EFFICIENT AND SECURE SCHEMES FOR PACKET DELIVERY IN WIRELESS SYSTEM APPLICATIONS

Thesis submitted to the Jawaharlal Nehru University

for the award of the degree of

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE

BY

ANAND KUMAR

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI–110067, INDIA

August-2021

Dedicated to

My

Great -grand

father

जवाहरलाल नेहरू विश्वविद्यालय

SCHOOL OF COMPUTER & SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

Declaration

I hereby declare that the thesis work entitled "**Efficient and Secure Schemes for Packet Delivery in Wireless System Applications**" being submitted to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi-110067, India**, in partial fulfilment of the requirements for the award of the degree of **Doctor of Philosophy**, is a record of bonafide work carried out by me under the supervision of **Dr. Karan Singh**. This thesis contains less than 100000 words in length, exclusive tables, figures and bibliographies.

The matter embodied in the thesis has not been submitted in part or full to any University or Institution for the award of any other degree or diploma.

Anand Kumar

Mr. Anand Kumar

Enrolment No.: 2001/10/MT/02

School of Computer and Systems Sciences

Jawaharlal Nehru University New Delhi-110067, India

Email:- anand_141@yahoo.com

जवाहरलाल नेहरू विश्वविद्यालय

SCHOOL OF COMPUTER & SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

Certificate

This is to certify that this thesis entitled "**Efficient and Secure Schemes for Packet Delivery in Wireless System Applications**" submitted by **Mr. Anand Kumar** to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi-110067, India** for the award of degree of **Doctor of Philosophy**, is a research work carried out by him under the supervision of **Dr. Karan Singh**.

Dr. Karan Singh
Assistant Professor
School of Computer and Systems Scienc
Jawaharlal Nehru University
New Delhi-110067

Supervisor

Dr. Karan Singh

School of Computer and Systems Sciences

Jawaharlal Nehru University

New Delhi-110067, India

01-09-2021

Dean

Prof. T.V Vijay Kumar

School of Computer and Systems Sciences

Jawaharlal Nehru University

New Delhi-110067, India

Acknowledgment

This thesis would not have been possible without the guidance and the help of several individuals who in one way or another contributed and extended their valuable assistance in the preparation and completion of this study.

First and foremost I offer my sincerest gratitude to my supervisor, Dr. Karan Singh because he gave me the opportunity to do research under his guidance and supervision. I received motivation, encouragement and support from him during all my studies. Also his unfailing help and guidance, sustained me to pursue this thesis. He has helped me even in adverse circumstances and always accommodated me in his timings as per my convenience. The thesis, as it stands emerged under his able supervision.

I would like to express my gratitude to Dean Prof. T.V.Vijay Kumar for showing faith in me. I would like to express my gratitude to Prof. C.P. Katti for giving guidance and support throughout this period.

I would like to thank my late Great grandfather whose personality, thoughts and saintly behaviour have always motivated to keep going in life.

Finally, I am forever indebted to my family for their understanding, endless patience and encouragement and faith in me when it was most required and many-many thanks to GOD.

Anand Kumar

Abstract

Wireless System is one of the emerging research area which is having the most demanding application such as healthcare system (HCS), Military application, IoT, Vehicular adhoc Networks and WSN Applications. HCS is one of the prime indicators of the norms that shape responsibilities, interactions, and inducements in the health sector. HCS improves the quality of the health industry by collecting homongenous data and making it easily accessible. In recent years with the rapid expansion of the internet and the emergence of hand-held devices, various healthcare applications became accessible legitimately. With the rise and accessibility of healthcare services, the amount of data to be stored increases exponentially

In spite of being so beneficial, there are various vulnerability factors, issues, and challenges that must be addressed by the health industry. Studies show that the system is vulnerable to certain security and privacy flaws. Upon analysing different healthcare application systems it was observed that the opponent can enter the medical details of patients faking medical practitioners by submitting false records of a patient. The requirement to protect healthcare data revolves around fundamental security principles: authenticity, confidentiality, integrity, availability, and non-denial of maliciously performed activities.

However, various solutions to resolve security and privacy issues and restore the basic security principles already exist. Providing security measures includes securing healthcare applications and their communication components. Achieving secure user authentication is the basis to attain other security measures. There are various

authentication schemes, but these traditional schemes fail at some parameters and are inefficient to differentiate between an authenticated user and a pretender. Also, it suffers the issue of being stolen or forgotten and has a high probability of being guessed by an adversary. This thesis suggests an advanced user authentication system for healthcare applications, a trust-based scheme for wireless body sensor networks, and an encryption-based scheme

Medical care is one of the most significant variables that influence how people view their quality of life. Security and privacy of patient's data in the healthcare sector is a matter of increasing importance. Implementing digital patient records, improved regulation, and the growing need for information between patients and service providers all converge towards the necessity for enhanced security to patient health information. Privacy is the fundamental governing principle of the patient and physician relationship for an operative effective healthcare service delivery. Security of HCS advances with a considerable challenge.

Medical care is one of the most significant variables that influence how people view their quality of life. Security and privacy of patient's data in the healthcare sector is a matter of increasing importance. Implementing digital patient records, improved regulation, and the growing need for information between patients and service providers all converge towards the necessity for enhanced security to patient health information. Privacy is the fundamental governing principle of the patient and physician relationship for an operative effective healthcare service delivery. However, there is a threat to privacy and security in HCS. Recent studies suggest threats such as information disclosure like accidental disclosure, insider curiosity, data breach by insider, data breach by an outsider,

and unauthorized intrusion. Therefore, HCS requires special measures to be taken to ensure data security and privacy. The thesis aims to provide such security measures that may improvise HCS service deliveries. Following are the thesis objectives.

Objective One: To focus on three issues-network internal security, resource management, and spiteful node detection and thus propose a dynamic and trustworthy lightweight trust assessment scheme for WBSNs would play a significant role in the appropriate usage of resources and minimize the computational overhead. To check the malicious activities that have been performed on nodes, some malicious nodes from the total nodes have been managed by the proposed network. The objective is acheived with two contributions. First one, proposed method is dynamic and trustworthy lightweight trust assessment scheme (RTAM) for WBSNs would play a significant role in the appropriate usage of resources and minimize the computational overhead. The second method is a novel and efficient, lightweight trust management scheme (ETAS) which incorporates both success rate and misbehaviour components during trust evaluation. The ETAS focus on whether biomedical sensor nodes are interacting or not within specified period of time to analyse their behaviour for efficient trust decision.

Objective Two: To design an RFID-enabled authentication scheme in the healthcare field that provides better and efficient medical privacy protection in IoT with low cost, prevents various kinds of security threats, and reduces performance overhead. RFID is one of the core identification technology which comes under the IoT environment as well as has a paradigm in the various fields of healthcare system. The one contribution is to design an RFID-enabled authentication scheme in healthcare field that provides better and efficient medical privacy protection in IoT with low cost, prevents various kinds of

security threats, and reduces the performance overhead. The security and privacy is done followed by the performance analysis. The security and privacy demonstrates that the An Efficient and Reliable ultra-lightweight RFID Authentication Scheme (SR2AS) has resistance to several known security attacks with second contribution.

Objective Three: To propose an encryption-based framework for mitigating the security issue related to data stored over the cloud. The framework for securing patient data privacy in health care system (FCT-SKE) is main contribution for this objective. This framework is assessed by its performance of prediction and security metrics. The data from the patient is initially fuzzified through the triangular membership function based on the threshold of features and encrypted through the Secret Key Encryption (SKE), which is the improved form of the AES algorithm. The doctor de-fuzzifies and decrypts the data and predicts the health status of the patient through the decision tree model. The web GUI regulates the data flow from the doctor to the patient with cloud interaction

List of Publications

Journal

[1] Anand Kumar, Karan Singh, T . Khan , A.Ahmadian , M.H.MD. Saad, and M. Manjul, "ETAS: An Efficient Trust Assessment Scheme for BANs" published, IEEE Access (SCIE, 2020 IF = 4.0), June 2021 10.1109/ACCESS.2021.3086534

[2] Anand Kumar with Karan Singh and T . Khan, "L-RTAM: Logarithm based Reliable Trust Assessment Model for WBSNs , published in Journal of Discrete Mathematical Sciences and Cryptography , Taylor & Francis , UK (SCOPUS, ESCI) https://www.tandfonline.com/doi/abs/10.1080/09720529.2021.1880145

[3] Anand Kumar with Karan Singh and et.al . ". SR^2AS: An Efficient and Reliable Ultra lightweight RFID Authentication Scheme for Healthcare Systems, Accepted in SOFA 2020 , Arad , Romania for Journal of Intelligent & Fuzzy Systems, (SCIE , IF 1.851)

[4] Anand Kumar with Karan Singh, FCT-SKE : A Novel Framework For Securing Patient Data Privacy In Health Care System, accepted with major revision in International Journal of Electrical and Computer Engineering , 2021(SCOPUS, Q2).

Conference

[1] Anand Kumar and Karan Singh, Efficient Trust Assessment Mechanism for E-Healthcare System, Presented in International Conference on Networks and Cryptology (NetCrypt 2020), 406 December, 2020, JNU, New Delhi, India

[2] Anand Kumar and Karan Singh, "Wireless Health Care System: An Overview", Presented in International Conference on Networks and Cryptology (NetCrypt 2020), 4-6 December, 2020, JNU, New Delhi, India

[3] Anand Kumar, Karan Singh , Anshita Dhoot , A.N. Nazarov, "Enhanced Lightweight and Secure Session Key Establishment Protocol For Smart Hospital Inhabitants", Presented in International Conference on Networks and Cryptology (NetCrypt 2020), 4-6 December, 2020, JNU, New Delhi, India

Table of Contents

List of Figures

List of Tables

List of Acronyms

AES	Advanced Encrypted Standard
ANN	Artificial Neural Network
bABE	Broadcast Attribute Based Encryption
BANs	Body Area Networks
BS	Base Station
BSN	Body Sensor Networks
CC	Cloud Computing
CDSS	Clinical Decision Support System
CH	Cluster Head
CLS	Certificate Less Signature
CM	Current Misbehavior
CPRBAAC	Cloud Based Privacy Aware Role Based Access Control
DoS	Denial-of-Services
DTM	Distributed Trust Model
ECC	Elliptic Curve Cryptography
EEG	Electroencephalogram
E-HCS	e-healthcare system
EMG	Electromyography
EPC	Electronic Product Code
ETAS	Efficient Lightweight Trust Management Scheme
FATD	Fault Aware Trust Determination
FCT-SKE	Fuzzy Cipher Text-Spiral Key Encryption
GDP	Group Device Pairing
GPS	Geographical Positioning System
GUI	Graphical User Interface
GWAS	Genome-wide association study
HCS	Health-care system
ICT	Internet Communication Technologies
IDMs	Implantable Medical Devices
IoT	Internet of Things
IPS	Intelligent Physiological Sensors
PDR	Packet Delivery Ratio
PDR	Packet Delivery Ratio
PHI	Patient's health information
PKES	Public key encryption with keyword search

PPDP	Privacy Preserving Disease Prediction
PSN	Physiological Sensors Node
PSNs	Physiological Sensors Nodes
PSO	Particle Swarm Optimization
PSTRM	
QoS	Quality of Service
RFID	Radio frequency identification
SF	Security Features
SKE	Secret Key Encryption
SNs	Sensor Nodes
SQL	Structured Query Language
TMIS	Telecare Medical Information Systems
TMS	Trust Management Scheme
TMs	Trust Models
TPM	Trusted Platform Module
TTRP	Trust and thermal aware routing protocol
UCI	Unique Client Identifier
UHF	Ultra-high frequency
UL	Unique Labels
VPN	Virtual Private Network
WBSN	Wireless Body Sensor Network
Wi-Fi	Wireless Fidelity
WS	Wireless System
WSA	Wireless System Application

Chapter-1

INTRODUCTION

Wireless System is one of the emerging research area with the most demanded applications such as health-care system (HCS), Military application, IoT, Vehicular AdHoc Networks and WSN Applications. HCS is one of the prime indicators of the norms that shape responsibilities, interactions, and inducements in the health sector.

This chapter is organized as follows; Section 1.1 explains the Wireless System Application (WSA), followed by Section 1.2, which discusses this thesis's motivation. Section 1.3 entails the uses of HCS, followed by Section 1.4in which challenges have been explained. Section 1.5 problem identification behind it has been elaborated, followed by the Section 1.6 in which research objectives have been discussed. In Section 1.7, research methodology has been discussed briefly, followed by Section 1.8 which explains the entire thesis organization.

1.1 Wireless System Application

The main objective of the work is to provide security to wireless system application. We have worked for the health-care system (HCS). HCS improves the quality of the health industry by collecting humongous data and making it easily accessible. The system produces extensive data related to the patient's health information (PHI) regularly, collated, inspected, and then distributed. Thus, improving efficiency and reducing the cost of health-care services. The emergence of HCS has transformed the relationship between patients with their health-care provider. It becomes difficult for any patient to keep in touch with

their physicians in person. HCS has facilitated health information exchange electronically. The use of new technologies contributes to reconstructing health-care and improving quality through innovations. Patients can access much information related to health, disease, and health-care services online through the Internet. The explosion of these technologies enables patients to access health information and facilitates doctors and other health-care service providers to access PHI and connect and collaborate.

Despite being so beneficial, various vulnerability factors, issues, and challenges the health industry faces must be addressed. Studies show that the system is vulnerable to security and privacy flaws upon analyzing different health-care application systems. The opponent can enter into the medical details of patients faking medical practitioners by submitting a patient's false records. The sensitivity of PHI demands high-security measures to prevent it from any unauthorized access. The disclosure of such sensitive information may cause severe damage to the patient and the family involved. The requirement to protect health-care data revolves around fundamental security principles: authenticity, confidentiality, integrity, availability, and non-denial of performed activities.

However, various solutions to resolve security and privacy issues and restore the basic security principles already exist. Providing security measures includes securing health-care applications and communication components. Achieving secure user authentication is the basis to attain other security measures. There are various authentication schemes, but these traditional schemes fails at some parameters and are inefficient in differentiating between an authenticated user and a pretender. Also, it suffers from the issue of being stolen or forgotten and has a high probability of being guessed by an adversary. This thesis suggests an advanced user authentication system for health-care applications, a trust-based scheme

for wireless body sensor networks, and an encryption-based scheme to secure PHI. All three schemes overcome the existing limitations and excel in performance and productivity.

1.1.1 The architecture of e-health care

The residential environment E-HCS consists of four layers in its architecture [1-2]. Layer 1 consists of multiple wearable sensors or sensors placed on the human body or rooted under the skin. These sensors monitor the human body's activities and collect data directly transmitted to the central system or supplementary layers for further processing. The second layer comprises devices that are helpful for interaction.

The type of monitoring device used depends upon the wireless communication protocol used. For example, a sensor-based on Bluetooth will require monitoring devices with Bluetooth inbuilt, like smartphones. This layer transmits the collected data to the next layer. The third layer performs all primary computing operations and has access to the Internet. This layer takes all critical decisions regarding the patient's health.

The significant role of this layer is to collect, filter and analyze the information. It connects to the next and final layer. The third layer transmits the analyzed data to the fourth layer, which consists of health-care service providers. Medical professionals have access to this data, and based on this data, they provide health-care services and emergency services to patients.

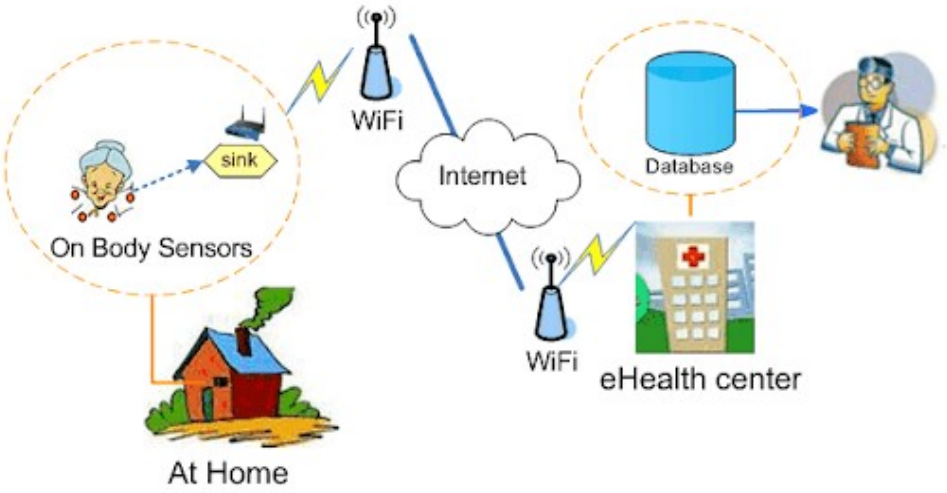


Figure 1.1: The architecture of E-healthcare [3]

1.1.2 Authentication

Authentication is a process of approving the identity of any entity. Technically authentication is defined as a process that authorizes or confirms user individuality to ensure that the user is who he claims to be. Every system which aims to preserve user's detailed datasets requires user login and a class of a verification process that goes the same for the HCS. The primary objective of authentication is to keep unauthorized users from availing the system facilities and ensure that only authorized users can access patients' health information (PHI). Regarding health-care, patient medication safety is a significant concern for global public health. According to the official statistics, due to the patients' improper identification, there are more mistreatments in the health-care systems. These medical errors are taken care of by RFID technology by making an essential contribution to the medical health-care system for asset tracking and patient information tracking [4].

RFID-enabled technology is the most promising and contactless technology used to identify objects using radiofrequency waves. The RFID system comprises some entities such as the tag, reader, and a backend server.

Moreover, most of the RFID tags are being used every day in our daily lives. However, there are two kinds of tags; active tag and passive tag. The passive tags are relatively cheaper than active tags because they do not have any battery to get the power and are charged with radiofrequency waves from the RFID reader.

The RFID reader contains three components: RF signal generator, microcontroller, and receiver or signal detector. Besides, the RF signal generator helps generate the radiofrequency waves transmitted through an antenna and receives the feedback signal which comes from the tags. In particular, the receiver of a signal detector further proceeds the information sent by the RFID tags. Accordingly, the backend server's prominent role is to store an object's specific information in its database, sent by the reader, and perform the high-load computation. The thesis work presents a secure RFID-based authentication protocol for the IoT health-care environment that ensures some security and privacy features, less communication cost, and less computational operations than many existing schemes.

1.1.3 Encryption

Encryption is the method that converts a piece of information into a secret code that hides the information's true meaning. Encryption has been a traditional and long-lasting way for sensitive information to be protected. In modern times, encryption protects data stored on computers and storage devices and data in transit over networks. In health-care regards,

encryption helps in protecting patient health information during its transmission from one user to another.

The health care data being the big data, is managed through several established clouds. The security of data in clouds is continuously under threat, especially in sharing the environment. Several security frameworks are present to secure the data. However, it is challenging to adverting the leakage of data altogether. PHI has become a target of hackers in recent times, and the protection of this data from an unauthorized person is a must. In large organizations that permit doctors to use smartphones and tablets, encryption is an essential means of keeping data secure. It protects patients' private and personal information from theft. It protects data when users have to use different types of devices. It combines with advanced authentication to make the data more secure. Besides, encryption prevents costly data breaches. The patients had to store their data in the centralized cloud to secure it from any attacks [5]. Even cryptography key mechanisms and role-based access control are exposed to cyber-attacks to increase crucial leakage probability through compromise in access policy [6-7]. Some existing solutions suffer from overheads, latency with user constrained environment.

The thesis work aims to resolve the health-care industry's security concern over large amounts of data stored in a cloud environment. The thesis work presents a novel encryption technique that ensures PHI security in the health-care system.

1.1.4 Trust assessment

In an HCS, the deployed sensors aim to derive and monitor a patient's health information. In this context, Wireless Body Sensor Network (WBSN) consists of many small size physiological sensors nodes (PSNs) to monitor blood pressure, sugar level, and chronic

diseases as well as report real-time data using wearable sensors [8]. However, WBSN suffers from various internal and external attacks [3]. Since WBSN deals with patients' sensitive information, transmitted data is crucial to preserve the privacy, accessibility, and integrity of sensed data. Cryptographic techniques can defend againstexternal security. Still, encryption and authentication techniques cannot guard against internal attacks (Whitewashing Attack, Sybil Attack, Bad-mouthing Attack, Ballot stuffing Attack, Ballot-box Stuffing, Positive and negative discrimination, Traitor Attack, Conflicting behaviour Attack) performed by internal malicious nodes. In internal attacks, a physiological sensors node (PSN) misbehaves within the network and other nodes to destroy the reputation and performance of the WBSN. Trust-based security techniques effectively guard sensitive data and networks against internal attacks such as on-off attacks, data attacks, and routing attacks [9-10]. Trust assessment models are primarily used to increase the system's reliability, enhance security against malicious activities, and improve cooperation among physiological sensor nodes (PSNs). Trust assessment models improve security and system efficiency by detecting and eliminating selfish PSNs from the WBSNs in a thoughtful way [11]. Trust is a value that denotes the level of reliability (trustworthiness) of physiological sensor nodes [12]. Based on the computed trust value, trust management systems make efficient decisions regarding trustworthy and faulty PSNs. Only trustworthy PSNs can participate in the WBSN to send/receive sensitive data [13-14].

Moreover, only trustworthy PSNs can become relay nodes and participate in routing for efficient network throughput. There are various trust assessment schemes such as weight, rate, fuzzy, and graph-based trust assessment schemes in WBSNs. Weight and rate-based schemes are suitable for such networks since they impose fewer computational and storage

requirements. These schemes incorporate misbehaviour components during a trust assessment to improve the attack detection capability of the proposed model. These trust assessment schemes compute various trusts such as direct trust, indirect trust, data trust, and aggregate trust to eliminate misbehaving nodes for better network performance in an open environment. To improve the network scalability, throughput with minimum computational overhead, PSNs are grouped into clusters. Clustered topology groups the PSNs into a load-balanced group with a cluster head (CH) within each group. The CH is assumed to be the most reliable and resourceful PSN responsible for computing and distributing the trust values of PSNs within a cluster. The thesis work presents a dynamic and trustworthy lightweight trust assessment scheme for WBSNs that plays a significant role in the appropriate usage of the node's resources. It ensures security from untrustworthy and malicious nodes. Also, it minimizes the computational overhead in comparison to the existing schemes.

1.2 Motivation

In recent years with the rapid expansion of the Internet and the emergence of hand-held devices, various health-care applications became accessible legitimately. With the rise and accessibility of health-care services, the amount of data to be stored increases exponentially.

This data includes the patient's details like age, sex, gender, and other details for identification, patient's health-related information like symptoms, disease, etc. It may also contain common knowledge related to health, disease, and medicine easily accessible by any user for reference.

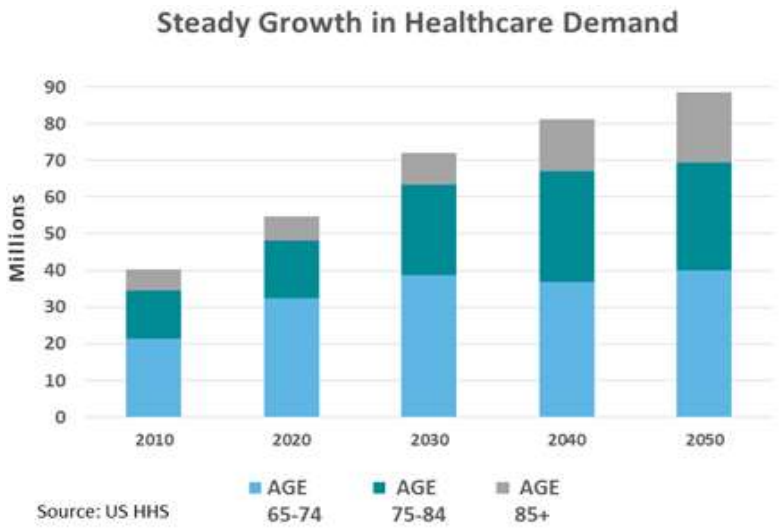


Figure 1.2: Demand in health-care with respect to age [1]

Thus, the increasing development in this field needs to incorporate special security measures to deal with massive data related to patients' health. As more and more medical data are converted into digital form, its secrecy and security are of more significant concern. The graph in figure 1.2 illustrates the health-care service demand concerning the age of a person. It clearly states that health-care services' demand is highest for people between the ages of 65-74, slightly lower for 75-84 years. The demand also increases with time and is predicted to be highest by 2050. Hence, there is a need to provide quality services to patients. In quality service, the security of the patient's sensitive information is inclusive.

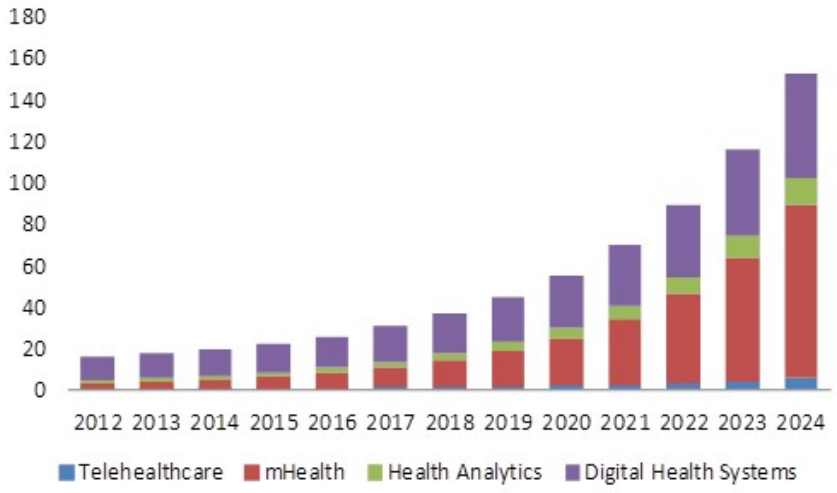


Figure 1.3: Demand in the various health-care system [2]

The graph in figure 1.3 illustrates that the demand for m-Health will increase in the coming years and is expected to cross 80 million in 2024. M-Health is defined as mobile telecommunications and multimedia devices working together to achieve health-care services and improve health-care service deliveries. Thus, the growing demand for health-care services leads to an increasing collection of patient data. Therefore, security and privacy have become a crucial need for the healthcare industry.

1.3 Uses of HCS

HCS has its potential application in offering varied services to patients and staff. A few of its applications are listed below.

Tracking: It is a function that identifies an object or a person in motion. Tracking can be real-time or in motion. It is applicable in continuous maintenance, availability of assets, and monitoring of its use, to track materials like specimens and blood to prevent any trouble during surgery. Tracking can be broadly categorized as health tracking and asset tracking. The former defines monitoring and analyzing the data points which are related to the health

of a patient. There are multiple health tracking devices available to enable GPS tracking, which records travel and provides devices to count the number of steps taken or track sleep patterns. Besides that asset tracking plays a crucial role in HCS. Many times, human errors lead to severe problems. However, we are never in a condition to take risks or bear errors in HCS for avoiding these errors, and hence asset tracking is incorporated. It can track health-care service providers or staff; it can help a medical team find the lost equipment or anything they need. Asset tracking helps to inquire how a piece of equipment or device is used; it enables replacing or relocating devices that are not in use. It ensures time-saving and easy management.

Monitoring: A HCS extensively relies on monitoring systems incorporated with new-age technologies. It is a function that keeps a check upon a patient's health, collects and analyzes data, and makes decisions according to the standard data or measurement. The detected data can alarm patients and health-care providers on the patient's critical condition. Also, it can regularly keep a record that whether the patient is doing fine or not. Monitoring has improved health-care service deliveries due to reduced complaints rates, improved patient's health, and rapid access to health-care services and needs.

Sensing: Multiple sensors can be deployed inside the human body or in the form of a wearable device. This function aims to sense specific activities of the body and collect the data. The patient and health-care service providers can access this data to check patients' day-to-day behaviour and recovery status, check on heart-rates, blood pressure rates, oxygen-level in the body, and much more.

Data Collection: Homongenous datas are generated while monitoring and tracking a patient's health. The collection of information aims at reducing processing time and

managing medical records—the data stored in large repositories or cloud, which enables remote access of data. Doctors or staff can access this data and provide an adequate level of service to the patient.

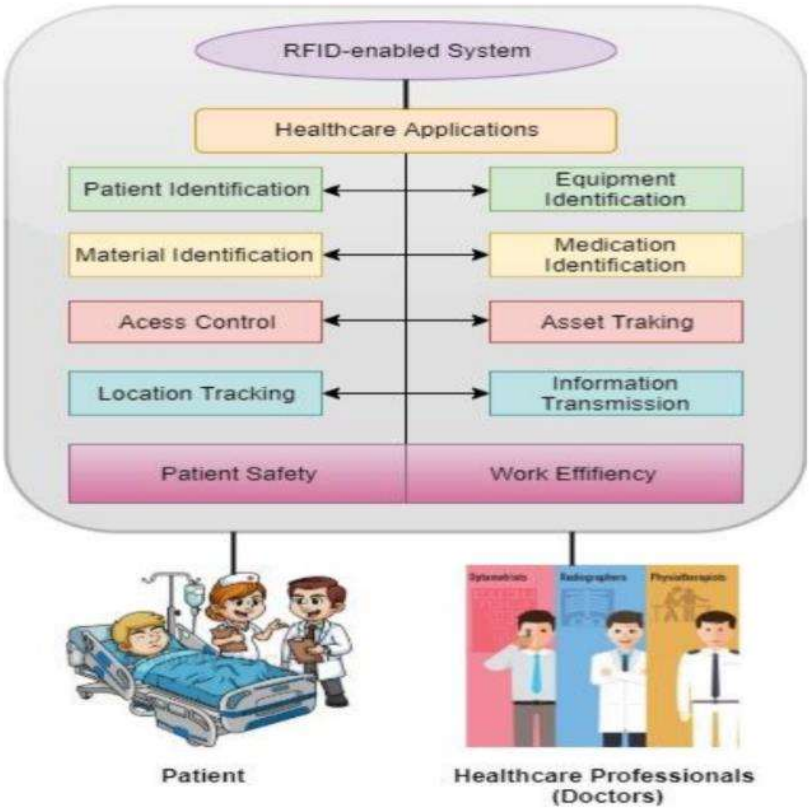


Figure 1.4: RFID-enabled health-care application

Also, the data may include general information related to health, disease, or medicine. Any user can refer to this information for their knowledge or as per need. However, it requires that correct and accurate data must be available. Also, it must maintain its consistency and authenticity. No unauthorized access should give personal information to the patient.

Identification and Authentication: Identifying a patient becomes necessary to avoid mishappenings in treatment like wrong dose or wrong medical procedures. In the case of infants, identification helps to prevent mismatching. Identification and authentication of

medical staff enable them to grant PHI access to improve their service and ensure patient data security.

Following are few more applications of the health-care system, which are as follows,

- Medical and health-care management
- Health education
- Strategic health planning
- Medical education and training
- Patient care and support
- Preventive health services
- Provision of health services
- Knowledge-based services
- Electronic medical record
- Telemedicine communication

The application of health-care highly depends upon the new-age technologies. RFID technology makes an essential contribution to the medical health-care system for asset tracking and patient information tracking [4]. Some of the RFID-enabled health-care applications such as patient identification, asset tracking, access control, location tracking, and many others have been shown in Figure 1.4 Over the last several years, the vast development of "Internet-of-Things" has grown up more and more in various ways, and several benefits have also been given to society. Figure 1.5 highlights that IoT enabled health-care applications. These technologies have offered even the least educated person to handle the devices quickly and track their health status using hand-held devices. These technologies helps in enhancing the health industry's services and help users quickly access

data and track their health status independently. However, increasing technologies and ease have increased risks to data breaches and security threats. HCS, besides getting benefits, suffers various challenges.

