Telecommunication Systems
https://doi.org/10.1007/s11235-024-01211-9

ORIGINAL PAPER

Safeguarding the Internet of Health Things: advancements, challenges, and trust-based solution

Misbah Shafi[1] · Rakesh Kumar Jha[1] · Sanjeev Jain[2] · Mantisha Gupta[3] · Zeenat Zahra[4]

Accepted: 17 August 2024

Abstract
The applications of IoHT have adapted a lot of contemplation as a result of recent IoT (Internet of Things) advancements. Irrespective of several fields in IoHT such as remote medical professional assistance, history of health-charting, integrated care management, decreased cost, disease management, disability management, home care management, individual healthcare assistance, health tracking, drug availability management, healthcare tracking management, and telesurgery. The evolvement in the field of the IoHT network has shown a drastic advancement in the standard of living. Despite the numerous fields of application in the IoHT network, the balance of security and privacy is one of the most pressing problems as far as life-critical solutions are concerned. There are several solutions to maintain security in the IoHT network. The most recent security enhancement schemes in the IoHT have been addressed in this paper. Furthermore, the latest possible challenges in the IoHT network are discussed. Moreover, an extensive survey on future research directions in the field of IoHT network security is illustrated. Additionally, we have proposed a security architecture based on trust assessment for IoHT systems to ameliorate the security of the network. The trust assessment is based on the artificial intelligence mechanism such that the security of the IoHT network is enhanced adaptively. This paper presents a novel IoHT security framework that integrates trust evaluation to dynamically address security challenges. It offers practical solutions for applications like telesurgery by adjusting measures based on real-time trust assessments, setting a new standard in IoHT security and guiding future research.

Keywords Trust management · Security in Internet of Healthcare Things (IoHT) · Artificial intelligence · IoHT system · Security attacks

✉ Rakesh Kumar Jha
jharakesh.45@gmail.com

Misbah Shafi
misbahshafi0@gmail.com

Sanjeev Jain
dr_sanjeevjain@yahoo.com

Mantisha Gupta
mantisha343@gmail.com

Zeenat Zahra
zeenatzahra1214@gmail.com

[1] Department of Electronics and Communication Engineering, Central University of Jammu, Jammu and Kashmir 180011, India

[2] Department of Computer Science and Engineering, Central University of Jammu, Jammu and Kashmir, India

[3] Department of Electronics and Communication Engineering, SMVD University, Katra 182320, India

[4] Department of Computer Science and IT, Central University of Jammu, Jammu and Kashmir 180011, India

1 Introduction

1.1 Motivation

oHT (Internet of Healthcare Things) has gained a lot of popularity in recent years among applications in the medical industry. The concept of Internet of Healthcare Things is defined as the discipline of Internet of Things (IoT) wherein sector of healthcare network is involved in particular. It integrates multiple healthcare system devices, healthcare data systems, and healthcare monitoring applications. The combined system enables seamless connectivity, management and analysis of the recieved information of the patients to enhance overall execution of the healthcare systems. Precisely, IoHT involves the real time health data collection from the patients remotely or in a mode of clinical setting. It facilitates the exchange of information to the parties of the healthcare network including caregivers, providers, or other related entities. The primary importance of the healthcare

Published online: 11 September 2024

data is that it can be used for health monitoring, diagnosis, chronic illness management, plans of personalized treatment, and other research purposes.

Wireless Communication Network (WCN) is used by healthcare organizations to coordinate people and medical devices. To make medical healthcare convenient, IoHT provides the advantage of addressing and monitoring the health of patients from a distance. Therefore, by using the IoHT system, well-maintained and precise diagnoses are adapted. As far as financial expenses are concerned, it is anticipated to save about $300 billion a year in cost [1–3].

With the current global pandemic COVID-19, the IoHT network provides access to monitor patients remotely. It has proved effective for those who require emergency care from a distance to maintain isolation as described by the COVID protocols. By utilizing advanced diagnostic tools, the IoHT network decreases the need for in-person consultations and thereby improves the standard of healthcare.

With the advancements of the IoHT network, dynamic scheduling, telemedicine, home care, and monitoring are all made possible. The introduction of artificial intelligence in IoHT has created a boost in semantic understanding and sensory capability. IoHT systems leverage medical equipment and services to enhance the user experience in the form of the best possible source, service, time, and diagnosis management [4]. One of the influential concepts that is credited with elevating the global standard of living is the adoption of the IoHT system. The aspect of security is of uttermost importance and therefore poses one of the most significant challenges in the IoHT domain. Consequences of inadequate security include invasions of security and privacy attacks that cause delayed interruption, eavesdropping, and illegal access. The data security in the IoHT has received immense attention. Therefore, security at various stages, including data monitoring, data acquisition, data transmission, data diagnosis, and data storage is required to be protected [5–7].

