniques to ensure the security and privacy of data by using signatures and the Castagnos-Laguillaumie cryptosystem. The performance of the ASAS scheme is also evaluated in terms of communication and computational cost showing that the proposed scheme is very affordable for efficient data aggregation.

X. Li *et al*. [43] present a privacy-preserved data aggregation scheme (PDDAS) designed to enhance user privacy at terminal nodes in IoT applications using Mobile Edge Computing (MEC). It addresses the problems of low latency and quick data access while

preventing the system from any kind of privacy leakages while collecting and processing data in the cloud computing architecture. The scheme employs homomorphic encryption using the Boneh Goh-Nissim cryptosystem that consists of three algorithms such as key generation, encryption, and decryption to protect sensitive data during aggregation. Encryption is applied to the data generated by the terminal devices before being sent to the edge server. The edge server then aggregates the data from the terminal devices and delivers the data to the public cloud center. Finally, the public cloud center utilizes its private key to decrypt and restore the aggregated plaintext data in the cloud server as shown in Fig 2.4.

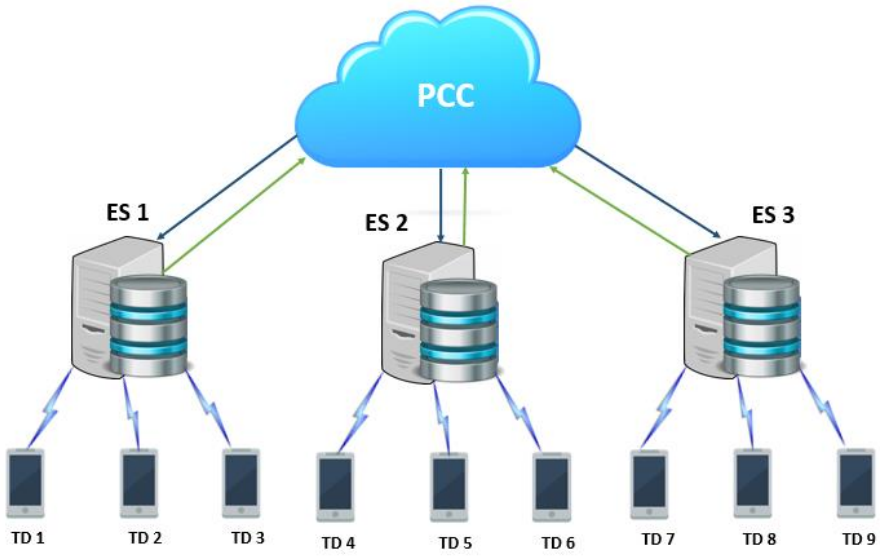

Fig 2.4: Communication model

Utilizing the resources at the edge, reduces the computational overhead and improves the effectiveness of the aggregation process. The scheme is evaluated by demonstrating its effectiveness in preserving privacy while maintaining data integrity and system authentication. This research also contributes to the field of IoT security by offering a solution for ensuring privacy, integrity, and authentication of data during aggregation in MEC-assisted environments. By evaluating the performance of the scheme, it can reduce communication costs by nearly fifty percent and save time during data aggregation to overcome the computational cost when compared to other conventional methods. Moreover, the features of MEC like limited terminal devices, heterogeneity, and diverse trust areas may lead to some new security and privacy

concerns. The typical security and privacy methods used in cloud computing might not work well for MEC. In the upcoming research, a lightweight data aggregation method is needed that emphasizes simpler methods for identity verification across multiple trust entities and designing strategies for data sharing while protecting privacy in every area that is appropriate for MEC.

Muhammad Usman *et al*. [44] propose a Privacy-Preserving Data Collection and Analysis (P2DCA) framework for IoMT applications to preserve the privacy of multimedia sensor nodes (MSNs) while collecting sensitive data. In IoMT, the multimedia sensor nodes (MSNs) collect and transmit data via base stations (BS). However, the mobile sink node gathers information from MSNs and uploads it to the cloud when the internet is down. Sometimes the MSNs disclose users' personal information such as ID and locations, which raises serious concerns about how to preserve user privacy while collecting mobile data for MSNs. Existing privacy-preserving schemes cannot work for real-time IoMT applications due to limited resources that cannot store data for long periods. In the P2DCA framework, the Wireless Multimedia Sensor Network (WMSN) is divided into multiple clusters managed by designated Cluster Heads (CHs) as shown in Fig 2.5. The CHs protect the privacy of their member nodes by collecting the user's data and their location before using mobile sinks. The mobile sink node collects this information and uploads it to the cloud server once they have registered.

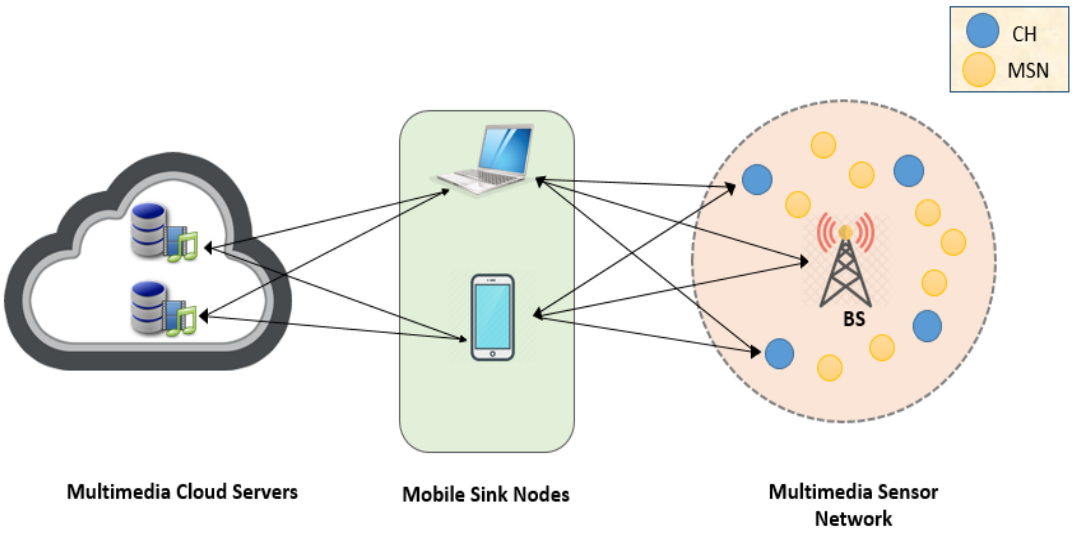

Figure 2.5: P2DCA framework

It allows mobile sink nodes to collect data timely and then perform analysis in a cloud environment by masking their sensitive data such as ID and location in the aggregated form while preserving the privacy of individual member nodes. The aggregated data is further analyzed in the cloud by using a Counter-Propagation Artificial Neural Network (CP-ANN) for video frames to get meaningful information. The experimental results demonstrate that the P2DCA framework efficiently extracts real-time data while protecting members' privacy, which applies to real-time IoMT applications.

Seyfollahi and A. Ghaffari [45] proposed a Reliable Data Dissemination for the Internet of Things (RDDI) scheme that addresses the challenge of securely and reliably collecting and sharing aggregated data by energy-constrained devices inside the IoT network. To tackle this issue, the Harris Hawks Optimization (HHO) algorithm is utilized to treat data dissemination as an optimization challenge and reduce the energy consumption cost by optimally selecting the Wireless Nodes (WNs) during data transmission. This algorithm develops an optimized routing solution for IoT by integrating routing data. The RDDI scheme consists of four distinct phases. First, the Cluster Head (CH) selection phase employs the Harris Hawks Optimization (HHO) algorithm, inspired by Harris hawks' hunting behavior, to choose CHs within the network. Second, in the Data Aggregation phase, the CHs gather data from sensor nodes situated in their respective clusters. In the Data Forwarding phase, CHs transmit the compiled data to the base station. Finally, in the Attack Detection and Prevention phase the CHs used a watchdog timer to identify possible security breaches in sensor nodes. When a vulnerable sensor node is detected, it is isolated from the network to ensure security. RDDI offers a hybrid approach to detect and prevent attacks by using a fuzzy clustering algorithm that is based on geographic information and implementing a WN behavior monitoring mechanism. To ensure safe data transmissions throughout the network, the WN nodes periodically verify CHs and deliver data to legitimate CHs. The scheme evaluates the performance of the HHO algorithm by using five metrics: reliability, end-to-end delay, energy consumption, computational overhead, and packet forwarding distance in multi-cluster scenarios. Comparisons with three other approaches, the results show that the RDDI scheme achieves a reduction in average energy consumption cost by 6.5% and makes improvements in packet forwarding distance to 20% and end-to-end delay to 17.5% respectively. However, the computational overhead cost is 12.8 sec which is greater than the two approaches. The results demonstrate that overall RDDI performs

well to achieve better reliability, end-to-end delay, energy consumption, and computational overhead cost than the other three comparative schemes. It highlights the effectiveness of the scheme for achieving a reliable data dissemination method in IoT systems. In future work, a fault-tolerant approach is designed for data dissemination to manage defective cluster heads, WNs, and connections.

Surbhi Bhatti *et al.* [46] proposed a hybrid Cryptographic scheme for mobile ad hoc networks (HCMANET) in healthcare systems. The existing schemes are computationally expensive and inefficient in terms of addressing security threats due to resource constraints in IoMT devices. The author employs two cryptographic algorithms (Logistic chaotic map and RSA algorithm) to securely exchange sensitive information in MANETs. In the previous schemes, the Secure Key Generator (SKG) based model is used for node authentication, key generation, and key distribution. The author extends SKG with RSA to authenticate registered nodes and monitor the functionality of mobile healthcare nodes within the network. In the system, the SKG known as the Master healthcare node (MHN) uses the logistic map-based chaotic functions for key generation because it takes less time to generate keys and is difficult to crack by intruders. It also provides better security minimal computing resources are available.

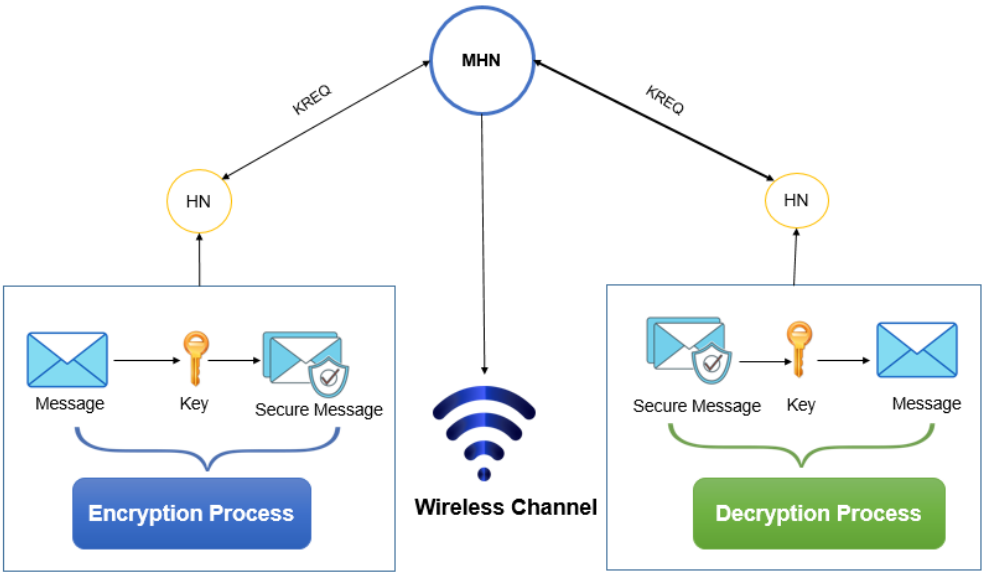

Figure 2.6: Hybrid Cryptographic model

Before data transmission, both sender and receiver healthcare Nodes (HN) send requests for secret keys from the MHN as shown in Figure 2.6. The receiver sends the request for a secret key (SK) using a Key Request (KREQ) packet after receiving the encrypted message, and once the SK is obtained it is for the decryption. The model protects the network from various security threats and detects malicious nodes as well. When a node consistently sends three KREQ packets, the MHN recognizes it as a malicious entity and disconnects it from the network. To evaluate the performance of the model using the NS 2 simulation tool, the results showed the ratio of Packet Delivery Ratio is better than other algorithms even in the presence of a DOS attack. The hybrid Cryptographic model also eliminates the need for Certificate Authority (CA) for key management and ensures better security, less computational power, and a cost-effective MANET model as compared to existing schemes.