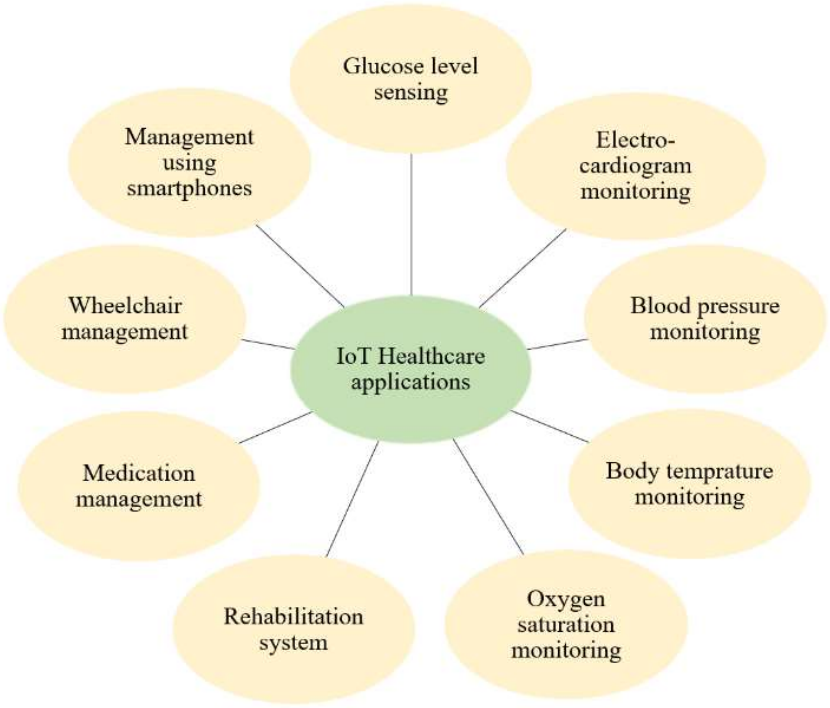


Figure 1.5: IoT-enabled health-care application

1.4 Challenges

The Healthcare system is a boon considering human health. There has been an emergence in technologies which is improving health-care services day-by-day. However, HCS still suffers from various issues and faces some challenges that have to be considered. Series of challenges are faced by not only the patient but also by health-care service providers and doctors. The emergence of modern digital technologies encourages the patient's capability of taking care on their own. Quality of care is becoming extremely relevant as patients

start exercising their right to choose with whom and how to engage as health-care consumers. As a result, health care organizations will need to focus on delivering facilities and services besides maintaining patient's trust. Patient safety is the main focus of health organizations and leaders in the health-care sector. Data related to any medical problem and its therapies can now be easily accessible on the Internet. These have altered the conversation of the supply-demand relation to the patient to some extent. The rise of social media often affects health-care experiences in various forms. The challenges faced by HCS in developing countries like India are much more than in developed countries. The reason is unequal resource distribution and poor telecommunication. Following are a few challenges faced by HCS.

Security and Privacy: With increasing demand in HCS, there is an increase in patient data collection; therefore, privacy, trust, and safety have become an essential need in HCS. Privacy and safety include the protection of sensitive data from unauthorized access and hence maintain security principles. The data must maintain confidentiality and authenticity. It must be available to an authorized user at the time of requirement. Thus, HCS must incorporate special security measures to keep all security principles and maintain user's trust in HCS.

Power Consumption: In an HCS, the number of wireless devices and sensors are rising. These devices have limited resources and power. Thus, it creates a need to manage and minimize the power consumption of each device. Frequently changing the battery is not feasible, especially if the sensor is implanted inside the human body. These devices utilize energy, which is involved in detecting and monitoring, and transmitting data to centralized

systems. Thus, power supply or consumption is the greatest challenge for HCS, which has to be taken care of by the researchers to formulate large battery life devices.

QoS support: It can claim that the health-care sector is accountable for many individuals and communities. It is mainly responsible for supplying consumers with the service that is their right and believe in providing the required quality of service. To fulfil the minimum requirement of HCS, Quality of Service (QoS) establishment is essential. Since HCS is all about data delivery, including health data, video, audio, and online streaming, an improved QoS mechanism reduces packet loss and packet delay. The support of audio, video, robotic channel, biometric data, medical image, and data access is needed to provide QoS.

Among the various fields that handle sensitive data, the health care system is one of the predominant domains. With recent advancements, the health care system generates the data stored and transfers it electronically to enhance its quality of service offered to the patients [15]. Over the past years, the data related to traditional medical privacy and many other similar cases are at serious risk of disclosure by the third party, an adversary, or an attacker. Some insurance companies leak personal medical privacy data, disrupt medical industries' healthy environment, and compromise individuals' privacy.

1.5 Problem Identification

Medical care is one of the most significant variables that influence how people view their quality of life. Security and privacy of patient's data in the health-care sector is a matter of increasing importance. Implementing digital patient records, improved regulation, and the growing need for information between patients and service providers all converge towards the necessity for enhanced security to patient health information. Privacy is the fundamental governing principle of the patient and physician relationship for an operative

effective health-care service delivery. Security of HCS advances with a considerable challenge. Recent studies suggest threats such as information disclosure like accidental disclosure, insider curiosity, data breach by insider, data breach by an outsider, and unauthorized intrusion. Vulnerabilities denoted as security and privacy challenges cannot be an obstacle to the health-care system's unveiling benefits. In simpler words, the emerging trends and their security issues must be addressed by adopting efficient preventive measures. Some of the questions related to security measures of the health-care system like authentication, encryption, and trust management are listed as follows,

- How to prevent unauthorized access to a patient's health information?
- How to manage the storage of a homogenous amount of health data?
- How to design a lightweight authentication scheme that can affect the employee in the health-care system?
- How to build a model to ensures various imperative security requirements such as the resistance to multiple attacks?
- How to develop a framework to secure data stored in the cloud?
- How to perform encryption with unbreakable security keys?
- To design a robust, lightweight trust assessment model for secure data monitoring by wireless body sensor networks?
- How to check malicious activities performed by body sensors?
- How to improve data trust, device trust, and user trust in IoT applications?
- How to reduce the resource consumed by the sensors during the transmission?

1.6 Research Objectives

Medical care is one of the most significant variables that influence how people view their quality of life. Security and privacy of patient's data in the health-care sector is a matter of increasing importance. Implementing digital patient records, improved regulation, and the growing need for information between patients and service providers all converge towards the necessity for enhanced security to patient health information. Privacy is the fundamental governing principle of the patient and physician relationship for an operative effective health-care service delivery.

However, there is a threat to privacy and security in HCS. Recent studies suggest threats such as information disclosure like accidental disclosure, insider curiosity, data breach by insider, data breach by an outsider, and unauthorized intrusion.

Therefore, HCS requires special measures to take to ensure data security and privacy. The thesis aims to provide such security measures that may improvise HCS service deliveries. Following are the thesis objectives. It aims to provide such security measures that may improvise HCS service deliveries. Following are the thesis objectives.

Objective I: To focus on three issues-network internal security, resource management, and spiteful node detection and propose a dynamic and trustworthy lightweight trust assessment scheme for WBSNs that would play a significant role in the appropriate usage of resources and minimize the computational overhead to check the proposed network that manages the malicious activities that have been performed in nodes, and separare some malicious nodes from the total nodes.

Objective II: To design an RFID-enabled authentication scheme in the health-care field that provides better and efficient medical privacy protection in IoT at low cost, prevents various security threats and reduces performance overhead .

Objective III: To propose an encryption-based framework to mitigate the security issue that is related to data.

1.7 Research Methodology

The flow chart given in figure 1.6 depicts the steps taken into consideration while working on this research work.

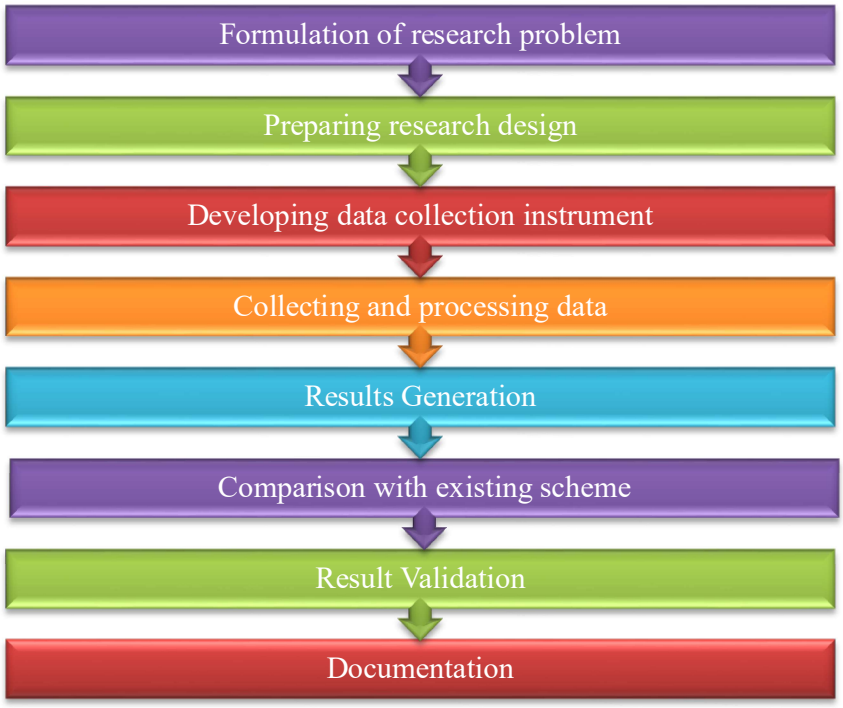


Figure 1.6: Research Methodology

The first step includes a literature review, identifying problems, and determining specific goals to be achieved at the end of this research work. The second step gives the study design. Step three determines the methods required for data collection and designing the

research tools. The fourth step collects data based on observations and surveys. The collected data is then analyzed and processed accordingly. The processing includes implementation and coding.

The obtained results are then compared with the existing models to find the differences from them. Performance figures like throughput, loss ratio, and reliability are requirements for output assessments. Based on the result, a particular conclusion is derived. This whole research process is then documented in the form of a thesis. The documentation defines the approach taken to develop a model and fulfil the desired research objectives.

1.8 Thesis Organization

Following is the systematized sequence of the remaining thesis chapters:

Chapter 2: This chapter shows the background and related work to the entire thesis contribution. It discusses the security, trust and privacy protection of the system.

Chapter 3: This chapter discusses the proposed work for trust management in healthcare system.

Chapter 4: This chapter discusses the authentication process for the Healthcare application.

Chapter 5: This chapter includes the privacy over the healthcare system and cloud security to protect our data.

Chapter 6: It concludes the work contribution of the thesis, also discusses the future work for open research area.

Chapter-2

BACKGROUND AND RELATED WORK

Wireless System has the power to transform human life into more comfortable one. In terms of networks, wireless is the term used to describe any computer network where there is no physical wired connection between sender and receiver, but instead of wired communication, they used radio waves to communicate. Wireless technologies will spawn new applications and industries to address healthcare issues in the coming years. These technologies have been designed so that any health provider and patients can collaborate and coordinate anywhere or anytime with each other. Wireless monitoring and communication allows patient mobility and efficient response in emergencies. The objective of this chapter is to provide background and related work. The remaining chapter is divided into following sections where Section 2.1 discusses the wireless system Application. Section 2.2 is discussing trust mechanism survey Section 2.3 provide network model and some concept regarding time window. Moreover, it provides a trust assessment scheme for WBSNs. Section 2.4 discusses the results of the proposed approach. Finally, Section 2.5 provide a summary.

Wireless systems designed to provide “anytime, anywhere” service, enabling data entry and data access by medical personnel at the point of care, direct data acquisition from medical devices, patient and device identification, and remote patient management. In the 21st century, as the world is moving towards digitalisation, the healthcare industry also started using more wireless devices than in earlier days. In the current scenario, many people prefer online counselling, and they avoid going to hospital in person . Due to wireless system healthcare personals are capable of detecting, monitoring, and providing feedback in real-time.

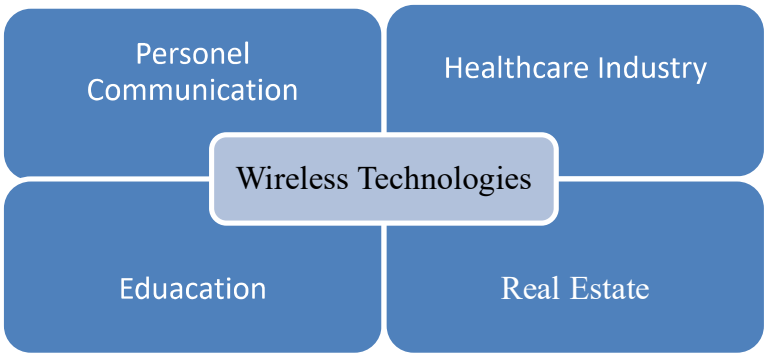


Figure 2.1: Application of Wireless System

In the last few decades, the Healthcare industry has seen a large transformation. New technologies have improved the existing methods to diagnose, monitor health conditions and alert medical professionals and patients with greater accuracy.

Our healthcare system has been going through technological evolution. As the healthcare industry started connecting more to the internet, the healthcare system's vulnerability also increased. The basic security requirements that every system must include is authentication, confidentiality, integrity, availability, non-repudiation. Here we present a background of existing wireless technologies for data transmission in the healthcare industry and the different security risks possible on these wireless technologies. Our aim of this paper is to survey literature and review state of art to understand various security challenges and available solutions and tries to answer the following research questions:

(i) What are the different wireless schemes used in healthcare systems?

(ii) What are the security challenges faced while using these healthcare technologies?

(iii) What do current healthcare providers use in the solutions to avoid these security risks?

2.1 Wireless Technology Used in Healthcare

A good security system must not compromise the fundamental security elements such as authentication, confidentiality, integrity, availability and nonrepudiation. The security requirements is to secure wireless environment in the healthcare industry.

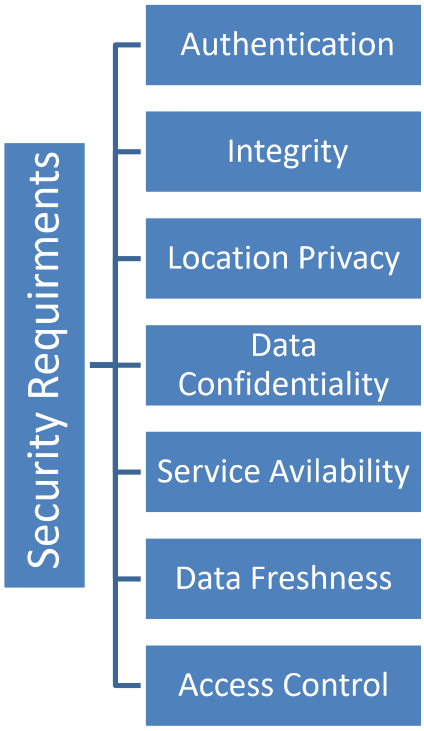


Figure 2.2: Security Requirements in the Healthcare System

Wireless Body Sensor Network (WBSN) consists of many small size physiological sensors nodes (PSNs) to monitor blood pressure, sugar level, and chronic diseases as well as report real-time sensor data using wearable sensors [16]. The monitored data is processed and transmitted to the base station (BS) in an open environment. WBSN plays a vital role in health-care application since it helps to detect health status at early stages and offers the flexibility of diagnosis remotely. Due to its deployment nature, WBSN suffered from various internal and external attacks [17]. Since WBSN deals with patients' sensitive information, transmitted data is crucial to preserve the privacy, accessibility, and integrity of sensed data.

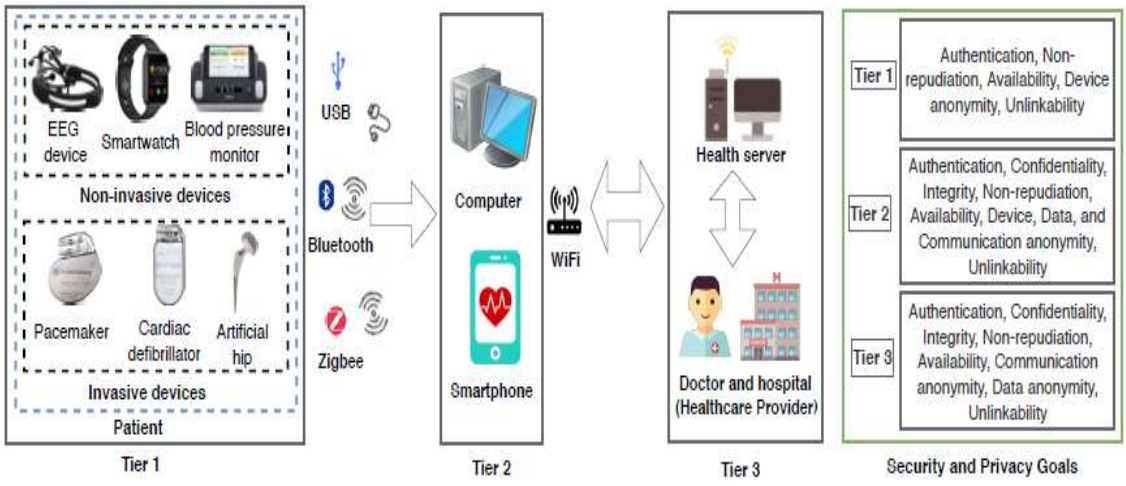


Figure 2.3: Security Goals [18]

Smart Sensors

Smart sensors make our life very comfortable, in healthcare, it offers novel solutions to several relevant challenges such as early detection and prevention of diseases, or minimally invasive management (e.g., cardiovascular diseases and cancer). Furthermore, the expansion of small and lightweight smart sensors plays a major role in unobtrusive, continuous monitoring of patients' status.

Wearable Devices

Due to the advancement in Wearable devices, it is possible to track our daily activities, sleeping patterns, heart rate, and movement tracking. These wearable devices have connected to our smartphone. In this way, the user can send their day-to-day activities reports to their doctors. Specially designed apps can do a lot more tasks using collected information using wearables. According to a survey conducted by Strategy Analytics (2019), global smartwatch shipments reached 12.3 million units in June 2019, representing a 44 per cent increase from 8.6 million units in June 2018. It shows the popularity of Wearable devices for healthcare services, particularly to maintain fitness, well-being and disease prevention demand for wearable devices has increased.

Smart Card and Smart Tags

Smart cards give patients, and providers access to patient data and weld on the patient's; this smart card system removes procedures such as filling out forms repeatedly. It also eliminates the number of duplicate tests. Doctors can access information from the patient's smart card. If a patient's blood type, allergies, and illnesses have been stored on a card, a medicine that causes allergy will not be applied to a patient without testing once again. Smart cards include/made to include a digital certificate so that a doctor asked for patient data, for instance, can be certain that the individual seeking the information is whom he/she claims to be. This system helps to figure out the patient's health history and what medicine he/she used in the past by putting all prescription details in the smart card.

Location Tracking

Smart wireless technology can track a person's location and help them in a critical situation. A patient with Alzheimer's disease or disabilities can be easily located using GPS, and their family members can easily assist them. Locating the people who had dementia may reduce the time and cost required to search and rescue operations. It also provides independence to people to roam freely without any hesitation.

Internet of Things in healthcare

IoT device plays an important role in health-care applications by monitoring the day-to-day physical activities of an individual's fitness goals. It provides remote access that helps patients consult their doctors and update them about their health regularly. IoT also urges the industry to become automated, providing more research across different cross-platforms. IBM utilized RFID technology at one of Ohio Health's hospitals to track handwashing after checking each patient. That operation could avoid infections that cause about 90 000 deaths and lose about $30 billion annually. IoT also makes this healthcare industry automated. [19] In case of accidents, IoT devices helps in informing the nearest hospitals or ambulance and give details on the injured person's status, like a heartbeat.

Figure 2.4: Healthcare Application [20]

Security threats

As healthcare is an open platform; hence, it is very much vulnerable to many attacks, which we will discuss in this section. Figure 2.5 presents the increasing rate of healthcare data in recent years. In the current scenario, man wearable devices and smart sensors used by patients and doctors are the main target of attackers?

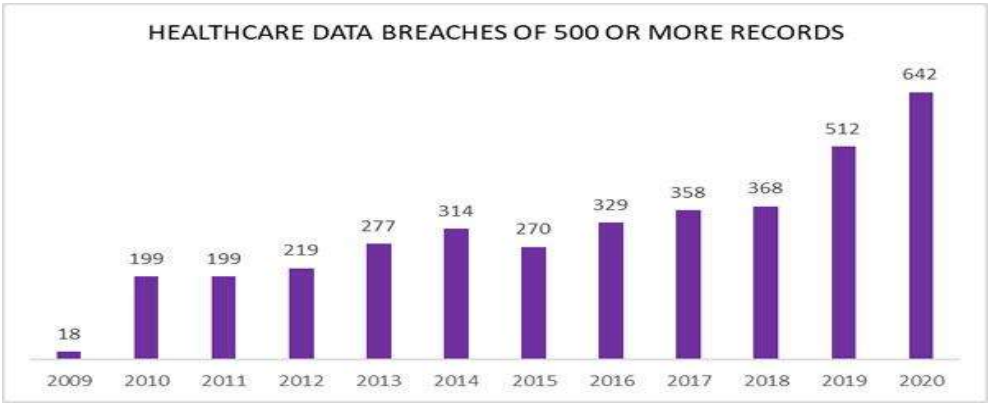


Figure 2.5: Increasing rate of Healthcare Data Breaches [20]

In [21], the authors explained the FITBIT device, which is worn on the wrist and affected by attackers. Fitbit lacks authentication on the tracker side, and potential attackers can easily get the data from users' knowledge. Fitbit Flex is vulnerable due to leaky BTLE (Bluetooth Low Energy) technology. This happens because it did not change the privacy address, or MAC address remains the same and can be easily accessed. In December 2014, Bitdefender researchers found it was surprisingly easy to intercept the Bluetooth communications between a Nexus 4 smartphone and an LG smartwatch.

Most of these wearable devices have no proper authentication system. If it is stolen or lost, it creates a very serious problem with personal data exposure. However, it is difficult to apply with higher security measurements due to its small size and limited bandwidth and, finally, easier to attack.

Many fitness bands have built-in GPS facilities, which helps to track any person's location. Some devices do not have GPS built-in but can use other techniques to estimate location, like using known WIFI base stations or mobile phone towers. After knowing the patient's live location may be that attackers can harm the person physically.

In wireless healthcare, applications have a variety of attacks possible. Active attacks in which attackers only intercept the message cannot change it, and another is the passive attack to change the actual message. In a passive attack, the attacker can capture patient wireless channels and extract the patient medical data. Later, he/she may tamper with the patient data, which can mislead the involved users (e.g., doctor, nurse, family member). For example, suppose a cardiograph sensor transmits normal data to the medical staff. If an attacker can modify the patient data during the communication and send the modified data to medical staff, it may cause an overdose of medicine being administered to the patient. In wireless networks [22], many routing attacks like Sybil attack, warmhole attack, and sinkhole attacks cause the serious problem by preventing or inserting data packets in transmission. Which further creates misinformation among doctors about the patient and which leads to mistreatment of the patient.

Cryptographic techniques can defend external security. Still, encryption and authentication techniques cannot guard against internal attacks (Whitewashing Attack, Sybil Attack, Bad-mouthing Attack, Ballot stuffing Attack, Ballot-box Stuffing, Positive and negative discrimination, Traitor Attack, Conflicting behaviour Attack) performed by internal

malicious nodes. In internal attacks, a physiological sensors node (PSN) misbehaves within the network and with other nodes to destroy the reputation and performance of the WBSN. Trust-based security techniques effectively guard sensitive data and network against internal attacks such as on-off attacks, data attacks, and routing attacks [23-24].

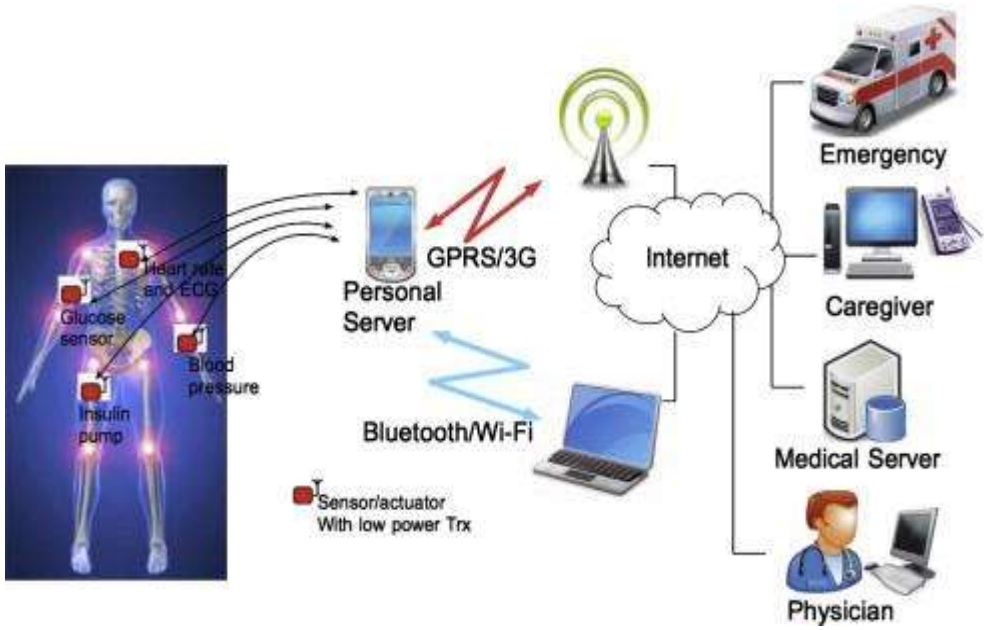


Figure 2.6: Four-layer Architecture of an e-healthcare System [22]

Trust assessment models are primarily used to increase the system's reliability, enhance security against malicious activities, and improve cooperation among physiological sensors nodes (PSNs). Trust assessment models improve security and system efficiency by detecting and eliminating selfish PSNs from the WBSNs in a thoughtful way [25]. Trust is a value that denotes the level of reliability (trustworthiness) of physiological sensors nodes [26]. Based on the computed trust value, trust management systems make efficient decisions regarding trustworthy and faulty PSNs. Only trustworthy PSNs can participate in the WBSN to send/receive sensitive data [27-28].

Moreover, only trustworthy PSNs can become relay nodes and participate in routing for efficient network throughput. There are various trust assessment schemes such as weight, rate, fuzzy, and graph-based trust assessment schemes in WBSNs. Weight and rate-based schemes are suitable for such networks since they impose fewer computational and storage requirements. These schemes incorporate misbehaviour components during a trust assessment to improve the attack detection capability of the proposed model. These trust assessment schemes compute various trusts such as direct trust, indirect trust, data trust, and aggregate trust to eliminate misbehaving nodes for better network performance in an open environment. To improve the network scalability, throughput with minimum computational overhead, PSNs are grouped into clusters. Clustered topology group the PSNs into a load-balanced group with a cluster head (CH) within each group. The CH is assumed to be the most reliable and resourceful PSN responsible for computing and distributing the trust values of PSNs within a cluster.

LEACH, HEED, and EEHC [25-27] can elect a reliable CH within a group PSNs. With the support of trusted PSNs, cluster head spots the spiteful (selfish) nodes. At the time of inter-cluster transmission, trusted routing gateway nodes or other CHs are also choosen as relay nodes to transfer the private information to BS. For multi-hop clustering, the system chooses reliable routing nodes for transmitting the information among cluster members (CMs) and CHs. The altered information about the whole network's exact values is maintained in a database [28-29]. The size of the database and the size of the network are directly proportionally to each other. It is infeasible for a single node to store and compute the whole network's trust value since single node failure can destroy the network's life. In this way, nodes' faith-dependent protection must notice the time, number, amount of

interaction, and trust value alteration. Distributed trust model (DTM) is suitable for a network consisting of 10 to 20 PSNs since DTM incurs high communication overhead for an extensive network. In this chapter, a DTM is used to evaluate the trustworthiness of PSNs since DTM incorporate suggestion of all PSNs during direct and indirect (feedback) trust evaluation for effective decision making [29-30]. Figure 2.7 shows the threats and their solution in WBSNs.

Generally, there are several benefits of having faith among PSNs in a network. Customary security solutions are incompatible with solving various issues, such as dedicated routers, access control, etc.. That can be resolved efficiently with the trust evaluation technique. Trust evaluation Monitor the behaviour, estimate the trust value, and then quantify it into highly trusted, trusted, distrusted, etc. Trust-based security solution set up trusted routing paths and identifies faulty nodes. Reliable routing nodes merely used in sending information to the head node. A similar tactic is used hierarchically to fulfil the purpose of sending data to the base station.

Security threats and possible security solutions in WBAN		
Security threats	**Security requirements**	**Possible security solutions**
Unauthorized access	Key establishment and trust setup	Random key distribution and Public key cryptography
Message disclosure	Confidentiality and privacy	Link/network layer encryption and Access control
Message modification	Integrity and authenticity	Keyed secure hash function and Digital signature
Denial of Service (DOS)	Availability	Intrusion detection systems and redundancy
Compromised node	Resilience to node compromise	Inconsistency detection and node revocation and Tamper – proofing
Routing attacks	Secure routing	Secure routing protocols
Intrusions and malicious activities	Secure group management and secure data aggregation	Secure group communication Intrusion detection systems

Figure 2.7: Security threats and possible security solutions in WBAN

2.2 Trust Mechanism

This section discusses the literature review of existing secure models in BANs. We have rigorously studied various research articles [20-21][23][25-35][30-54] related to authentication and trust in a body sensor network with their strength as well as research gaps and observe security threats along with their requirements and possible prevention techniques (refer figure 5).

Li et al. [29] recommend a user-aided "multi-party authenticated key agreement protocol" known as group device pairing (GDP) to establish initial trust. The initial trust among SNs is set up by generating multiple shared secret keys. GDP employs a symmetric-key cryptography scheme to perk up the performance of the authentication method. Moreover, GDP does not rely on any supplementary hardware appliance. In this chapter, Key management and initial trust establishment in WBANs are two main issues addressed with device pairing. The author states that it is challenging and demanding tasks to provide a user-friendly and efficient trust initialization process in a resource constraint WBAN. Moreover, the author believes that key pre-distribution based security solutions are not suitable for BANs.

Mana et al. [38] suggest a trusted based key management scheme for WBANs to enhance the protection and confidentiality of sensitive health data by managing the symmetric session keys. The author states that physiological data transmission (end-to-end) plays a vital role in achieving high reliability. With the proposed scheme, secure data transmission can be achieved by proficiently generating and distributing cryptographic keys among base

station (sink) and sensor devices. Theoretical analysis exhibits its effectiveness in terms of energy-saving and security.

Liu et al. [39] projected a "Certificateless Remote Anonymous Authentication" method for WBANs, a lightweight and efficient system to guard BSN users' privacy. With this certificate less signature (CLS) scheme, Patients can efficiently and securely enjoy and benefit from remote medical health services. Moreover, the identities of patients are not disclosed to the outside world. The experimental, theoretical, and comparative analysis shows that the suggested scheme achieves an acceptable security level with minimal communication overhead.