1.2 Related work

To meet the security essentials of the IoHT network, several conventional security measures were incorporated. Traditional security solutions, however, cannot ensure appropriate and complete security due to system constraints including power consumption, extremely low latency, dependability, and accuracy. To strengthen the physical security of the IoHT network against node replacement and node manipulation threats, a two-stage authentication mechanism is proposed in [8]. There are three types of nodes in this network. The first type is the node of the patient, the second is the sink node, and the third is the node of the server. The sink node connects the patient node to the healthcare cloud server and commences the authentication procedure. The authentication process is divided into two steps. The first step begins between the sink and server nodes. The second stage of authentication is carried out by the sink node and patient node.

In [9], the Convolutional Neural Network (CNN) prediction model is used to examine the security performance of the IoHT network. The four convolution layers and four inception branch blocks constitute the model. The models use the existing healthcare data and extract its data features. The model employs Secrecy Outage Probability (SOP) to analyze security performance. The approach reduces the Mean Squared Error (MSE) by 20%. A technique of secret sharing and data mending is provided in [10] to secure data acquisition in the IoHT system. The Slepian-Wolf Coding (SWC) is used in the sharing mechanism. For data storage, multiple cloud servers are used. With the aid of a patient access control approach, these servers provide collaborative creation of patient data sharing with healthcare professionals and healthcare centers.

The KATAN secret cipher method in IoHT is used to demonstrate safe data acquisition [11]. KATAN refers to a specific block cipher in the KATAN family, which is designed to be compact and efficient. There are four tiers in the network. The IoT network sensors constitute the top layer. The fog layer is the second one. The cloud computing layer comes in at layer three, and the healthcare provider follows at layer four. The two methods employed in the first two layers are the secret cipher share algorithm and the hardware-based cipher algorithm. Data privacy is offered through the KATAN algorithm, which is predicated on secret cipher sharing. At the cloud computing layer, the distributed database method is employed to secure the patient's personal data. In [12], the signature technique is used to improve the confidentiality and security of healthcare data acquisition. To increase privacy, noise is added to the acquired healthcare data.

For data integrity and data authentication, an edge server is used in [13]. Before sending the health data to the edge server, data is encrypted to protect privacy. Decryption is carried out by the cloud server to ensure data availability. According to [2], the identity management methodology improves IoHT security. The method entails mapping the credential information of the user. The information of the credentials is encrypted using a hashing algorithm attribute-based encryption. While creating an account, the output token is created using Elliptic Curve Cryptography (ECC). The fog node controls the key verification identity management. A password strength assessment mechanism is used to investigate password-based security issues [14]. The method employs the personal data of the user to evaluate password strength and select a password with a greater level of security.

For the IoHT network, the security framework is examined by the Identified Security Attributes (ISA). The decision-making utilizes the Technique for Order Preference by

Similarity to Ideal Solution (TOPSIS) and analytical hierarchical procedure. Two processes together form the security framework. In the first process, weight attributes are derived using an analytical hierarchical approach, and in the second process, security criteria are assessed using the TOPSIS methodology [15]. In [16], the blockchain-based technique is used to increase IoHT security. The health information of the user is obtained by an Unmanned Ariel Vehicle (UAV). The closest server to the UAV is chosen for the data storage. Two procedures are followed by the authentication. Encryption is the first step, and blockchain is the second. By using tokens to establish communication, the UAV subsequently sends the shared key to the body sensor hives. The health data is then stored by the UAV using blockchain.

A trigonometric map-based cryptosystem is used to securely communicate the medical image data. To determine hamming distance, the cryptosystem creates the first three keystreams from the most recent trigonometric map. On the output distance vector and keystream, the bit XOR concept is used. The encrypted image is created by bit XORing the output from the prior operation with the generated vector [17]. The trust-based security is defined as the approach of securing the network based on the estimated trust. For IoHT network, the trust based security involves the security of the network based on the level of the trust achieved by the entities of the network. To incorporate such mechanisms trust models are used to estimate security strengths determining the level of the trust. In [18], trust assessment is carried out via the technique of artificial neural networks. By combining the evaluation of parameters such as compatibility computation, packet delivery computation, node identification, and trust computations of dependability, the degree of trust is assessed. The encryption system uses a combination mechanism that uses the safe hash algorithm and ECC.