Yanambaka *et al.* [47] introduce PMSEC: a lightweight device authentication scheme for the healthcare system. In IoMT systems, there is a large number of medical devices are connected to the internet to exchange information with each other through the edge server. If any malicious device accesses the server, it can lead the system towards network attacks and make it vulnerable for all connected devices. In the previous schemes, symmetric and asymmetric protocols were used to protect the devices against cyber-attacks by providing universal keys to only authorized medical individuals. But these protocols are not entirely secure, if an attacker gets the universal key, it could potentially damage the patient's information. The authors employ Physical Unclonable Functions (PUFs) by using PMSEC to address the issues of security, low processing power, and limited memory present in the existing protocols. PUFs generate unique cryptographic keys for each device by providing the input to the PUF module. It also eliminates the need to store keys in memory and generates these keys only when required. The PUF module is integrated between IoMT devices and edge servers to provide secure data transmission in a network. The module initially introduced each device to the network and registered on the server then verified the authenticity of medical devices before exchanging the patient's data with the medical team. To verify the authenticity, the IoMT device sends a challenge to the server which generates a response back to the device by using the PUF module and if the responses match with the challenge it means the device is authenticated. The results show that the scheme takes only 1.2sec - 1.5sec for device validation and provides a robust, scalable, and lightweight device authentication solution for the IoMT system. The

scheme is applicable in different healthcare scenarios irrespective of the communication protocol used between the devices without storing the data in server memory to enhance the security of the system.

IoMT systems face the challenges of high energy consumption costs, high transmission costs, and data redundancy that delays the detection of emergency data. To address these issues, an efficient data aggregation system is required to handle massive volumes of heterogeneous data effectively while reducing transmission costs. For this purpose, Khan *et al.* [48] present a fuzzy-based data aggregation system (FDAS) to create a synchronized tree mechanism for sensor nodes to collect patient healthcare data and send it to intermediate nodes for aggregation. These nodes forward the aggregated data to fog servers for local temporary storage and then to the cloud server for cloud storage. Medical Professionals access the specific information of patients from the cloud server via fog servers. The FDAS employs a fuzzy logic method to eliminate redundant values. The fuzzy logic method selects the optimal parent node among other candidate nodes based on parameters like neighbor count and residual energy. To reduce duplicate values, FDAS assigns Boolean values '0' only if the patient's healthcare readings are present within the normal range of previous values, otherwise, transmits the actual readings to the doctor. The Simulation results demonstrate that FDAS performs better than other aggregation schemes in terms of cost-effectively minimizing communication overhead and energy consumption. Therefore, FDAS is an effective solution for heterogeneous data aggregation methods in IoMT environments since it uses the fuzzy logic method and Boolean assignment to eliminate redundancies.

The Secure Aggregated Data Collection and Transmission (SADCT) scheme was introduced by Mughal *et al.* [49] to ensure data security during the collection and forwarding phase while preserving the anonymity of the patient’s identity. It utilizes an authenticated server for node authentication and securely storing their registration credentials. The Authenticated nodes act as intermediaries that forward the healthcare data to the fog server. Measuring the performance of SADCT by using the ns2 simulation tool is achieved by comparing it with other base schemes like SAPS, MDK, SPPDA, and AMAS. SADCT performed better than other base schemes regarding energy consumption, storage utilization, communication, and computational

costs. However, further work is needed to reduce data duplication at sensing nodes and minimize transmission costs during the aggregation and transmission processes.

Medical institutions accumulate vast amounts of medical data to train high-quality deep-learning models that help doctors in diagnosis. However, due to the sensitive nature of medical data, the implementation of data fusion is very challenging. The existing schemes use Federated Learning (FL) for model training, but it is not fully secure due to inference attacks caused by privacy leaks. Moreover, a server could also potentially forge aggregated results in the FL framework, which could have raised serious security concerns for medical systems. To address these issues, Wang *et al.* [50] proposed a Robust Federated Learning with Privacy Preservation (RFLPV) scheme to preserve gradient privacy through the addition of pairwise masks and using homographic hashing and secret sharing cryptographic techniques to design an efficient verification mechanism for IoMT system. To evaluate the performance of RFLPV scheme, the experimental results showed that it ensures data privacy and consumes less computational and communication costs compared to existing schemes. Therefore, it shows that the RFLPV is more efficient and secure than other FL schemes.

2.4 Comparison of Batch Verification and Data Aggregation Schemes

This section analyzes the performance of various batch verification and secure data aggregation schemes in tabular form shown in Table 2.1 to measure the performance under different parameters and identify the pros and cons of each scheme that will be resolved in future research studies.

Table 2.1: Summary of batch keying and data aggregation schemes for IoMT

Schemes	Mechanism	Advantages	Limitations	Results
SATS [27]	XOR operation is used for batch key verification instead of	Securely transfer aggregated data with minimal computational	The value of the secret key is null which may raise some	Better communication and computational cost as compared to

	complex multiplication.	and communication overhead for resource-constrained network devices.	security concerns.	other existing schemes for both HN, and FS.
SL-IPDE [28]	Employ cryptographic hash function with (XOR) operations and key chain method to ensure data integrity of Cloud-based IoT systems.	Lightweight methods are used to decrease the computation and storage overhead making it suitable for resource-constrained devices.	Relying on a single semi-trusted server for batch integrity audits is not enough for data authentication.	Achieves better performance and reduces computational and storage costs as compared to bilinear pairing-based schemes.
CBRDIBA [29]	Data owner's validate data by Lucas Search and Hash Value Tags (HVT's) methods to address the failures in batch auditing protocols and ensure data integrity.	Efficiently work with a single data owner.	Requires more improvement to reduce the complexities of computational and communication overhead.	Provide better security against the advanced level of collusion attacks.
GROUPIT [30]	A lightweight group key management scheme is used for key management and provides secrecy of data by updating keys when memberships change.	Computational overhead is reduced when membership changes from linear to constant time scale.	Avoid updating keys simultaneously for multiple devices and user groups when several devices change dynamically.	Reducing Computational overhead and saving user storage space by managing each device separately.
ECCBV [31]	Compare batch verification techniques based on elliptic curve cryptography in WSN's	Identifying the best Batch verification for resource-constrained IoT devices in WSNs	Batch verification algorithms with small batch sizes take more time in signature	It helps researchers to find appropriate batch verification algorithms for different network sizes.

		reduces verification time.	verification time than other algorithms.	
CL-AS [32]	It verifies large amounts of user data through effective batch verification methods and distributes keys after the client's registration.	Each entity independently establishes a certificate-less MHCS system to protect the system against identity, traceability, and forgery attacks.	The KGC is considered a semi-trusted entity because it has the potential to access user's private data for financial gain.	Fulfill the security requirements without increasing computational overhead.
BA-LS [33]	Utilize Lucas sequences related to the Fibonacci series for batch auditing. Batch keys for each data block by DO and send encrypted blocks to TPA and then CSP for authentication.	TPA uses the polynomial commitment method to check the integrity of data and recover corrupted files easily.	Support multi-cloud storage for more fast and efficient batch auditing for large volumes of data.	Identify corrupted data files and reduce communication overhead by switching it from linear to constant scale.
RFIDBA [34]	Employ homogeneous linear equations to validate multiple RFID tags simultaneously and identify illegal tags to ensure security.	Reduced the tag authentication time and storage cost by using the batch keying (XOR) method and also resisted the attacks.	Improve the protocol further to be easily implemented in healthcare scenarios	Provide better security and accuracy by using multiple tags authentication protocol.
DMK [35]	Employ Chebyshev Polynomials and chaotic maps for one-way hashing and generating common multiparty keys to establish secure communication between nodes.	It provides resilience against security attacks and performs well to reduce communication and computational costs.	It is suitable for resource-constrained devices but it is not practically deployed for IoT systems.	Reduced 58% communication cost and 60% computational cost as compared to previous schemes

CLSBV [36]	Employs elliptic curve and symmetric polynomial algorithms to ensure multiple signature verification.	Validate multiple signatures at the same time and address the issue of batch failures.	Deployed this model for practical IoT-based systems.	Reduce communication overhead and computational cost as compared to previous schemes.
SMKD [37]	Employ node authentication and multi-party session key generation mechanism to reduce computational overhead.	It reduces computational overhead and multi-party keys when the network expands.	Minimize the computational cost but increase communication and storage costs simultaneously.	It performs better than other schemes in terms of reducing transmission costs.
ASW-GR [38]	Leverages the Chinese remainder theorem (CRT) and Fermat's little theorem to dynamically update aggregate signatures for group tokens.	It ensures the conditional privacy, authentication, and forward/ backward secrecy for aggregated signatures.	Improve the ASW-GR by ensuring the confidentiality of sensitive healthcare in future work.	The ASW-GR is computationally efficient and existentially unforgeable under the aggregated chosen-key security model.
ID-LBVA [39]	It consists of two identity-based locally verifiable signature verification techniques to ensure the confidentiality and integrity of data.	The EU-CMA security model proves its security making it more secure than existing techniques.	Conduct further research to minimize the transmission costs while maintaining its security.	The experimental results show that it requires only 0.01 sec for verification which makes it computationally efficient.
ESDTA [40]	SMA and SMD algorithms are used for data aggregation and ensure the integrity of data by timestamp verification and remove redundant values by	Deal with security attacks and provide efficiency in terms of computational, communication, and energy consumption costs.	More research are required to improve the security and efficiency of data.	NS 2.35 simulation tool is used to measure the performance of a scheme that is more efficient and secure than previous ones.

	comparing hash values.			
EHDA [41]	Used symmetric key cryptography to address the issues of high communication cost, energy consumption cost, and storage overhead in IoT systems.	Minimize transmission costs by compressing data files before aggregation.	Reducing computational overhead is considered for further research.	Decrease the communication cost by 30-50% and achieve a 90% transmission ratio in data delivery.
ASAS [42]	Used Castagnos-Laguillaumie cryptosystem. And signature techniques to authorize TDs and FNs.	It is an efficient, secure, and affordable data aggregation scheme.	It allows the anonymous TDs to upload their data on PCS which raises the security risks.	Practically implemented on a simulation tool to better understand its performance.
LVPDA [43]	Employs homomorphic encryption using Boneh Goh-Nissim cryptosystem for data aggregation and maintains the integrity and privacy of data.	Ensuring privacy, integrity, and authentication of data during aggregation while preserving user privacy as well.	Require a light-weighted aggregation scheme for identity verification.	Reduced communication costs by 50% and saved more time.
P2DCA [44]	Protect the privacy of each node by dividing the framework of WMSN into multiple clusters to collect the personal data of each node and then perform data aggregation.	It works for real-time IoMT applications.	Only protect the privacy of member nodes but do not focus on the security of communication channels.	Efficiently extracts real-time data while protecting the privacy of each member node
RDDI [45]	Utilize the HHO algorithm and	It performs well to reduce energy	More research are required to	Reduce energy consumption cost

	fuzzy clustering algorithm to reduce energy consumption costs by selecting the optimal Wireless node and monitoring WN to ensure safe data transmission.	consumption and end-to-end delay costs.	reduce computational overhead and save more time.	by 6.5% and end-to-end delay to 17.5% as compared to previous schemes.
HCMANET [46]	Employ two cryptographic algorithms (Logistic chaotic map and RSA algorithm) to securely exchange sensitive information and need less time for generating keys.	These hybrid cryptographic algorithms provide better security when minimal resources are available.	The schemes required further modifications to deal with the advanced level of attacks comes with the existence of malicious nodes.	The results show that it required less time for computation and packet delivery as compared to the existing schemes
PMSEC [47]	Employs Physical Unclonable Functions (PUFs) by using PMSEC to generate cryptographic keys for each device to ensure only authenticated devices transmit data in the network.	The PUF module-based PMSEC scheme provides a lightweight and scalable device authentication method.	The client-side message authentication scheme is considered in further research.	It takes only 1.2sec - 1.5sec for device validation
FDAS [48]	It utilizes fuzzy logic and Boolean operation for data aggregation and removing redundancies.	Reduces communication overhead and energy consumption compared to other schemes.	It only focuses on removing redundancies and data aggregation but does not consider data integrity and authentication	FDAS approach significantly reduces data size and communication costs making it suitable for healthcare applications.