Li et al. [40] discussed a trust management scheme (TMS) to deal with the security issues in BANs. The author employs the recommendation trust of WBAN nodes and conducts several experiments to analyze the projected scheme's usefulness and validity. The authors state that the data generated from the WBAN is essential and highly sensitive, so trust evaluation is essential to discover the faulty SNs and enhance dependability. Recommendations trust values of all neighbour of a node (say A) are stored in vectors, and they are similarly measured using a cosine product vector rule by identifying the angles between them. A collaborative filtering approach and Resnick's standard prediction formula is employed to compute BAN nodes' trust score. There are various research gaps in this chapter, such as i) not comprehensive ii) no severity analysis, iii) no proof regarding the robustness of the trust model iv) various attacks are not considered.

Guo et al. [41] proposed an "A Lightweight Encryption Scheme Combined with Trust Management for Privacy-Preserving in Body Sensor Networks". The lightweight

encryption scheme incorporated with trust management is based on mixing a cypher algorithm to improve sensitive health information's privacy and reliability. Moreover, an authentication scheme with trust management helps find reliable nodes to participate in the processing and transmitting private data. Besides, the authors list an excellent survey on the safety and privacy of important health data in mobile health-care. The major limitation of this scheme is that various attacks are not considered during the simulation. Moreover, there is no theoretical analysis for its validity and complexity with existing schemes and also they are not discussed comprehensively.

I. Hayajneh et al. [42] designed a lightweight authentication protocol for Medical Sensor Networks to spot various security and privacy issues during remote patient health condition monitoring. The proposed protocol for BSNs is a public key-based authentication (Rabin authentication algorithm) based protocol in which SNs gather health information and performs appropriate action as per the received command. The suggested authentication protocol's key plan is to enhance the "signature-signing process" that makes it appropriate for delay-sensitive medical sensor network applications. The research outcomes show good efficiency in providing authenticated commands to the SNs embedded (mounted) on/inside the body. The performance and efficiency are measured using the MIRACL library and Tmote Sky mote, respectively.

Thamilarasu et al. [43] discuss Challenges, Reviews, vision, and Recommendations for Securing WBANs to improve privacy and critical health information reliability. The author states that the participating nodes in the ad-hoc environment are vulnerable to several attacks. Securing the SNs from malicious attacks is itself a big challenge in WBANs due to its deployment nature. The authors analyze the existing security solutions and highlight

their pros and cons and some recommendations to improve security in WBANs against malicious behaviour. Moreover, security solutions are categorized into various security categories depending upon several parameters and attacks. The author believes that security enhancement using the trust concept might be an efficient solution to resolve the issues mentioned above and their limitations.

Omala et al. [44] recommended a well-organized remote authentication scheme (RAS) for WBANs. The author states that a patient's physiological data in limited range WBANs is transmitted (forwarded) to the remote server via intermediate portable devices (Smartphone) might be captured and modified by internal/external adversaries. The modified physiological data due to an open environment might lead to a poor diagnosis, which may be lethal for a patient. To resolve the issues mentioned above and improve security, reliability, and privacy, we have designed a robust RAS for WBANs to mitigate convergence and performance. The proposed schemes reduce 50% of running time at the client side when compared to other protocols.

Bhangwar et al. [45] suggest a "Trust and Thermal Aware Routing Protocol (TTRP)" for WBANs to improve reliability, confidentiality and the privacy of transmitted physiological data. The authors state that conventional cryptographic and biometric algorithms are not beneficial in BSNs since they do not deal with nodes' malicious behaviour, cost-inefficiency, and high complexity than trust-based schemes. Moreover, the temperature generated by sensor nodes due to electromagnetic radiations might be dangerous for sensitive tissues. To resolve the issues mentioned above and limitations of existing security schemes for WBANs, we proposed a resource-efficient, lightweight, temperature and trust-based thermal aware solution for WBANs. TTRP is a multi-factor routing scheme that

incorporates trust and nodes' temperature to detect (restrict) and segregate faulty nodes to provide a reliable health-care service.

Priya et al. [46] discussed a trusted routing scheme for WBANs to diminish the information (data) misfortune. The authors assume that sensor devices implanted on the human body in a clustered way where cluster head (CH) is elected using well known "particle swarm optimization" (PSO) and accumulate the trust scores of other SNs. We apply a fluffy (fuzzy) based trust induction model and scheduling algorithms and self-adaptive greedy buffer allocation to reduce energy consumption. Moreover, the proposed secure model improves the delivery ratio and throughput and reduces congestion compared to other existing schemes—a trust routing path selected by considering the trusted sensor nodes.

Chitra et al. [47] proposed a "Fault aware trust determination (FATD) algorithm for wireless body sensor network (WBSN)". The trust algorithm assigns a trust score between -1 to 1. The biomedical sensor node's is trust score computed by incorporating the node's movement, receiver signal strength, and battery terminal voltage. The proposed work is simulated on MATLAB to analyze efficiency and throughput. This work's major drawback is that FATD is not robust against BAN's attack since they do not incorporate adequate trust metrics for achieving security.

Anguraj et al. [48] projected a "Trust-based intrusion detection and clustering approach for wireless body area networks" for efficient transmission of critical medical data in an open environment. The cluster head within a group is elected by employing a multi-objective firefly algorithm. A hybrid encryption method and target function is used to encrypt sensitive data and improve throughput, respectively. The simulation results using NS-2

exhibit is acceptable performance in packet delivery ratio (PDR), delay, precision, and recall.

Roy et al. [43] proposed "A Novel Trust Evaluation Model Based on Data Freshness in WBAN" to detect selfish (non-eligible) nodes by employing a trust model along with data freshness factor. The author states that health-related data is sensitive and prone to various threats that lightweight trust models can efficiently protect instead of cryptographic algorithms. A selfish node performs unexpectedly in several ways, such as dropping the fresh data packet and forward old (or useless) data to the destination for incorrect decision-making. Moreover, sometimes-unintentional problems have arisen due to the low residual energy of IPS or network issues such as congestion, delay, etc.

Wang et al. [50] discussed a trust improvement technique based on TPM for clustered WSNs by dividing the network into numerous rounds. Every round employs a "setup phase" as well as a "steady-state phase." The proposed method employs Setup μTESLA, STEADY-μTESLA, SET-SCHNORR authentication protocols to make it lightweight, energy-efficient, attack-resistant, along with less communication overhead. The key role of the Trusted Platform Module (TPM) is to assess the integrity of cluster heads (CHs) and to establish as well as maintaining trust relationships among SNs as CHs play a vital role in node misbehaviour (attack) detection. However, no valid proof is given to justify its suitability in real-time industrial applications.

Ostad Sharif et al. [51] recommended a key agreement protocol for WBANs to provide security and reliability. The author believes that WBANs often collect and exchange essential and critical (private) medical information. Due to mobility, openness, and public

channels, WBANs are prone to attacks for preventing the WBANs from the attacks, privacy protection and mutual authentication schemes are required to protect the critical and confidential physiological data. To fulfil the purpose mentioned above, we design a robust authentication and key agreement protocol that incurs less communication overhead and mitigates de-synchronization and wrong session key agreement attacks. Moreover, the AVISPA tool and a random oracle model are employed to comparatively examine the proposed scheme's security level. The suggested scheme is also robust against active as well as passive attacks.

Nidhya et al. [52] discussed a survey related to security and privacy issues of sensed heterogeneous (critical) sensed data in Remote Healthcare Systems using WBANs. The author states that critical health data plays a vital role in accurate decision-making that certified medical professionals should access and take any action required for better treatment. The author [38-39] discussed the advantages and limitations (security threats levels) in WBANs. These security threats can emerge at either data (information) gathering level, storage level, or transmission level, and the security threats at data collection levels are data collision attack, jamming attack, selective forwarding attack, Sybil attack, data flooding attack, and Spoofing attack.

Moreover, the transmission-level of security threats are defined as Eavesdropping, Data tampering attack, Man in middle attacks, Scrambling attacks, Signaling attacks, Data interception attack, Hello flood attack, and Wormhole attack. The security threats at storage levels are Malware attack and Social engineering attacks etc. The author states that access control, availability, dependability, and flexibility are major privacy requirements in WBANs.

Karchowdhury et al. [53] presented an exhaustive survey on attacks for WBANs. The authors explained why the vulnerability of security threats arises due to its Adhoc, openness topology and suggest various prevention and privacy techniques to improve the efficiency of remote health-care systems.

Moreover, the authors state that remote health-care through WBANs is a demanding and attractive application area of WSNs because of its benefits on humans' lives. With remote health care using WBANs, a patient with diabetes, sugar, blood pressure, Nosocomephobia, and hypertension needs not to be admitted (stay) in hospitals for many days and can perform their everyday activities. The author suggests that a robust security scheme is vital to protect sensitive data from several internal/external threats and discusses layer-wise attacks with their definitions and misbehaviour.

Usman et al. [54] proposed a "trust-Based DoS Mitigation Technique for Medical Implants in Wireless Body Area Networks" by employing a three-level trust model as well as considering the resource limitation of sensor devices. They allowed the maximum data rate at each level according to the environment (home, office, public place) to transmit sensitive information. Moreover, the non-sharable trust threshold was changed by the base station according to environmental conditions. With this three-level trust model, along with a non-sharable trust threshold, these schemes effectively detect and isolate DoS attack. Although, no mathematical, as well as theoretical analysis was given in favour of its robustness.

TABLE 2.1: ATTACKS ADDRESSED BASED ON THE MONITORED BEHAVIOUR [25,27]

Trust metric	Monitored behaviour	Attack addressed

Data packets forwarded	Data packet (message) forwarding	Selfish behaviour, Black-hole, denial of service, sinkhole, selective forwarding,
Stability of reported values/data	reliability of sensing results reported values such as energy, humidity	Compromised nodes
Reputation	Trust value observed by third parties	Badmouthing attack
Battery/lifetime	Remaining power resources	Node availability
Cryptography	Capability to perform encryption	Authentication attacks
Sensing communication	Reporting of events (application-specific)	Selfish node behaviour at the application level
Packet address modified	Address of forwarded packets	Sybil, wormhole
Control packets forwarded	Control message forwarding	Control/routing message dropping
Availability based on beacon/hello messages	Timely broadcast of periodic routing information	Passive eavesdropping, selfish node
Routing protocol execution	Routing protocol-specific actions	Misbehaviours associated with particular routing protocol actions
Data packet precision	Data integrity	Data message modification
Control packet precision	Control packet integrity	Sybil, message modification

Remu et al. [27] proposed a "Naive Bayes based Trust Management Model for Wireless Body Area Networks" to ensure security from selfish nodes. The authors have employed a

naïve based classifier to classify a biomedical sensor node as a trusted or faulty node. The proposed model has been trained in MATLAB by taking 80 data sets randomly and got predicted classification as HIGH (H), LOW (L) and MODERATE (M). The significant limitations of this scheme are the uncertainty of trust estimation and computational complexity. Moreover, the trust update mechanism is not defined.

Roy et al. [55] presented a "Security and Privacy Issues in Wireless Sensor and Body Area Networks." The authors focus on the importance of body area networks in monitoring the vital physiological parameters.

Moreover, the authors discuss security issues and motivate them to design efficient, lightweight security schemes. Furthermore, the chapter discusses the threats and countermeasures and lists some existing chapter with their research gaps.

As per figure 2.8, we can conclude from the above existing work about possible security solutions according to the attack's nature and requirements. Moreover, we have seen that very few security solutions employ the trust concept. Table 2.1 indicates the suggested security solutions with their advantages, disadvantages and complexity analysis.

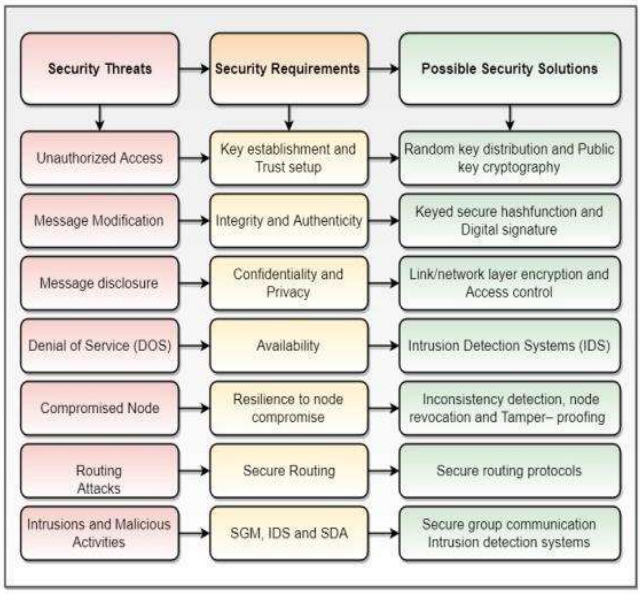


Figure 2.8: WBAN: Security Threats, Requirements and Possible Security Solutions

Trust-aware security models have become a promising and exciting technique for BSNs since they impose less overhead than cryptographic algorithms. Trust models (TMs) for BSNs [22-26,28-29,40-41,48-49] are broadly classified into data TMs and node TMs [56-57], which are further subdivided into centralized, distributed and hybrid TMs[21,23,25,30-35]. Centralized TMs fails due to a single point of failure, and distributed TMs incur high overhead. Hybrid TMs for clustered BSNs are a feasible solution [30-33] over-centralized and distributed TMs inaccuracy, overheads, cost, and convergence. Moreover, there exist various bases of trust computation in TMs such as weight-based, rate-based, fuzzy-based, Bayesian, entropy-based, game theory, [20, 23-25,28], but weight-based TMs seems to be an effective and reliable solution for BSNs since it is a small network [46, 48] where weights can adjust according to the patient condition[20, 23, 25]. Furthermore, weight-based TMs enforce less complexity than other bases of trust computations.

Farhana Jabeen et al. [1] stated trust and reputation arrangement in health-care structure. They discussed taxonomy, needs and open challenges. Trust has been considered as a salient element regarding health care. Omala et al. [12] recommended a well-organized remote authentication scheme (RAS) for WBANs to improve security, reliability, and privacy. The robust RAS for WBANs is efficient in terms of attacks mitigation, convergence as well as performance. The proposed schemes reduce 50% of running time at the client side when compared to other protocols. Bhangwar et al. [13] proposed a resource-efficient, lightweight, temperature and trust-based thermal aware solution for WBANs. The suggested scheme is a multi-factor routing scheme that incorporates trust and the temperature of nodes to detect (restrict) and segregate faulty nodes to provide a reliable health-care service. Priya et al. [14] discussed a trusted routing scheme for WBANs to diminish the information (data) misfortune. The authors applied a fluffy (fuzzy) based trust induction model and scheduling algorithms and self-adaptive greedy buffer allocation to reduce energy consumption.

Moreover, the proposed secure model improves the delivery ratio and throughput and reduces congestion compared to other existing schemes. Chitra et al. [15] proposed a trust algorithm that assigns the trust score between -1 to 1. The biomedical sensor node's trust score is computed by incorporating the node's movement, receiver signal strength, and battery terminal voltage. The proposed work is simulated on MATLAB to analyze efficiency and throughput. This work's major drawback is that FATD is not robust against BAN's attack since they do not incorporate adequate trust metrics for achieving security. Anguraj et al. [48] projected a "Trust-based intrusion detection and clustering approach for wireless body area networks" for efficient transmission of critical medical data in an open

environment. The cluster head within a group is elected by employing a multi-objective firefly algorithm. Hybrid encryption method and target functions are used to encrypt sensitive data and improve throughput, respectively. The simulation results are using NS-2 exhibit acceptable performance in packet delivery ratio (PDR), delay, precision, and recall. Roy et al. [49] proposed a Data Freshness-based trust assessment scheme in WBAN to detect selfish (non-eligible) nodes by employing a trust model and data freshness factor. Wang et al. [50] discussed a trust improvement technique based on TPM for clustered WSNs by dividing the network into numerous rounds.

Every round employs a "setup phase" as well as a "steady-state phase." The proposed method employs Setup μTESLA, STEADY-μTESLA, SET-SCHNORR authentication protocols to make it lightweight, energy-efficient, attack-resistant, along with less communication overhead. The key role of the Trusted Platform Module (TPM) is to assess the integrity of cluster heads (CHs) and to establish as well as maintaining trust relationships among SNs as CHs play a vital role in node misbehaviour (attack) detection. Ostad Sharif et al. [51] recommended a key agreement protocol for WBANs to provide security and reliability. The author designed a robust authentication and key agreement protocol that incurs less communication overhead and mitigates de-synchronization and wrong session key agreement attacks.

Moreover, the AVISPA tool and a random oracle model are employed to comparatively examine the proposed scheme's security level. The suggested scheme is also robust against active as well as passive attacks. Nidhya et al. [52] discussed a survey related to security and privacy issues of sensed heterogeneous (critical) data in Remote Healthcare Systems Using WBANs. The security threats at data collection levels are data collision attack,

jamming attack, selective forwarding attack, Sybil attack, data flooding attack, and Spoofing attack. Moreover, the transmission-level security threats defined as Eavesdropping, Data tampering attack, Man in middle attacks, Scrambling attacks, Signaling attacks, Data interception attack, Hello flood attack, and Wormhole attack. The security threats at storage levels are Malware attack and Social engineering attacks etc. The author states that access control, availability, dependability, and flexibility are major privacy requirements in WBANs.

Karchowdhury et al. [53] present an exhaustive survey on attacks for WBANs. The author suggests that a robust security scheme is vital to protect sensitive data from several internal/external threats and discuss layer-wise attacks with their definitions and misbehaviour.

Usman et al. [54] propose a "trust-Based DoS Mitigation Technique for Medical Implants in Wireless Body Area Networks" by employing a three-level trust model as well as considering the resource limitation of sensor devices. Theye allowed the maximum data rate at each level according to the environment (home, office, public place) to transmit sensitive information. Moreover, the non-sharable trust threshold is changed by the base station according to environmental conditions. With this three-level trust model, along with a non-sharable trust threshold, these schemes effectively detect and isolate DoS attack.

Remu et al. [8] proposed a "Naive Bayes based Trust Management Model for Wireless Body Area Networks" to ensure security from selfish nodes. The authors have employed a naïve based classifier to classify a biomedical sensor node as a trusted or faulty node. The proposed model has trained in MATLAB by taking 80 data sets randomly and got predicted

classification as HIGH (H), LOW (L) and MODERATE (M). The significant limitations of this scheme are the uncertainty of trust estimation and computational complexity.

Moreover, the trust update mechanism is not defined. FenyeBao et al. [4] proposed on Hierarchical Trust arrangement in the case of Wireless Sensor Networks. They also discussed the applications of it in the case of trust-based routing and Intrusion Detection. Daojing He et al. [58] wrote research on attack-resistant and lightweight trust management for medical sensor networks.

2.3 Authentication Schemes

RFID-based authentication for the health-care domain has become one of the hot topics of research in several health-care applications [60-61]. The immediate adoption of RFID technology in health-care or medical is to ensure secure access of patients, infant protection, patient tracking, reliability to patients' medical data, medication safety, the management of patient's records, managing patient location, types of equipment, employee, location tracking of medical assets, related to sensitive information of the patients, and so forth [62-65]. RFID is the most promising technology in the ubiquitous environment, allowing almost all objects to identify via radio frequency (RF) waves wirelessly. Over the past years, many researchers have presented many RFID authentication schemes for safeguarding the RFID system from various malicious attacks and privacy concerns. It is hard to provide all security privacy requirements because insecure communication is used between tags and readers in the low-cost RFID system. Therefore, we discuss some of the existing RFID authentication schemes with their techniques, strengths, and pitfalls to address such issues.

Xie et al. [66] introduced a cloud-centred RFID authentication scheme that preserves the tags and readers' privacy. In this scheme, a virtual private network (VPN) agency is deployed to organize the secure backend channels. Moreover, this scheme considered the cloud database as an encrypted hash table. The scheme uses simple bitwise XOR ($\oplus$), concatenation ($\|$) operations, a cryptographic hash function $h(.)$, PRNGs, and encryption $E(.)_k$ / decryption $D(.)_k$ Function by employing asymmetric algorithm. However, Abughazalah et al. [2015] showed that the security weaknesses of Xie's scheme could not withstand the reader impersonation and tag location tracking attack as well as invasion of the tag's data privacy.

Abughazalah et al. [2015] first showed the Xie et al. [66] scheme's security weaknesses, which was vulnerable to tag location tracking attack, reader impersonation attack, and privacy invasion of the tag's data. Furthermore, they presented an improved version of Xie's scheme, namely, a secure and improved cloud-centred RFID scheme to ensure security and privacy for the tags. The scheme uses simple bitwise XOR ($\oplus$), one-way hashing $h(.)$, PRNGs and performs symmetric operations. The authors had guaranteed that their scheme achieves several security features such as tag location privacy, tag anonymity, replay, tag/reader impersonation, and de-synchronization attacks. However, Surekha B et al. [] showed that the vulnerability of Abughazalah's scheme, which could not withstand the tag location privacy property.

Xie et al. [66] presented a cloud-centred RFID authentication approach through an insecure or wireless communication channel between cloud server and reader named cloud-RAPIC. The scheme uses simple bitwise XOR ($\oplus$), one-way hash $h(.)$, PRNGs, and performs

encryption $E(.)_k$/ decryption $D(.)_k$ By employing symmetric algorithms through the shared master keys, this scheme preserves the tag privacy property and protects data secrecy. However, this scheme's computational cost is a significant pitfall because it performs complicated hash operations in each authentication session run. Also, the scheme could not realize the identity authentication feature between the cloud server and the reader.

In [64], the authors presented a lightweight RFID-based scheme for the IoT environment's medical health-care domain. The scheme provides privacy protection for individuals or personnel against easily private data leakage by malicious outsiders. The scheme utilizes simple XOR ($\oplus$), concatenation ($\|$), circular left rotation $Rot(.,.)$, and cross $Cro(.,.)$ operations. The authors claimed that their scheme could not achieve all the necessary security features, but it can withstand the known security features such as mutual authentication, tag anonymity, forward secrecy, DoS and replay attacks. However, Aghili et al. [67] pointed out that it is susceptible to tag traceability, secret disclosure, and reader impersonation attacks. Moreover, the scheme could not provide the feature of tag anonymity as well as reader anonymity.

In [65], the authors presented a lightweight RFID-based scheme for cloud health-care systems. In cloud-centred health-care systems, the sensitive medical information associated with the individuals and patients can be compromised through the malicious cloud server, leading to a high risk of leakage of the individual's sensitive information. The authors used simple bitwise XOR ($\oplus$), circular left rotation $Rot(.,.)$, PRNGs, and quadratic re*SID*uals operations. The scheme resists known security attacks, including tag tracking, de-synchronization, and replay attacks.

To overcome the vulnerabilities of Fan's scheme [65], Aghili et al. [67] have presented an improved version, namely, a secure and lightweight RFID scheme for Medical IoT applications named SecLAP. The scheme uses simple bitwise XOR ($\oplus$), concatenation ($\|$), circular left rotation $Rot_l(.,.)$, circular right rotation $Rot_r(.,.)$, cross $Cro(.,.)$, and a secure and lightweight modular rotate $MRot_{(K)}(.,.)$, operations. The authors provide a security guarantee against the tag/reader impersonation, de-synchronization, replay, and tag traceability attacks. However, Safkhani et al. [68] showed that Aghili's scheme [67] is insecure against partial and full secret disclosure and traceability attacks.

In [66], the authors presented a secure and enhanced RFID scheme to prevent private or sensitive information from the health-care environment's back-end database. The scheme uses puncturable concatenation ($\|$) , PRNGs, pseudo-random function (PRF), indistinguishability obfuscation, and encryption $E(.)_k$ / decryption $D(.)_k$ By using symmetric key k. The scheme is secure against various security functionalities such as mutual authentication, data integrity, confidentiality, eavesdropping, man-in-the-middle (MITM), malicious server attack, and tag tracking attacks.

After an extensive study of the various literature reviews related to the health-care system, we got the great inspiration to design a lightweight privacy protection RFID authentication scheme that can be employed in the health-care system and which ensures the various imperative security requirements such as the resistance to DoS attack, the location privacy attack, the replay attack, non-traceability, and anonymity.

In 2014, Zhenguo Zhao [69] proposed a secure RFID authentication scheme based on elliptic curve cryptography (ECC) that can apply in telecare medical information systems

(TMIS). This scheme ensures that the protocol is safe under some security attacks and more reliable for health-care systems. However, the authors showed that their scheme is secure against forwarding untraceability and more suitable health-care environments. However, in 2016, Farash et al. [70] found Zhenguo Zhao scheme shows the security weakness against forwarding untraceability.

Xie et al. [66] presented an RFID authentication scheme based on the cloud server. Unfortunately, this scheme shows the security weakness against location tracking attacks, invasion of data privacy, and reader impersonation attacks. To fix the shortcomings of Xie's scheme, Abughazalah et al. [71] presented an improved version of a new RFID authentication scheme based on the cloud that achieves data secrecy and mutual authentication. Moreover, this scheme also has good performance for storage and scalability.

In respect of the health-care IoT environment, He and Zeadally [72] show a complete security and performance analysis of various RFID authentication schemes based on ECC techniques. Furthermore, the IoT application brings many changes such as convivence to physicians and patients in several medical fields, such as real-time monitoring, patient's medication records, blood bank management, patient information management, medical emergency management, and many others. In addition to that, usually cryptographic ECC tool used to achieves better security privacy and performance requirements. In 2018, Wazid et al. [73] showed the weakness of their scheme that cannot support dynamic implantable medical devices (IDMs), which are used to implant in the human body for improving some functionalities of many organs; for instance, an insulin pump used in the human body for monitoring the level of blood pressure.

In 2017, Rahman et al. [74] proposed a framework related to privacy-preserving for RFID based health-care environments to fulfil the various typical security requirements. Furthermore, privacy-preserving has two significant concerns that show an important paradigm in the RFID-enabled health-care environment. In this way, the primary concern describes an RFID authentication protocol that preserves privacy for monitoring purpose and senses RFID tags for different identification methods. Despite the first one, the secondary concern describes that while providing the health-care services with the help of tag ID, the privacy-preserving access control system is needed to prevent unauthorized access of secret information. Despite such privacy concerns, the framework solves the trade-off problem between privacy and scalability in the RFID systems. According to the authors, data security, privacy, and access are the paramount factors of RFID adoption in health-care systems.

In 2018, Chiou and Chang [75] proposed an enhanced authentication approach for an RFID system, which can also employ in the mobile RFID system. This scheme's main feature is to provide security in mobile devices, mobile RFID systems and make them more efficient and convenient for the wireless environment. Also, the scheme can successfully employ mobile devices that show proof of using mobile or wireless RFID systems. Moreover, the secure channel is not required in this scheme and the Electronic Product Code (EPC) Class-1 Gen-2 standards. The scheme holds some security requirements, namely the resistance against replay attacks, the de-synchronization attacks, and the reader tracking attacks. Unfortunately, Priyanka and Turuk [76] claim that the high computational cost does exist in Rahman et al.'s scheme.

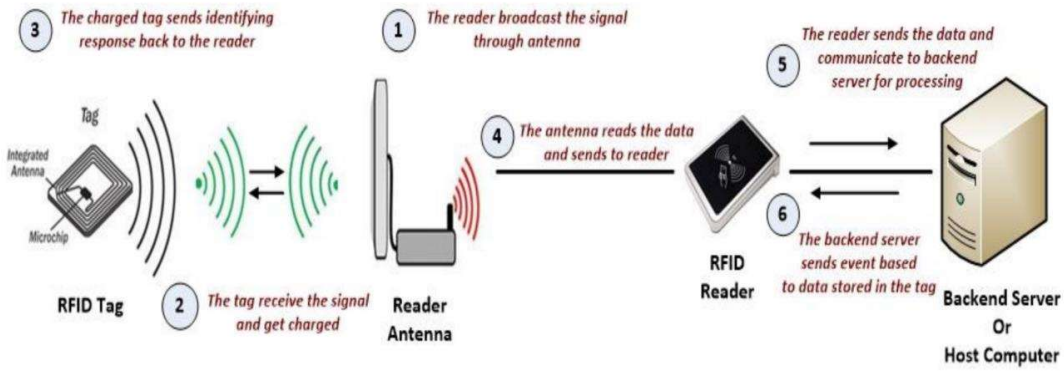


Figure 2.9 RFID-enabled health-care System

In 2018, Fan et al. [77] introduced a lightweight RFID scheme employed in the IoT environment for protecting the medical privacy of the stored information. However, the author ensures that their scheme provides resistance against various typical attacks: as replay attack, synchronization attack, and anti-Denial-of-service (anti-DoS) attack. Subsequently, Aghili et al. [67] pointed out that their protocol cannot withstand some severe vulnerabilities such as the tag traceability attack, the secret disclosure attack, and the reader impersonation attack. Also, their scheme does not preserve the anonymity of the reader as well as the tag.

In 2019, Aghili et al. [67] presented an improvement in Fan's et al. protocol named secure LRAP protocol, also known as SecLAP. Unfortunately, Safkhani et al. [68] show the security weakness of Aghili et al.'s protocol, i.e., SecLAP cannot withstand the partial secret disclosure attack, the entire secret disclosure attack, and the traceability attack. In addition to that, the privacy of the tags and the readers was compromised by the disclosed parameters.

Typically, an RFID system's main objective is to ensure the authentication and integrity of the system. More specifically, the privacy-preserving of the tags must be satisfied.

Security Ensures the rejection of fake RFID tags and identifies the counterfeit tags during communication with the reader.

Privacy Ensures that the privacy protection of valid or legitimate tags are ensured during communication with the reader.

2.4 Security Mechanism for Privacy

A novel Privacy-Preserving Disease Prediction (PPDP) system proposed enhancing the data records of health-care privacy inside the cloud server. The developed method encrypted the out-sourced health care data available inside the cloud effectively. However, the PPDP served several advantages; it lacked assuring privacy with several security issues that are hard to resolve [78]. A key protocol was developed to secure the health care data with bi-linear pairing cryptography and tri-party one-round authentication. The security analysis through the proposed key protocol showed robust performance over the attacks. The major drawback was that it lacked in providing direct order operation in the Cloud [79]. A light-weighted homomorphic encryption approach has been proposed for securing the cloud data. A comprehensive analysis was performed to validate the performance and observed high accuracy with minimum overheads in anomaly detection. The proposed technique can handle big data; it faced data ownership and security [80].

For supporting the privacy of patient data, a Clinical Decision Support System (CDSS) was proposed. The system incorporated the naïve Bayes classifier that extracts the sensitive

information which are secured in the cloud. This extraction was very significant for big data in the clinical domain. The primary issue was the possibility of collusion problem among the processing unit and the cloud server [81]. Another homomorphic based encryption model proposed to secure the analytical services through the Domingo-Ferrer approach in the cloud. The DomingoFerrer approach analyses the performance of the cloud and improves its security and storage activity. The time taken to perform the cryptic mechanism on data is high and more improvement is required for the cloud storage process [82].

A two-stage algorithm has been introduced for privacy-preserving of medical data in the environment of the cloud. The Repeated Gompertz and the Random Projection matrix combinedly provided enhanced anomaly detection. The time cost involved in the two-stage computation is very high [83]—a novel approach for securing the private key proposed through the Lloyd-based methodologies by addressing privacy-preserving issues. The proposed framework secured the stored data against the attackers. The limitation was that only a few attacks were considered for validating the performance [84]. Chen and Hoang [85] provided a Cloud-Based Privacy-Aware Role-Based Access Control, i.e. CPRBAC model for the existing resources in the health-care cloud. The work designed a scheme that is active auditing to report and monitor the legal operations. However, no cryptographic primitive gets used to ensure data confidentiality and data integrity in this work.