To provide security to the electronic health data, an effective IoT-enabled watermarking technique while addressing the conflicts of ownership, data integrity, data confidentiality, and data privacy [19]. In [20], a blockchain-based mechanism has been incorporated with a hybrid computing paradigm to ensure security with low latency, devoid of single-point failure, and low storage cost in the network of IoHT. The methodology involves ring-based access control with selective decentralization such that the records of the patient and the device authentication remain preserved. In [21], a privacy-preserving forward algorithm has been incorporated to enhance security in IoHT. The mechanism enables monitoring in the cloud for the remote healthcare network. It involves the Hidden Markov Model (HMM) for monitoring with a single server. In [22], privacy preserving optimization scheme has been incorporated to provide a secured clinical pathway in the network of healthcare. The information is communicated without the revelation of the personal information of the patients including gender, age, and name, nor the information of the hospital records including disease type, medication, treatment, estimated expenses, and physical index. Table 1 provides a broad outline of the latest methodologies incorporated to enhance the security of the IoHT network. It involves mechanisms based on specific objectives such as cryptographic techniques, intrusion detection system methods, authentication protocols, and enhanced secure data transmission procedures. It is made evident how these tactics help to safeguard sensitive medical data and maintain system integrity by these methodologies in the IoHT network.

Existing IoHT security models often use static methods that fail to address evolving threats. This paper introduces a dynamic, trust-based framework, advancing theoretical understanding and offering practical benefits for applications like remote medical procedures and health tracking. It significantly enhances both theoretical and practical aspects of IoHT security, addressing current and future challenges.

1.3 Novelty

In this paper, an extensive survey on the security in IoHT is focused on. The related recent work on the attack possibilities and their countermeasures in the IoHT has been investigated. Overall, the prime contributions of the paper are given below.

- The security architecture of IoHT has been identified.
- The recent methodologies, their performance parameters, and attack types in IoHT are well-investigated.
- The most fundamental challenges in the security of IoHT are well elaborated in the paper.
- To improve and preserve the overall security of the IoHT network we have proposed the intelligent trust-based scheme in IoHT.

1.4 Organization

The paper is organized as follows. Section 1 presents the introduction. Section 2 describes the architecture of IoHT based on the security perspective. The process flow in the IoHT is well discussed in Sect. 3. The open challenges in the security of IoHT are well illustrated in Sect. 4. The proposed system to enhance the security in IoHT is presented in Sect. 5. Section 6 describes the future research directions given security in IoHT. Security standards in IoHT are discussed in Sect. 7. To the closure of the paper, the conclusion is given in Sect. 8.

Table 1 Most recent security enhancement methodologies in Internet of Healthcare Things

Ref	Technique/ scheme	Objective	Target parameters	Target attacks	Network type
[23]	Improved CLAS	To enhance security using CLAS for WMSN	Computational time, communication cost	First message attack	Healthcare WMSN
[24]	Smart service authentication	To enhance mutual authentication protocol for TMIS using cloud environment	Computational time	Health report revelation attack, server spoofing, DoS, smart card stolen card, non-repudiation	Medical Healthcare system network
[25]	Boneh-franklin identity based distributed decryption scheme	To design a lightweight decryption scheme while maintaining the security	Time consumption	Ciphertext attack	Electronic personal health care system
[26]	blind batch encryption scheme	To obtain an optimized balance between privacy and security	Time cost	Collision attack, External attack, reuse attack, MIM attack replay attack privacy attack	Smart healthcare system network
[27]	Fuzzy commitment scheme	To resist against mobile device loss attack	Time cost	Stolen smart card attack, mobile device lost attack, impersonation attack	Wireless medical sensor network systems
[28]	Blockchain-based trust management technique	To enhance the secure communication between the patients and healthcare professionals	Trust value	Insider attacks	Medical smartphone networks
[29]	Software-Defined Networking	Security improvement in data sharing healthcare systems	Response time	Identity theft attack, insider attack	Data sharing healthcare system networks
[30]	Mobile agent based ID scheme	High accuracy based intrusion detection	Detection accuracy, energy usage	DoS, data falsification and fabrication, privacy attack	Internet of medical things network
[31]	Mosaic Gradient perturbation scheme	To enhance the privacy and deteriorate the risk of model inversion attack	Accuracy, time computation	Model inversion attack	Smart healthcare systems network
[32]	Anomaly intrusion detection	Detecting illegal behavior using machine learning	Accuracy, time cost	Replay attack, malware attack, shoulder surfing attack	Medical IoT system networks
[33]	Additive homomorphic encryption scheme	To improve secure monitoring in wireless IoT based body sensors	Computation time	Chosen plaintext attack, weekly unforgeable attack	Wireless body sensor networks
[34]	Blockchain scheme	Secure data transmission	Verification error, cost of witnessing	Man in the middle attack	Body area networks
[35]	Elgamal blind signature technique	To develop a privacy-preserving scheme for searching medical records	Execution time	Violent ergodic attacks	Internet of healthcare things network