			during data transmission.	
SADCT [49]	Provide security on aggregated data by authenticating the server for node authentication and securely storing their registration credentials.	It ensures data security during the collection and forwarding phase while preserving the anonymity of the patient's identity.	Reduce data duplication at sensing nodes to minimize the transmission costs during the data aggregation.	The results show that it performs better than other existing techniques in term of storage utilization, energy consumption, communication, and computational costs.
RFLPV [50]	It preserved the privacy of data through the addition of pairwise masks and homographic hashing and secret sharing cryptographic techniques.	It is an efficient, robust and secure FL techniques for model training that protect the IoMT system from attacks caused by privacy leakages.		The experimental results showed that it ensures data privacy and consumes less computational and communication costs compared to existing schemes.

The above section presents different security solutions to maintain system integrity and confidentiality of data but the attackers continuously tried to breach the network and come up with new attacks. For this purpose, batch authentication and secure data aggregation schemes have been developed to determine the security gaps against the advanced level of attacks and reduce the overall transmission cost to improve the performance of the system. The key advantage of better communication, computational, and energy consumption cost is observed in these schemes mentioned in Table 2.1. In [27], [28], [29], [30], [31], [32], [33], [34], [35], [36],[37], [38] and [39] schemes the batch auditing and verification protocol ensures data integrity by identifying corrupted data files while reducing the communication cost and computational overhead. However, the data aggregation schemes [40], [41], [42], [43], [44], [45], [46], [47], [48], [49] and [50] check the accuracy of data by Timestamp verification and authenticate registered nodes by generating cryptographic keys and minimize the energy consumption cost by identifying the optimal node path. After the comparative analysis of these

schemes, many lightweight schemes do not reduce the computational, communication, and energy consumption costs simultaneously. These schemes offer authentication for only one factor, the device authentication or data authentication but none of them worked on both of these factors.

2.5 Research Gap and Directions

For secure and lightweight data aggregation schemes, ensuring the security of sensitive data is a key factor that cannot be ignored. Many researchers already worked on reducing the data transmission costs and improving the security strengths of IoMT systems but still, some vulnerabilities need to be tackled. In [27], the data transmission cost in terms of communication, computation, and energy consumption cost is reduced but the security of data is compromised while transferring data from SN to HN. The value of the secret key is null at the initial stage and it allows attackers to decrypt and modify data if it recovers the value of the batch key. So, the main concern is to reduce data transmission costs and improve security strengths to build a more efficient, secure, and lightweight IoMT system.

2.6 Summary

This chapter analyzes various batch authentication and data aggregation schemes to observe different key components such as security, authentication, and aggregation. To measure the efficiency of these schemes by evaluating their performance under different performance evaluation parameters like computational overhead, energy consumption, and communication cost. It also emphasizes the importance of a lightweight batch auditing and data aggregation scheme that can reduce transmission costs as well as provide a high level of security.

CHAPTER 3

METHODOLOGY

3.1 Overview

This chapter describes the methodology to provide an overview of all steps involved in the research process. It analyzes the literature review, identifies the gaps, designs the model, and uses simulation tools for performance evaluation.

3.2 Operational Framework

The Internet of Medical Things (IoMT) is a new emerging technology that offers remote healthcare services like patient monitoring, disease detection, telemedicine, digital record maintenance, etc. that allows doctors to continuously monitor patients' healthcare data from remote locations. The new advancements have improved people's lives, but they also raised some security and privacy challenges that need to be resolved. To deal with these challenges, further research is required to identify the new privacy and security issues in IoMT systems. However, there are many schemes and literature available to tackle these challenges but each scheme has some limitations that require more research in this area.

The operational framework of this research work consists of three major phases: Analysis, Design and Development, and Performance Evaluation Phase as shown in the below Figure 3.1.

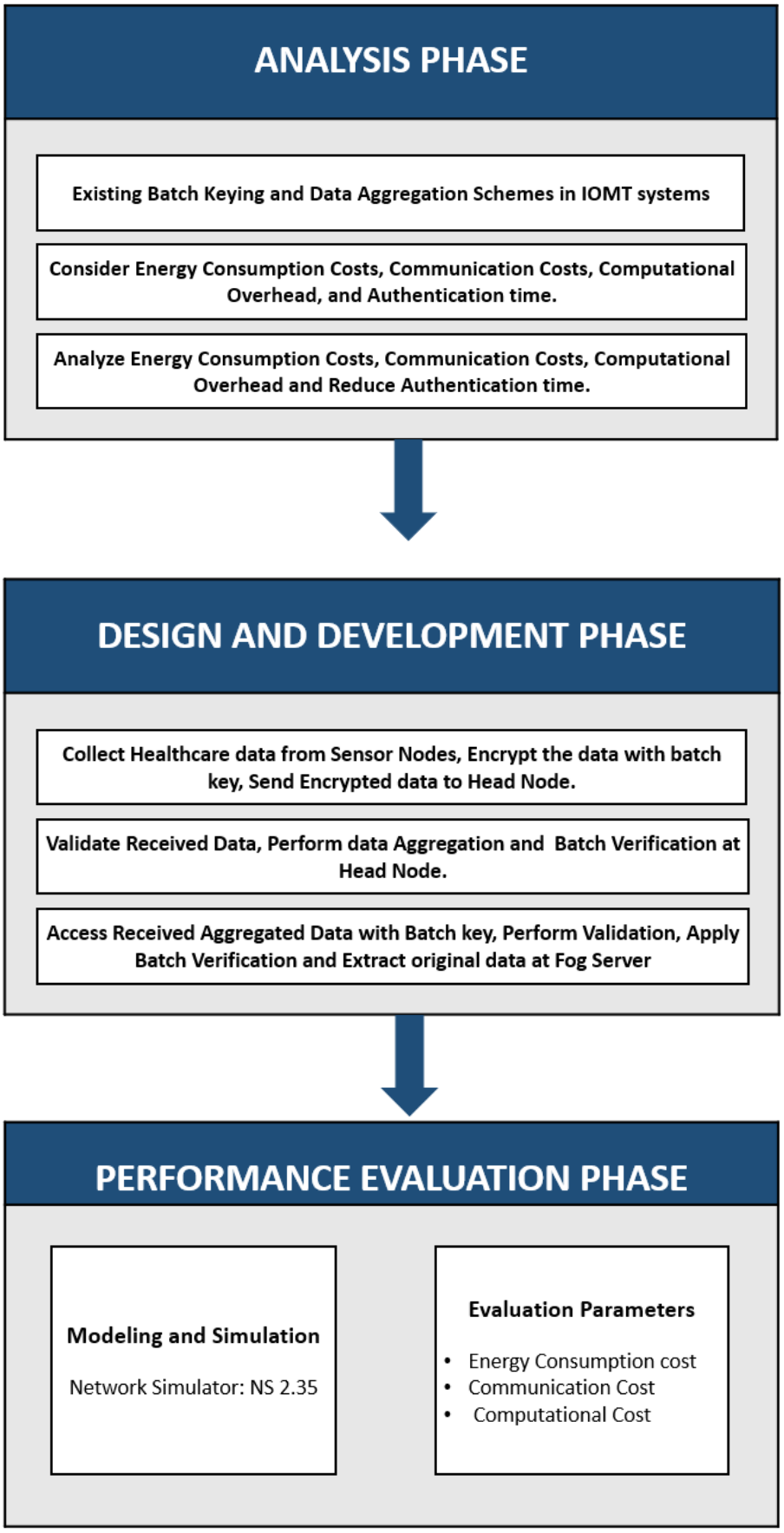

Figure 3.1: Operational Framework of the Research

In the first phase, the systematic literature review based on efficient batch key and data aggregation in the IoMT network is studied to analyze the methodology, working mechanism, and pros and cons of latest schemes. However, the relevant keywords used in base scheme are utilized to identify the relevant scheme papers. Thoroughly examining the title, abstract, methodology, and results of the most recent schemes provides insight into the latest potential security and privacy issues that need to be addressed. Analyzing the relevant papers helps to find out the evaluation criteria to measure the performance of these schemes. The most common evaluation metrics are communication cost, computation cost, energy consumption cost, authentication time, etc. that are considered in the relevant research papers. The main objective of these papers is to reduce these costs and develop a secure and efficient communication medium for data transmission. These schemes satisfy some performance evaluation metrics and protect the system from attacks but it also has certain limitations. Almost 50 relevant papers were studied, and 20 of the most recent and closely related to the research topic were selected for the literature review.

In the second phase, after analyzing the literature review and identifying the research gaps there is a need to design and develop a system to resolve the problems. Based on the literature review, the key challenges are reducing data transmission costs while making the system resilient against all kinds of attacks. Our aim is to build a lightweight and secure data aggregation system that utilizes batch key encryption technique to reduce transmission costs and protect against cyber-attacks. The design and development phase are divided into three main categories: data collection, data aggregation, and data extraction. Data is the main element in the whole process, so for collecting data different sensor devices are attached to the patient's body. The sensor devices gather patient healthcare information, encrypted it by using the batch key, and then transmit only out-of-range healthcare parameter values to the nearest HN for further processing and aggregation. The HN validates data by timestamp and hash verification methods to check the integrity and freshness of received messages. After successfully completed validation process, HN aggregate all the sensor-based messages into one aggregated message and then perform batch verification using XOR operation before forward it to the FS for extraction. FS validates received data by the same method used for HN then performs batch key verification with XOR operation to extract the aggregated message. Obtaining sensor data is only possible if the calculated hash at FS matches the hash of the received message otherwise

discard the message due to integrity violation. FOR loop is used to retrieve the data of each node. Upon successful extraction of the node's data, FS sends an acknowledgment message to the HN. FS temporarily stores data before forwarding it to the Cloud Server (CS) for long-term storage. A detailed description of the proposed scheme, system model, and algos are mentioned in the next chapter to completely understand the working mechanism of the whole process.

In the last phase, the performance of the proposed scheme is evaluated by the simulation method. The NS 2.35 is a very reliable and efficient simulation tool for measuring the performance of the proposed protocol via graphs under different evaluation metrics. The performance evaluation metrics considered in the proposed scheme are communication cost, computational overhead, and energy consumption cost. Based on their results, the proposed protocol was compared with the existing protocols such as SATS [27], LVPDA [43], and ID-LBVA [39] to identify how well it performs to others. The proposed scheme is evaluated through simulation using the network simulator NS 2.35. The simulation is implemented through TCL and C++ files in NS 2.35 that allow the testing of the proposed protocol under different evaluation metrics to analyze performance like communication cost, energy efficiency, and computational overhead.

3.3 Summary

This chapter provides a detailed explanation of the operational framework and its phases to determine how the problem is identified in the literature review and which factors are considered in the proposed solution to deal with the problems. It also provides an overview of the different steps involved in the proposed solution and also provides information on three different schemes from the literature review that are compared with the proposed scheme to examine its performance efficiently.