Narayan et al. [86] introduced a Patient-Centric EHR system for letting people share selected portions of the cloud that includes their health-care data reports. They accepted a Broadcast Attribute-Based Encryption (bABE) that enforces control of medical files. In the intervening time, they provide public-key encryption with the keyword search,

i.e. PKES on the encrypted data. However, the design has scarcity in algorithmic details about adopting schemes like bABE and PKES. .Wang et al. [87] proposed a protocol for privacy-preserving for calculating the distance of edit among two sequences of the genome. The work estimated the edit distance through its transformation over the computational problem for setting the size of interaction with approximation problem. Computing the set interacting size has been done by multi-party evaluation. This scheme can be computing the complete two genome sequences' edit distance within a few seconds with a minute or minor error. Lu et al. [88] have proposed a secure out-sourcing scheme of Genome-Wide Association Study, i.e. GWAS, to identify association among the gene's transfigurations with several existing diseases. The necessary calculation of GWAS grounded on the statistical data of its genetic data.

2.4 Summary

In this chapter, we have discussed the background and litreture survey of related issues. Here wireless system Application, Authentication schemes, trust management and privacy mechanisms are discussed in difference sections. The trust schemes and their literature survey related to propsed work is explained with details. The authentication technologies with litreture survey has also been discussed. In last section the privacy issue with related work is briefed. All sections have suitable figures and terminologies.

Chapter-3

An Efficient Trust Assessment Scheme for Healthcare System

Wireless body sensor networks (BSNs) have recently emerged and suggested vital requirements for various telehealth applications such as blood pressure monitoring and sugar level monitoring without dependence on any fixed (static) infrastructure such as hospitals. The chapter recommends a novel and efficient, lightweight trust management scheme (ETAS) deployed in health applications domains and does not rely purely on any encryption technique. Trust management (in BANs) has found a useful tool to improve cooperation among sensor nodes, security, and reliability. Existing trust models for BANs impose high overhead (communication, memory) and cannot improve sensor nodes' dependability.

Moreover, previous trust models do not consider data trust, patient's body temperature, and energy trust, which play a significant role in protecting and decision-making in body sensor networks. The chapter focuses on developing an exciting comprehensive, novel trust estimation framework for body sensor networks to enhance reliability, dependability, security by isolating compromised (malicious, faulty, hotspot) nodes with great resource (power, memory) efficiency. The proposed model (ETAS) incorporates several exclusive (unique) features like efficient trust evaluator, secure and attack resistance, and competent trust aggregator function to achieve a total trust score.

The trust evaluator function is a multi-trust strategy to deal with severe internal security threats [24] such as badmouthing attack, ballot-stuffing attack, Sybil attack, traitor attack, grudge attack, whitewashing attack, On-off attack, etc. with less resource consumption. Moreover, the proposed scheme (ETAS) incorporates both the success rate and misbehaviour component during trust evaluation. The proposed design (ETAS) efficiency is validated through several outcomes (experiments) and theoretical analysis in terms of

energy consumption, attack detection, mitigation, trust computation cost, and packet delivery ratio. The leftover part of this manuscript is divided into five more sections. Section 3.1 focuses on some problem formulation for WBANs security with their limitations and comparative analysis. Section 3.2 discusses motivation, and 3.3 discusses the research contribution, i.e. the suggested trust model and project their extended validation, respectively. Followed by that Section 3.4 explains the proposed lightweight trust-aware security scheme. Section 3.5 shows the results and discussion of the simulation analysis and reveals the projected scheme's achievements (ETAS), and finally, Section 3.6 concludes with summary.

3.1 PROBLEM FORMULATION

A wireless body area network (also known as WBAN, BAN, BSN, and MBAN used interchangeably) is a multi-hop, the temporary wireless network of low powered BAN devices (wearable computing devices (sensors), e.g. Electrocardiogram (ECG), Electromyography (EMG), Electroencephalogram (EEG)) that may be implanted, embedded (mounted) on/inside the body (hand, cloths pockets, etc.) in a fixed position[21]. A WBAN system is a consequence of a wireless sensor network that employs WPAN as gateways devices to attain longer ranges and adequate access to patient real-time (current) health records through internet service [22]. WBANs serve a vital role in diverse fields such as monitoring, security, sports, and military. A WBAN consist of inexpensive, limited power intelligent physiological sensors (IPS), employs multi-hop communication to monitor health conditions (domains) as well as early detection of various health status or physiological changes in patients affliction from several chronic diseases such as heart attacks, asthma, diabetes without requiring any location information through measuring changes[23]. If the patient's location is required, then motion detectors sensors help discover the patients' location. The monitored (recorded) medical information is processed by an external processing unit and instantly transmitted to worldwide doctors.

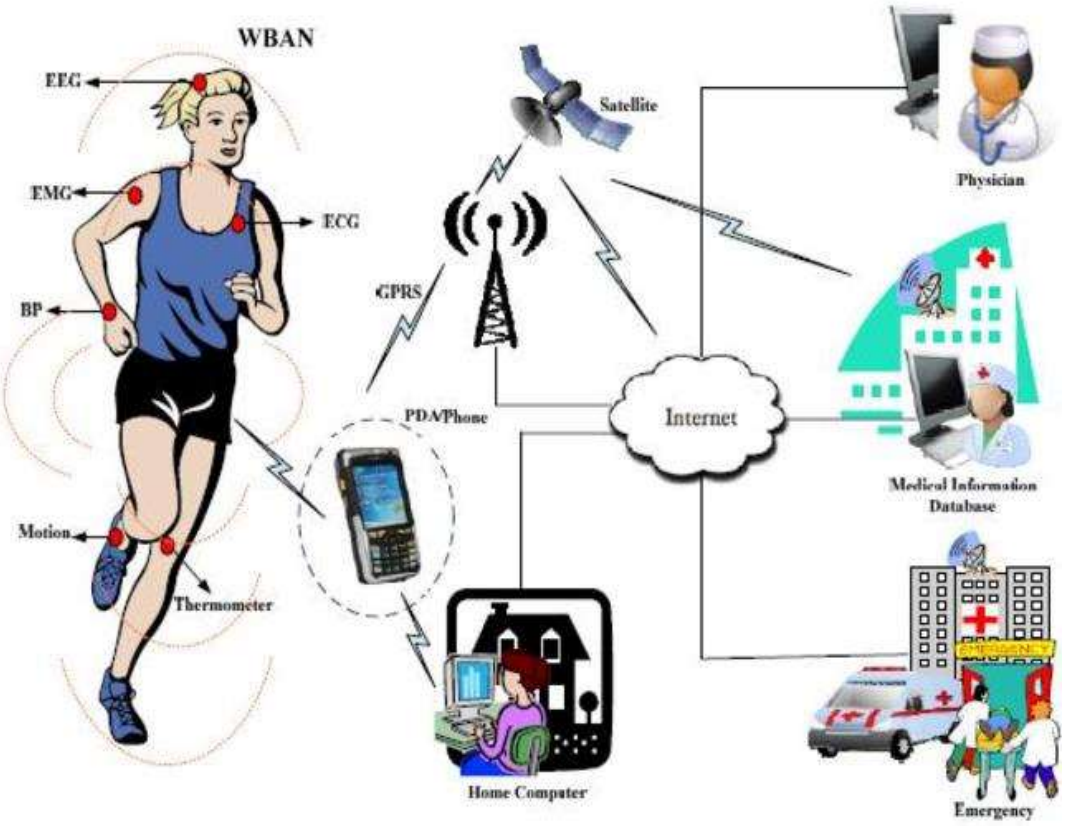


Figure 3.1: WBAN architecture and application scenario [20]

Moreover, emergency alarms (message) can be sent through a computer/mobile system to save patients' lives whenever any emergency such as heart attack, insulin level declines, etc., is detected. If insulin level declines, the sufficient dose is wirelessly injected by doctors with data terminals [24]. The IEEE 802.15.6 is the most modern standard to facilitate security in WBANs. WBANs entirely rely on the recorded (monitored) information via IPSs (or biosensors) as any incorrect information about health might be dangerous for patients' life [20].

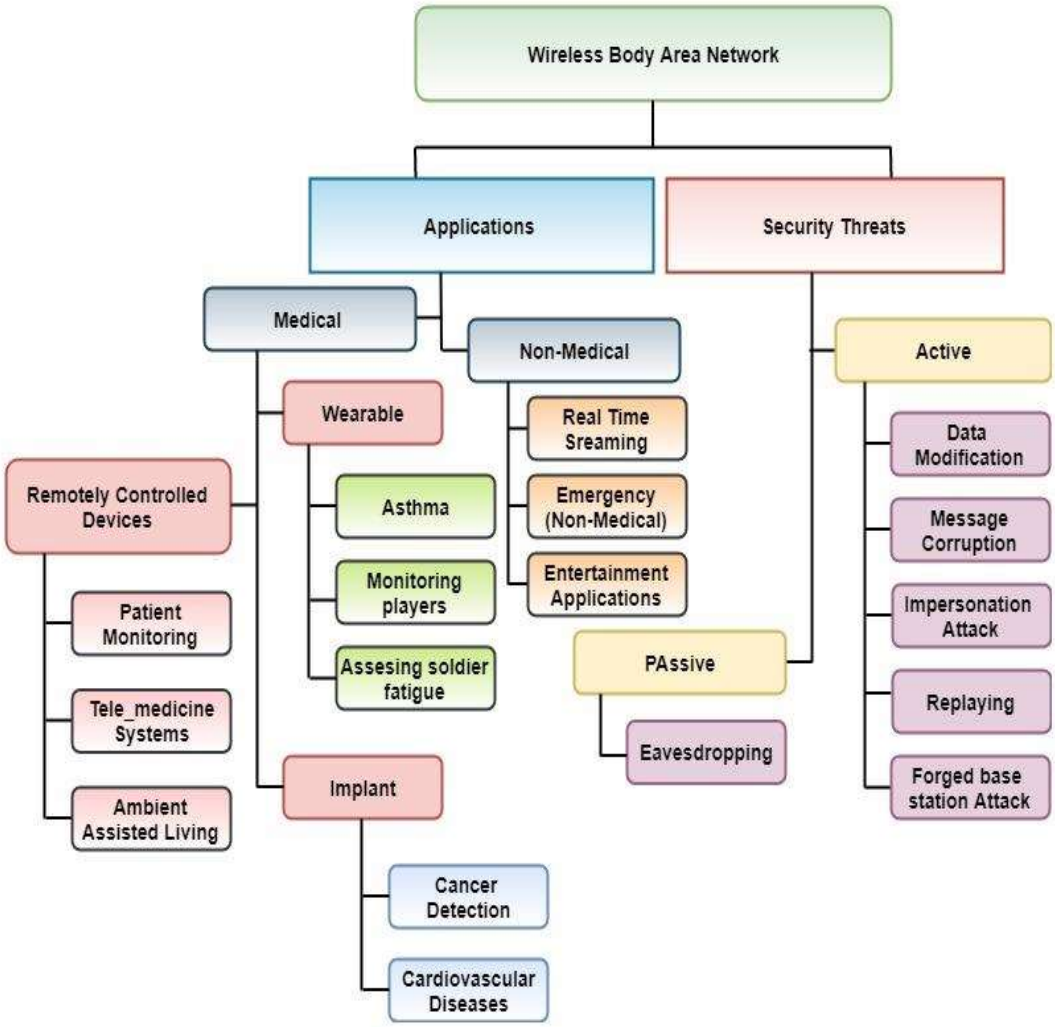


Figure 3.2: WBAN applications and security threats

In such cases, when the sensor node (SN) itself behaves maliciously (intentionally or unintentionally due to primitive stage technology issues.), cryptographic (authentication, authorization, hash) techniques [25-27] are infeasible to protect the network since they impose high overhead as well as unable to mitigate insider attacks [27-29]. Figure 3.2 shows various applications and security threats in WBANs.

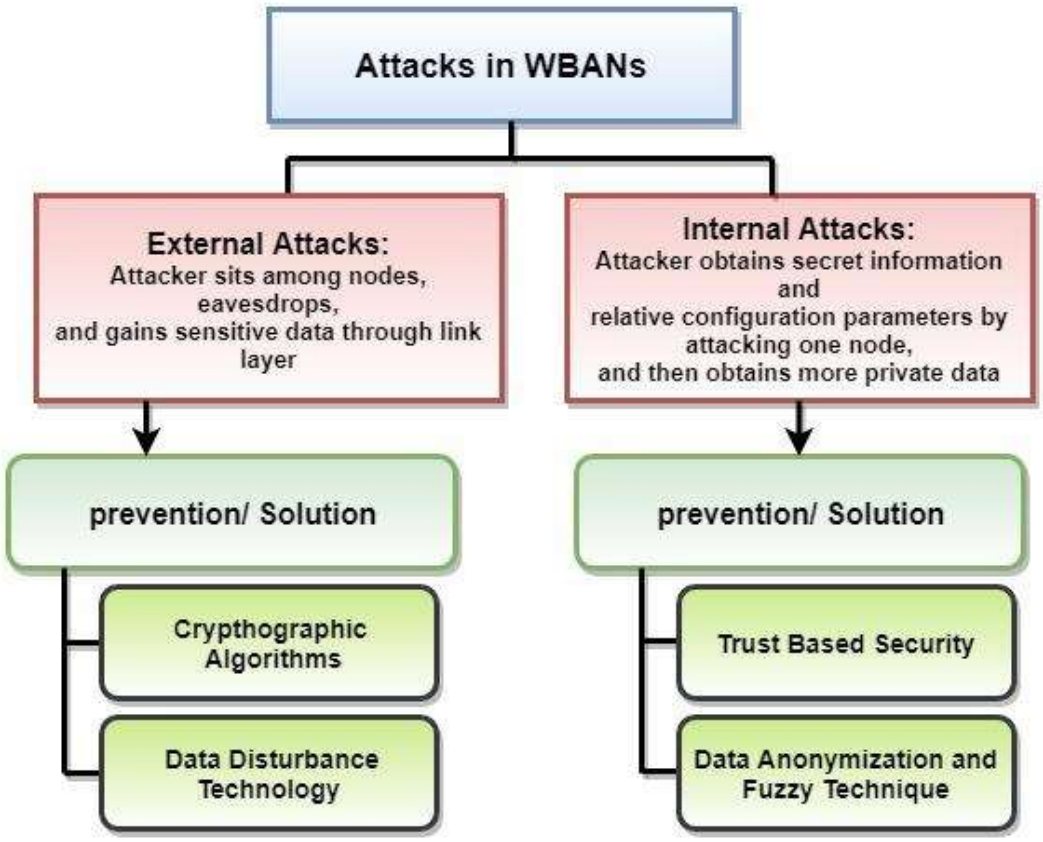


Figure 3.3: WBAN attacks and their prevention techniques

Figure 3.3 shows various possible solutions to achieve security from internal/external attacks. Trust management schemes proved as an efficient and reliable tool [56-57] to catch and mitigate (diminish) sensor nodes. Trust evaluation (or TMSs) monitors the SNs behaviour, estimates the trust value, and then quantified it into highly trusted, trusted, and distrusted. Trust value (score) is a level (quantification or measure) of belief of one entity towards another entity [90-91]. Trust is a dynamic, context-dependent as well as complex concept in WSNs. There are various advantages [89-93] of trust models, such as

- Detect various kind (intentional or unintentional) of misbehaviours of IPS
- Provide access control as well as reliable shorter routing paths
- Monitor and detects delay contributing IPSs, estimate trustworthiness level of communicating parties in real-time healthcare applications
- Impose lower overhead (resource, computation) than cryptographic algorithms

- Vital for internal threats (badmouthing attack, ballot-stuffing attack, whitewashing attack, Sybil attack, traitor attack, grudge attack, etc.) and ensure data integrity as well as data freshness by the continuous monitoring process
- Appropriate to provide security for the energy-starved environment with low computational and communication costs.

Figure 3.4 summarizes the motivation for trust in WSN, their design criteria, types, and associated attacks in a well-structured way.

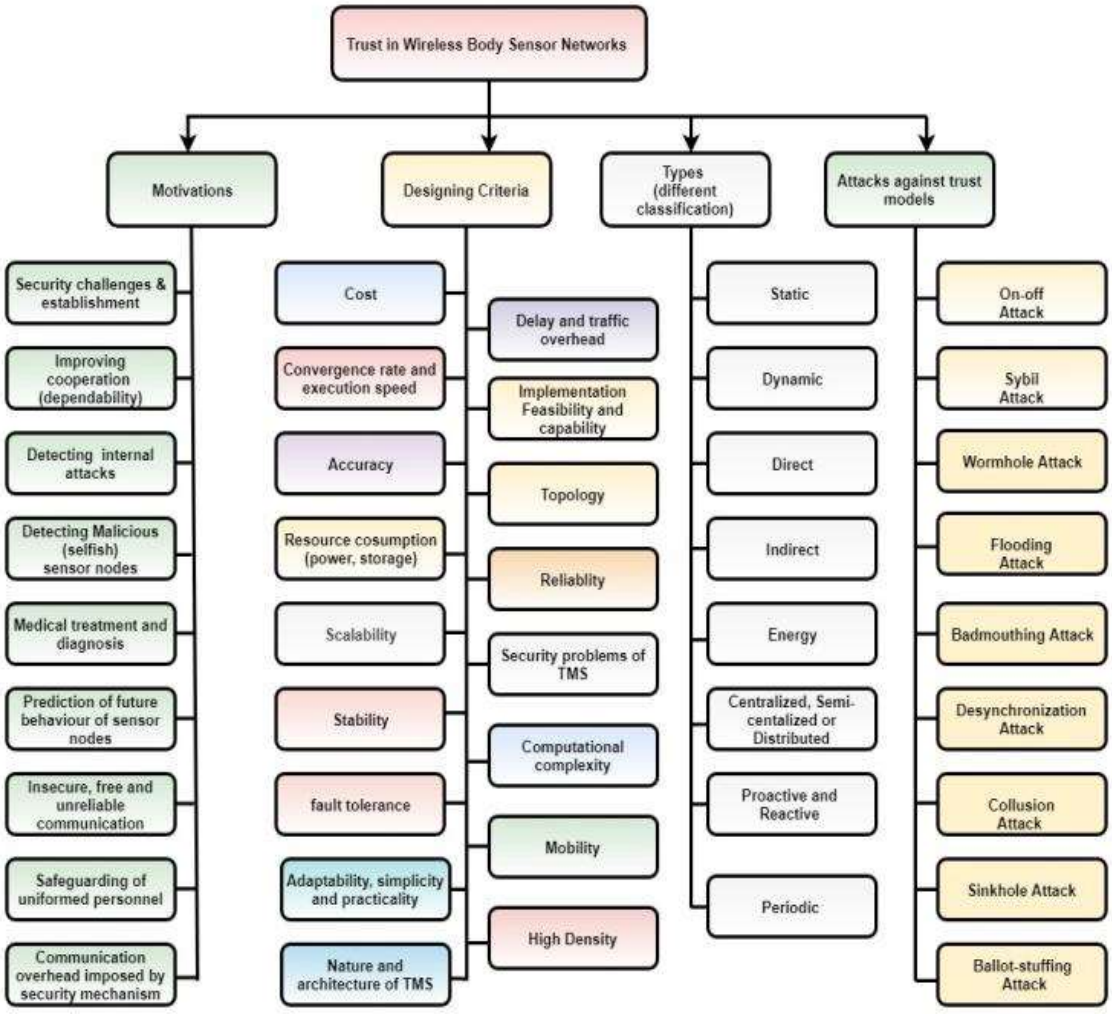


Figure 3.4: Trust in WBANs: Motivation, Design Criteria, Types and Attacks

The reliability of WBANs depends on the cooperation (collaboration) level of nodes and data generated by them [95]. Sometimes it is challenging to know about interactions of

nodes within the specified time. Moreover, interacting nodes are trustworthy or not is itself a big deal [96-9]. We have designed a trust model that incorporates triple trust (energy trust, communication trust, and data trust) to deal with selfish nodes and malicious (unexpected) behaviour to resolve the issues mentioned above. Communication trust is a level of assurance that nodes are communicating or not in a specified time or not. Depending upon the number of interactions, we evaluate communication trust. Data trust is a level of assurance of data collected, generated, and exchanged by physiological sensors is trustworthy or not. The concept of energy trusts helps resolve when a node might misbehave due to a faulty (insufficient) battery.

However, considerable research work has been carried out to protect BSNs; only little effort has been made for internal adversaries [98, 36], such as badmouthing attack, ballot-stuffing attack, Whitewashing attack, On-off attack [21], etc. by employing the trust concept that can lead to extremely unsafe health conditions. The chapter provides motivation and scope for the researchers in the field of trust-based security of BANs. Let us discuss a motivating example for researchers and scientist. For example, if the blood glucose sensor of a diabetic patient is hacked, and a faked high blood glucose concentration value is reported, the insulin pump will be activated, and a dose of insulin injected, which can lead to various chronic diseases or even more severe result if the injection of insulin occurs too frequently. Therefore, in addition to the existing security solutions for BANs, it is also critical to evaluate the trust in BANs. Moreover, sometimes fresh (current monitored) data is not accessible to doctors, leading to non-detection of various severe abnormalities, leading to severe consequences (i.e., death) on the patient.

3.2 MOTIVATION

Body sensor networks (BSNs) consist of various IPSs to monitor patient health status remotely. The quality of data generated and collected through sensors (data freshness without any delay) plays a vital role in decision-making for better care of the patient. There are several issues and challenges such as security [21-24], data quality [20] and its management [25], sensor validation [26], data consistency and freshness [27-29], interoperability [30-31], cost [32], transmission delay, consistent performance [33-34] and inference [35]. There exist [22, 24, 27-29, 56, 89, 93-95, 97-98, 36-39, 41-46, 48-49, 51,

53] various secure models for WBANs based on authentication, authorization, access control [30], key management [29, 42], and encryption. However, these models cannot satisfy the fundamental requirement (resource efficiency, dependability, data availability, and integrity) of body sensor networks since they impose extra overhead by employing heavyweight algorithms and not employing the multi-trust concept. Moreover, cryptographic security solutions are not effective in alleviating internal adversaries (badmouthing attack, Sybil attack, traitor attack, grudge attack, ballot-stuffing attack, On-off attack) since they assume that all the participated entities are trusted (reliable), so protect against only external attacks. Existing WBANs trust models [22-26, 28-29, 40-41, 48-49] failed (in terms of dependability, resource efficiency) due to the incorporation of weak trust function (linear, static). [56] [92] [49-50] states that static trust functions with stable punishment coefficient are vulnerable to security threats.

Furthermore, the trust mentioned above schemes does not consider the temperature of biomedical sensors nodes since the increased temperature can damage sensitive tissues. Due to the unreliable communication medium, the transmitted information (data set) of sensors readings must validate to diminish possible weaknesses and false alarms generations. The patient health data observed by the sensor nodes must be secure, have limited access, and should not mix with other patient data during collection and transmission. Moreover, an efficient security model for resource-constrained WBANs should be accurate, cost-effective, scalable, transparent, and less complex since BANs deals with sensitive and significant health data [51-54].

3.3 RESEARCH CONTRIBUTION

To eradicate the drawbacks of existing inadequate trust models [20-21, 23, 25-27, 29, 34, 38, 40, 45, 46-54, 56, 96] and other security schemes [22, 24, 28-29, 89, 93-94, 97-98, 41-45, 48-49], we have designed a comprehensive and innovative trust model incorporating several unique (distinctive) features to enhance collaboration and dependability among IPSs for developing a robust and trusted BSN system. These unique features are listed below as follows

1) Generate and assign a unique identity (ID) to every IPSs for more natural and secure communication and protection from external threats.

2) Present a vigorous distributed trust model by incorporating a multi-factor (temperature, misbehaviour, data trust, energy trust, number of interactions) trust approach to ameliorate collaboration and dependability among IPSs (CMs and CH) with moderate (acceptable) communication overhead. Moreover, our proposed scheme ETAS provides better telehealth service by considering the temperature factor of IPSs since high temperature of biomedical sensor nodes generated due to excessive communication can damage sensitive tissues.
3) Design an intelligent and reliable decision-making system by employing efficient and lightweight outlier detectors [94] and trust aggregators [30].
4) Provide a flexible (adjustable) reward and penalty coefficient in the trust model. These parameters can tune according to a patient's health condition (i.e., application requirements).
5) Independent of the platform and specific routing scheme.
6) The proposed approach allows only trusted nodes to be part of a body sensor network by isolating hotspot nodes.

The effectiveness, efficiency, and affirmation of the suggested trust model [ETAS] is demonstrated by simulation (MATLAB R2016a) experiments and theoretical analysis.

3.4 PROPOSED LIGHTWEIGHT TRUST–AWARE SECURITY SCHEME

This section discusses a multifactor (direct and indirect communication trust, data trust, energy trust, weight, and frequency of misbehaviour) based TM to prevent the WBAN from the aforementioned internal attacks. The projected TM (ETAS) is a distributed TM in which each biomedical SNs compute the trust value of other SNs and generate data packets. Relay nodes are used to forward trust values or data packets towards the sink node. The distributed approach is suitable for small networks [22, 23, 30] since fewer sensor nodes (10-100) incur low communication overhead. This section is classified into four subsections. The first subsection discussed network topology and various assumption made in the proposed work. The second subsection assigns unique labels to each biomedical sensor node to make communication easier. The third subsection discussed the

core part of the research work that is the trust estimation function. The fourth subsection discusses the hotspot node detection algorithm that incorporates the temperature of relay nodes, trust values, and residual energy of SNs to make an effective decision.

3.4.1 NETWORK TOPOLOGY AND ASSUMPTIONS

We presume that the IPSs is implanted in the human body (i.e., patient) in a distributed way where an IPS may be either biomedical SN or relay node that can interact (forward trust values) multi-hop communication. Similarly, relay nodes will forward the trust values to the sink node or another relay node. Relay nodes usually have high sensing power than biomedical SNs and estimate neighbouring relay nodes' temperature level by counting the packets transmitted and received. Furthermore, the source and sink node are honest nodes with the highest processing power. Moreover, we incorporate a logical time window to monitor patient health (physiological activities) at regular intervals (say (Δt)) for accurate decision-making.

It contains recently experienced information and drops more senior information for the effective cure of remote patients since recent health activities are more important than more senior information. WBANs are usually static [21-23] as IPSs are implanted on the same patient body at all times. Here, we are not focusing on memory overheads since storage capacity within IPSs is sufficient [34-38] to hold a patient health record that was a severe issue in ordinary WSNs deployed in a hostile environment. [29-31] can be used to secure the communication channel. To reduce the transmission and power overhead [56], we consider a flexible domain (say Ð) of trust values where $Ð \in [0\ 10]$.

Although any splendiferous range can be set, [56] suggest lower range results in low overhead during the exchange of trust values. We assume BS is a central command authority and cannot be captured by adversaries. Moreover, it can find and replace fault IPS for the adequate functioning of the remote healthcare system. The relay nodes are selected based on the distance from the sink and residual energy of sensor nodes. A node has the shortest distance from the sink node and has the highest residual energy selected as the relay node.

3.4.2 ASSIGNING UNIQUE LABELS (IDs) TO IPSs

Different (unique) labels (IDs) to each IPSs play a significant role in providing security from external attacks such as spoofing attack and makes communication easier. To generate unique labels (UL) for each IPS, we employ a hashing technique which takes a random number (say r) a key (say k) as follows

$$UL = ((k \oplus \text{r} \,||H((k+1) \oplus ID|| \text{r})) \quad (1)$$

3.4.3 TRUST ASSESSMENT SCHEME

After investigating several recent trust proposals (refer to Table II), we found considerable shortcomings in existing TMs such as static TM without any punishment, non-adaptive, high overhead, temperature unaware, non-flexible without severity analysis. Most WBAN TMs incorporate exhausted data (information) in decision-making, leading to uncovering (non-detection) numerous severe decrease symptoms.

A robust TM must focus on the primary requirements of WBAN and offer flexibility in adjusting some parameters (severity coefficient) such as reward and punishment for good and bad IPSs. A thorough explanation of the proposed TM (ETAS) provided in the following subsections.

1) Communication and Data Trust Calculation

This section discusses the trust computation process based on the interactions among biomedical sensor nodes. If the biosensors are frequently interacting, then we defined it cooperative interactions otherwise non-cooperative interactions.

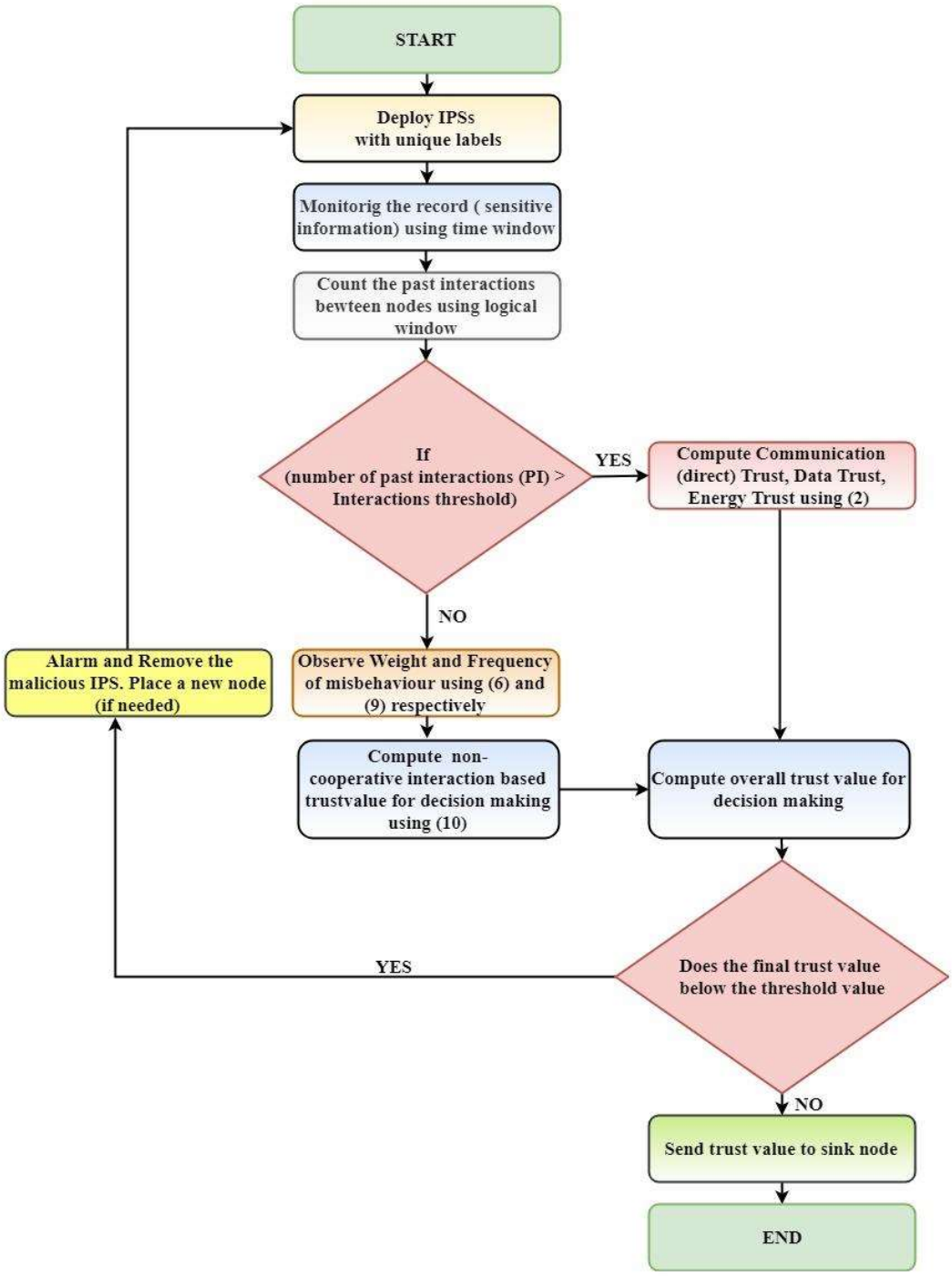


Figure 3.5: Flow chart of the proposed approach

If the numbers of past communications are equal to or exceeding the interaction threshold, we apply a success rate based dynamic approach in which the domain of trust values, penalty and incentive can be regulated according to the demand of actual application and

system requirements. On the other hand, if the numbers of past interactions are more petite than interaction thresholds, we compute current and aggregate misbehaviour and weight and frequency and misbehaviour to isolate hotspot nodes.