Table 1 (continued)

Ref	Technique/ scheme	Objective	Target parameters	Target attacks	Network type
[36]	Hash functions and XOR operations	To develop a secure data communication mechanism between the devices in healthcare IoT	Latency, communication time, energy of sensor devices	Replay attack, forgery attack, de-synchronization attack, attacks on availability, key agreement, mutual authentication, and untraceability	Internet of health care things network
[37]	One way hash function and bitwise XOR operation	To develop an anonymity preserving authentication mechanism	Computational cost	Replay attack, DoS attack, man in the middle attack	Digital Health Networks
[38]	Multistage blockchain	To propose a trustworthy and secure healthcare system that provides smart interoperabilitywith wireless body area network	Encryption efficiency, encryption time, information entropy	Differential attack	Healthcare system interoperated with wireless body area network
[39]	Software defined networking and reinforcement learning	To create an adaptive intrusion detection and prevention system in healthcare network	Accuracy, TPR, FPR, F1, probability density function	unauthorized access; DoS attack, MIM attack, traffic analysis attack	Healthcare network

Ref	Technique/ scheme	Objective	Target parameters	Target attacks	Network type	Motivation
[40]	blockchain-based multifactor authentication protocol	to enhance security in Internet of Medical Things (IoMT) applications through a blockchain-based multifactor authentication protocol	Time consumption, energy consumption		Internet of Medical Things	Research gap from [23–48]: Higher complexity, decentralized mechanism, Higher latency, more specific to data security, higher cost, self managing networks with complex coordinations
[41]	Blockchain technique	It integrate healthcare digital twins in the Metaverse with blockchain to provide security	Synchronization speed, resource utilization, throughput, user satisfaction score	No adaptibility	Digital Twin healthcare network	
[42]	Meta-Learning techniques	To develop Intrusion Detection System for IoMT using meta learning techniques	Accuracy, recall, precision, F1-score, mis-classification rate, and time complexity	Known and zero-day attacks	IoMT	
[43]	Cheon-Kim-Kim-Song Fully Homomorphic Encryption (CKKS-FHE) Scheme	To secure healthcare communication using CKKS-FHE encryption and IOTA Tangle with Masked Authenticated Messaging protocol	Average create, attach and fetch times, payload size, and computational time	Power analysis attack	IoT network with healthcare data	

Table 1 (continued)

Ref	Technique/ scheme	Objective	Target parameters	Target attacks	Network type	Motivation
[44]	Integration of blockchain and edge computing	To improve the healthcare data security, edge computing and blockchain with PoTE (Proof of Trust and Expertise) consensus	Block time, average processing time, computational efficiency, latency, throughput, network utilization	Data based attacks	Decentralized healthcare based network	
[45]	Practical Byzantine Fault Tolerance algorithm (cryptographic technique)	Reputation incentive committee Consensus-based for Matchmaking Encryption in IoT healthcare (RCME) to enhance security in resource-constrained IoT healthcare environment	Computation delay, communication overhead, number of recievers	chosen ciphertext attacks	IoT healthcare network	Solving the issues with the proposed scheme: Easier integration, centralized security mechanism, lower latency, provides security to the network, potential lower cost, centralized control and management
[46]	SACS (Smart Contract-Based Access Control) blockchain based scheme	To enhance the security of the patient data, SACS based 6G blockchain is utilized for the healthcare sector	Communication cost, computational cost,	Replay attacks, man in the middle attacks	Healthcare peer to peer network	
[47]	Block chain based mutual authentication	To develop mutual authentication and key agreement protocol for the enhancement of data security in IoHT system	Computational cost, number of users, communication cost	Eavesdropping, tampering, brute-force cracking, interception,and deletion	IoT-enabled decentralized healthcare environment	
[40]	Proverif and ban logic based block chain mechanism	To execute a blockchain-based multifactor authentication protocol that enhances IoHT security	Communication overhead, communication cost, computation overhead	Man in the Middle attack, the DoS attack, and the impersonation attack	IoHT network	
[48]	Using bert and deep learning	To implement a hybrid BERT and deep learning model for intrusion detection in IoMT systems using network flows and patient biometrics	Precision, recall and F1 score, validation loss, training loss	web attacks, distributed denial of service attacks	IoHT network	