CHAPTER 4

BATCH KEY-BASED SECURE DATA AGGREGATION PROTOCOL

4.1 Overview

This section presents a detailed description of the proposed protocol that includes the system model, its components, and algorithms for data aggregation and extraction at HN, and FS. The system model provides the information and working of each entity used in the proposed solution. In the proposed solution, both algorithms briefly explain the comprehensive details of each step written in them to understand the data aggregation and data extraction process completely.

4.2 Batch Key Based Secure Data Aggregation Protocol

In the IoMT system, the main challenge while transmitting wireless data from sender to receiver node is ensuring its security because there is always a risk of data manipulation by intruders if the security of any node or communication medium is compromised. The unauthorized alteration of sensitive healthcare data creates a serious impact on medical decisions. To address security issues in IoMT systems, the proposed secure batch verification and data aggregation schemes are presented to ensure the integrity and authenticity of data by time verification and hash comparison methods. In the existing schemes, to reduce computational cost the value of the secret key is null which creates security risks during data transmission.

This section presents the proposed batch key-based data aggregation protocol (BK-SDA) to resolve the problems discussed in the previous chapters. The proposed BK-SDA protocol provides a batch key verification method to protect the security and authenticity of data during wireless communication. The process is divided into three main phases: transmission of local sensing data, Data Aggregation on received messages at HN, and data Extraction on received aggregated messages at FS as shown below in Figure 4.1.

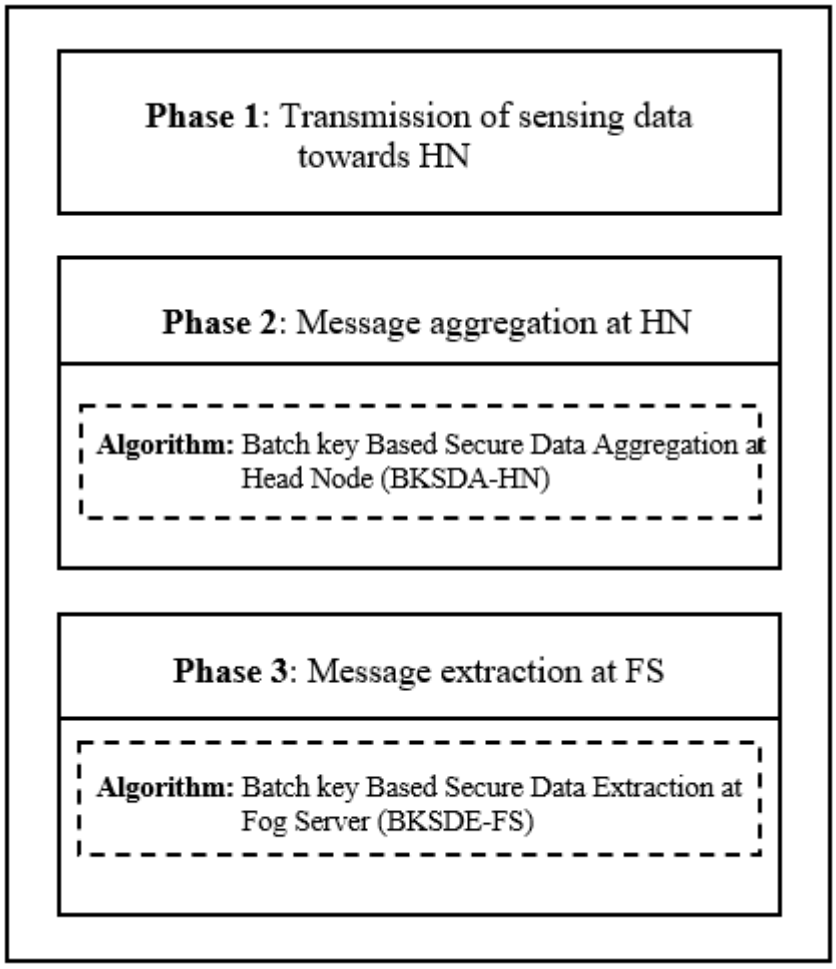

Figure 4.1: Phases of BK-SDA scheme

In Phase 1, the local smart sensor devices are attached to the patient's body to collect their healthcare data and then encrypt it with a batch key. The batch key is a unique identifier used in data communication to group multiple data packets together for processing as a single

unit. It's commonly employed in scenarios where large volumes of data are transferred or processed, ensuring that all related transactions are handled consistently. The data encrypted with the batch key is transmitted to the nearest HN for data aggregation and the same batch key is shared with the FS for data decryption.

In Phase 2, the HN received encrypted data from sensor devices and validated it through hash-value comparison and timestamp verification to ensure its security. The primary role of the HN is to aggregate data from nearby sensor devices or other HNs that cannot directly access the FS. If an HN does not have direct access to the Fog Server, it will transmit its aggregated data to the nearest HN that has direct access to the Fog Server. The HN also performs batch verification on the aggregated data using the XOR method before forward towards the FS.

In Phase 3, the FS sequentially received aggregated data and then applied the same verification method that was already used at HN to ensure the integrity and freshness of the message. After completing the verification method, FS extracts aggregated messages by taking XOR with the batch key and then using the FOR-loop technique to extract and decrypt the data of sensor nodes and get the original patient healthcare value. The Fog Server sends an acknowledgment message to the aggregate node after completing the extraction process.

4.3 System Model

In this section, the system model of the proposed secure batch key-based aggregation (BK-SDA) scheme consists of four components. These components are the Sensor Node, Head node, Fog server, and Cloud server to facilitate secure peer-to-peer and HN-to-HN data communication as shown in below Figure 4.2.

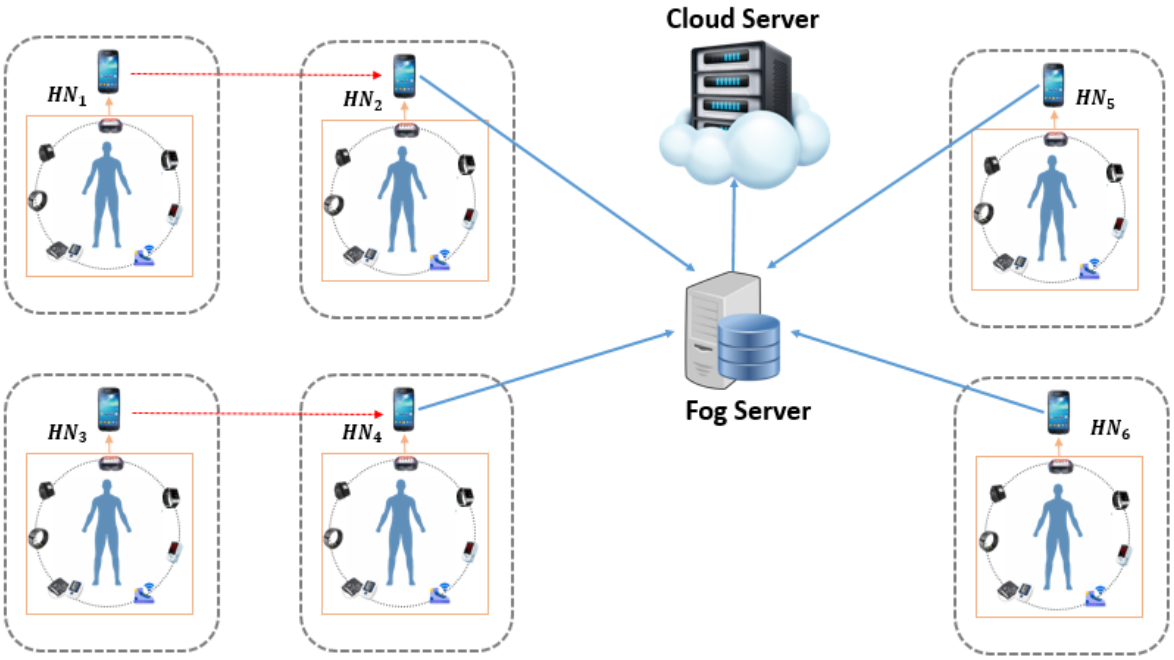

Figure 4.2: System Model of BK-SDA scheme

4.3.1 Sensor Node

To measure real-time patient healthcare data, the smart sensor devices are attached to the patient's body to gather information which is shared with a Head node (HN) for data aggregation. This information is securely transmitted from the individual sensor nodes to the HN by using a wireless communication channel. Each SN sends the encrypted information to the HN using a batch key only if the patient's healthcare parameter values are not similar to the normal values.

4.3.2 Head Nodes

The Head node (HN) acts as a central repository between sensing devices and FS. It collects encrypted healthcare data from multiple sensor devices for data aggregation and then

forwards the aggregated data to the fog server for further processing. There are six head nodes ($HN_1, HN_2, HN_3, HN_4, HN_5, HN_6$) are used for aggregation in the above scenario shown in Figure 4.2. The four head nodes (HN_2, HN_4, HN_5, HN_6)directly access the fog server but the remaining two head nodes (HN_1, HN_3,) cannot have direct access of fog server, so they transmit their data to the neighboring aggregated nodes (HN_2, HN_4).The HN_4 receives aggregated data directly from its sensors as well as fromHN_3. It further aggregates this data by using a delimiter before sending it to the fog server. Similarly, HN_1 shares its aggregated data with its neighboring nodes HN_2 then performs further aggregation before forwarding it toward the fog server. The interaction supports multi-hop data aggregation to ensure all sensing information ultimately reaches the FS.

4.3.3 Fog Server

The Fog server (FS) receives the aggregated healthcare data from aggregate nodes. It performs initial message verification on the received message using batch key (XOR) operation before extracting the original data. After extraction, the FS uploads the data to the cloud server for storage. Medical professionals obtain patient's healthcare data by sending its request to the fog server. The fog server then retrieves the required data from the cloud server and shares it with the doctors to remotely monitor the patient’s healthcare conditions and make appropriate decisions accordingly.

4.3.4 Cloud Server

The cloud server (CS) is an entity that can store data from fog servers. At the request of medical professionals, the cloud server shares the patient’s data with the FS and then sends it to the doctor for remote analysis.

4.4 Algorithms for Batch Key Based Secure Data Aggregation Protocol

In IoMT systems, multiple algorithms have already been developed to ensure secure data aggregation and extraction using batch keys. However, the purpose of the proposed BK-SDA protocol is to reduce data transmission costs and make the system resilient against security attacks. The proposed algorithms shown in Figure 4.3 and Figure 4.4 provide a detailed explanation of each step to understand how it works.

4.4.1 Algorithm for Secure Batch Verification and Data Aggregation at Head Node (SBVDA-HN)

The proposed Secure Batch Verification and Data Aggregation at Head Node (SBVDA-HN) algorithm focuses on aggregation of data received from Sensor Nodes (SNs) or other Head Nodes (HNs). Each node sends its encrypted data to the head node for data aggregation and then forwards it to the FS for storage. To understand the terms presented in the proposed algorithms, the Table 4.1 provides a list of notations that are used to identify the variables, parameters, and mathematical operations used throughout the algorithms for secure data communication between nodes.