3.4.4 COOPERATIVE INTERACTION (SUCCESS RATE) BASED TRUST CALCULATION

The communication (cooperative) trust and data trust of bio-medical SN (say y) at bio-medical SN (say x) during Δt ($T_{x,y}^{C,D}(\Delta t)$) when the number of past interactions (PIs) is greater than or equal to the interaction threshold is defined by (2)

$$T_{x,y}^{C,D}(\Delta t)) = \left[Ð \times \left(\frac{S_{x,y}^{C,D}(\Delta t)+1}{\left(S_{x,y}^{C,D}(\Delta t)+U_{x,y}^{C,D}(\Delta t)\right)+2} \right) * \frac{1}{\sqrt{\Gamma*(U_{x,y}^{C,D}(\Delta t)+1)}} * \left\{ 1 - \frac{1}{S_{x,y}^{C,D}(\Delta t)+1} \right\}^{\alpha} \right] \quad (2)$$

Where Δt is the time window which consists of several time units whose length can be adjusted depending on the network scenario. This logical time window adds newer experiences and forgets older experiences as the time elapses. Moreover, it helps to monitor the good and bad behaviour of biomedical sensor nodes. Superscript C, D denote communication and data interactions and [.] denote the greatest integer function. $S_{x,y}^{C,D}(\Delta t)$ and $U_{x,y}^{C,D}(\Delta t)$, denotes cooperative and non-cooperative interactions used in the proposed work. Parameters Γ can be tuned according to application requirement to give harsh punishment with the increase in (non-cooperative) unsuccessful interactions. The first term $\frac{S_{x,y}^{C,D}(\Delta t)+1}{\left(S_{x,y}^{C,D}(\Delta t)+U_{x,y}^{C,D}(\Delta t)\right)+2}$ shows predictability trust, which is a Bayesian formulation using a beta reputation system. The second term $\frac{1}{\sqrt{\Gamma*(U_{x,y}^{C,D}(\Delta t)+1)}}$ is punishment term whose value depends on the parameter Γ, when there are no unsuccessful interactions (i. e. $U_{x,y}^{C,D}(\Delta t) = 0$) between SN x and y. The linear term $1 - \frac{1}{S_{x,y}^{C}(\Delta t)+1}$ slowly tends to 1 with an increase in $S_{x,y}^{C}(\Delta t)$ indicates a minor alteration in the trust value of node x for node y. The exponent parameter $\alpha \geq 1$is a reward parameter that gives the harshness to the

trust function whose value can adjust according to network scenario and application requirement and plays a significant role to cope with untrustworthy nodes with greater values of reward parameter α.

Based on the communication and data trust values obtained by (2), a biomedical sensor node is categorized into three potential states as follows using (3)

$$S\left(\mathrm{T}_{x,y}^{C,D}(\Delta t)\right) = \begin{Bmatrix} (\rho\%\ of\ Đ; Đ) \\ (0; Ø) \\ (Ø; \rho\%\ of\ Đ) \end{Bmatrix} \begin{Bmatrix} highly\ trusted\ node \\ malicious\ node \\ legitimate\ node \end{Bmatrix} \quad (3)$$

The parameters Ø is the trust threshold whose value is considered one-third of the maximum trust value ($Đ/3$). The parameters ρ and Đ are the adjustable parameters whose values can regulate according to actual application requirements or network scenario. This approach provides complete flexibility in adjusting the trust value and a threshold value of trust using the application variable ρ. In this work, we have chosen $\rho = 60$. Moreover, a successful data report between two biomedical sensor nodes (say x and y) is also verified by comparing the data values reported with an error tolerance parameter(ξ). The error tolerance parameter is an error threshold for the data values reported by the bio-medical sensor nodes. It helps to identify the faulty nodes that are misbehaving with private physiological information.

3.4.5 NON- COOPERATIVE INTERACTION BASED TRUST CALCULATION

When biomedical sensor nodes do not frequently interact within a specified time, i.e., when several past interactions (PIs) is less than the interaction threshold, then instead of computing indirect (feedback) trust, we compute the weight and frequency of misbehaviour to isolate hotspot nodes since indirect trust are not able to catch on-off attack[21], collusion attack [28], etc. Besides, we use the previous communication trust score of SNs with aggregate misbehaviour and current measured misbehaviour to obtain a strong current trust value of a node at time Δt. The current misbehaviour (CM) of a bio-medical SN (say y) at bio-medical SN (say x) during Δt $(\mathrm{M}^{\mathrm{current}}_{x,y}(\Delta t))$ is defined as follows using (4)

$$\mathrm{M}^{\mathrm{current}}_{x,y}(\Delta t) = \frac{\text{malicious behaviour}}{\text{malicious behaviour+expecte (good)behaviour}} \quad (4)$$

In order to analyze the persistency of misbehaviour, we launch an aggregate misbehaviour component as follows using (5)

$$M^{aggregate}_{x,y}(\Delta t)) = \min\{f * M^{current}_{x,y}(\Delta t) + (1-f) * M^{aggregate}_{x,y}(\Delta t - \Delta)), 1\} \quad (5)$$

Where f is the forgetting factor that provides flexible weightage to the previous aggregate misbehaviour.

As we know, the biomedical sensor network deals with patients' critical information, so it is vital to analyze the weight of misbehaviour after a fixed interval of time. The weight of misbehaviour within time (Δt) is defined as follows using (6)

$$M^{weight}_{\Delta t} = \max(f_1 r_1, f_2 r_2, f_3 r_3, \ldots\ldots\ldots f_i r_i, \ldots\ldots f_L r_L) \quad (6)$$

Where L denotes the number of time units in a time window(Δt). The term $f_i r_i$ denotes forgetting factor value as well as the rate of misbehaviour at i^{th}unit of time. Note that $f_1 < f_2 < f_3 < f_4 < \cdots \ldots \ldots f_L$. This indicates our proposed approach assigns more weightage to recent misbehaviour rather than the older one that makes it a realistic approach. The rate of misbehaviour for time unit (say i) is defined as follows using (7)

$$r_i = \left\{\frac{U_i}{S_i + U_I}\right\} \quad (7)$$

Where U_i *and* S_i Denote the number of malicious and good behaviours at time unit i. Since the forgetting factor should increase with time, it must depend on the number of time units (L) in a time window and the current period (i). The term forgetting factor (f_i) is defined as follows using (8)

$$f_i = \psi^{L-i} \quad (8)$$

Where $0 < \psi < 1$.

In order to mitigate severe attacks, we integrate a new term known as misbehaviour frequency ($M^{frequency}_{\Delta t}$) to analyze the behaviour of nodes in terms of the number of misbehaviours during some time. To compute misbehaviour frequency, we consider two time periods: active period ($A_{\Delta t}$) and passive period($P_{\Delta t}$). Active period ($A_{\Delta t}$) is defined as when a particular node is misbehaving, i.e. rate of misbehaviour is more significant than some specified threshold, and the passive period defined as when a particular node is performing well. The frequency of misbehaviour within time (Δt) is defined as follows using (9)

$$M_{\Delta t}^{frequency} = \left\{ \frac{A_{\Delta t}}{A_{\Delta t} + P_{\Delta t}} \right\} \quad (9)$$

The history of misbehaviour frequency is recorded in a logical array for decision making. It plays a vital role in the final trustworthiness evaluation of biomedical SNs. The final trust value based on the misbehaviour($T_{x,y}^{Misbehaviour}$) at time Δt defined as follows using (10)

$$T_{x,y}^{Misbehaviour}(\Delta t) = \begin{Bmatrix} Ð * (1 - M_{\Delta t}^{weigh}) \; if \; M_{\Delta t}^{weigh} > M_{\Delta t}^{frequency} \\ Ð * [\gamma * (1 - M_{\Delta t}^{weigh}) + (1 - \gamma) * (1 - M_{\Delta t}^{frequency}) \; otherwise \end{Bmatrix} \quad (10)$$

Using (2) and (10), a hotspot (malicious) node can be accurately identified as follows using Algorithm 1.

Energy Trust

Energy Trust is defined as "the belief of one biomedical sensor node that other biomedical sensor node still has adequate energy to perform its intended function". We believe that selfish biomedical SNs needed the extra energy to initiate severe selfish behaviours to destroy the credibility of BAN. First, we define the energy threshold E_{th} and estimate residual energy (E_{res}) of a biomedical sensor node. After estimating the value of E_{res}, we evaluate the energy consumption rate (E_c) which depends on the ray projection method [90]. We assume that with stable environmental conditions, the energy consumptions rate of SN is stable. Energy trust (T_E) of a biomedical sensor node is defined using (11)

$$T_E = \begin{cases} 0 \; if \; E_{res} < E_{th} \\ 1 - E_c, \; else \end{cases} \quad (11)$$

3.4.6 HOTSPOT NODE DETECTION ALGORITHM

In this subsection, an efficient multifactor hotspot node detection algorithm is discussed to detect malicious nodes in BANs. The hotspot node detection algorithm incorporates the temperature of biomedical sensor nodes, trust value, and residual energy of nodes to make correct decisions about a node's status. We assume that while each packet's time is forwarding, 0.1 units increase a relay node's temperature. According to the algorithm, if the temperature of the relay node (say i) is more significant than equal to the temperature

threshold or the final trust value is less than the trust threshold or the energy level of a node is less than the energy threshold, then node (i) will be hotspot node otherwise it is a reliable node. Once a node is detected as a hotspot node, the base station eliminate this node from the network to improve the network lifespan since hotspot nodes consume more energy to spread false information.

Algorithm 1: Hotspot Node Detection Algorithm
Input: temperature of nodes, trust values, trust threshold, energy, energy threshold **Output:** hotspot node

Step 1. ∀ Packet forwarding, Temp=Temp + 0.1 unit.
 	
Step 2. If (temperature of relay node (i) ≥ temperature threshold) || (final trust value < trust threshold) || (energy level of a node < energy threshold)
then
node (i) hotspot node
else
If (temperature of relay node (i) < temperature threshold) && (final trust value ≥ trust threshold)&& (energy level of a node ≥ energy threshold)
then
node (i) is a reliable node
Step 3. Go to step 1

3.5 RESULTS AND DISCUSSION

This section discussed the theoretical analysis and experimental results to prove the recommended trust management scheme's validation against BAN's attacks. In the theoretical analysis, a logical and contradictory approach is used to prove the robustness of ETAS. The detailed description of both (theoretical analysis and experimental results) is in the following subsections.

3.5.1 Theoretical Analysis

Theorem 1: In node to node trust assessment and decision making, ETAS is potent against biomedical sensor nodes' selfish behaviour.

Proof (by contradiction): Suppose a node (say y) fruitfully deceived another node (say x), then $U_{x,y}^{C,D}(\Delta t) \geq S_{x,y}^{C,D}(\Delta t)$ and $T_{x,y}^{C,D}(\Delta t) \geq Ø$ The parameters Ø is the trust threshold

whose value is considered one-third of the maximum trust value ($Ð/3$). There exist three cases for this selfish behaviour

Case 1: if the node (x) and node (y) do not interact with each other, i.e., $U_{x,y}^{C,D}(\Delta t) + S_{x,y}^{C,D}(\Delta t) = 0$ then Eq.(10) incorporate the misbehaviour component and forgetting factor to caught its malicious behaviour.

Case 2: if $S_{x,y}^{C,D}(\Delta t) = 0$ and $U_{x,y}^{C,D}(\Delta t) \geq 1$ then $T_{x,y}^{C,D}(\Delta t) = 0$ using Eq. (2). If the number of interactions is more diminutive than the interaction threshold, then Eq.(10) will compute the trust value.

Case 3: if the node (x) and node (y) interact at least once within (Δt) time, i.e., $U_{x,y}^{C,D}(\Delta t) + S_{x,y}^{C,D}(\Delta t) > 1$ and $U_{x,y}^{C,D}(\Delta t) \geq S_{x,y}^{C,D}(\Delta t)$ then the predictability trust term $\frac{S_{x,y}^{C,D}(\Delta t)+1}{\left(S_{x,y}^{C,D}(\Delta t)+U_{x,y}^{C,D}(\Delta t)\right)+2)}$ will always be less than 50% (i.e., 0.5) and the value of $T_{x,y}^{c,d}(\Delta t)$ will be less than $Ø$ for any value of α, which contradicts the hypothesis.

Theorem 2: In node to node trust assessment and decision making, ETAS is potent against on-off attack.

Proof (by contradiction):

Case 1: When the number of interactions ≥ interaction threshold

Suppose a malicious node (say y) provide false information regarding interactions (say x), then $S_{x,y}^{C,D}(\Delta t) \geq U_{x,y}^{C,D}(\Delta t)$ and $T_{x,y}^{C,D}(\Delta t) \geq Ø$. In this case, the term $\frac{S_{x,y}^{C,D}(\Delta t)+1}{\left(S_{x,y}^{C,D}(\Delta t)+U_{x,y}^{C,D}(\Delta t)\right)+2)} < 1$ and $T_{x,y}^{C,D}(\Delta t) < Ø$. It proves that ETAS is potent against on-off attack.

Case 2: When the number of interactions < interaction threshold

In this case, a selfish node will try to show its trust score greater than equal to the trust threshold i.e. $T_{x,y}^{Misbehaviou}(\Delta t) \geq Ø$. As the interactions are less, the frequency of misbehaviour will be less than the weight of misbehaviour. In this case, the value of the trust $T_{x,y}^{Misbehavio}(\Delta t)$ will be less than the trust threshold $Ø$. It means ETAS is potent against an on-off attack against on-off attack.

3.5.2 Experimental Results

This section discussed the severity analysis of the suggested trust function and experimental results on MATLAB to exhibit the effectiveness of the proposed trust management scheme in terms of severity of trust values, energy efficiency, packet drop ratio, and malicious node detection under varying network size.

TABLE 3.3 **List Of Parameters**

Parameter/feature	Value
Range of biosensors	10-50 (variable)
Geographical Region	100x100 Meter
Communication medium	Wireless channel
Topology	Distributed/Random
Coverage	30 Meter
The initial energy of the biosensor	5 J
Range of relay nodes	5-10 (variable)
Range of malicious relay modes	3-4 (variable)
Number of malicious nodes	8-10 (variable)
Number of the sink node	1
Position of the sink node	(50m,50m)
Transmission range of relay nodes	25 meter
Trust threshold (Ø)	10 /3
Temperature threshold	60
Domain (Ð)of trust values	0 to 10
Application adjustment variable (ρ)	60
Error tolerance parameter(ξ)	0.5
Number of time units (L) in a time window	5
Energy Threshold (E_{th})	20% of initial energy (E)
Γ	.5
Ψ	[0 1]
A	2

We have compared our suggested trust model (ETAS) with PSTRM [93] and BAN-TRUST [40]. PSTRM [93] is the latest trust model that guarantees high detection of malicious nodes under a small network size, such as telehealth application. BAN-TRUST [40] is specially designed for body area networks and exhibit good performance. Table III shows the parameters used in implementing the proposed work to analyze the suggested approach's effectiveness (ETAS).

1. Effect of malicious nodes on trust value

In this subsection, we discuss the effect of malicious nodes on trust values. Figure 3.6 shows the effectiveness of ETAS in terms of success ratio and change in trust values of SNs. The term success ratio is the ratio of successful (cooperative) interactions to total interactions. When the numbers of cooperative interactions are increasing, the trust in ETAS is gradually increasing. However, in BAN-TRUST [40] and PSTRM [93], the trust value does not reach 10 with 100% successful interaction. Moreover, in PSTRM [93], the trust values are not gradually increasing with increasing cooperative interactions. The main reason behind the effectiveness of ETAS is that its main focus is on the interaction of nodes. ETAS adopt an appropriate trust evaluation strategy by counting the number of interactions between SNs. Furthermore, ETAS consider dynamic reward and punishment parameter along with misbehaviour component to punish the selfish nodes. ETAS has also been tested by performing ballot-stuffing attacks, whitewashing attacks, and on-off attacks since these attacks are very severe for patients' health-related information. Figure 3.7 shows the effect of the on-off attack on the trust model. When the numbers of nodes are $10, 20, 30, 40, 50$, then on-off attacks reduce the trust value by 0.2 (2.2%), 0.2 (2.5%), 1.5(18.75%),0 .4(6.4%), 0.1 (2%) respectively. The average change in trust values of genuine nodes is 6.37%. The accuracy of obtained information is 93.63% which is better than other existing trust models for BANs. However, we have analyzed the combined effect of various attacks (ballot-stuffing attack, whitewashing attack and on-off attack) in figure 3.8. We intentionally inject up to 60% of malicious nodes in BAN and found that ETAS perform better over BAN-TRUST [90] and PSTRM [93] due to the robust trust model. Furthermore, we generate more selfish nodes to analyze the detection capability of ETAS, BAN-TRUST [40] and PSTRM [93]. Figure 3.9 show that ETAS can effectively identify up to 92% malicious nodes in a network of 50 nodes since the hotspot node detection algorithm employs the temperature condition, trust value and residual energy of SNs.

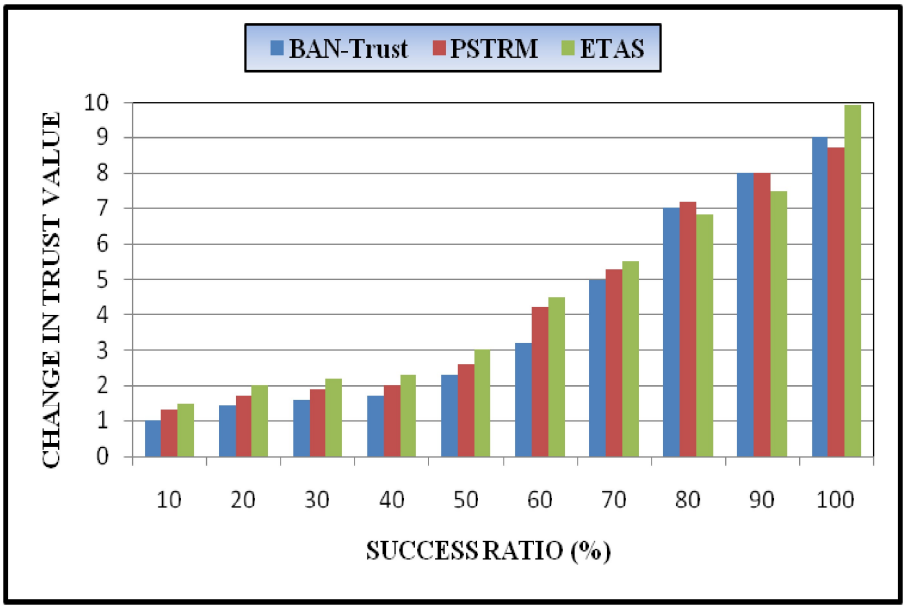


Figure 3.6: Success ratio Vs Trust values.

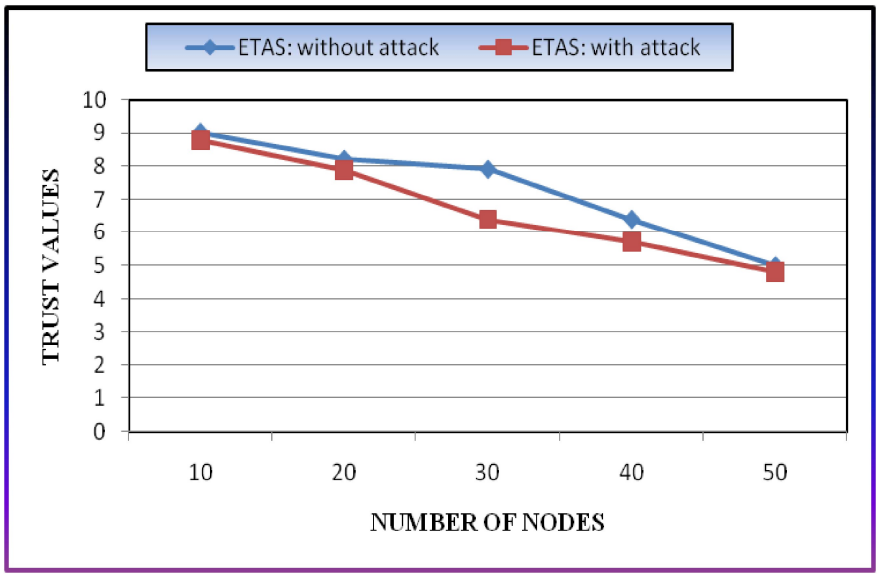


Figure 3.7: Effect of the on-off attack on trust values.

The temperature and trust aware hot spot node detection algorithm minimize the risk of damaging a patient's sensitive tissues caused by the high temperature of biomedical sensor nodes generated due to excessive communication. The simulation result proves that ETAS is a great trust model that exhibits such excellent efficiency in improving dependability and malicious node detection for BANs.

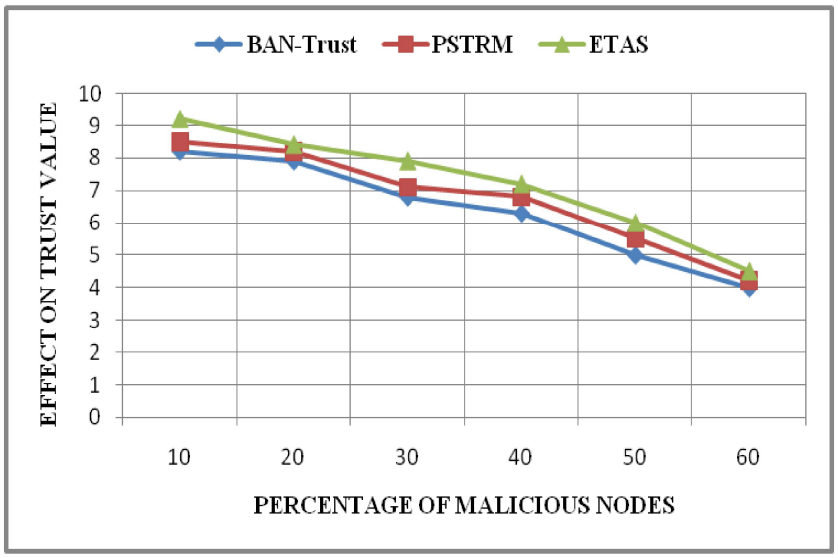


Figure 3.8: Effect of malicious nodes on trust values.

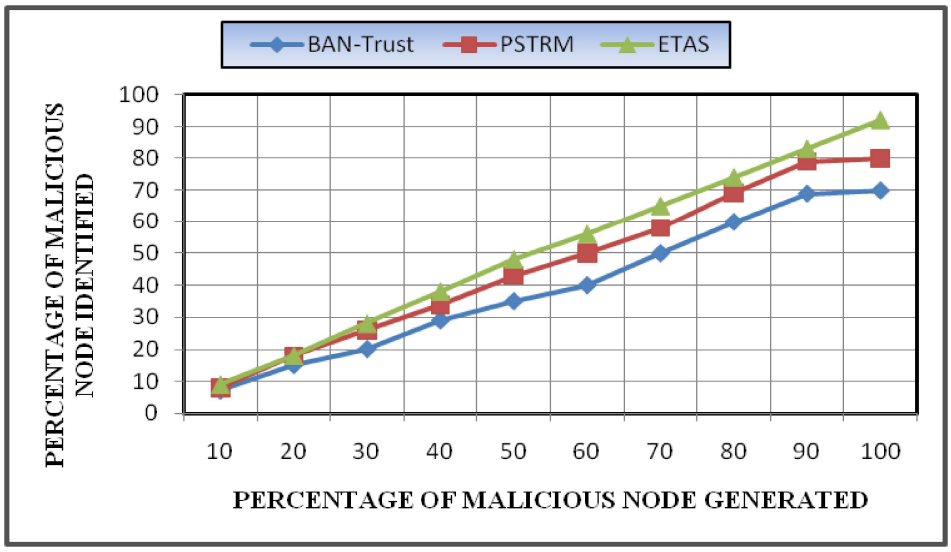


Figure 3.9: Malicious node detection.

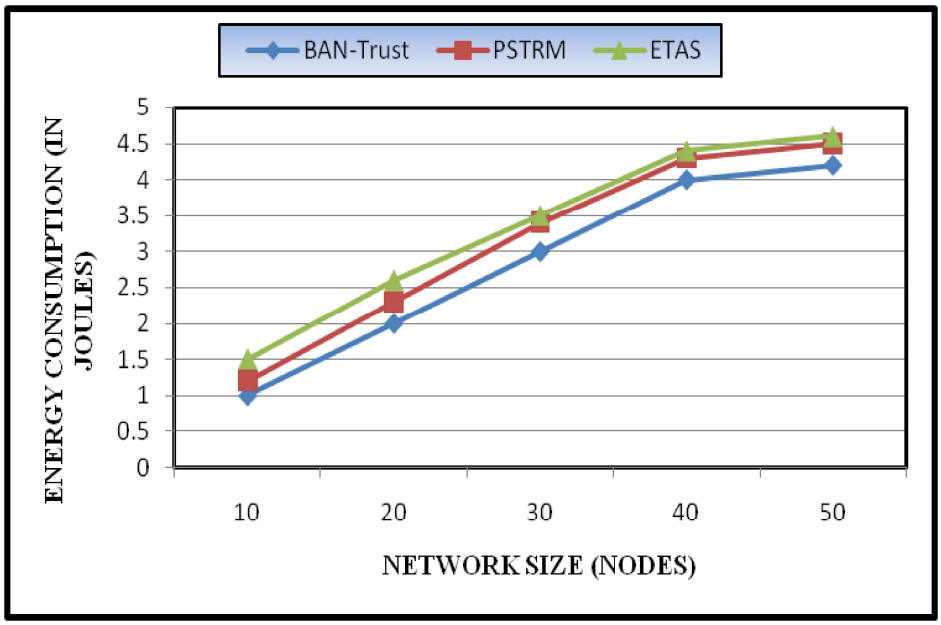


Figure 3.10: Analysis of energy consumption.

Figure 3.10 exhibits the energy utilization (in joules) of ETAS with [93][40]. Energy consumption (utilization) is the energy required to perform the intended function during network lifespan. ETAS consume less energy than other existing trust models since computational complexity and bits must store/process the minimal trust values.

The ETAS performs 9% and 2.2% better over BAN-TRUST [40] and PSTRM [93] in terms of energy consumption. ETAS computational complexity largely depends on the number of interaction among node.

We have analyzed the effect of selfish SNs on the packet delivery ratio (PDR). The PDR has been defined as the number of packets received by the base station (sink) successfully. Figure 3.11 shows that when the numbers of selfish nodes are 10%, then the ETAS packet delivery ratio is 0.9, 11% *and* 16.66 % better than PSTRM and BAN-TRUST, respectively. Moreover, in a network of 50 malicious nodes, ETAS is 32 % and 34% better than PSTRM and BAN-TRUST, respectively.

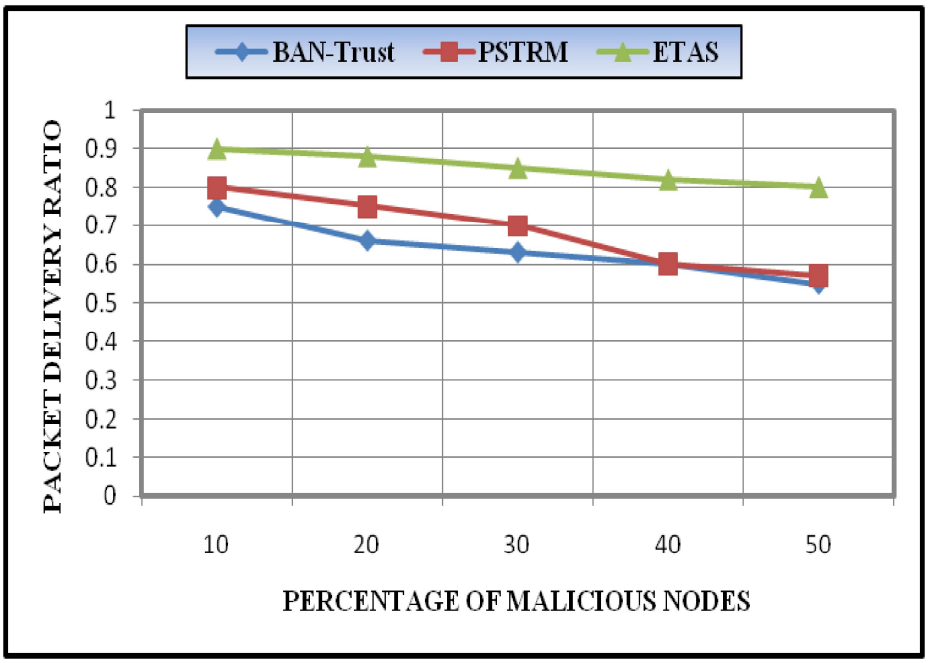


Figure 3.11: Effect of malicious nodes on the packet delivery ratio

3.6 SUMMARY

This chapter presents a weight-based efficient trust management scheme (ETAS) for BANs. ETAS is multi-factor trust management schemes that incorporate triple trust, namely communication trust, data trust and energy trust, to get the dependability status of biomedical SNs. Relay nodes are selected based on the remaining energy of nodes and distance from the sink node.

Moreover, the proposed trust management scheme considers the interaction threshold in trust evaluation. Finally, we present a hotspot node detection algorithm that effectively detects faulty nodes based on temperature, residual energy, and sensor nodes' trust values. The experimental results show the effect of successful interactions on trust value, the effect of malicious nodes on trust value and packet delivery ratio. Furthermore, comparative energy consumption is also analyzed. Finally, the proposed trust assessment scheme (ETAS) is better than existing schemes since PSTRM has already proved better than other existing trust models.

Chapter-4

An Efficient and Reliable ultra-lightweight RFID Authentication Scheme for Healthcare Systems

With the fast development of the Internet of Communication Technologies (ICT), the Internet is becoming more popular and widely used globally. Radio Frequency Identification (RFID) has become a prominent technology in healthcare systems used to identify the tagged objects. The RFID tags are attached to the billions of different healthcare devices or things in several healthcare applications. However, the tags' security and privacy are regarded as the two biggest concerns in the RFID system, where an adversary might eavesdrop, tamper or even intercept the transmitted messages.