*CLAS, Certificateless aggregate signature; WMSN, Wireless medical sensor networks; TMIS, Telecare medical information system; MIM, Man in the middle; DoS, Denial of Service; IoT, Internet of Things; TPR, True positive rate; FPR, False positive rate

1.5 Ethical considerations

The proposed security framework categorizes ethical principles in the form of data confidentiality, information consent, and the bias mitigation. The patients or the applicants for data collection are informed about the objectives, threats and benefits of this research work. The primary importance is given to the consent that is required to be obtained before the data collection of the patients or applicants. Data confidentiality and privacy is maintained such that personal information is not compromised and is used only for research purposes. The methodology incorporates measures not to include data that may involve any sort of bias in trust level estimates, to guarantee equity and fairness in trust level estimation of the node.

2 System architecture of IoHT

Irrespective of the numerous applications of the IoHT network, there are certain challenges associated with it. Providing security in the network of IoHT is one of the prime challenges required to be fulfilled. The network of IoHT is susceptible to numerous attacks as far as different levels of the network are concerned. The overall architecture with a security perspective of the IoHT architecture is shown in Fig. 1. It illustrates the architecture of the IoHT network wherein medical devices in the form of sensors, medical servers, cloud servers, healthcare applications, and healthcare experts are interconnected using network infrastructure. The figure also represents the possible attacking scenario in the IoHT network to show the possible vulnerable sites of the IoHT network. The basic architecture of the IoHT consists of a 3S-level system. It includes sensor-level network, server-level network, and service-level network. Each of the levels in view of security is briefly discussed below:

2.1 Sensor level

All the medical devices and numerous types of sensors such as heart rate sensors, temperature sensors, and position sensors form the primary base of the IoHT architecture. These devices support different types of network topologies depending on the corresponding specifications and standards. The devices and the sensors are used to detect and measure the changes in environmental, physiological, and substantial quantities. These sensors and devices sense and gather the data for further processing.

At the sensor level, the limitations of resources provide inadequate support in guarding and providing an efficient security mechanism against potential attackers. Therefore, increases the threat of security attacks at the device and sensor level. Various types of attacks are possible at the device and sensor level in the architecture of the IoHTs. These attacks include Sybil attacks [49], eavesdropping, physical attacks [5], forgery attacks [50], side-channel attacks, remote hijacking, false data injection attacks [51], distributed denial of service attacks, eavesdropping, impersonation and spoofing attacks[52].

2.2 Server level

The data sensed by the devices and sensors are communicated to the servers through wireless body area networks including Bluetooth, Zigbee, and WiFi standards. The servers act as a data storage unit. The storage and processing at the cloud perform various functions such as ultimate data aggregation, data analytics, and data inference. The utilization of the cloud provides the solution to the processing of huge data volumes. Thereby, providing efficiency in terms of compatibility with off-shelf analysis, affordability, scalability, and performance as a whole. Cloud storage in particular offers permanent storage services that can prove beneficial for the cases of history-based data analytics. The data is further processed by incorporating advanced intelligent algorithms to decide as per the visualization and representation of the received data.

The use of the cloud in the IoHT offers off-site data storage. However, the security challenges offered by the cloud create serious security threats. The breakthrough in the servers creates breaches and therefore menaces in terms of integrity, confidentiality, privacy, and secrecy. The emergent risks in the latest intelligence-based attacks have a major impact on the security network of IoHT and therefore, must be addressed with efficient and effective potential solutions. The latest attacks possible at the server level includes quantum attack [53], dictionary attack [54], collision attack [11], User to Root (U2R) attacks [55], machine learning attacks [56], Man in the middle attack [57], exposure attacks [58], insider attacks [59, 60], and routing attacks [61].

2.3 Service level

The data analytics of the received data is evaluated by intelligent algorithms for the appropriate prediction of healthcare events such as disease detection, clinical diagnosis, medical decision support, need for immediate medical attention, medical emergencies, and health monitoring evaluation. The inference with intelligence in the IoHT to provide corresponding service and attention enhances fundamental and necessary decision support to healthcare professionals. The service level incorporates enhancement in the computational, availability, and execution capabilities. The inherent sensitivity of health data, the highly dynamic roles of stakeholders, the heterogeneity in Electronic Health Records (EHRs),