Table 4.1: List of Notations

Sr.no	Symbols	Description
1.	SN_{ij}	Sensor Node ID
2.	CS_{ij}	Cipher Message at Sensor Node
3.	Em_{ij}	Encrypted Message at Sensor Node
4.	ts_{ij}	Timestamp of Sensor Node
5.	TS_{ij}	Timestamp of Head Node
6.	A_m	Aggregated Message
7.	S_k	Secret Key
8.	σs_{ij}	Hash Function of the Sensor Node
9.	σa_{ij}	Hash Function of the Head Node
10.	HN_{ij}	Head node ID
11.	BK_{ij}	Batch Key at Fog Server
12.	OM_{ij}	Original message extracted at the Fog Server

Initially, the SN gathers the healthcare data by attaching sensing devices to the patient's body. It encrypts this collected information by taking XOR with the batch key (BK_{ij}) to get cipher text (CS_{ij}). The batch key is also shared with the FS for decryption. Each SN forwards its data to the HN only if the patient's healthcare data value does not exist in the normal range. The hash value $\sigma s_{ij=}H(SN_{ij}||CS_{ij}||\text{ts}_{ij})$ is also calculated at the SN that contains Node ID, Cipher message, and Timestamp. This generated hash σs_{ij} is then appended with the encrypted message MSG= ($SN_{ij}, CS_{ij}, \text{ts}_{ij}, \sigma s_{ij}$) before moving it towards the HN for aggregation and verification process.

Require: A_m= 0, S_k= Random number, Msg (Em_{ij},CS_{ij})

Steps:

Receive Encrypted Messages from the Sensor node or Head node

1. **IF** T (ts$_{ij}$)' - T (ts$_{ij}$) < ΔT **then**
2. **Calculate** $\sigma_{ij} \leftarrow$ H (SN_{ij}|| ts$_{ij}$|| CS_{ij}) **of received message**
3. **IF** $\sigma s_{ij} \leftarrow \sigma s_{ij}$' then
4. **IF arr** [HN_{ij}] **contains** SN_{ij} **then**
5. A_m=A_m || CS_{ij}
6. S_k= $S_k \oplus CS_{ij} \oplus T(ts_{ij})$
7. **ELSE**
8. A_m=A_m||Em_{ij}
9. S_k= $S_k \oplus Em_{ij} \oplus T(ts_{ij})$
10. **ENDIF**
11. **ELSE**
12. Remove messages due to integrity violation
13. **ENDIF**
14. **ELSE**
15. Remove Outdated Messages
16. **ENDIF**

Calculate Hash Signature for Fog server

17. $\sigma a_{ij} \leftarrow$ H(HN_{ij} || S_k || T (ts$_{ij}$))

Send Aggregated Messages to the Fog server

18. A_m= ($HN_{ij}, S_k, \sigma_{ij}, \text{ts}_{ij}$)

Figure 4.3: Algorithm of SBVDA-HN

The proposed SBVDA-HN algorithm received encrypted messages from sensor nodes and the head nodes that do not directly access the FS. The aggregated message variable (A_m) is initially set to zero because no values are stored in it. After that, assign any random number for the secret key (S_k) instead of zero which could be vulnerable to security attacks during data transmission. The HN conducts data verification by timestamp and hash value comparison technique on received data to ensure the integrity and freshness of each message before starting the aggregation process. In the timestamp verification process, subtract the received timestamp T (ts_{ij}) with the generated timestamp T (ts_{ij})′ at HN, if it is less than the threshold value by satisfying this condition T (ts_{ij})'- T (ts_{ij}) < Δ T then accept the message otherwise discard the outdated message. After that, compare the calculated hash (σs_{ij}) with the received hash (σs_{ij})' if both are equal that means data integrity is verified otherwise discard the message due to integrity violation.

Once the verification process is completed, the HN checks the received message by running the IF-ELSE condition to identify where the data came from. If the arr [AN_{ij}] contains the sensor node ID (SN_{ij}) it shows received message came from sensor nodes. All received messages are then concatenated with the aggregated message ($A_m = A_m||C_{ij}$). Then perform batch verification ($S_k = S_k \oplus CS_{ij} \oplus T(ts_{ij})$) on received messages by taking XOR between the secret key, cipher message, and timestamp. Otherwise, the received data is from a different HN that cannot directly access the FS. The data aggregation is again performed on this data by concatenating the encrypted aggregated message (Em_{ij}) with the actual aggregated message (A_m) by using the condition ($A_m = A_m||Em_{ij}$). It also performs batch verification on aggregated messages like($S_k = S_k \oplus Em_{ij} \oplus T(ts_{ij})$) by taking XOR between the secret key, encrypted aggregated message, and timestamp. The batch verification process is used to generate a shared secret key ((S_k) between the HN and FS to secure their communication. The HN also calculates its hash $\sigma s_{ij} \leftarrow$ H(AN_{ij} || S_k || T (ts_{ij})) and attached with the aggregated message before sending this message to the FS for data extraction.

4.4.2 Algorithm for Secure Batch Verification and Data Extraction at Fog Server (SBVSE-FS)

The Proposed Secure Batch Verification and Data Extraction at Fog Server (SBVSE-FS) algorithm received aggregated messages (A_m) sequentially from nearby aggregate nodes. Upon receiving the messages from HNs, the Fog server started the process of decryption to extract the original message of each sensor device. Before initializing this process, the SBVDE-FS algorithm checks the authenticity of received messages by Timestamp and hash verification methods to ensure the integrity and freshness of aggregated messages. In the Timestamp verification method, if the condition T (TS_{ij})' - T (TS_{ij}) < ΔT is true which means the Timestamp of the received message was not changed so the message's freshness remains the same. For checking the integrity of the received message, the hash comparison method is used. If the calculated hash value at FS ($\sigma\ a_{ij}$) is the same as the hash value of the received aggregated message (σa_{ij})' that means message integrity is not violated during transmission. Once this verification process is completed successfully, the FS continues the process of extraction otherwise discard the message due to security failure.

After the verification process, the FS executes the IF-ELSE condition to identify the origin of received messages whether it comes directly from the nearby aggregate node or another aggregate node that is unable to directly access the FS. If the arr [AN_{ij}] contains the sensor node ID (SN_{ij}) that shows the message comes from the nearby HN otherwise it is from the distant HN. The SBVDE-FS algorithm then performs batch verification by taking XOR with the batch key (BK_{ij}) to extract aggregated message (A_m). Next, extract the Secret Key (S_k) by taking the XOR between Timestamp ($T(ts_{ij})$), Secret Key (S_k) and encrypted received message (CS_{ij}) or (Em_{ij}) to start the extraction of original sensor node data. Now, FS runs For Loop by using the condition FOR count= (1→q) where q denotes the number of nodes to get the encrypted message of the sensor device. Each loop extracts the data of an individual node that contains Node ID (SN_{ij}), Timestamp (TS_{ij}), and Hash Value (σs_{ij}) and used array Arr [count] to store the extracted data of each node on their specific location But for extracting original sensor node data, FS compare the calculated hash (σs_{ij})' of sensor node with the extracted hash value (σs_{ij}) of received message to check the integrity of data. If both hash values are the same

(σs_{ij}) = (σs_{ij})' that means the sensor node data is not altered during the data transmission from the sender node to the FS. Then the FS started extraction of original data by taking XOR between Cipher Message (CS_{ij}) and batch key (BK_{ij}). Once the extraction process is completed, the FS sends an acknowledgment message to HN.

Require: Receive aggregated message (A_m) from HN

Perform Batch Verification on Aggregated Messages

Steps:

1. **IF:** $T(TS_{ij})$' - $T(TS_{ij})$< ΔT **then**
2. **IF:** σa_{ij} = σa_{ij}' **then**
3. **IF: arr [**HN_{ij}**] contains** SN_{ij}**then**
4. **Extract:** $A_m \leftarrow CS_{ij} \oplus BK_{aij}$
5. $S_k = S_k \oplus CS_{ij} \oplus T(ts_{ij})$
6. **FOR count←(1→q) do**
7. $CS_{ij} = (SN_{ij}, TS_{ij}, \sigma s_{ij})$
8. Arr[count]= CS_{ij}
9. count ++
10. **ELSE:**
11. **Extract:** Am ← $Em_{ij} \oplus BK_{aij}$
12. $S_k = S_k \oplus Em_{ij} \oplus T(TS_{ij})$
13. **FOR count←(1→q) do**
14. $Em_{ij} = (SN_{ij}, TS_{ij}, CS_{ij}, \sigma s_{ij})$
15. Arr[count]= Em_{ij}
16. count ++
17. **ENDIF**
18. **ELSE:**
19. Remove Message due to integrity violation at Head Nodes
20. **ENDIF**

Calculate Hash: $\sigma s_{ij} \leftarrow$ H ($SN_{ij} \| TS_{ij} \| CS_{ij}$)

21. **IF:** σs_{ij}= σs_{ij}' **then**
22. **Extract the Original Message:** $OM_{ij} \leftarrow CS_{ij} \oplus BK_{aij}$
23. **ELSE:**
24. Remove Message due to integrity violation at Sensor Nodes
25. **ENDIF**
26. **ELSE:**
27. Remove Outdated Message
28. **ENDIF**

Send an Acknowledgment Message to the Head Node after completing Extraction at the Fog Server

Figure 4.4: Algorithm of SBVDE-FS

4.5 Security Analysis

Our proposed batch key-based data aggregation protocol (BK-SDA) scheme provides a secure and lightweight solution for remote healthcare monitoring systems. It focuses on protecting the systems against security attacks by ensuring the authenticity and integrity of sensitive healthcare data during the aggregation and sharing process. In this section, we explore the BK-SDA scheme's defense mechanism against security attacks. Some of the security attacks are discussed below:

4.5.1 Replay Attack

In a replay attack, the adversary does not directly modify the contents of intercepted messages. Instead, it stores the transmitted messages and then strategically retransmits them at a later time to disrupt the intended flow of information exchange between the two nodes. Our proposed BK-SDA scheme deals with this issue by providing timestamp verification on all messages. This method ensures that every message exchange within a network includes the exact time when it was created. In our proposed method, the SN sends the encrypted messages to the HN by taking the XOR between the secret key, cipher message, and timestamp (S_k= $S_k \oplus CS_{ij} \oplus T(ts_{ij})$). Upon receiving these messages, the HN checks the timestamp to identify the freshness of the received message by checking the condition T (TS_{ij})' - T (TS_{ij}) < ΔT. If the condition is true, it indicates that the message is received within a given timeframe, so the message is considered valid for further processing. However, if the condition is false, the message is considered outdated and discarded. The FS also uses the same timestamp verification method to ensure all messages are fresh and valid to secure the communication and protect the network from replay attacks.

4.5.2 Denial of Service Attack

A Denial of Service (DoS) attack happens when too many fake messages are sent to a network, making it difficult to identify legitimate messages. These misleading messages are sent by the malicious node to slow down or even stop the network from working properly. To counter this attack, the proposed BK-SDA protocol allows only authenticated nodes to

participate in the network communication. To ensure the integrity of messages, the proposed scheme used the hash function to verify the authenticity of received messages at destination nodes. The Timestamp Verification and Hash Value Verification methods confirm that the message has not been altered during transmission and is timely delivered making it suitable for secure communication.

4.5.3 Man in The Middle Attack

In a man-in-the-middle attack, the attacker sneaks the sensitive information between two nodes by placing an adversarial node between them. The adversarial node receives messages from one node and sends them to the other, making each node believe they are directly communicating with each other. The attacker intercepts and sometimes alters sensitive data, which can create serious security threats for the system. To address this attack, the proposed BK-SDA scheme utilizes batch key-based verification techniques and hash functions to protect the integrity and authenticity of transmitted messages. The batch key-based encryption and decryption techniques apply strong security credentials on received messages to protect the security of transmitted messages. The hash is compared at the receiving node to verify the authenticity of the sending node. If the hashes do not match, the system discards the message due to an integrity violation to protect the network from attacks.

4.6 Summary

This chapter provides a details description of the system model and its components such as Sensor Nodes, Head Nodes, Fog Servers, and Cloud Server. It also explains the proposed BK-SDA protocol and the working of its algorithms. The SBVDA-HN algorithm is implemented on HN for secure data aggregation and the SBVDE-FS algorithm is implemented on FS to securely extract data received from HN. The complete step-by-step working of both of these algorithms is written in the chapter. Finally, a security analysis of the proposed scheme is conducted to evaluate its effectiveness in defending the network against security attacks.