On the other hand, the users' privacy (patients, doctors, and nurses) may be breached. In past years, a variety of ultralightweight RFID authentication schemes have been proposed in the healthcare sector. However, all these schemes were pointed out as insecure against various security attacks such as tag/reader impersonation, de-synchronization, replay, full-disclosure attacks, etc. Keeping these security flaws, we have presented an efficient and reliable ultralightweight RFID authentication scheme for healthcare systems to enhance patients' medication safety. The scheme uses simple bitwise XOR, circular left and right rotations, and a newly proposed ultralightweight reformation operation to achieve higher-level security.

The security and privacy have been done, followed by the performance analysis. The security and privacy demonstrate that the SRP2AS is resistant to several known security attacks. The performance analysis demonstrates that the fewer computation overhead with less storage on the RFID tags can be practically implemented in real-time healthcare environments. The remaining part of this chapter is structured as follows. A brief description of existing related work with their approaches, advantages, and pitfalls are inside it Section 4.1- problem formulation. Section 4.2, preliminaries have been discussed,

followed by Section 4.3, the proposed scheme has been explained in detail. Section 4.4, evaluation and analysis, has been discussed, followed by Section 4.5, summary.

4.1 PROBLEM FORMULATION

With the ongoing advancement of Internet Communication and Technologies (ICT) and the rapid development in automated medication system, RFID is gaining popularity in the healthcare environment to enhance patient medication safety. Medication errors can inflict serious harm to the patient. RFID has become a core identification technology in the pervasive computing infrastructure that uniquely identifies several objects simultaneously over a secure channel. RFID is widely used in numerous real-life applications like automatic payment, e-passport, e-healthcare systems, and supply chain, and many other fields. In the present scenario, RFID is becoming more and more prominent in healthcare systems, and it has several benefits in the healthcare domain, such as preventing possible thefts, mitigating human resources, improving productivity, and reducing the cost and time [A].

Smart healthcare is becoming an emerging field that provides several facilities, including gain health monitoring, ease access, and mobility to users (patients, doctors, nurses, and other medical staff). The information associated with patients is stored at the cloud server and can be remotely accessed over the Internet or mobile networks by the users at anyplace, anytime.

The RFID system comprises of three major components: RFID tags, RFID readers, and a back-end server. The tag is a tiny microchip embedded with the object(s). The tags can be categorized into three different ways, such as passive tags, active tags, and semi-active tags. The RFID tags are resource-constraint devices with limited computing capability and low storage and restrict the utilization of cryptographic primitives. The RFID reader reads/writes data over the tag. The backend server stores the sensitive information associated with the RFID tags.

In healthcare systems, the cloud server is used instead of the physical server or backend server because of its storage limitation. Furthermore, the cloud server has several

advantages of a backend server, such as cost-effectiveness, higher efficiency, better scalability, and disaster recovery.

The two secure and insecure communication channels have been used during message transmission. A secure communication channel has been used between reader and server. On the contrary, insecure or wireless communication channels have been used between tags (for example, patients) and readers (doctors and nurses). Due to this, security and privacy issues may arise in RFID authentication schemes.

Therefore, there is a severe need to design a safe and secure RFID-based authentication scheme to protect the patients' data privacy, patients' medical records, and his/her associated sensitive medical information. The RFID tag operates on three different frequencies, namely low frequency (LF), high frequency (HF), and ultra-high frequency (UHF). The LF has a frequency range from 125 kHz to 134 kHz and reads range up to 10 cm with the low data rate, HF has a range frequency of approximately 13.56 MHz and reads range up to 1 m with the moderate data rate, and UHF has a frequency range from 860 to 960 MHz and read range up to 10 to 15 m, respectively.

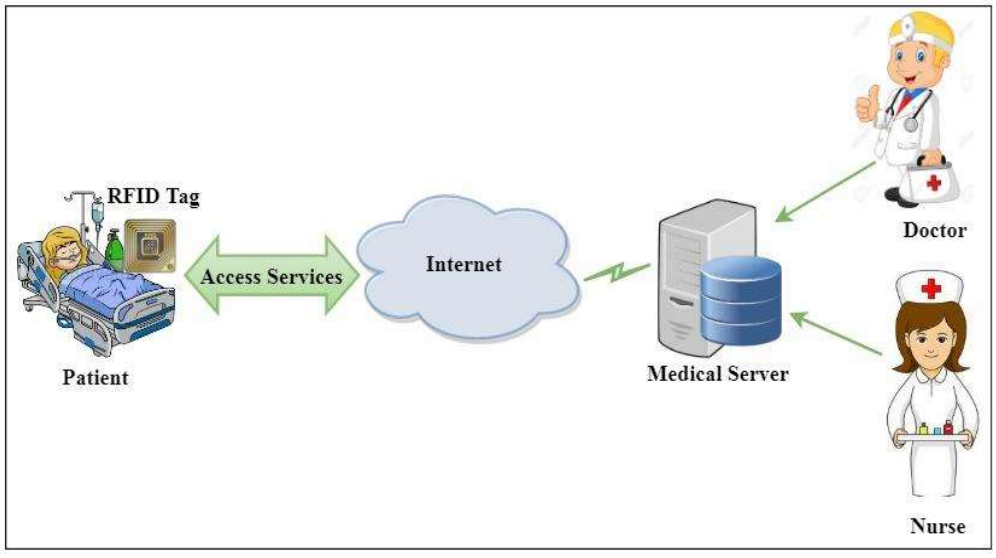


Figure 4.1: A typical scenario for the healthcare environment

Ensuring security and privacy guarantees is our proposal's main contribution; the RFID system may suffer security threats and privacy violations during communication, because the communication channe isl assumed to be wireless between tag and reader.

This chapter presents a novel reformation method to fix the shortcomings of ultra-lightweight primitives used in previous RFID authentication protocols. The new reformation method has a binary string output corresponding to two binary input strings of the same length. However, the extensive use of T-functions (XOR, AND, and OR) provides low security, or it may lead to various malicious activities in protocol designing. Therefore, any RFID authentication protocol(s) must satisfy various security properties such as eavesdropping, impersonation, loss and message interruption, location tracking.

4.1.1 Objectives

To achieve a secure RFID authentication system, we present the main objectives of our protocol which are listed as:

- To accomplish mutual authentication between tag and backend servers.
- To preserve the feature of tag anonymity and tag location privacy.
- To defeat various known security attacks, including replay attacks and de-synchronization attacks.
- To minimize the storage and computation cost of the tags.

4.1.2 Our contribution

We have discussed all the security related issues of various related existing schemes in the related work. To overcome such issues, we have presented an efficient and reliable ultra-lightweight RFID authentication scheme for healthcare systems named SR^2AS. Before introducing the scheme, the key contributions of our proposed scheme are presented as follows:

- This work has put forward an efficient and reliable ultra-lightweight RFID authentication scheme to enhance patients' medication safety.
- This chapter exploits simple bitwise XOR, circular left and proper rotations, newly proposed ultra-lightweight operations to encrypt data to reduce the tags' computation cost.
- The security analysis demonstrates that the SRP^{2}AS accomplishes mutual authentication, confidentiality, location privacy, and resists various known attacks, including impersonation, replay, and de-synchronization attacks.
- The performance comparison has been performed with the other similar existing schemes, which demonstrate that SR^{2}AP dramatically reduces the storage requirements and computational cost of tags.

4.2 PRELIMINARIES

Our proposed scheme consists of non-triangular functions such as reformation $Ref(X,Y)$ and circular left and right $Rot_{l\ or\ r}(X,Y)$ operations instead of simple T-functions (triangular functions such as XOR, OR, and AND). The reformation, circular left and right operations are defined as:

4.2.1 Definition of reformation

Consider that the two n-bit length strings X and Y are given as , where

$$X = x_{n-1}x_{n-2} \dots x_0, \quad x_i \in \{0,1\}, i = 0,1,2, \dots, n-1,$$

$$Y = y_{n-1}y_{n-2} \dots y_0, \quad y_j \in \{0,1\}, j = 0,1,2, \dots, n-1.$$

The $reformation$ of X with Y is represented as $Ref(X,Y)$, then we have

$$Ref(X,Y) = z_{n-1}z_{n-2} \dots z_0, z_i = F(x_i, y_i)$$

Where

$$F(x_i, y_i) = \begin{cases} (x_{i-1} \oplus y_i)\ mod\ n, & x_i > y_i \\ (x_i \oplus y_i)\ mod\ n, & x_i = y_i. \\ (x_i \oplus y_{i-1})\ mod\ n, & x_i < y_i \end{cases}$$

The new proposed $reformation$ of string X with Y is denoted as $Ref(X,Y)$. For better understanding of this new ultralightweight $Ref(X,Y)$ the operation, an example is illustrated below.

Now, we assume that X and Y are two 8-bits length strings: $X = 1001\ 0110$ and $Y = 0011\ 1001$

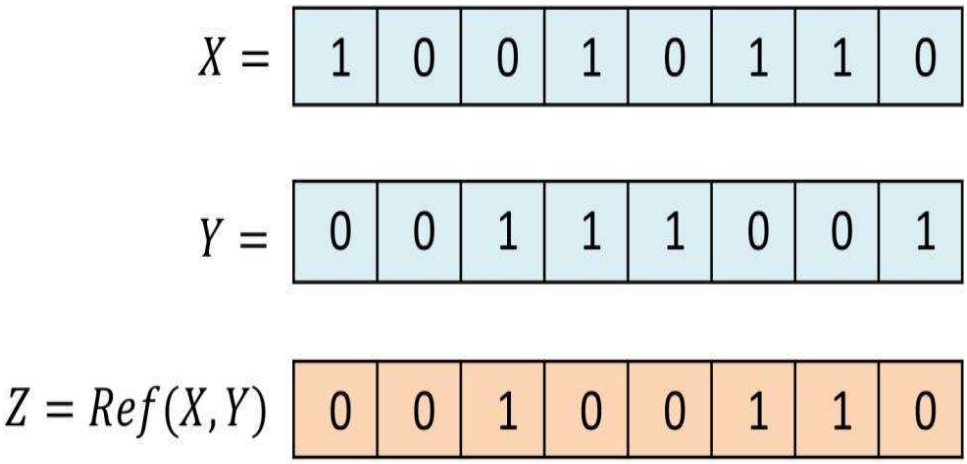


Figure 4.2: The reformation $Ref(X,Y)$ operation

4.2.2 Circular rotation operations

The left rotate operation is used in our proposed protocol [99]. The left rotate operation is represented as $Rot_l(X,Y)$. However, $Rot_l(X,Y)$ represents a left rotation of X by $wt(Y)(mod\ L)$ bits. The hamming weight of Y is $wt(Y)$ can also be defined as the number of 1's present in string Y. Hence, the outcome of $Rot_l(X,Y)$ might be X itself with the probability of $1/L$. In this case, the probability distribution will be uniform.

- **Left rotate operation** Consider that the two 8-bit length strings X and Y given as

$$X = 10110100, Y = 01011100$$

Now, we compute left rotate operation on X and Y, then we have

$Rot_l Rot(X,Y) = X$, is left rotate by $wt(Y)$. Here, the Hamming weight of string Y is $wt(Y) = 4$. Now, $wt(Y)(mod\ 8) = 4\ mod\ 8 = 4$.

Therefore, $Rot_l(X,Y) = Rot_l(X,4) = 01001011$.

- **Right rotate operation** Consider that the two 8-bit length strings X and Y are given as

$$X = 10110100, Y = 01011100$$

Now, we compute right rotate operation on X and Y, then we have

$Rot_r Rot(X,Y) = X$ is suitable to rotate by $wt(Y)$. Here, the Hamming weight of string Y is $wt(Y) = 4$. Now, $wt(Y)(mod 8) = 4\ mod\ 8 = 4$.

Therefore, $Rot_r(X, Y) = Rot_r(X, 4) = 01001011$.

Table 4.1: Notations and their descriptions

Notation	Description
$Ref(X, Y)$	Reformation operation between two same length strings X and Y
$Rot_l(X, Y)$	Circular left rotate operation of X by $wt(Y)$
$Rot_r(X, Y)$	Circular right rotate operation of X by $wt(Y)$
$wt(Y)$	Hamming weight of Y
K	A secret key shared between tag and backend server
IDS	Index pseudonym stored in the tag
ID	Identification number of an RFID tag
n_1, n_2	Random numbers generated at the reader
$\oplus$	Exclusive-OR operator
$?=$	Comparison operator
L	Number of bits in each parameter

4.3 PROPOSED SCHEME

The proposed scheme mainly comprises two phases, Phase-I introduces the initialization phase, and Phase-II introduces the authentication phase. Before initializing the authentication phase, we make first some important assumptions for our scheme.

4.3.1 Assumptions considered

We are considering some underlying assumptions for designing our proposed protocol:

- **Passive adversary ($\mathcal{P}_{\mathcal{A}}$):** The passive adversary $\mathcal{P}_{\mathcal{A}}$ eavesdrop all communications between RFID components, i.e., the tags, the readers, and a back-end server's database. Besides, $\mathcal{P}_{\mathcal{A}}$ tries to find out some sensitive information or some secret key associated with the targeted tag. However, $\mathcal{P}_{\mathcal{A}}$ cannot alter or even insert any message during the communication.
- **Active adversary ($\mathcal{A}_{\mathcal{A}}$):** The active adversary $\mathcal{A}_{\mathcal{A}}$ can insert, modify, alter, inject, or even delete any message instead of eavesdropping. $\mathcal{A}_{\mathcal{A}}$ can also impersonate a legitimate tag or reader by spoofing or replay attack and causes de-synchronization between tag and backend server by jamming or message interruption. Moreover, $\mathcal{A}_{\mathcal{A}}$ also tries to find out some sensitive information or some secret key associated with the targeted tag, same as $\mathcal{P}_{\mathcal{A}}$.

- **Secure Communication:** The communication is regarded as secure between reader and server.
- **Insecure Communication:** The communication is regarded as wireless and insecure between tag and reader, where an adversary can be easily tapped or recorded the communication data.

4.3.2 Initialization Phase

In this phase, we define some statements for each legitimate entity before initiating the authentication process which are listed as:

- The initiator stores a unique identity ID, a shared secret key K, an index IDS, the permutation operation, and the left rotate operation stored into each tag's memory space.
- For each tag, the initiator stores ID, K, a new and old pseudonym IDS_{new}, IDS_{old}. Respectively in the backend server. Initially, $IDS_{old} = IDS$ and $IDS_{new} = Null$.
- The tag and reader has a pseudo-random number generator.
- The database of the backend server stores the exact contents, including the key of all tags.
- The reformation and circular left/right rotate operation is stored in the tag's memory.
- The tag and reader have limited resources, while the backend database has no such limitations.
- The backend server database maintains the other information about the tags.

4.3.3 Authentication phase

In this phase, Figure 4.3 puts a complete description of our proposed scheme. The execution steps of SRP^{2}AS listed as:

$\boldsymbol{Step\ 1\ M_1 : R \rightarrow T : \{"Hello"\}}$

Initially, the reader sends a *"Hello"* message to the RFID tag for initializing a new authentication session.

$\boldsymbol{Step\ 2\ M_2 : T \rightarrow R : \{IDS\}}$

After receiving the message, the tag transmits an index pseudonym IDS to the RFID reader.

***Step* 3 M_3 : $R \rightarrow T : \{A, B, C\}$**

Upon receivingIDS, the reader uses this received IDS as an index to search the secrets of tags in the back-end server database. If it finds a match, the reader generates two L-bits pseudo-random numbersn_1, n_2.

Moreover, it computes the response messages A, B, and C. After that, the reader transmits these messages to the tag.

- Computes: $A = Ref(Rot_l(TID, K), ID) \oplus n_1$.
- Computes: $B = IDS \oplus n_1 \oplus n_2$.
- Computes: $C = Ref(Ref(IDS \oplus K, n_1), n_2) \oplus ID$.

***Step* 4 M_4 : $T \rightarrow R : \{D\}$**

After receiving A , B , and C , the tag extracts n_1 from A by XORing $Ref(Rot_l(TID, K), ID)$ with A and n_2 from B by XORing IDS, n_1, B. Then, the tag computes a local value of C' and checks whether $C'_{L\ or\ R} ? = C_{L\ or\ R}$, if so, the tag authenticates the reader as a legitimate reader and computes the response messages$D$. After that, the tag transmits the response message $D_{L\ or\ R}$ to the reader.

- Extracts $n_1 = A \oplus Ref(Rot_l(TID, K), ID)$.
- Extracts$n_2 = B \oplus IDS \oplus n_1$.
- Computes: $C = Ref(Ref(IDS \oplus K, n_1), n_2) \oplus ID$.
- Verify: $C'_{L\ or\ R} ? = C_{L\ or\ R}$.
- Computes: $D = Rot_r(Ref(Rot_l(ID \oplus n_1, K), R \oplus n_2)n_2)$.

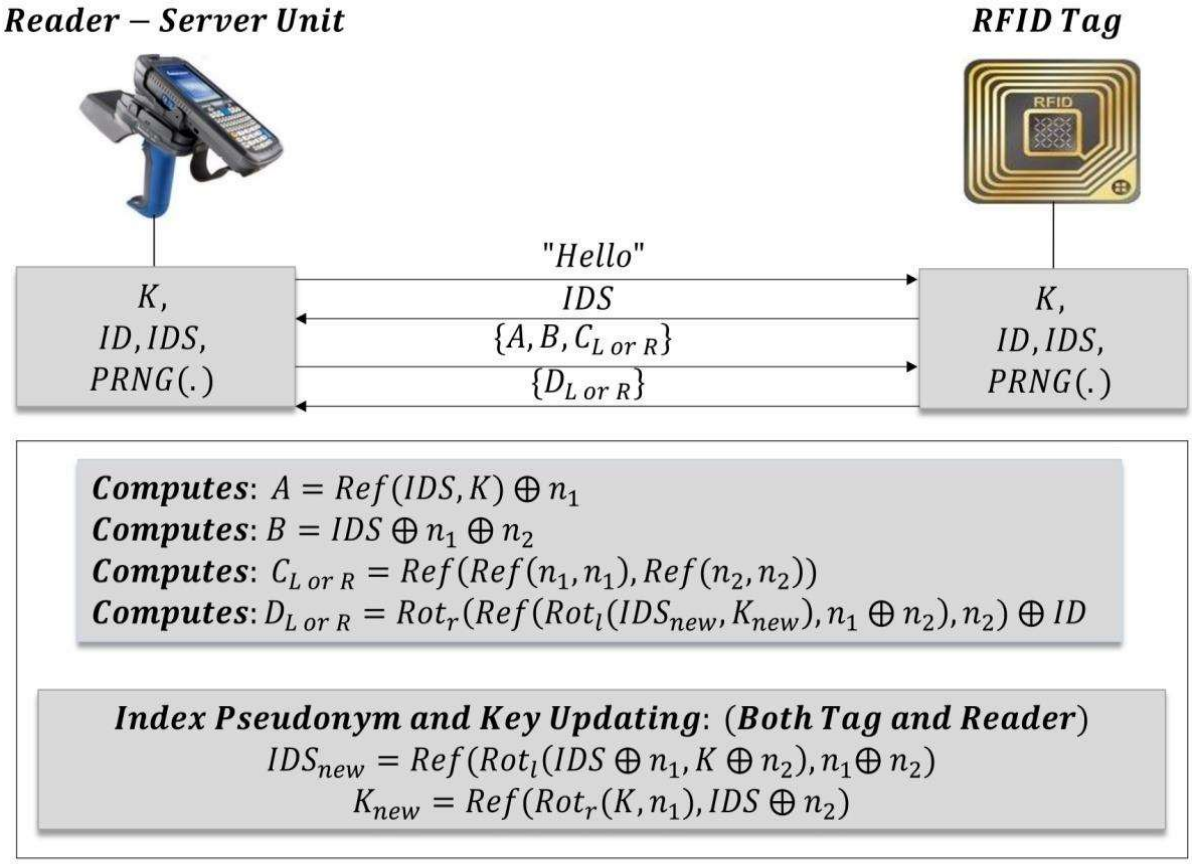
Step* 5 M_5 : *Verification at Reader − Server Unit

Upon receiving $C_{L\ or\ R}$, the reader computes a local value of D' and check whether $D'_{L\ or\ R} ? = D_{L\ or\ R}$, if so, the reader authenticates the tag as a legitimate tag and updates its index pseudonyms IDS_{old} and IDS_{new} in the database.

- Computes: $D' = Rot_r(Ref(Rot_l(ID \oplus n_1, K), R \oplus n_2)n_2)$.

- Verify: $D'_{L\ or\ R} ? = D_{L\ or\ R}$ and updates $IDS_{old} = IDS$ and $IDS_{new} = Ref\,(Rot(Ref\,(IDS \oplus R_1, K_1), K_2)$.

Figure 4.3: Proposed authentication scheme



4.4 EVALUATION AND ANALYSIS

This section summarizes a comparative study of security and privacy analysis, followed by the performance measured with four various state-of-the-arts RFID authentication schemes. All four schemes have based on the cloud server presented by Xie et al. [66] in 2013, Abughazalah et al. [71] in 2015, Fan et al. [77] in 2018, Aghili et al. [67] in 2019, respectively. All existing related authentication schemes have some pitfalls in terms of their security privacy features and computation complexities.

4.4.1 Informal Security Analysis

Table 2 summarizes the security and privacy study of SRP^{2}AS. It mainly analyzes to show the resistance against various common attacks and meet necessary security features.

4.4.2 Mutual Authentication

It means that both the legitimate participants are used in the scheme successfully to authenticate each other. It is well known that shared secrets such as TID, ID, K, random numbers n_1, n_2 are used to compute the response messages A, B, C, and D. Furthermore, the tag legitimate tag authenticates the legitimate reader by verifying the transmitted messages A and C with the corresponding local values of A' and C'. Similarly, the reader successfully authenticates the tag by verifying the transmit message D with its local value D'. Thus, SRP^{2}AS preserves the property of mutual authentication.

4.4.3 Forward Security

In forward security, the previously transmitted messages between tags and servers, cannot reveal if the adversary knows the present sensitive data, such as shared secret keys and random numbers. In SRP^{2}AS, consider an adversary which has compromised a tag and retrieves the values of ID, IDS, and K someday, then the adversary is still unable to infer or forge the previous sensitive information as well as secret keys of the same tag, because each updated equations have two random numbers. Therefore, the adversary will not compromise the previous messages from the same tag.

4.4.4 Tag Anonymity

The feature of tag anonymity is considered an important feature that prevents identity information tracking and achieves identity privacy protection. Thus, an adversary cannot obtain the tag's identities even if he/she illegitimately access the related information. In SRP^{2}AS, the tag uses its ID and index pseudonym IDS as the identity, and it does not expose them. The used pseudonym IDS and key K are updating in each successful authentication session run. Therefore, the tag ensures anonymity property. Besides, there is no use of unbalanced operations (OR, AND) in the updating process. Moreover, the adversary does not have an advantage over tag tracking via IDS. Thus, our scheme preserves the tag anonymity property.

4.4.5 Tag location Privacy

It is considered that an adversary is not permitted to trace the location of a tag or its past location. Therefore, there is an essential need to protect data and protect privacy related to users or patients'. In SRP^{2}AS, the tag's responses have changed by employing a fresh random number n_1, n_2.

Moreover, it updated the tag's value. Thus, the adversary obtains new responses in each authentication session since he/she eavesdrops on a session. Furthermore, the tag's responses are changed because of new fresh random numbers, even if the previous authentication session has been aborted.

4.4.6 Resists Impersonation Attack

In this attack, the active adversary can impersonate the channel and authenticates himself/herself as a legitimate tag/reader without compromising the confidential data. The adversary can compute the tag's response D to impersonate the tag. So, it is infeasible to compute the response for an adversary without knowing the values of ID and K. In this way, our proposed scheme strongly resists the impersonation attack.

4.4.7 Resists Replay Attack

Suppose an adversary may obtain data and use this data to authenticate as the legitimate tag. The replay attacks arises in the authentication schemes due to random numbers generated by the tag and the reader and then utilizes these numbers to compute the tag's response D.

In our proposed scheme, the tag will use different random numbers to compute the response D in each authentication session. If an adversary tries to replay previous messages, then he/she cannot obtain the random numbers. Also, the adversary cannot forge messages as a legitimate tag. Moreover, the tag device is not affected by replays of messages. Hence, SRP^{2}AS strongly resists replay attacks.

4.4.8 Resists Disclosure Attack

The adversary retrieves the shared secrets between the tag and the reader in an authentication session run. On the other hand, the passive adversary may eavesdrop the transmitted message over an insecure channel and obtain the updated shared secrets used in the next authentication session. In our proposed scheme, the adversary cannot obtain sensitive information even if he/she has response messages A, B, C, and D. Moreover, the used reformation operation makes it more complex for an adversary to compromise the tag's shared secrets. Thus, our scheme is secure against the disclosure attack.

4.4.9 Resists De-Synchronization Attack

In SRP^{2}AS, the tag and the server only update the index pseudonym IDS after a successful authentication session. We store two pseudonyms on the server-side for each tag to overcome the de-synchronization attack. One is IDS_{old} which is an index used in the previous successful authentication session and IDS_{new}, they have used in the current session.

However, if an adversary block or alters the transmitted messages in such a way, so that the consistency of the one-time pseudonym between tag and reader will break, i.e., suppose that only server will update the index pseudonym IDS, but the tag did not update due to adversary acts.

In the next authentication session, when the tag transmits its IDS to the server, the server firstly compares it with its stored IDS_{new}, but IDS is not the same as IDS_{new} because of the uncompleted previous authentication session.

So the server compares it with the old pseudonym IDS_{old}. Furthermore, the process is further considered for authentication. In this way, the proposed scheme strongly resists the de-synchronization attack.

Table 4.2 Comparison of Security and privacy features between various authentication schemes

Scheme/Features→ ↓	Xie et al. [66]	Abughazalah et al. [71]	Fan et al. [77]	Aghili et al. [67]	Proposed Scheme
SF1	✗	✗	✓	✗	✓
SF2	✗	✓	✓	✓	✓
SF3	✗	✓	✓	✓	✓
SF4	✓	✓	✓	✓	✓
SF5	✗	✗	✗	✗	✓
SF6	✓	✗	✓	✓	✓

Let us assume that SF1: Tag anonymity, SF2: Tag location privacy, SF3: Resists impersonation attack, SF4: Resists replay attack, SF5: Resists disclosure attack, and SF6: Resists de-synchronization attack.

4.4.10 Performance Evaluation

The performance evaluation of our SRP^{2}AS scheme with several existing authentication schemes in terms of computation, communication, and storage costs illustrated in Table 4.3, Table 4.4, and Table 4.5.

Computation Cost: we have utilized reformation operation $Ref(X,Y)$ and circular left rotates operation $Rot(X,Y)$ in our proposed protocol with less storage and less computational complexity and it shows better performance. The analysis shows that SRP^{2}AS is more preferable for low-cost tags for RFID systems.

Table 4.3 Computation cost comparison

Protocol→ ↓	Cost
Xie et al. [24]	$\oplus, \|\|, Hash, E_k(.), D_k(.)$
Abughazalah et al. [25]	$\oplus, \wedge, \|\|, Hash, E_k(.), D_k(.)$
Fan et al. [32]	$\oplus, \|\|, Cro, Rot$
Aghili et al. [33]	$\oplus, \|\|, Cro, Rot, MRot_K(.,.)$
Proposed Scheme	$\oplus, Rot_{l\ or\ r}, Ref$

Communication Cost: The total number of transmitted messages have been used for mutual authentication. In our proposed scheme, four communication rounds have only been

used in the whole mutual authentication process. Hence, the total communication cost is $4L$ bits.

Table 4.4 Communication cost comparison

Scheme→ ↓	Cost	No. of communication rounds
Xie et al. [24]	$8L$	2
Abughazalah et al. [25]	$7L$	2
Fan et al. [32]	$8L$	2
Aghili et al. [33]	$9L$	2
Proposed Scheme	$3L$	2

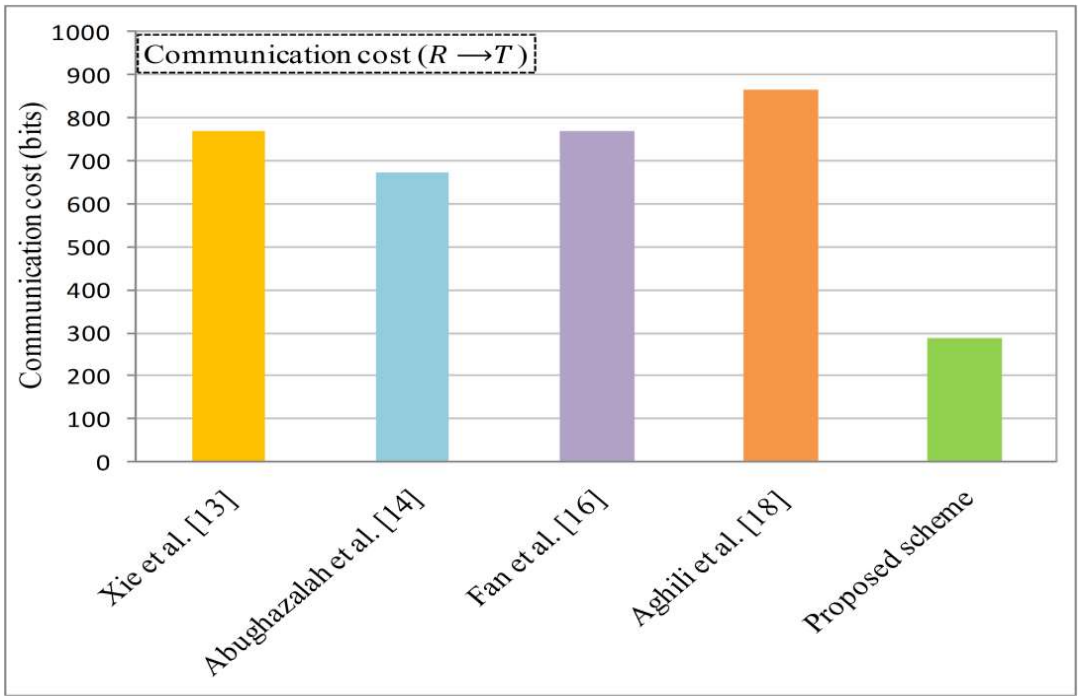


Figure 4.4: Communication overhead.

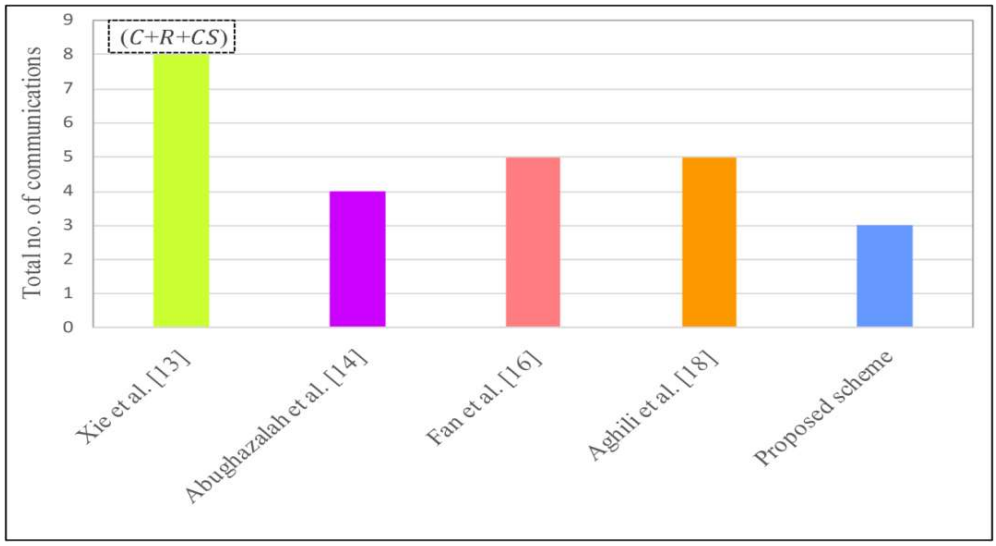


Figure 4.5: Total number of communication rounds.