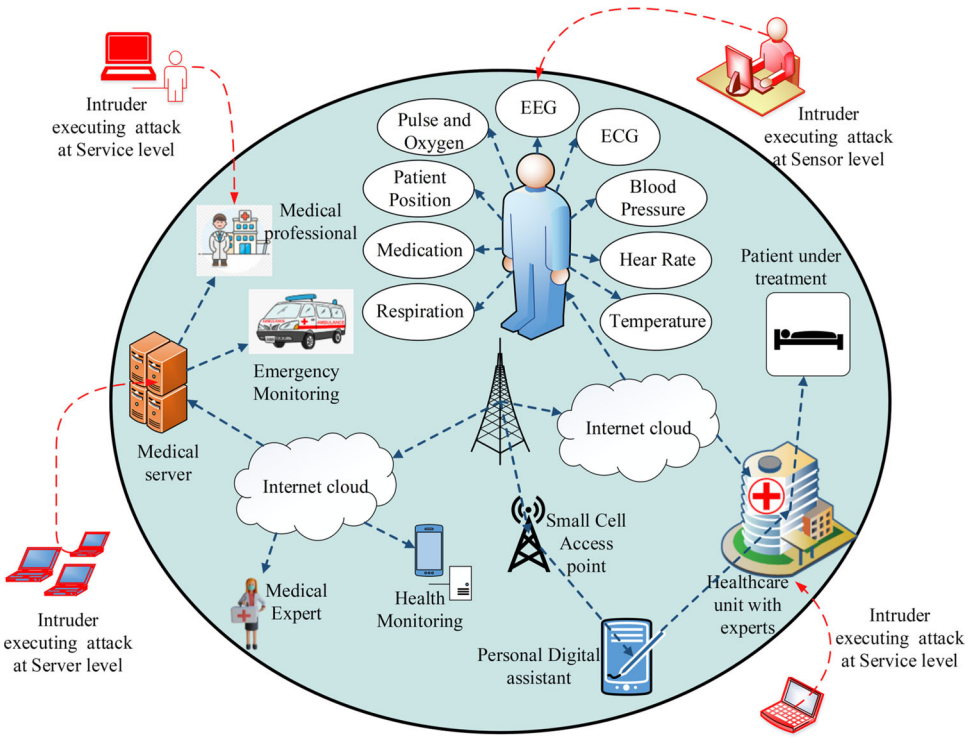


Fig. 1 System architecture of IoHT network with the possible attacking scenarios

and potentially dire implications from failures are just a few examples of the domain-specific challenges in IoHT services.

The challenges in the network of IoHT services raised favorable sites for the attacker that paved the way for numerous security attacks. The most recent attacks at the service level include key logging attack [14], 'physical medical devices capture attack [62], impersonation attack [63], bad-mouthing attack, good-mouthing attack, on–off attack [64], inside attacks [65], address resolution protocol spoofing attacks [39], reuse attack, replay attack [26], injection attacks [66], tracking attacks [67], jamming attack [68], and chosen ciphertext attack [69], and botnet attacks [70].

3 Process flow of intelligent IoHT

Various methods were followed to incorporate intelligence in IoHT [71–80]. In this section, a general adaptive and intelligent mechanism in IoHT is investigated. It involves the methodology followed in IoHT to provide a clear idea of the operation. The process in IoHT involves a three-layer methodology. The first layer is the layer of devices. The second layer is the layer of communication and the third layer is the layer application process layer. The over all layered structured of IoHT is shown in Fig. 2. It depicts the layer-based architectural network of IoHT system. It outlines 3 layered structure including layer of devices, layer of communication and layer of processing. Each layer is illustrated with the specific role and integrations within the system with a clear understanding of process flow in the IoHT network.

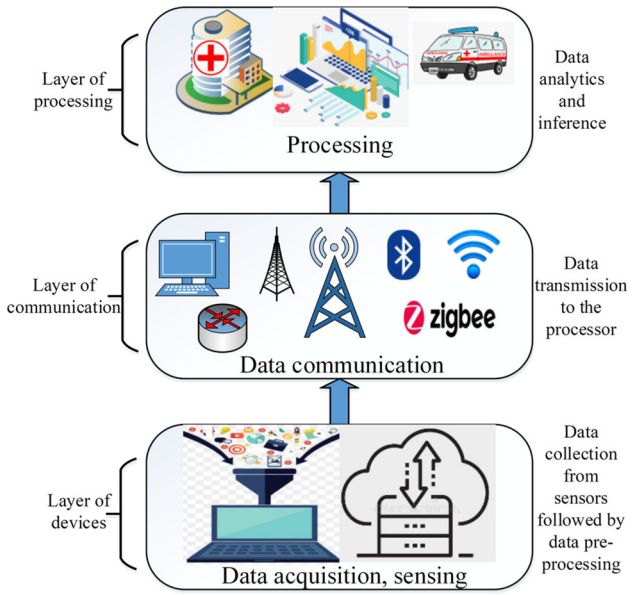


Fig. 2 IoHT system in the context of the layered architecture

3.1 Layer of devices

The layer of devices performs the data acquisition from the devices at the user end. The devices include different types of sensors for example temperature sensor, heart rate sensor,