CHAPTER 5

PERFORMANCE EVALUATION OF BATCH KEY-BASED SECURE DATA AGGREGATION PROTOCOL

5.1 Overview

This chapter includes the details of establishing a simulation setup and the system requirements to implement the algorithms of the proposed scheme. The extracted results are displayed in the form of graphs to visually analyze their work. For performance evaluation, the proposed scheme is compared with some other related comparative schemes to check its efficiency under different evaluation metrics.

5.2 Simulation Environment

An extensive simulation is performed on the NS-2.35 tool to validate the performance of the proposed BK-SDA protocol. The NS 2.35 is a free and open-source network simulator tool installed on an Ubuntu-based environment to manage device operations. The main requirements for the experimental setup of NS 2.35 are Ubuntu OS, Core i5 processor, and VMware workstation (virtual machine) to run dual operating systems. The system should have at least 6 GB of RAM and at least 10 GB free disk space is available to handle simulation tasks efficiently. The GCC 4.8 compiler is needed for the setup because NS-2.35 is designed to work with older versions of GCC. Additionally, libraries such as TCL, OTcl, and Nam, must be installed to ensure the full functionality of the NS-2 simulation tool. This environmental setup ensures a stable and efficient setup for conducting simulations with NS-2.35.

Table 5.1: System Setup

Components	Requirement
Operating System	Ubuntu 14.04 LTS
Processor	Core i5
RAM	6 GB
Disk Space	10 GB
Compiler	GCC 4.8 or earlier version
Libraries	TCL, OTcl, and Nam

For simulation setup, the 1600 X 1600-meter network area is selected for the installment of different network devices such as SNs, HNs, FS, and CS. The list of different simulation parameters and their values that are used for the simulation process is written in Table 5.2.

Table 5.2: Simulation Parameters

Parameters	Value
Network Area	1600 X1600 m
Number of Sensor Nodes	20~200
Cluster Radius	500 m
Sensing Radius	150 m
Initial Energy	1000 J
Transmission Power at SN	0.192 µJ
Receiving Power at SN	0.055 µJ
Communication Channel	Wireless
Propagation Model	Two Ray
Transmission Power at HN	0.05928 µJ
Receiving Power at HN	0.05 µJ
SN per Group	5-20 nodes
Number of HN's	1-10
MAC Protocol Type	MAC/802-11
Queue Type	DropTail / PriQue
Antenna Type	Omni Antenna
Router Trace	ON
MAC Trace	OFF
Agent Trace	ON
Assign Time Slots	0.1-1 sec

In this simulation environment, the SNs receive and transmit data with the help of Omni Antenna because it can detect signals from all angles. The initial value of SN is 1000 Joule at the start of the simulation process. The number of sensor nodes lies within the range of (20~200) nodes and each node contains at least 160 meters of network area for data transmission. The cluster radius for each HN is 500 m and the sensing radius is 150m for SNs. The two-ray propagation model is used to detect path failures among different network antennas for wireless communication. After completing the simulation setup, the TCL files, C++ languages, and AWK scripts are utilized to implement network simulation and obtain results. The TCL files are used for the node configuration, message initialization, and the establishment of simulation parameters. To implement the data transmission operations among nodes are managed by creating a separate function in the C++ language.

After that, the AWK script is utilized to extract results from trace files generated by the simulations. Based on the results, the comparative analysis is performed with three other related schemes SATS [27], LVPDA [43], and ID-LBVA [39] to analyze its performance.

5.3 Performance Analysis of Batch Key-based Data Aggregation Protocol

To validate the effectiveness of the proposed BK-SDA scheme, different evaluation parameters such as computation cost, energy consumption cost, and communication cost are considered to measure its performance. Moreover, the performance of the proposed scheme is compared with three other latest secure data aggregation-based schemes to check how well it performs than other ones.

5.3.1 Computational Cost

In WSNs, the computational cost is the main factor that must be considered to evaluate the performance of any algorithm. The proposed BK-SDA is compared with SATS [27],

LVPDA [43], and ID-LBVA [39] schemes to check its performance in terms of computational cost.

Figure 5.1 shows the computational cost of multiple schemes for different numbers of sensor nodes at the HN. It is observed that when the number of SN is minimum like SN=1, the computational cost of proposed BK-SDA schemes is 18.322 ms, SATS is 12.432 ms, LVPDA is 28.6599 ms, and ID-LBVA is 10.446 ms respectively. And, when the number of SN is maximum that is 10, the computational cost of proposed BK-SDA schemes is 135.659 ms, SATS is 105.214 ms, LVPDA is 157.4184 ms, and ID-LBVA is 120.783 ms respectively. The results show that the proposed BK-SDA scheme performs better than LVPDA but it requires a little bit more computational cost as compared to SATS and ID-LBVA at HN. The graph illustrated in Figure 5.1 is linear and it shows that when the number of devices is increased the BK-SDA requires more computational resources to execute its respective algorithms as compared to SATS and ID-LBVA.

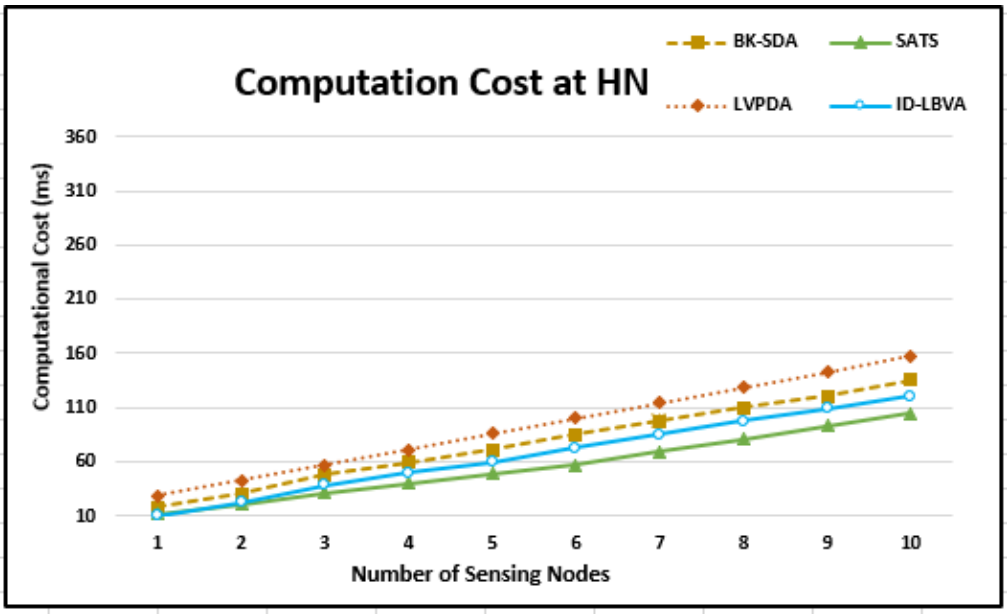

Figure 5.1: Computational Cost at HN

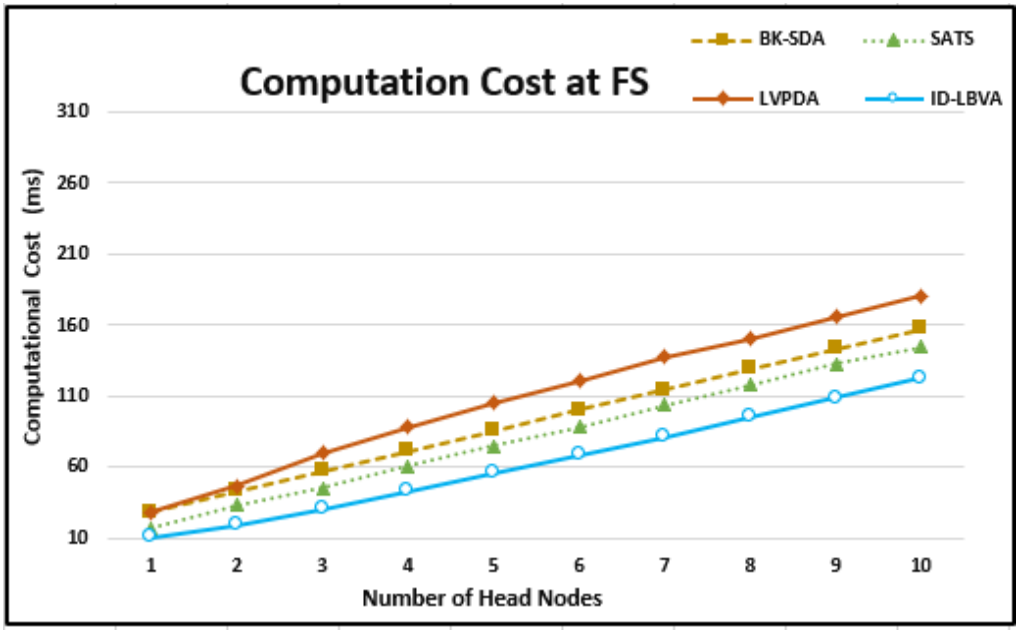

Figure 5.2: Computational Cost at FS

In Figure 5.2 when the number of HN is 1, the computational cost of proposed BK-SDA schemes is 28.325 ms which is less than other relevant schemes like SATS is 23.3162 ms, LVPDA is 28.3162 ms, and ID-LBVA is 10.2598 ms respectively. The computational cost of proposed BK-SDA schemes is 180.0747 ms when the number of HN is 10 while SATS is 151.0747 ms, LVPDA is 157.0747 ms, and ID-LBVA is 122.6187 ms respectively. The graph shown in Figure 5.2 is linear to indicate that when the number of HN is changed the performance of the proposed BK-SDA is better than LVPDA but requires more computational cost to complete its tasks as compared to SATS and ID-LBVA. The proposed BK-SDA scheme consumes less computational resources but it gradually consumes more resources when the number of nodes is increased at FS as compared to SATS and ID-LBVA.

The comparative analysis of computational cost for HN and FS shown in Figure 5.1 and Figure 5.2 depicts that both graphs are linear and grow smoothly. The overall results show that the BK-SDA scheme required more computational resources as compared to other schemes because the proposed scheme is not light weighted. During data transmission, the random value is assigned for secret key that is null in previous schemes ,so that's why BK-SDA consume little bit more computational power as compared to SATS and ID-LBVA.

5.3.2 Energy Consumption Cost

In WSNs, the energy consumption cost is evaluated by simulations and obtained results by using Trace files and AWK files. The Trace files print the residual energy of all nodes under different log parameters. Moreover, extracting the values of energy consumption cost is possible by using the AWK files. The energy consumption cost of the proposed BK-SDA is compared with SATS, LVPDA, and ID-LBVA schemes to check its performance.

In Figure 5.3, the graph shows the performance of the BK-SDA scheme in terms of energy consumption cost for SNs. The energy consumption cost is presented in these graphs show how much energy is consumed during message transmission. The initial value of energy consumption cost is set to 0.0001 J for SNs. At t = 0.8 sec the energy consumption cost for BK-SDA is 0.00031 J which is less than the other three comparative schemes such as SATS = 0.00035J, ID-LBVA =0.00037 J and LVPDA = 0.00051 J. The growth of the proposed scheme is not fast enough and the graph shows that it consume less energy consumption cost as compared to other related schemes even the time changed.