Storage cost isthe number of critical elements and the static tag ID stored in the tag's internal memory. In our proposed scheme, the tag stores a total of three strings, such as its unique ID, a shared secret key K, and an index pseudonym IDS. Hence, each tag needs the storage of $3L$ bits.

Table 4.5 Storage cost comparison

Scheme→ ↓	**Entity**	**Cost**
Xie et al. [24]	T	$3L$
	$R+CS$	$7NL$
Abughazalah et al. [25]	T	$2L$
	$R+CS$	$6NL$
Fan et al. [32]	T	$4L$
	$R+CS$	$8NL$
Aghili et al. [33]	T	$4L$
	$R+CS$	$8NL$
Proposed Scheme	T	$4L$
	$R+CS$	$4NL$

T: Denotes the overhead at Tag-side, R: Denotes the overhead at reader-side, CS: Denotes the overhead at cloud server-side, N: Total number of tags in the system, and L: Denotes the number of bits stored in each parameter.

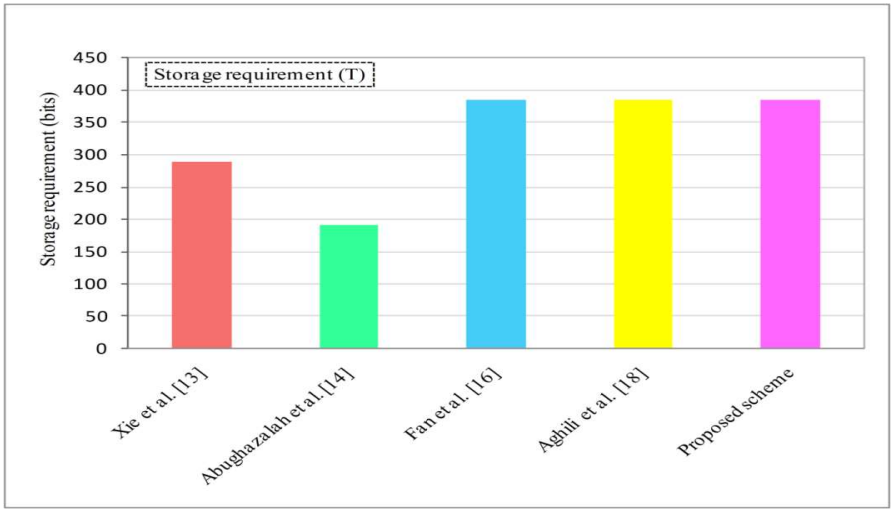


Figure 4.6: Storage requirements on the tag.

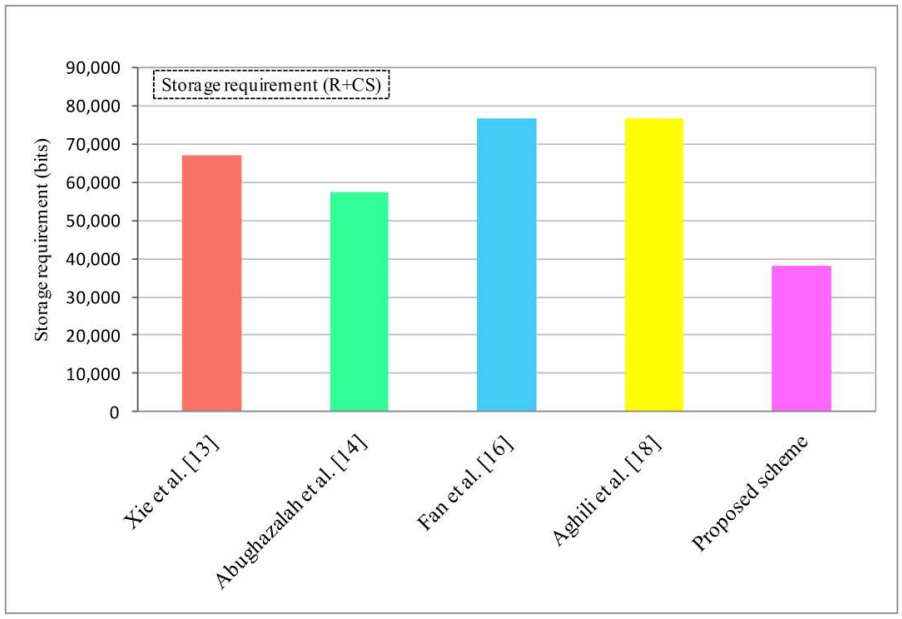


Figure 4.7: Storage requirements on the reader and cloud server

Server search cost (scalability): An RFID authentication scheme's scalability is taken into account to search a much needed record from the database in a single search attempt. In our scheme, the reader finds the matched record (such as ID, K) from the database only in a single search. Thus, the proposed scheme takes constant time, i.e., $\mathcal{O}(1)$, to search a matched record. Our scheme outperforms in terms of scalability.

Table 4.6 Comparison of server search cost between various authentication schemes

Scheme→ ↓	Xie et al. [66]	Abughazalah et al. [71]	Fan et al. [77]	Aghili et al.[67]	Proposed Scheme
Server search cost	$\mathcal{O}(N)$	$\mathcal{O}(N)$	$\mathcal{O}(N)$	$\mathcal{O}(N)$	$\mathcal{O}(1)$

4.5 Summary

Over the past years, RFID technology has been widely used in various applications globally; with regards to an RFID system, security and privacy are considered two main concerns. Considering these problems, we have put forward an efficient and reliable ultra-lightweight RFID authentication scheme (SRP^{2}AS) for healthcare systems to enhance patients' medication safety. The protocol utilizes simple bitwise XOR, circular left and right operations, and a newly proposed reformation method to resists well-known attacks.

The proposed protocol is highly efficient and also achieves higher-level security as compared to other related existing protocols. The security and privacy analysis demonstrate that SRP^{2}AS can withstand various security attacks, including tag impersonation, replay, disclosure, and de-synchronization attacks. Compared to other protocols, the performance analysis demonstrates that our scheme consumes fewer computation cost and storage on RFID tags. Therefore, the scheme shows better performance and is well suited for the health-care environment. We plan to deploy the proposed protocol in real-time healthcare systems to improve the patients' medication safety for future perspectives.

Chapter-5

Framework for Securing Patient Data Privacy in Health Care System

The cloud plays a vital role in storing and securing digital data effectively in the sharing the environment. The clouds have been established in different fields that handle sensitive data of either organizations or individuals. The health care data being the big data, is managed through several established clouds. The security of data in clouds is always under threat, especially in sharing the environment. Several security frameworks have been developed to secure the data.

However, the leakage of data cannot be averted altogether. For mitigating the security issue, a novel FCT-SKE framework is proposed. The framework encloses the fuzzy operation and cryptographic mechanism for securing the patient data. The patient's data is initially fuzzified through the triangular membership function based on the threshold of features and encrypted through the Secret Key Encryption (SKE), which is the improved form of the AES algorithm. The doctor de-fuzzifies and decrypts the data and predicts the patient's health status through the decision tree model.

The web GUI regulates the data flow from the doctor to the patient with cloud interaction. The FCT-SKE framework is assessed by its performance of prediction and security metrics. The FCT-SKE is observed to be effective in providing security than the existing AES. Similarly, the prediction of data is better than the existing models. The proposed frameworks can improve through effective feature extraction with reduced dimensionality.

This chapter has been organized as follows , Section 5.1 explains the secure data delivery in the health care system, followed by Section 5.2 explains the proposed work that contributed towards research. Section 5.3 discusses the results and discussions, followed by the conclusion of the chapter in Section 5.4.

5.1 Secure Data Delivery in Health Care System

In the modern world, the functioning of any organization or enterprises largely depends on data. The data has been observed to be a significant asset in the digital ecosystem. With a recent surge and its importance, the data requires effective management for storage and sharing. Cloud computing (CC) is found to be the solution for handling the data with beneficial features like automation, flexible deployment, configuration, connectivity, and scalability [100]. These advantages have made the organizations to adopt it; however, the process resulted in various privacy and security problems [101]. In the cloud environment, Data security has been often defined as information shielding over storage and sharing of data against the organizational inertia, loss of governance, and indefinite provider's agreement [102].

Among the various fields that handle sensitive data, the health care system is one of the predominant domains. With recent advancement, the health care system generates the data stored and transfers it electronically to enhance its quality service offered to the patients [103]. Unlike other data, the health care data is very vast, and it can be handled effectively only with the cloud service model. In general, the ecosystem of Healthcare contains several individuals, from physicians to the patient, even the lab technician. Cloud Computing helps to organize the healthcare settings including the health record of various levels [104]. However, the mentioned security issues need to mitigate for deploying health care cloud systems.

In confliction to most beliefs, the risk to face healthcare records to host in the cloud servers from being attacked internally from those people who are authorized user to have credentials for accessing the data inside the organization, the administrations of the database or its managers of keys are attacker who is pointedly shoddier than the other kind of exterior attacks [105]. The patients had to store their data in the centralized cloud to secure it from any attacks [106]. Even cryptography key mechanism and role-based access control are exposed to cyber-attacks to increase the probability of crucial leakage through compromise in access policy [107-108]. Some existing solutions suffer from overheads, latency with user constrained environment.

5.2 PROPOSED WORK

For resolving the security concern over the health care big data in the multi-user cloud environment, a novel Fuzzy Cipher Text-Spiral Key Encryption (FCT-SKE) is proposed. The key for encrypting the data gets accomplished by enhancing the Advanced Encryption Standard (AES). After obtaining the final fundamental matrix, it gets subjected to the spiral mechanism for key generation. The data in the FCT-SKE framework provides additional security through the fuzzy operation. The patient data is initially fuzzified and encrypted to store in the cloud. Hence even with the slightest possibility of key leakage, the attacker cannot access the data directly as it is fuzzified.

For securing the healthcare system data effectively in a cloud environment through the projected FCT-SKE framework, the following contributions have been carried out:

a. The patient data is fuzzified effectively before being encrypted with the security keys
b. The spiral operation is adopted to modify the pattern of the security key and make it unbreakable.
c. The prediction over the patient data is performed effectively through the decision tree algorithm
d. The performance analysis is carried out on both the security and prediction metrics to validate the proposed FCT-SKE framework.

5.2.1 Preliminaries and Fuzzy Logic

Fuzzy logic is a renowned concept; it also makes sense to the process related to the vague or ambiguous value and deals with Boolean Logic Data [109]. Both are featuring values of their range lying within 0 to 1 through a membership function. Membership Function of Triangular helps fuzzify the clinical dataset and gather more information about the medical patient. This triangular curve of a vector ‘a’ also depends on the other three scalar parameters. [110-111], x, y, and z, as given by

$$\mu_T(a: x, y, z) = \begin{cases} \dfrac{a-x}{y-x} & x < a \leq y \\ \dfrac{a-b}{z-x} & b < a \leq z \\ 0 & otherwise \end{cases} \ldots\ldots\ldots (1)$$

AES does all of its evaluation on bytes rather than using bits. Generally, it is employed with sizes of three keys that consist of 128, 192, and 256 bits with the total number of rounds being 10, 12, and 14, respectively. To encrypt and decrypt, AES employs as given in []. The plain text transformed into the cypher-text by the round number, i.e. Nr, that identified the key's different bit.

5.2.2 SYSTEM ARCHITECTURE

The proposed FCT-SKE architecture for securing the healthcare data inside the cloud has been given in figure 5.1. The proposed framework has been developed with two different data flows. The first flow occurs between the user and the cloud to be considered as UC flow. Another flow occurs between the cloud and doctor to be reflected as CD flow. The operations and the components in each flow differ and aid in effectively securing patient data privacy.

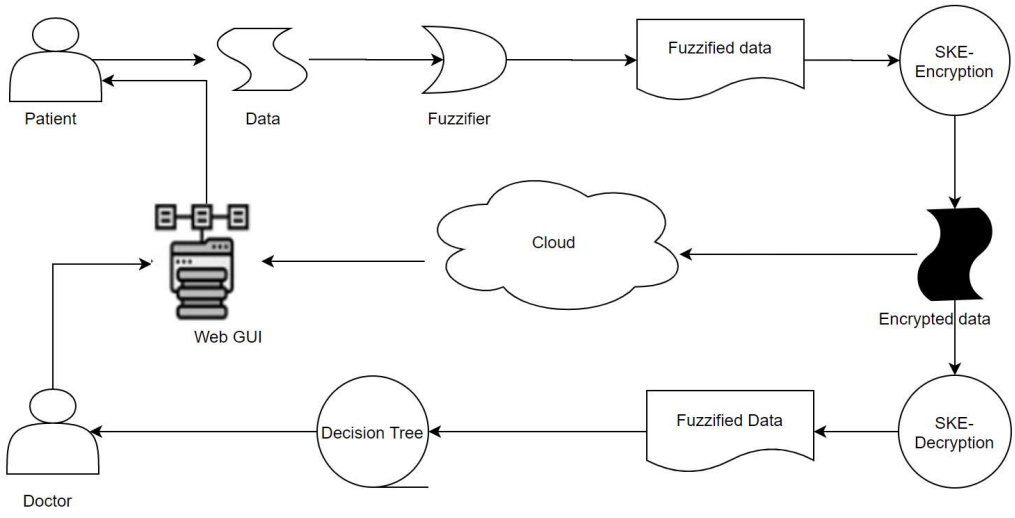


Figure 5.1: The proposed framework for FCT-SKE

UC data flow: The data from the patient is initially collected based on their health status. The obtained patient data is initially subjected to fuzzy logic operation with the fuzzifier. The fuzzy logic operation converts the patient data in terms of 1 and 0. The fuzzified data is then encrypted using the proposed SKE algorithm; the encrypted fuzzified patient data is uploaded to the cloud.

CD data flow: The doctor or any medical practitioners can download the patient cloud data. The downloaded encrypted data is decrypted effectively through the SKE algorithm. After decrypting the patient data is provided to the decision tree for predicting the patient's health status, the predicted results is provided to the doctor or medicinal practitioners who process their suggestions to the user.

Web GUI: It is an essential component in the proposed framework. It establishes the data communication possible among the patient, doctor and the cloud. The WebGUI obtains patient and doctors' information from the cloud, and then the doctors send their recommendation to the user through the WebGUI.

5.2.3 SECURITY MECHANISM

Fuzzification: The proposed framework encloses the initial fuzzy operation and the cryptic mechanism to secure the cloud. The fuzzy operations are generally rule-based, and the rule for fuzzifying the patient data is defined below.

The fuzzification process begins with estimating min-max values for each feature, and its average value forms the threshold.LetX_{ij}be the patient data feature where 'i' represent the individual patient and j represent the order of feature. Every feature is assigned with a certain minimum threshold value $th_{j.}$ The rule for fuzzification has been given in equation (1) as,

$$minimum\ feature\ value = \min(X_{ij}) \dots\dots (2)$$

$$maximum\ feature\ value = \max(X_{ij}) \dots\dots (3)$$

$$mean\ value\ (or) Threshold\ value = \frac{\min(X_{ij}) + \max(X_{ij})}{2} \dots\dots (4)$$

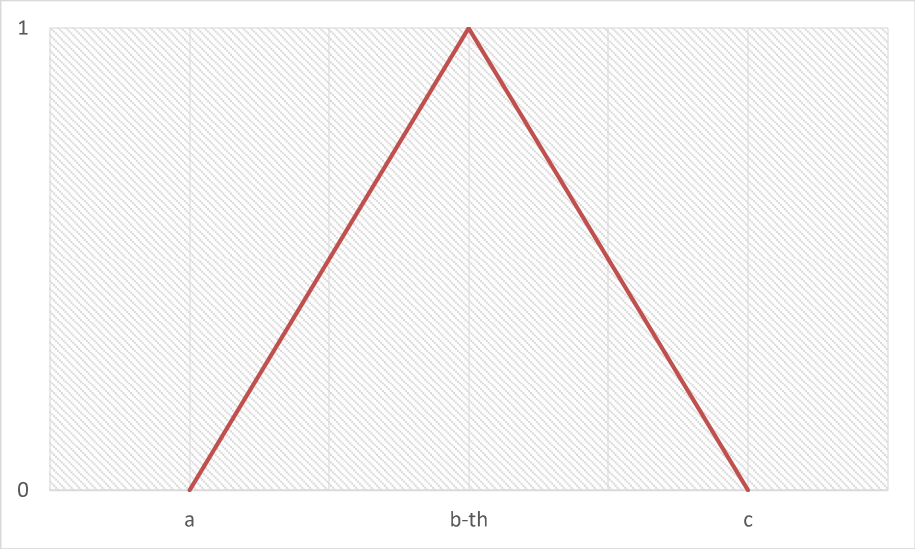


Figure 5.2: Triangular function for features.

Encryption: The fuzzified data encrypted with the proposed SKE algorithm, which is the enhanced AES model. The key generation improved with the spiral technique established over the final key-matrix. Let us consider the matrix T with size 4x4 generated based on eth fuzzified data through the HEX approach. Two matrices C and K, get established as the constant matrix and critical matrix of the same size as the matrix T., Another constant matrix of size 16x16 established as the S_{box}.

Algorithm for encryption

Input: matrix T, C, K and S_{box}

Output: Doctor Private Key

1: get T

2: $T \leftarrow Sub - Bytes(K, S_{Box})$

3: $T(a, b) \leftarrow S_{Box}(x, y)$

4: $T \leftarrow Shift - rows(T)$

5: $if\ a = 1\ or\ b = 1 or\ a = b$

6: $T\ (a, b)\ \leftarrow\ T\ (a, b)$

7: else If a<b

8: $T\ (a, b)\ \leftarrow T\ (a + 1, b - 1)$

9: else if a > b

10: $T\ (a, b)\ \leftarrow T\ (a - 1, b + 1)$

11: $T\ \leftarrow Mix\_Column(T, C)$

12: $for\ a\ \rightarrow\ 1\ to\ 4$

13: $T(:,\ i) \leftarrow\ C\ x\ T\ (:,\ i)$

14: $T\ \leftarrow Add\_Round\_Key\ (T, K)$

15: $T(:,\ i) \leftarrow\ T(:,\ i)\ \oplus K(:,\ i)$

16: $Randomspiral\ (forward, backward)$

17: Get the private doctor for its crucial PR

18: end

Decryption: Since AES is the symmetrical algorithm, all the rounds are involved in generating the key reversed once the decryption key is provided. The decrypted data is provided to the decision tree model for prediction.

5.2.4 SECURITY AND PREDICTION MODEL

Security is an essential aspect of preserving patient data privacy in the cloud environment. Each data related to the patient is initially fuzzified based on the triangular membership function so that the fuzzified data have been encrypted with the proposed SKE algorithm, and this proposed SKE algorithm is the enhanced form of the AES algorithm. Let K be the final key-matrix that gets generated with the traditional AES algorithm.

$$K = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 \\ 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \end{bmatrix}$$

Two spiral techniques are proposed in the framework; the first technique is the forward spiral technique and initiated when the random value has been chosen as 1. The second technique is the reverse spiral technique and gets initiated when the random value is chosen as -1. These forward and reverse spiral techniques reorganize the traditional key structure, making it robust and secure. The model keys from the given key matrix K are as follows.

When random value = 1

The key generated is 0 1 9 8 16 17 25 24 2 3 11 10 18 19 27 264 5 13 12 20 21 29 28 6 7 15 14 22 23 31 30

When random value = -1

The key generated is 31 30 22 23 15 14 6 7 29 28 20 21 13 12 4 527 26 18 19 11 10 2 3 25 24 16 17 9 8 0 1

The proposed framework has a prediction model to predict the health status of the patient. The prediction model is constructed through the decision tree. The decision tree model is generated with the dataset initially and the prediction model is used to construct. The decrypted data is de-fuzzified and provided to the decision tree model to predict the patient heath and provide it to the doctor for further examination. The algorithm for the constructed decision tree is as follows:

Input: R is the Dataset record, T is the Training Data, and there are attributes_available to compute in the next branch.

Output: The output will be in the model of the Decision Tree.

Step 1: we create node N.

Step 2: if the entire records available in the T have a similar target class.

Step 3: then, it returns the N as its leaf node along with its target class.

Step 4: if it is having an empty $attributes\_available$

Step 5: then, it returns N as its leaf node along with the top target class for its records.

Step 6: Get the $best\_attribute$ as $(T, attributes\_available)$

Step 7: the formula is:

$$attributes\_available = attributes\_available - best\_attribute.$$

Step 8: it splits the records which have been based on its $best\_attribute(best\_attribute, T)$

//for every splits, there will be a grown subtree that calls the

//to build a model of decision tree

Step 9: it splits Ti of the T for each splits for the $best\_atttribute$

Step 10: it attaches a new returned node to it $(split\ records\ Ti, attributes\_available)$

Step 11: end of the For Loop

5.3 RESULT AND DISCUSSION

This proposed framework for the security of data available in the cloud has been implemented by using data and Java after accumulating inside dropbox. The cloud interface is achieved by using the JAX-WS web services held with Apache Tomcat. This SQL database gets updated at the end of the server to store data. Java supported the internet browser to create the client-side. The rest of the basic configuration uses the Intel processor with a memory of 16 GB at 2.45 GHz with a disk of 1 TB storage capacity. The heart disease dataset from the UCI repository employed 19 features for analyzing the proposed framework's performance. The threshold value for each component is given below in table 1.

The FCT-SKE framework is analyzed based on the time involved in encrypting, decrypting, uploading and downloading, along with key generation time—the prediction performance is estimated with accuracy and error values.

Table 5.1: Feature for heart disease and its threshold values

Feature	Threshold value
Sex	1.5
Body Weight	101.5
High	170.5
Smoker	0.5
Alcohol	0.5
Limb-Ache	0.5
Systolic BP	183
Diastolic BP	102
Max. Systolic BP	230
Effusion	0.5
Artery Stenosis	0.5
Heart Failure	0.5
Palpitation	0.5
Carotid	0.5
Serum Creatinine	462.5
Serum Potassium	3.9
Serum Sodium	137.5
Uric Acid	373.5
Hypertension Type	6.3

5.3.1 SECURITY ANALYSIS

Key Generation Time

The time has been taken for generating the keys based on the number of users. From the obtained results, it has been observed that the time taken to generate a key is the minimum when the number of users is less. It increases steadily with the number of users, as shown in figure 5.3. In comparison with the traditional AES algorithm, the time taken for key generation is slightly less.

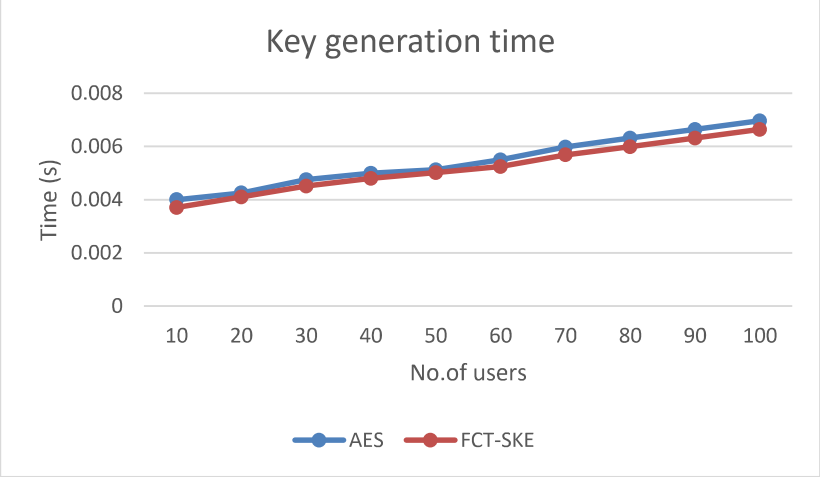


Figure 5.3: Key generation time

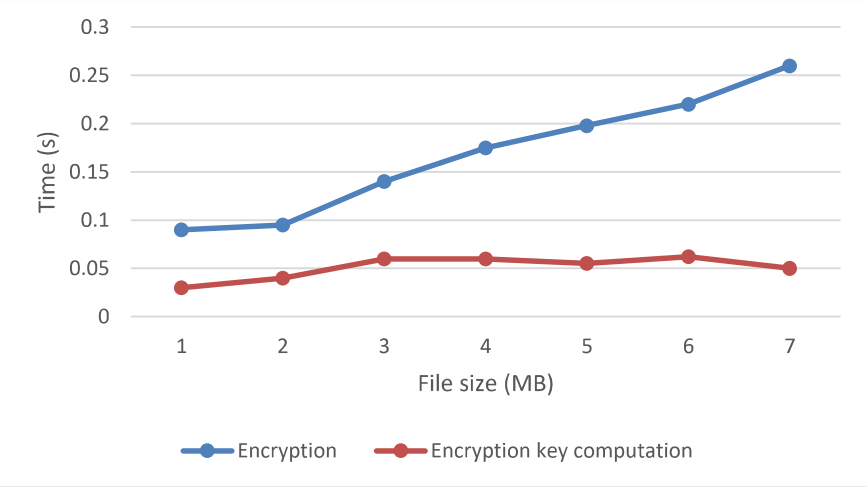


Figure 5.4: Time for encryption

Time for uploading, Encryption, Downloading and Decryption

The following significant time parameter is the time incurred for uploading, downloading, encryption and decryption. As mentioned above, the time taken for all the process is the minimum when the file size is the minimum, and it increases with the increase in file sizes—the time for the encryption process and encryption key computation given in figure 5.4. The figure observed that the time for encryption computation is almost the same for varying file sizes. A similar pattern is observed in the decryption computation figure 5.7. However, both the encryption and decryption process time increase with increment in file size, as in figure 6 and 9. Both the uploading and downloading time for files increases by increment in the file size, as in figure 5.5 and 5.6. The time taken for downloading the file is more than uploading it. A similar aspect is found among encryption and decryption time.

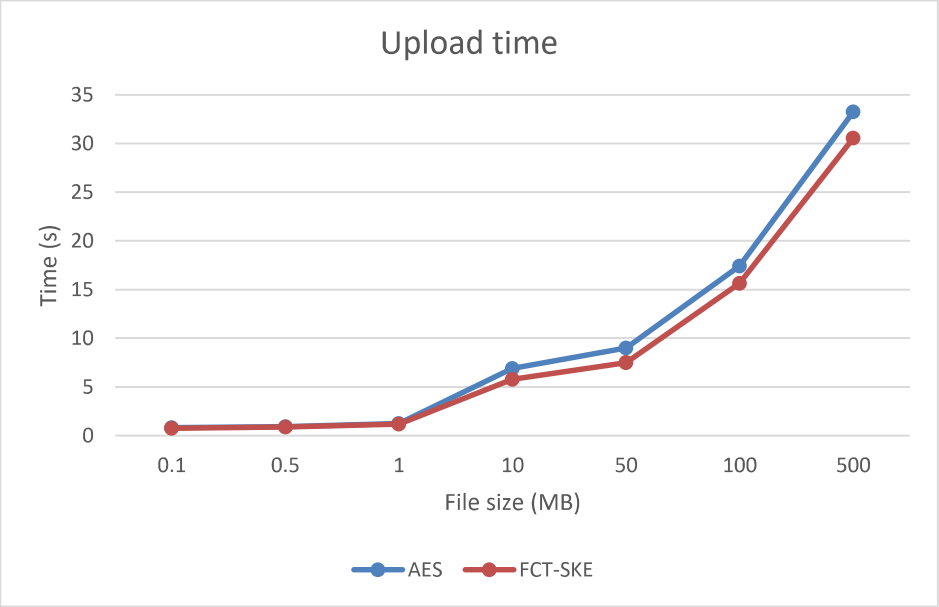


Figure 5.5: Time for uploading

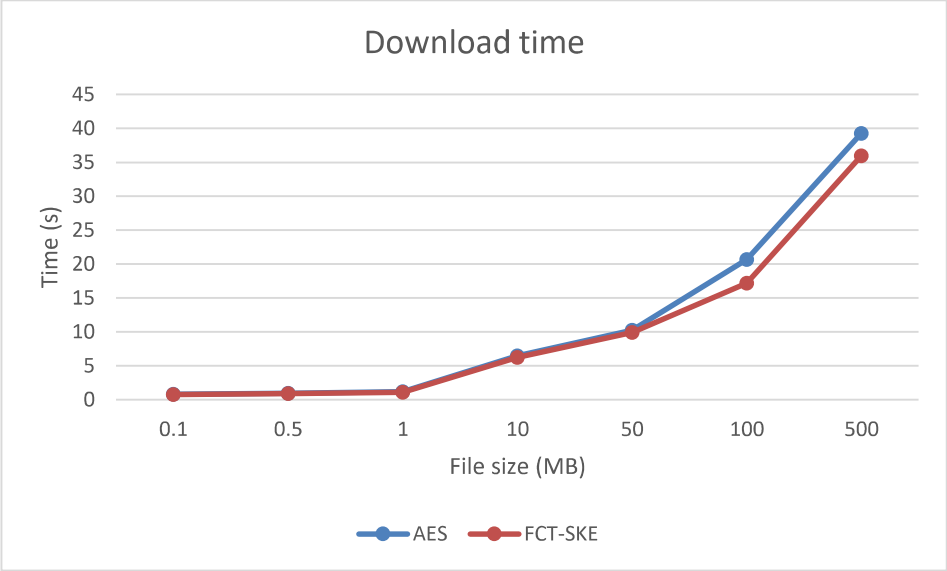


Figure 5.6: Time for downloading

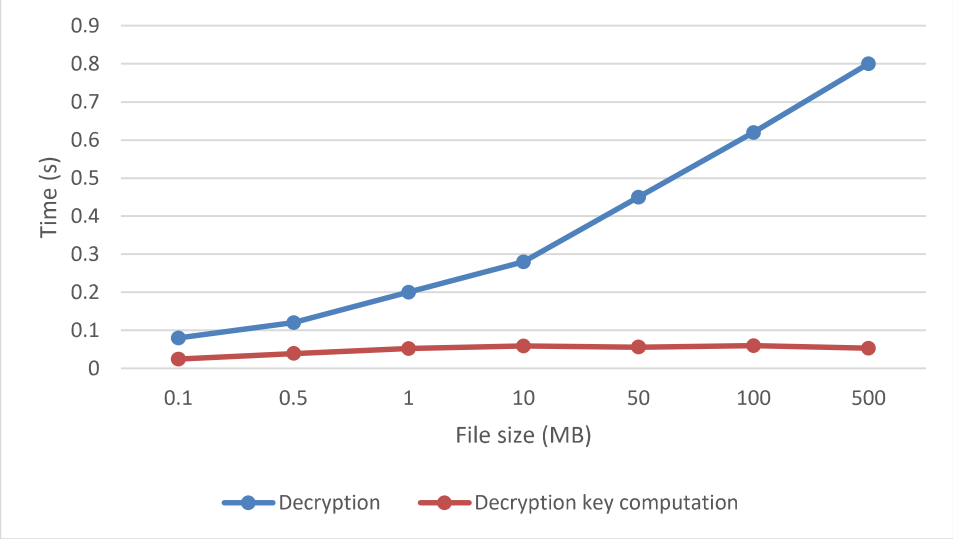


Figure 5.7: Time for Decrypting

Prediction Analysis

The decrypted data is de-fuzzified and used for predicting the heart disease of the patient using the decision tree algorithm—the performance of the decision tree algorithm in predicting heart disease as given in table 5.2.