oxygen saturation level sensor, and so on. The data sensed by the sensors undergoes pre-processing before transmitting it to the communication layer. The pre-processing involves the analysis of data such that the data is transformed into a specified format for effective and easy handling and computation. The processed data is then transmitted to the layer of communication.

3.2 Layer of communication

The layer of communication incorporates the procedure of transmission to the application part. The transmission of the data can be incorporated via a base station or through other wireless communication technologies. These wireless communication technologies include Bluetooth, Wireless Fidelity (Wi-Fi), Zigbee, Light Fidelity (Li-Fi), and radio frequency mobile communication. The fundamental operation of this layer is the transmission of the appropriate data to the application processing layer.

3.3 Layer of application processing

The layer of application processing involves the analysis of the retrieved sensed data. The assessment of received data defines the allocation of suitable applications such that the patients are proactively connected to the medical attention. The layer offers the visualization of the patient to connect with the end service providers including ambulances, hospitals, medicine supply chains, and the attention of medical professionals.

4 Security standards

This section describes the security standards for the IoHT found in the international norms. Data information, the sensor devices, and the networks including servers are the thrust areas that fall under the aspects of security. There are numerous ways to implement security in Information and Communication Technology (ICT). In contrast to the conventional ICT architectural notion, the architectural element takes security architecture into account to safeguard an IoT and IoHT system. To provide a high-level understanding of IoHT security, an architecture is developed. The protection of the data occupies prime importance in the IoHT network. The data acquired from the sensor, data to be transmitted in the network, and data meant for controlling actuators operate life-critical execution. Therefore, the safeguarding of the data in the IoHT must be ensured with utmost accuracy. This aspect encompasses several IoT data protection techniques, including encryption, key cryptography, replay protection, authenticity, and secrecy. The framework element offers standardized procedures for creating and implementing IoHT systems that have security-related problems. Various security-related general topics and considerations are covered by several international standards. This aspect has to do with standards that offer information on the general implementation and applicability of the IoHT system.

For the implementation of IoHT environment, networks connecting IoHT units are crucial. The network factor is connected to secure transport challenges from a security standpoint. The protocol factor, however, also contains standards about network protocols because we considered the network protocol to be a separate element. The policy element relates to standards for organizations, laws, and policies that deal with security in the IoHT system. Standards relating to privacy include numerous perspectives and details on several subjects that compensate the core standards in terms of network protocol, platform, and use case. The protocol is connected to network protocol-related standards that offer secure communication in IoHT. For particular IoHT domain, network protocols, and platforms, relates to authentication, authorization, and access control. Application instances for various IoHT contexts with security-related problems are provided by several standards. There are two possibilities for addressing the standards in IoHT. The security framework to define the standards in IoHT network is The first possibility is the choice of standards for interoperability and the second possibility is the standard for both security and interoperability. In addition, Fig. 3. shows the overview of security standards in IoHT. The security standards as per various elements are characterized into the following categories [81–83]. The description for each of the standards is given as follows:

4.1 IEEE 1888.3 standards

The IEEE 1888.3 standards state the requirements of security and privacy for pervasive control network protocol. The network satisfying these standards provides secure mechanisms with high energy efficiency and Quality of Service (QoS) for the IoHT and IoT network in general. The standard offers various architectures and architectural components that are required to satisfy the criteria of security. The criteria of security specified by the standard include confidentiality, integrity, authentication, and access control. Additionally, the standard specifies security mechanisms included in handshaking, access control, and communication sequence authentication.