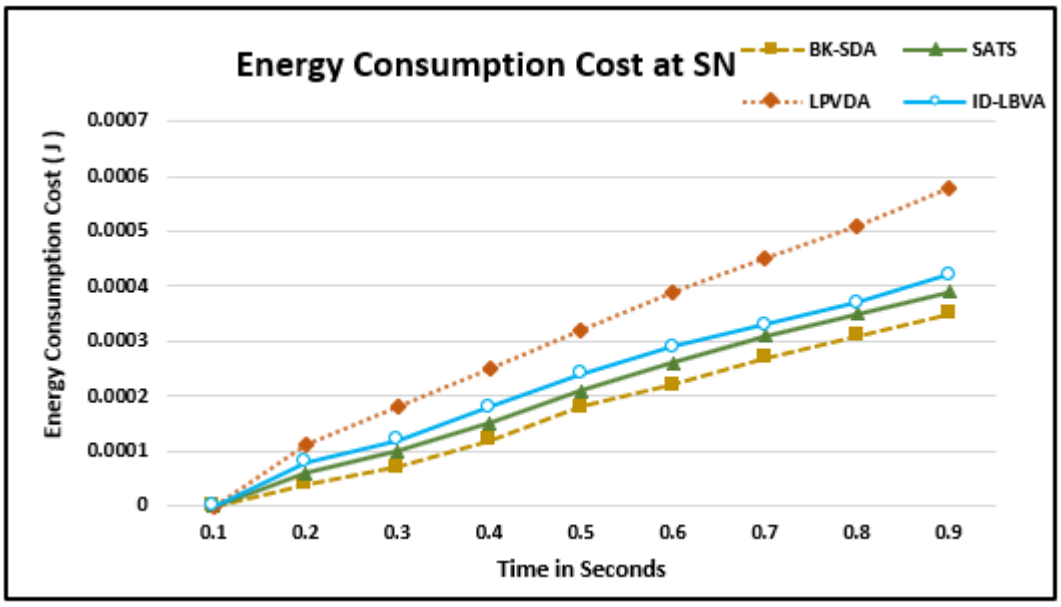

Figure 5.3: Energy Consumption at different SN

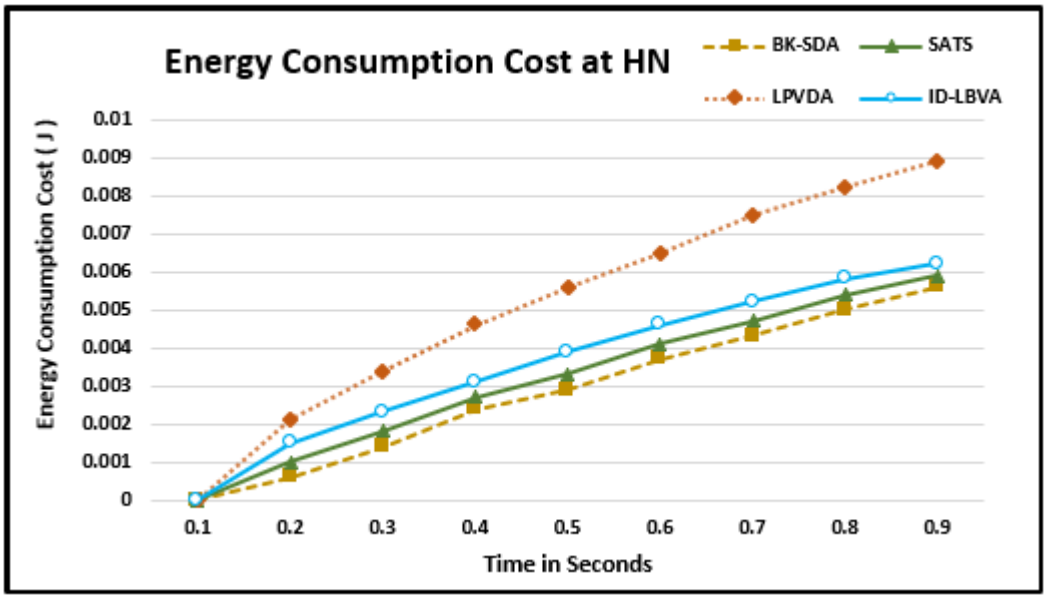

Figure 5.4: Energy Consumption at different HN

In Figure 5.4, the graph demonstrates the energy consumption cost for HNs when t=0.8 sec. The initial energy level is also set to 0.001 J for HN. The energy consumed by the BK-SDA scheme is 0.005 J, SATS is 0.0054J, ID-LBVA is 0.0058 J and LVPDA is 0.0082 J respectively. The results of Fig 5.3 and Fig 5.4 show that the proposed BK-SDA scheme consumes less energy than SATS, ID-LBVA, and LVPDA schemes for both SNs and HNs.

5.3.3 Communication Cost

The communication cost depends on the number of nodes on the fog server. In Figure 5.5, the displayed graph shows the performance of the BK-SDA scheme with three other schemes that are SATS, ID-LBVA, and LVPDA for different numbers of SNs at FS. When the number of SNs = 44, the communication cost of BK-SDA is 15.3482 ms, SATS is 19.2561 ms, LVPDA is 21.3193 ms and ID-LBVA is 17.3671 ms. The results shown in Figure 5.5 demonstrate that the communication cost of BK-SDA scheme is better than other comparative schemes in terms of the communication cost for different numbers of SNs at FS.

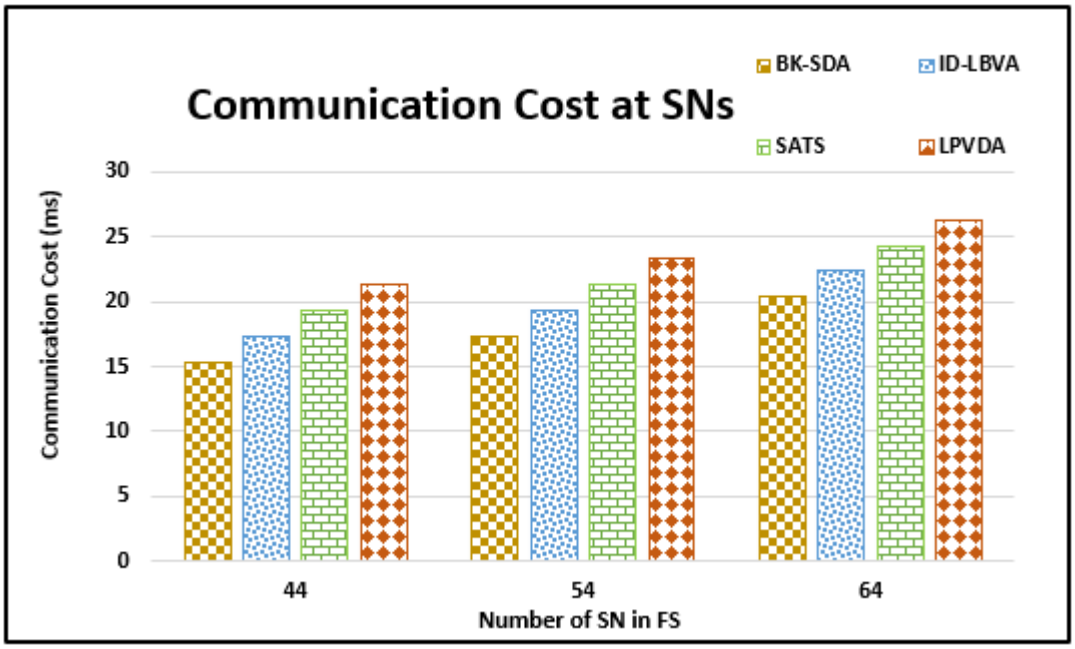

Figure 5.5: Communication Cost at SNs

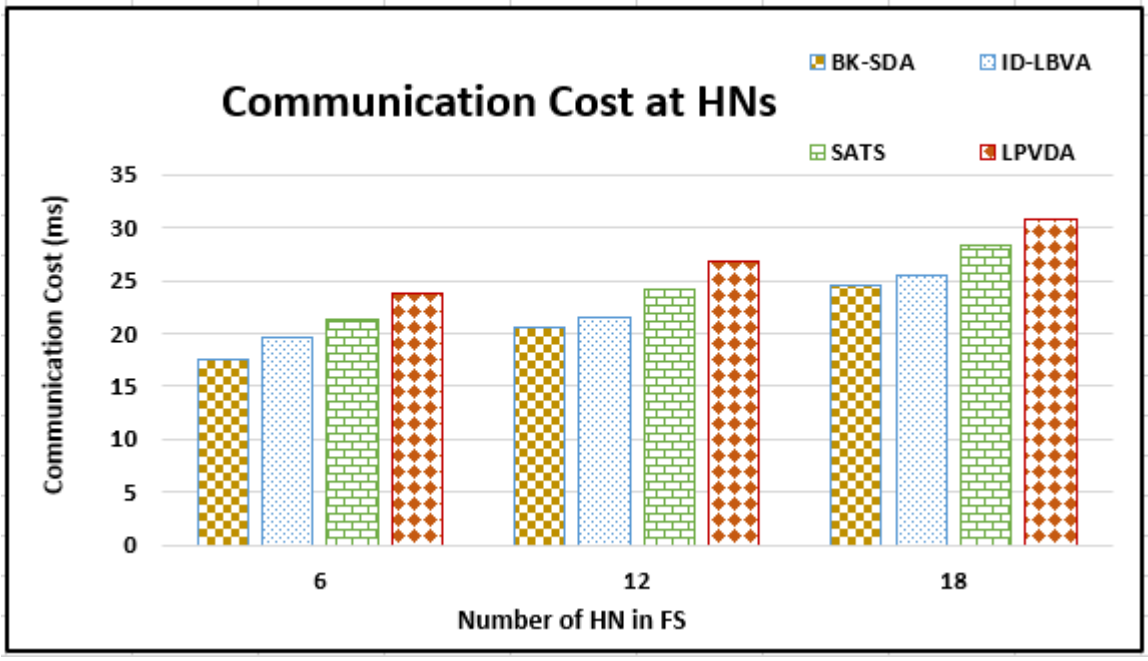

Figure 5.6: Communication Cost at HNs

The graph shown in above Figure 5.6 displayed the communication cost for different numbers of HNs at FS. The value of the proposed BK-SDA scheme is 19.5437 ms when the number of HN is 6, while the values of other schemes like SATS are 20.2561 ms, LVPDA is 23.7877 ms, and ID-LBVDA is 19.543 ms respectively. The graph in Figure 5.6 proved that the value of the proposed BK-SDA scheme is less than other related schemes and it performs more beneficial than other ones. The overall results showed that the communication cost is reduced in BK-SDA scheme because the number of messages transmitted over the network in one aggregated form so they required less communication cost.

5.4 Summary

The purpose of the proposed BK-SDA scheme is to reduce the data transmission cost and make it more secure and feasible for data communication. To measure the performance of the proposed BK-SDA scheme, different evaluation metrics are considered such as computation cost, energy consumption cost, and communication cost. The results demonstrate that the performance of the BK-SDA scheme is better than other comparative schemes in terms of communication and energy consumption cost but not for the computational cost. The NS 2.35 simulation tool is used to obtain the simulation results.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Overview

This chapter summarizes the key findings of the research work and sheds light on future work to further improve the performance of secure data aggregation protocols. The primary focus of the research work is to build a lightweight data aggregation protocol for secure data communication and transmission. For this purpose, the NS 2.35 simulation tool is used to analyze the performance of the proposed protocol. By comparing it with other already existing protocols under different performance evaluation parameters, the results demonstrate that it performs better than others.

6.2 Conclusion

The IoMT is an innovative technology that contains medical sensors to remotely monitor patient's healthcare data and transmit it to the doctors to provide medical treatment immediately. For online data transmission, security is a main factor that has always been a concern for healthcare systems to protect the sensitive information of patients that comes to them via the Internet. To establish a secure and cost-effective network, different research has been already done to implement a secure and lightweight data aggregation system but still, some issues need to be resolved. The main aim of the proposed BK-SDA scheme is to reduce data transmission costs and minimize the risks of security attacks. For this purpose, the BK-SDA scheme used the batch key-based XOR method and chose random values for the secret key to decrease the risks of security attacks while transferring sensitive data from SN to HN and then FS. The BK-SDA protocol consists of two algorithms, the SBVDA-HN algorithm collects data

from SNs and provides batch key verification and data aggregation methods before forwarding the data to the FS. And, the other SBVDE-FS algorithm also performs batch verification on received data before starting the data extraction process at FS. The performance of the BK-SDA protocol is evaluated using the NS 2.35 simulation tool. The TCL script files are used for node placement and its configuration and the C++ files are used to implement and control the functionality of the proposed BK-SDA protocol. The experimental results showed that the performance of the proposed BK-SDA scheme is better than SATS [32], LVPDA [43], and ID-LBVA [39] schemes in terms of communication cost, and energy consumption cost at both HN and FS.