Table 5.2: Prediction performance

Parameters	Values
Correctly Classified Instance	78.118 %
Incorrectly Classified Instances	21.882 %
Kappa statistic	0.2612
Mean absolute error	0.1425
Root mean squared error	0.2957
Relative absolute error	81.8416 %
Root relative squared error	95.7428 %

The accuracy of the decision tree in the proposed model is compared with the existing models. The accuracy of the proposed model is about 78.118%. The obtained accuracy is compared with the existing ANN, C4.5 and its combined ANN-C4.5 [112] algorithm as in figure 5.8.

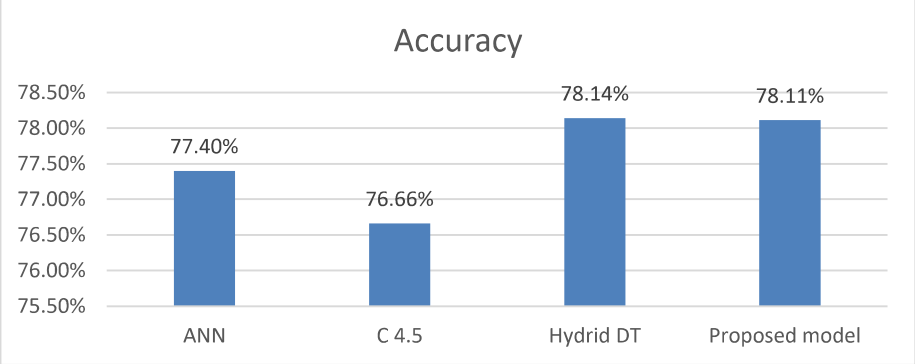


Figure 5.8: Comparison of the Prediction model

5.4 SUMMARY

The novel framework of FCT-SKE is proposed to secure the privacy of the health care data in the cloud. The cloud encloses the fuzzy operation and an improved AES based encryption employed over the patient health data. In the proposed framework, the health data initially fuzzified by using the triangular membership function based on the established threshold function. The fuzzified data is encrypted with the proposed SKE algorithm. The key matrix generated through the AES and the key generation is modified with spiral operation in forward and reverse order. The data are uploaded securely into the cloud. The doctors can download and decrypt the data through the private key. The decrypted data is provided to the eth decision tree model to predict the patient's health status. The web GUI governed the distribution of results among the respective patients from doctors through the cloud.

The performance of the proposed FCT-SKE framework is evaluated based on security and prediction metrics. The security metrics involved are the time for encryption, decryption and uploading and downloading of data. The prediction metrics is evaluated with accuracy and error metrics. Both the security and performance metrics compared with the existing frameworks. The performance of eth proposed framework is effective on security metrics and almost bettered the prediction models on decision trees. Future work may involve increased prediction performance through effective feature extraction with reduced dimensionality.

Chapter-6

Conclusion and Future work

Wireless systems application such as Health care system, which has wireless body sensor networks (BSNs), has recently emerged and has suggested vital requirements for a variety of telehealth applications such as blood pressure monitoring and sugar level monitoring without dependence on any fixed (static) infrastructure such as hospitals. The chapter recommends a novel and efficient, lightweight trust management scheme (ETAS) deployed in health applications domains and does not rely purely on any encryption technique. Trust management (in BANs) has been found as a useful tool to improve cooperation among sensor nodes, security, and reliability. Existing trust models for BANs impose high overhead (communication, memory) and cannot improve sensor nodes' dependability. Moreover, previous trust models do not consider data trust, patient's body temperature, and energy trust, which play a significant role in protecting and decision-making in body sensor networks. The chapter focuses on developing an exciting comprehensive, novel trust estimation framework for body sensor networks to enhance reliability, dependability, security by isolating compromised (malicious, faulty, hotspot) nodes with great resource (power, memory) efficiency.

This chapter presents a weight-based efficient trust management scheme (ETAS) for BANs. ETAS is multi-factor trust management schemes that incorporate triple trust, namely communication trust, data trust and energy trust, to get the dependability status of biomedical SNs. Relay nodes are selected based on the remaining energy of nodes and distance from the sink node. Moreover, the proposed trust management scheme considers the interaction threshold in trust evaluation. Finally, we present a hotspot node detection algorithm that effectively detects faulty nodes based on temperature, residual energy, and sensor nodes' trust values. The experimental results show the effect of the percentage of successful interactions on trust value, the effect of malicious nodes on trust value and packet delivery ratio. Furthermore, comparative energy consumption is also analyzed. Finally, the proposed trust assessment scheme (ETAS) is better than existing schemes since PSTRM has already proved better than other existing trust models.

This research chapter discussed a logarithm based realistic trust model to increase security, reliability, and dependability (i.e., cooperation) among PSNs. The proposed scheme (L-RTAM) uses time window concepts to calculate direct communication, indirect communication trust, and data trust. L-RTAM increase and decrease the trust score of PSNs according to their cooperative nature. The experimental results show that L-RTAM is effective in trust evaluation, malicious PSNs detection, and False alarm generation. In the future, we will try to add energy trust to the existing trust model. Moreover, we are willing to examine the scalability, rate of convergence, and average energy consumption of the L-RTAM.

Over the past years, RFID technology is widely used in various applications across the world. With regards to an RFID system, security and privacy is considered as two main

concerns. Considering these problems, we have put forward an efficient and reliable ultralightweight RFID authentication scheme (SRP^2AS) for healthcare systems to enhance patients' medication safety. The protocol utilizes simple bitwise XOR, circular left and right operations, and a newly proposed reformation method to resist well-known attacks. The proposed protocol is highly efficient and also achieves higher-level security as compared to other related existing protocols. The security and privacy analysis demonstrate that SRP^2AS can withstand various security attacks, including tag impersonation, replay, disclosure, and de-synchronization attacks. Compared to other protocols, the performance analysis demonstrates that our scheme consumes fewer computation cost and storage on RFID tags. Therefore, the scheme shows better performance and is well suited for the healthcare environment. We plan to deploy the proposed protocol in real-time healthcare systems to improve the patients' medication safety for future perspectives.

As we all know better, IoT is a vast domain that contains lots of promising technologies, whereas RFID is one of the core identification technology that comes under the IoT environment and has a paradigm in the various fields of the healthcare system. With the rapid development of medical technologies, there is an essential need to deploy more and more privacy associated with medical data. This chapter presents a secure RFID-based authentication protocol for the IoT healthcare environment that ensures some security and privacy features, less communication cost, and less computational operations than many existing schemes. In the medical environment, an RFID system receives more and more attention for security purposes.

The novel framework of FCT-SKE is proposed to secure the privacy of the health care data in the cloud. The cloud encloses the fuzzy operation, and an improved AES based

encryption employed over the patient health data. In the proposed framework, the health data is initially fuzzified by using the triangular membership function based on the established threshold function. The fuzzified data is encrypted with the proposed SKE algorithm. The key matrix is generated through the AES and the key generation is modified with spiral operation in forward and reverse order. The data are uploaded securely into the cloud. The doctors can download and decrypt the data through the private key. The decrypted data is provided to the eth decision tree model to predict the patient's health status. The web GUI governed the distribution of results among the respective patients from doctors through the cloud.

The performance of the proposed FCT-SKE framework is evaluated based on security and prediction metrics. The security metrics involved are the time for encryption, decryption and uploading and downloading of data. The prediction metrics is evaluated with accuracy and error metrics. Both the security and performance metrics are compared with the existing frameworks. The performance of eth proposed framework is effective on security metrics and almost bettered the prediction models on decision trees. Future work may involve increased prediction performance through effective feature extraction with reduced dimensionality.

6.1 Future Work

The aim of this work is to propose a secure mechanism for Wireless Systems Applications. The main contributions are authentication, trust management and privacy of health care systems. The future scop of work is as follows:

1. The trust mechanism is based on weight mechanism which may improve using Fuzzy logic, game theory.

2. The proposed authentication scheme extensive use of T-functions (XOR, AND, and OR) provides low security, or it may lead to various malicious activities in protocol designing. The scheme may use the BAN logic to improve the performance.

3. The propsed solution may utilized the Mechine Learning Algorithms for trust calculation and privacy.

References

[1] Farhana Jabeen, Zara Hamid, Adnan Akhunzada,Wadood Abdul,and Sanaa Ghouzali, "Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues" IEEE Access (2018): Digital Object Identifier 10.1109/ACCESS.2018.2810337.

[2] Ghamari, Mohammad, et al. "A survey on wireless body area networks for ehealthcare systems in residential environments." Sensors 16.6 (2016): 831.

[3] Xuemin (Sherman) Shen and Xiaodong Lin "Bibliography on Secure E-Healthcare Systems" Broadband Communications Research (BBCR) Group Department of Electrical and Computer Engineering University of Waterloo, Waterloo, Ontario, Canada

[4] F. Bao, I. Chen, M.Chang, and J. Cho,(2012) "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Netw. Service Manag., vol. 9, no. 2, pp. 169–183

[5] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee, (2009) "Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698–1712

[6] D. Kumar, T. C. Aseri, and R. B. Patel, (2009) "EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks," Comput. Commun., vol. 32, no. 4, pp. 662–667

[7] G. V. Crosby, N. Pissinou, and J. Gadze (2006) "A framework for trust-based cluster head election in wireless sensor networks," in Proc. Second IEEEWorkshop on Dependability and Security in Sensor Networks and Systems, pp. 10–22.

[8] O. Younis and S. Fahmy, (2004) “HEED: A hybrid, energy-efficient, distributed clustering approach for Ad-Hoc sensor networks,” IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379

[9] H.S. Ng, M.L. Sim, and C.M. Tan, (2006) “Security Issues of Wireless Sensor Networks in Healthcare Applications,” BT Technology J., vol. 24, no. 2, pp. 138-144

[10] Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul (2019) "A Novel and Comprehensive Trust Estimation Clustering-Based Approach for Large Scale Wireless Sensor Networks." IEEE Access 7 58221-58240.

[11] Aziz, Ahmed, and Karan Singh (2019) "Lightweight Security Scheme for Internet of Things." Wireless Personal Communications 104, no. 2, pp. 577-593.

[12] Omala, Anyembe Andrew, Kittur P. Kibiwott, and Fagen Li. "An efficient remote authentication scheme for wireless body area network." Journal of medical systems 41, no. 2 (2017): 25.

[13] Bhangwar, Ali Raza, Pardeep Kumar, Adnan Ahmed, and Muhammad Ibrahim Channa. "Trust and thermal aware routing protocol (TTRP) for wireless body area networks." Wireless Personal Communications 97, no. 1 (2017): 349-364.

[14] Priya, Nachimuthu Sangeetha, R. Sasikala, Srinivasan Alavandar, and L. Bharathi. "Security Aware Trusted Cluster Based Routing Protocol for Wireless Body Sensor Networks." Wireless Personal Communications 102, no. 4 (2018): 3393-3411.

[15] Chitra, A., and G. R. Kanagachidambaresan. "Fault aware trust determination algorithm for wireless body sensor network (WBSN)." In Proceedings of first international conference on smart system, innovations and computing, pp. 469-476. Springer, Singapore, 2018.

[16] Ching, Ke Wan, and Manmeet Mahinderjit Singh. "Wearable technology devices security and privacy vulnerability analysis." International Journal of Network Security & Its Applications 8, no. 3 (2016): 19-30.

[17] Kumar, P. and Lee, H.J., 2012. Security issues in healthcare applications using wireless medical sensor networks: A survey. Sensors, 12(1), pp.55-91.

[18] https://www.esecurityplanet.com/mobile/apple-watch-security-risks-and-benefits

[19] Sundaravadivel, Prabha, Elias Kougianos, Saraju P. Mohanty, and Madhavi K. Ganapathiraju. "Everything you wanted to know about smart health care: Evaluating the different technologies and components of the internet of things for better health." IEEE Consumer Electronics Magazine 7, no. 1 (2017): 18-28

[20] Bui, Vinh, Richard Verhoeven, Johan Lukkien, and Rafal Kocielnik. "A trust evaluation framework for sensor readings in body area sensor networks." In Proceedings of the 8th International Conference on Body Area Networks, pp. 495-501. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2013.

[21] Yu, Han, Zhiqi Shen, and Cyril Leung. "Towards trust-aware health monitoring body area sensor networks." International Journal of Information Technology 16, no. 2 (2010): 1-20.

[22] Boukerche, Azzedine, and Yonglin Ren. "A secure mobile healthcare system using trust-based multicast scheme." IEEE Journal on Selected Areas in Communications 27, no. 4 (2009): 387-399.

[23] He, Daojing, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V. Vasilakos. "A distributed trust evaluation model and its application scenarios for medical sensor networks." IEEE Transactions on Information Technology in Biomedicine 16, no. 6 (2012): 1164-1175.

[24] Javadi, Saeideh Sadat, and M. A. Razzaque. "Security and privacy in wireless body area networks for health care applications." In Wireless networks and security, pp. 165-187. Springer, Berlin, Heidelberg, 2013.

[25] Wu, Guo Wei, Zuo Song Liu, and Poria Pirozmand. "A fuzzy trust model for public key distribution in body area networks." In Advanced materials research, vol. 989, pp. 4837-4840. Trans Tech Publications, 2014.

[26] Wu, Xu. "A lightweight trust-based access control model in cloud-assisted wireless body area networks." International Journal of Security and Its Applications 8, no. 5 (2014): 131-138.

[27] Remu, Sm Rakibul Hasan, Md Omar Faruque, Rezowan Ferdous, Md Murshedul Arifeen, Sudman Sakib, and SM Salim Reza. "Naive Bayes based Trust Management Model for Wireless Body Area Networks." In Proceedings of the International Conference on Computing Advancements, pp. 1-4. 2020.

[28] Farhana Jabeen, Zara Hamid, Adnan Akhunzada,Wadood Abdul,and Sanaa Ghouzali, "Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues" IEEE Access (2018): Digital Object Identifier 10.1109/ACCESS.2018.2810337.

[29] Li, Ming, Shucheng Yu, Joshua D. Guttman, Wenjing Lou, and Kui Ren. "Secure ad hoc trust initialization and key management in wireless body area networks." ACM Transactions on sensor Networks (TOSN) 9, no. 2 (2013): 18.

[30] Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A Novel and Comprehensive Trust Estimation Clustering-Based Approach for Large Scale Wireless Sensor Networks." IEEE Access 7 (2019): 58221-58240.

[31] Karthik, N., and V. S. Ananthanarayana. "A hybrid trust management scheme for wireless sensor networks." Wireless Personal Communications 97, no. 4 (2017): 5137-5170.

[32] Kim, Tae Kyung, and Hee Suk Seo. "A trust model using fuzzy logic in wireless sensor network." World academy of science, engineering and technology 42, no. 6 (2008): 63-66.

[33] Wu, Xiaoling, Junjie Huang, Jie Ling, and Lei Shu. "BLTM: beta and LQI based trust model for wireless sensor networks." IEEE Access 7 (2019): 43679-43690.

[34] Zhao, Jin, Jifeng Huang, and Naixue Xiong. "An effective exponential-based trust and reputation evaluation system in wireless sensor networks." IEEE Access 7 (2019): 33859-33869.

[35] Yang, Liu, Yinzhi Lu, Sheng Liu, Tan Guo, and Zhifang Liang. "A dynamic behavior monitoring Game-Based trust evaluation scheme for clustering in wireless sensor networks." IEEE Access 6 (2018): 71404-71412.

[36] Movassaghi, Samaneh, Mehran Abolhasan, Justin Lipman, David Smith, and Abbas Jamalipour. "Wireless body area networks: A survey." IEEE Communications surveys & tutorials 16, no. 3 (2014): 1658-1686.

[37] Lim, H. S., Moon, Y. S. and Bertino, E. (2010), "Provenance based Trustworthiness Assessment in Sensor Networks," in Proc. 7th In!. Workshop Data Manage. Sens. Netw., pp. 2-7.

[38] Mana, Mohammed, Mohammed Feham, and Boucif Amar Bensaber. "Trust Key Management Scheme for Wireless Body Area Networks." IJ Network Security 12, no. 2 (2011): 75-83.

[39] Liu, Jingwei, Zonghua Zhang, Xiaofeng Chen, and Kyung Sup Kwak. "Certificateless remote anonymous authentication schemes for wireless body area networks." IEEE Transactions on parallel and distributed systems 25, no. 2 (2013): 332-342.

[40] Li, Wenjia, and Xianshu Zhu. "Recommendation-based trust management in body area networks for mobile healthcare." In 2014 IEEE 11th International conference on mobile ad hoc and sensor systems, pp. 515-516. IEEE, 2014.

[41] Guo, Ping, Jin Wang, Sai Ji, Xue Hua Geng, and Neal N. Xiong. "A lightweight encryption scheme combined with trust management for privacy-preserving in body sensor networks." Journal of medical systems 39, no. 12 (2015): 190.

[42] IHayajneh, Thaier, Bassam Mohd, Muhammad Imran, Ghada Almashaqbeh, and Athanasios Vasilakos. "Secure authentication for remote patient monitoring with wireless medical sensor networks." Sensors 16, no. 4 (2016): 424.

[43] Thamilarasu, Geethapriya, and Adedayo Odesile. "Securing wireless body area networks: Challenges, review and recommendations." In 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1-7. IEEE, 2016.

[44] Omala, Anyembe Andrew, Kittur P. Kibiwott, and Fagen Li. "An efficient remote authentication scheme for wireless body area network." Journal of medical systems 41, no. 2 (2017): 25.

[45] Bhangwar, Ali Raza, Pardeep Kumar, Adnan Ahmed, and Muhammad Ibrahim Channa. "Trust and thermal aware routing protocol (TTRP) for wireless body area networks." Wireless Personal Communications 97, no. 1 (2017): 349-364.

[46] Priya, Nachimuthu Sangeetha, R. Sasikala, Srinivasan Alavandar, and L. Bharathi. "Security Aware Trusted Cluster Based Routing Protocol for Wireless Body Sensor Networks." Wireless Personal Communications 102, no. 4 (2018): 3393-3411.

[47] Chitra, A., and G. R. Kanagachidambaresan. "Fault aware trust determination algorithm for wireless body sensor network (WBSN)." In Proceedings of first international conference on smart system, innovations and computing, pp. 469-476. Springer, Singapore, 2018.

[48] Anguraj, Dinesh Kumar, and S. Smys. "Trust-based intrusion detection and clustering approach for wireless body area networks." Wireless Personal Communications 104, no. 1 (2019): 1-20.

[49] Roy, Sanjoy, and Suparna Biswas. "A Novel Trust Evaluation Model Based on Data Freshness in WBAN." In Proceedings of International Ethical Hacking Conference 2018, pp. 223-232. Springer, Singapore, 2019.

[50] Wang, Tianshu, Kongfa Hu, Xichen Yang, Gongxuan Zhang, and Yongli Wang. "A trust enhancement scheme for cluster-based wireless sensor networks." The Journal of Supercomputing 75, no. 5 (2019): 2761-2788.

[51] Ostad-Sharif, Arezou, Morteza Nikooghadam, and Dariush Abbasinezhad-Mood. "Design of a lightweight and anonymous authenticated key agreement protocol for wireless body area networks." International Journal of Communication Systems 32, no. 12 (2019): e3974.

[52] Nidhya, R., and S. Karthik. "Security and Privacy Issues in Remote Healthcare Systems Using Wireless Body Area Networks." In Body Area Network Challenges and Solutions, pp. 37-53. Springer, Cham, 2019.

[53] Karchowdhury, Sagarika, and Mainak Sen. "Survey on Attacks on Wireless Body Area Network." International Journal of Computational Intelligence & IoT, Forthcoming (2019).

[54] Usman, Muhammad, Muhammad Rizwan Asghar, Imran Shafique Ansari, and Marwa Qaraqe. "Trust-Based DoS Mitigation Technique for Medical Implants in Wireless Body Area Networks." In ICC 2019-2019 IEEE International Conference on Communications (ICC), pp. 1-6. IEEE, 2019.

[55] Roy, Moumita, Chandreyee Chowdhury, and Nauman Aslam. "Security and Privacy Issues in Wireless Sensor and Body Area Networks." In Handbook of Computer Networks and Cyber Security, pp. 173-200. Springer, Cham, 2020.

[56] Rani, Rinki, Sushil Kumar, and Upasana Dohare. "Trust evaluation for light weight security in sensor enabled internet of things: game theory oriented approach." IEEE Internet of Things Journal 6, no. 5 (2019): 8421-8432.

[57] Kumar, Nagesh, Yashwant Singh, and Pradeep Kumar Singh. "An energy efficient trust aware opportunistic routing protocol for wireless sensor network." In Sensor Technology: Concepts, Methodologies, Tools, and Applications, pp. 628-643. IGI Global, 2020.

[58] Daojing He, Chun Chen, Sammy Chan, Jiajun Bu, and Athanasios V. Vasilakos "ReTrust: Attack-Resistant and Lightweight Trust Management for Medical Sensor Networks" IEEE transactions on information technology in biomedicine, VOL. 16, NO. 4, JULY 2012.

[59] Rao, J. Durga, and K. Sridevi. "Novel security system for wireless body area networks based on fuzzy logic and trust factor considering residual energy." Materials Today: Proceedings (2020).

[60] S. Ajami, A. Rajabzadeh, Radio Frequency Identification (RFID) technology and patient safety, J. Res. Med. Sci. 18 (9) (2013) 809–813.

[61] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.

[62] Das, M. L., Kumar, P., & Martin, A. (2020). Secure and Privacy-Preserving RFID Authentication Scheme for Internet of Things Applications. *Wireless Personal Communications*, *110*(1), 339-353.

[63] Pakniat, N., & Eslami, Z. (2020). Cryptanalysis and improvement of a group RFID authentication protocol. *Wireless Networks*, 1-10.

[64] Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics, 14(4), 1656-1665.

[65] Fan, K., Luo, Q., Zhang, K., & Yang, Y. (2020). Cloud-based lightweight secure RFID mutual authentication protocol in IoT. Information Sciences, 527, 329-340.

[66] Xie, W., Xie, L., Zhang, C., Zhang, Q. and Tang, C., 2013, April. Cloud-based RFID authentication. In 2013 IEEE International Conference on RFID (RFID) (pp. 168-175). IEEE.

[67] Aghili, S. F., Mala, H., Kaliyar, P., & Conti, M. (2019). Seclap: Secure and lightweight rfid authentication protocol for medical iot. Future Generation Computer Systems, 101, pp. 621-634

[68] Safkhani, M., Bendavid, Y., Rostampour, S., & Bagheri, N. On Designing Lightweight RFID Security Protocols for Medical IoT. Cryptology ePrint Archive, Report 2019/851, 2019. https://eprint. iacr. org/2019/851.

[69] Zhuang, X., Zhu, Y., & Chang, C. C. (2014). A New Ultralightweight RFID Protocol for Low-Cost Tags: R^2AP. Wireless Personal Communications, 79(3), 1787-1802.

[70] Farash, M. S., Nawaz, O., Mahmood, K., Chaudhry, S. A., & Khan, M. K. (2016). A provably secure RFID authentication protocol based on elliptic curve for healthcare environments. Journal of medical systems, 40(7), pp. 165.

[71] Abughazalah, S., Markantonakis, K. and Mayes, K., 2014. Secure improved cloud-based RFID authentication protocol. In Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance (pp. 147-164). Springer, Cham.

[72] He, D., & Zeadally, S. (2014). An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. IEEE internet of things journal, 2(1), pp. 72-83.

[73] Wazid, M., Das, A. K., Kumar, N., Conti, M., & Vasilakos, A. V. (2017). A novel authentication and key agreement scheme for implantable medical devices deployment. IEEE journal of biomedical and health informatics, 22(4), pp. 1299-1309.

[74] Rahman, F., Bhuiyan, M. Z. A., & Ahamed, S. I. (2017). A privacy preserving framework for RFID based healthcare systems. Future generation computer systems, 72, pp. 339-352.

[75] Chiou, S. Y., & Chang, S. Y. (2018). An enhanced authentication scheme in mobile RFID system. Ad Hoc Networks, 71, pp. 1-13.

[76] Priyanka, Y. J., & Turuk, A. K. (2018, March). RFID Authentication Protocol for mobile readers satisfying EPC-C1-GEN2 standard of Passive Tags. In 2018 Technologies for Smart-City Energy Security and Power (ICSESP) (pp. 1-5). IEEE.

[77] Fan, K., Jiang, W., Li, H., & Yang, Y. (2018). Lightweight RFID protocol for medical privacy protection in IoT. IEEE Transactions on Industrial Informatics, 14(4), pp. 1656-1665.

[78] Zhang, C., Zhu, L., Xu, C., & Lu, R. (2018). PPDP: An efficient and privacy-preserving disease prediction scheme in cloud-based e-Healthcare system. *Future Generation Computer Systems*, *79*, 16-25.

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

[80] A. Alabdulatif, H. Kumarage, I.Khalil, and X. Yi, Privacy-preserving anomaly detection in cloud with lightweight homomorphic encryption,Journal of Computer and System Sciences.2017; vol.90, pp.28-45

[81] X. Liu, R. Lu, J. Ma, L.Chen, and B. Qin, Privacypreserving patient-centric clinical decision support system on naive Bayesian classification,IEEE journal of biomedical and health informatics. 2016;vol.20, no.2, pp.655-668.

[82] A.Alabdulatif, and M. Kaosar, Privacy preserving cloud computation using Domingo-Ferrer scheme,Journal of King Saud UniversityComputer and Information Sciences.2016; vol.28, no.1, pp.27-36.

[83] L. Lyu, J.C. Bezdek, Y.W. Law, X.He, and M. Palaniswami, Privacy-preserving collaborative fuzzy clustering,Data& Knowledge Engineering. 2018.

[84] H.H. Nguyen, Privacy-Preserving Mechanisms for k-Modes Clustering,Computers& Security. 2018.

[85] Chen, L., & Hoang, D. B. (2011, November). Towards scalable, fine-grained, intrusion-tolerant data protection models for healthcare cloud. In *2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 126-133). IEEE.

[86] Narayan S., Gagné M., Safavi-Naini R. Privacy preserving EHR system using attribute-based infrastructure; Proceedings of the ACM Cloud Computing Security Workshop; Chicago, IL, USA. 8 October 2010; pp. 47–52.

[87] Wang, X. S., Huang, Y., Zhao, Y., Tang, H., Wang, X., & Bu, D. (2015, October). Efficient genome-wide, privacy-preserving similar patient query based on private edit distance. In *Proceedings of the* 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 492-503).

[88] Lu W. -J, Yamada Y, Sakuma J. Privacy-Preserving Genome-Wide Association Studies on Cloud Environment using Fully Homomorphic Encryption. 2015; 15:1.

[89] Sumalatha, M. S., and V. Nandalal. "An intelligent cross layer security based fuzzy trust calculation mechanism (CLS-FTCM) for securing wireless sensor network (WSN)." Journal of Ambient Intelligence and Humanized Computing (2020): 1-15.Harvard.

[90] JIANG, Jinfang, and H. A. N. Guangjie. "Survey of Trust Management Mechanism in Wireless Sensor Network." Netinfo Security 20, no. 4 (2020): 12.

[91] Yang, Kai, Shuguang Liu, Xiuguang Li, and Xu An Wang. "DS evidence theory based trust detection scheme in wireless sensor networks." In Sensor Technology: Concepts, Methodologies, Tools, and Applications, pp. 321-334. IGI Global, 2020.

[92] Bayrakdar, Muhammed Enes. "Cooperative communication based access technique for sensor networks." International Journal of Electronics 107, no. 2 (2020): 212-225.

[93] Nunoo-Mensah, Henry, Kwame OseiBoateng, and James DzisiGadze. "PSTRM: Privacy-aware sociopsychological trust and reputation model for wireless sensor networks." Peer-to-Peer Networking and Applications (2020): 1-21.

[94] Ishmanov, Farruh, Sung Kim, and Seung Nam. "A secure trust establishment scheme for wireless sensor networks." Sensors 14.1 (2014): 1877-1897.

[95] Mainanwal, Vikash, Mansi Gupta, and Shravan Kumar Upadhayay. "A survey on wireless body area network: Security technology and its design methodology issue." In 2015 international conference on innovations in information, embedded and communication systems (ICIIECS), pp. 1-5. IEEE, 2015.

[96] Weast, John C., Cory J. Booth, Deepak Vembar, and Lenitra M. Durham. "Extension of trust in a body area network." U.S. Patent Application 14/573,992, filed June 23, 2016.

[97] Hu, Chunqiang, Hongjuan Li, Yan Huo, Tao Xiang, and Xiaofeng Liao. "Secure and efficient data communication protocol for wireless body area networks." IEEE Transactions on Multi-Scale Computing Systems 2, no. 2 (2016): 94-107.

[98] Joshi, Ashish, and Amar Kumar Mohapatra. "Authentication protocols for wireless body area network with key management approach." Journal of Discrete Mathematical Sciences and Cryptography 22, no. 2 (2019): 219-240.

[99] Tian, Y., Chen, G., & Li, J. (2012). A new ultralightweight RFID authentication protocol with permutation. Communications Letters, IEEE, 16(5), 702–705.

[100] Gholami, A., & Laure, E. (2016). Security and privacy of sensitive data in cloud computing: a survey of recent developments. *arXiv preprint arXiv:1601.01498*.

[101] Khandelwal, M., & Saini, H. (2019, October). Review on Security Challenges of Cloud Computing. In *International Conference on Advancements in Computing & Management (ICACM-2019)*.

[102] Kaur, C., Mourad, H. M., & Banu, S. S. (2019). Security and Challenges using Clouds Computing in Healthcare Management System.

[103] Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, *7*, 61656-61669.

[104] Vulapula, S. R., & Srinivas, M. (2018). Review on Privacy Preserving of Medical Data in Cloud Computing System. *Indian Journal of Public Health Research & Development*, *9*(12), 2261-2269.

[105] Wang, B., Song, W., Lou, W., & Hou, Y. T. (2017, May). Privacy-preserving pattern matching over encrypted genetic data in cloud computing. In *IEEE INFOCOM 2017-IEEE Conference on Computer Communications* (pp. 1-9). IEEE.

[106] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth Cloud Security Challenges: A Survey. *Journal of healthcare engineering*, *2019*.

[107] Hur, J. (2011). Improving security and efficiency in attribute-based data sharing. *IEEE transactions on knowledge and data engineering*, *25*(10), 2271-2282.

[108] Mao, X., Li, X., Wu, X., Wang, C., & Lai, J. (2018, August). Anonymous Attribute-Based Conditional Proxy Re-encryption. In *International Conference on Network and System Security* (pp. 95-110). Springer, Cham

[109] Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks." IEEE Access 7 (2019): 58221-58240.

[110] Dubois, D. &Prade, H. (1982). A class of fuzzy measures based on triangular norms: a general framework for the combination of information, International Journal of General Systems 8: 43–61.

[111] Salim Rezvani,Comparative of Two Triangular Fuzzy Sets with α -cut , Journal of Physical Sciences, ,2015,Vol. 20, 111-132 ,ISSN: 2350-0352.

[112] Maji, S., & Arora, S. (2018). Decision Tree Algorithms for Prediction of Heart Disease. Lecture Notes in Networks and Systems, 447–454. doi:10.1007/978-981-13-0586-3_45