6.3 Future Work

In the future, the batch key generation using the proposed model will be extended for multi-party key establishment. More evaluation metrics like bandwidth utilization, memory consumption, and throughput should be considered to evaluate the performance. To improve the performance of secure data aggregation protocols, there are some additional evaluation metrics like bandwidth utilization, memory consumption, throughput, etc. should be considered in future research work.

REFERENCES

[1] Krichen, M. (2023). A survey on formal verification and validation techniques for internet of things. *Applied Sciences,* 13(14), 8122.

[2] Jamshed, M. A., Ali, K., Abbasi, Q. H., Imran, M. A., & Ur-Rehman, M. (2022). Challenges, applications, and future of wireless sensors in Internet of Things: A review. *IEEE Sensors Journal*, 22(6), 5482-5494.

[3] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access,10,*3224-3230.

[4] Hamdan, S., Ayyash, M., & Almajali, S. (2020). Edge-computing architectures for Internet of things applications: A survey. Sensors, 20(22), 6441.

[5] Lata, S., Mehfuz, S., & Urooj, S. (2021). Secure and reliable wsn for internet of things: Challenges and enabling technologies. *IEEE Access*, 9, 161103-161128.

[6] Abu Odeh, A., S Qasaymeh, S., Alnajjar, I., & Ali Qasaymeh, M. (2024). A Survey of Energy-Efficient Routing Protocols for WSN based IoT Networks. *International Journal of Computing and Digital Systems*, 15(1), 1-9.

[7] Ullah, A., Azeem, M., Ashraf, H., Alaboudi, A. A., Humayun, M., & Jhanjhi, N. Z. (2021). Secure healthcare data aggregation and transmission in IoT—A survey. *IEEE Access, 9*, 16849-16865.

[8] PremaLatha, V., Sreedevi, E., & Sivakumar, S. (2019). Contemplate the internet of things transforming as medical devices- the internet of medical things (IOMT). In *2019 International Conference on Intelligent Sustainable Systems (ICISS)*. IEEE, 276-281.

[9] Alamer, A. (2023). An efficient group signcryption scheme supporting batch verification for securing transmitted data in the Internet of Things. *Journal of Ambient Intelligence and Humanized Computing*, *14*(5), 5885-5902.

[10] Subhan, F., Mirza, A., Su'ud, M. B. M., Alam, M. M., Nisar, S., Habib, U., & Iqbal, M. Z. (2023). AI-enabled wearable medical internet of things in healthcare system: A survey. *Applied Sciences, 13(3),* 1394.

[11] Jan, M. A., Zhang, W., Khan, F., Abbas, S., & Khan, R. (2024). Lightweight and smart data fusion approaches for wearable devices of the Internet of Medical Things. *Information Fusion, 103*, 102076.

[12] Cao, S., Lin, X., Hu, K., Wang, L., Li, W., Wang, M., & Le, Y. (2021). Cloud computing-based medical health monitoring IoT system design. *Mobile Information Systems*, *2021*, 1-12.

[13] Sharmila, E. M. N., Rama Krishna, K., Prasad, G. N. R., Anand, B., Kwatra, C. V., & Kapila, D. (2024). IoMT—Applications, Benefits, and Future Challenges in the Healthcare Domain. *Advances in Fuzzy-Based Internet of Medical Things (IoMT),* 1-23.

[14] Rani, S., Kumar, S., Kataria, A., & Min, H. (2024). SmartHealth: An intelligent framework to secure IoMT service applications using machine learning. *ICT Express*, 10(2), 425-430.

[15] Bharati, S., Podder, P., Mondal, M. R. H., & Paul, P. K. (2021). Applications and challenges of cloud-integrated IoMT. *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications*, 67-85.

[16] Nguyen, D. C., Pham, Q. V., Pathirana, P. N., Ding, M., Seneviratne, A., Lin, Z., ... & Hwang, W. J. (2022). Federated learning for smart healthcare: A survey. *ACM Computing Surveys (CSUR)*, *55*(3), 1-37.

[17] Kumar, S., Arora, A. K., Gupta, P., & Saini, B. S. (2021). A review of applications, security, and challenges of Internet of Medical Things. *Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications*, 1-23.

[18] Hasan, M. K., Weichen, Z., Safie, N., Ahmed, F. R. A., & Ghazal, T. M. (2024). A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. IEEE Access.

[19] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., & Douligeris, C. (2020). Security in IoMT communications: A survey. *Sensors*, *20*(17), 4828.

[20] Bojjagani, S., Brabin, D., Kumar, K., Sharma, N. K., & Batta, U. (2024). Secure privacy-enhanced fast authentication and key management for IoMT-enabled smart healthcare systems. *Computing*, 1-32.

[21] Nair, A. K., Sahoo, J., & Raj, E. D. (2023). Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Computer Standards & Interfaces*, 86, 103720.

[22] Chen, C. M., Liu, S., Li, X., Islam, S. H., & Das, A. K. (2023). A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT. *Journal of Systems Architecture*, *136*, 102831.

[23] Bojjagani, S., Brabin, D., Kumar, K., Sharma, N. K., & Batta, U. (2024). Secure privacy-enhanced fast authentication and key management for IoMT-enabled smart healthcare systems. *Computing*, 1-32.

[24] Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare internet of things. *Wireless Networks*, *27*, 5503-5509.

[25] Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., & Tsatsoulis, C. (2019). Review of security and privacy for the Internet of Medical Things (IoMT). In *2019 15th international conference on distributed computing in sensor systems (DCOSS).* IEEE, 457-464.

[26] Alalhareth, M., & Hong, S. C. (2024). Enhancing the Internet of Medical Things (IoMT) Security with Meta-Learning: A Performance-Driven Approach for Ensemble Intrusion Detection Systems. *Sensors*, 24(11), 3519.

[27] Said, G., Ghani, A., Ullah, A., Azeem, M., Bilal, M., & Kwak, K. S. (2022). Light-weight secure aggregated data sharing in IoT-enabled wireless sensor networks. *IEEE Access*, *10*, 33571-33585.

[28] Hussien, Z. A., Abdulmalik, H. A., Hussain, M. A., Nyangaresi, V. O., Ma, J., Abduljabbar, Z. A., & Abduljaleel, I. Q. (2023). Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. *Applied Sciences*, *13*(2), 691.

[29] Wang, W., Sun, Y., & Li, Y. (2022)." *Security-Enhanced Certificate-Based Remote Data Integrity Batch Auditing for Cloud-IoT*." Security and Communication Networks, 2022.

[30] Kung, Y. H., & Hsiao, H. C. (2019). GroupIt: Lightweight group key management for dynamic IoT environments. *IEEE Internet of Things Journal*, *5*(6), 5155-5165.

[31] Kumar, P., Sharma, S. K., & Kadam, K. U. (2022). Empirical Evaluation of ECC Batch Verification Algorithms of Digital Signature in Wireless Sensor Network. *Electronics/Elektronika*, *26*(2), *1450-584*.

[32] Wang, W., Huang, H., Wu, Y., & Huang, Q. (2019). Cryptanalysis and improvement of an anonymous batch verification scheme for mobile healthcare crowd sensing. *IEEE Access*, *7*, 165842-165851.

[33] Han, J., Li, Y., Liu, J., & Zhao, M. (2019). "*An efficient Lucas sequence-based batch auditing scheme for the internet of medical things*." IEEE Access, 7, 10077-10092.

[34] Kang, J., Fan, K., Zhang, K., Cheng, X., Li, H., & Yang, Y. (2021). "*An ultra-lightweight and secure RFID batch authentication scheme for IoMT*." Computer Communications, 167, 48-54.

[35] Mahmood, Z., Ullah, A. and Ning, H., (2019) Distributed multiparty key management for efficient authentication in the Internet of things. *IEEE Access*, *6*, 29460-29473.

[36] Xiong, H., Wu, Y., Su, C., & Yeh, K. H. (2020)."*A secure and efficient certificate-less batch verification scheme with invalid signature identification for the internet of things*." Journal of Information Security and Applications, 53, 102507.

[37] Altowaijri, S. M. (2021). Reducing Cybersecurity Risks in Cloud Computing Using A Distributed Key Mechanism. *International Journal of Computer Science & Network Security*, *21*(9), 1-10.

[38] Zhang, Wu, S., A., Luo, H., & Chen, J. (2024). CRT-based group rekeying with efficient dynamically aggregate signature for IoMT. Ad Hoc Networks, 159, 103501.

[39] Mao, W., Jiang, P., & Zhu, L. (2023). Locally Verifiable Batch Authentication in IoMT. *IEEE Transactions on Information Forensics and Security 26(5), 1977-1986.*

[40] Azeem, M., Ullah, A., Ashraf, H., Jhanjhi, N. Z., Humayun, M., Aljahdali, S., & Tabbakh, T. A. (2021). "*Fog-oriented secure and lightweight data aggregation in IoMT*". IEEE Access, 9, 111072-111082.

[41] Ullah, A., Said, G., Sher, M., & Ning, H. (2020). Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. *Peer-to-Peer Networking and Applications*, *13*, 163-174.

[42] Wang, H., Wang, Z., & Domingo-Ferrer, J. (2019). Anonymous and secure aggregation scheme in fog-based public cloud computing. *Future Generation Computer Systems*, *78*, 712-719.

[43] Zhang, J., Zhao, Y., Wu, J., & Chen, B. (2020). LVPDA: A lightweight and verifiable privacy-preserving data aggregation scheme for edge-enabled IoT. *IEEE Internet of Things Journal*, 7(5), 4016-4027.

[44] Usman, M., Jan, M. A., He, X., & Chen, J. (2019). P2DCA: A privacy-preserving-based data collection and analysis framework for IoMT applications. *IEEE Journal on Selected Areas in Communications*, *37*(6), 1222-1230

[45] Seyfollahi, A., & Ghaffari, A. (2020). "*Reliable data dissemination for the Internet of Things using Harris hawks optimization*". Peer-to-Peer Networking and Applications, 13, 1886-1902.

[46] Sirajuddin, M., Rupa, C., Bhatia, S., Thakur, R. N., & Mashat, A. (2022). "*Hybrid Cryptographic Scheme for Secure Communication in Mobile Ad Hoc Network-Based E-healthcare System.*" Wireless Communications and Mobile Computing, 2022.

[47] Yanambaka, V. P., Mohanty, S. P., Kougianos, E., & Puthal, D. (2019). PMSEC: Physical unclonable function-based robust and lightweight authentication in the Internet of medical things. *IEEE Transactions on Consumer Electronics*, *65*(3), 388-397.

[48] Khan, M. N. U., Tang, Z., Cao, W., Abid, Y. A., Pan, W., & Ullah, A. (2023). Fuzzy-Based Efficient Healthcare Data Collection and Analysis Mechanism Using Edge Nodes in the IoMT. *Sensors*, *23*(18), 7799.

[49] Mughal, M. A., Ullah, A., Yu, X., He, W., Jhanjhi, N. Z., & Ray, S. K. (2024). A secure and privacy-preserved data aggregation scheme in IoMT. *Heliyon*

[50] Wang, R., Yuan, X., Yang, Z., Wan, Y., Luo, M., & Wu, D. (2024). RFLPV: A robust federated learning scheme with privacy preservation and verifiable aggregation in IoMT. *Information Fusion,* 102, 102029.