4.2 National Institute of Standards and Technology (NIST) security framework

The security standards and framework offered by the NIST emphasize the major areas to find the security requirements

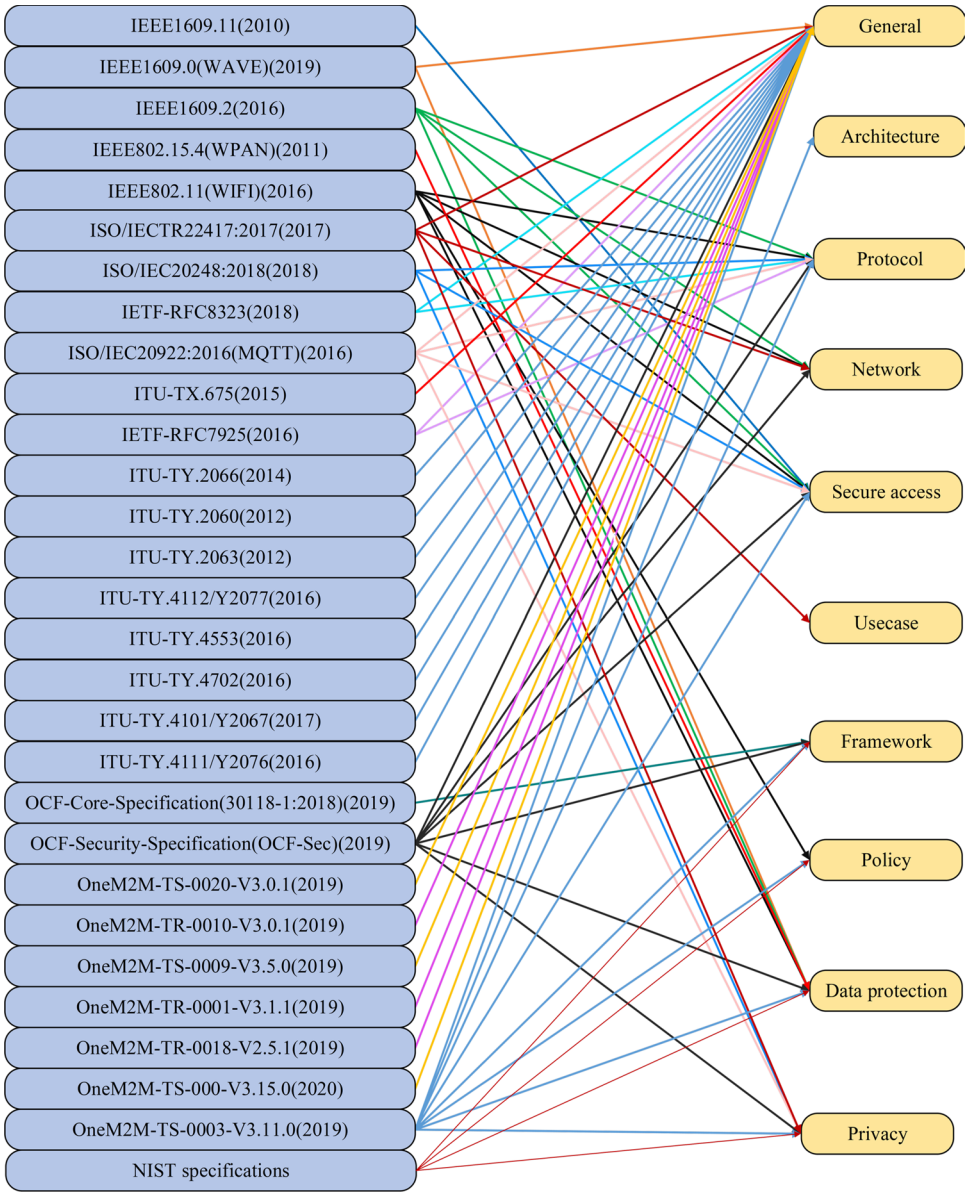


Fig. 3 Security standards in the IoHT framework representing standards with their corresponding target parameter

that can be potentially adapted to the communication network of IoHT. The NIST cybersecurity framework involves the standards for industry, organizations to balance the cybersecurity risks due to infrastructure. IoHT is also considered as part of such critical infrastructure and therefore offers cybersecurity outcomes, activities, and informative references to develop the individual organizational profile. The NIST privacy framework offers the identification of the privacy risks and protection of the privacy of the individual in an organization network of IoHT. NIST SP 800-53 offers the privacy and security controls of the data and information of the system network. NIST SP 800-53R offers the management of availability, integrity, and confidentiality of the information of the communication network such as the network of IoHT-based environments.

4.3 IEEE-SA standards

There are various network-related standards from IEEE-SA. The IEEE 802 family of standards for Local Area Network (LAN) and Metropolitan Area Network (MAN) includes several wireless network and wired network protocols. In an IoHT communication environment, wired network technologies are still in use, and network protocols adhere to many of the same standards. IEEE 802.11 defines the standard for Wi-Fi and IEEE 802.15.4 defines the standard for Bluetooth, Wireless Highway Addressable Remote Transducer Protocol (HART), ZigBee, Thread, IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN), and Z-Wave. However, since these standards can facilitate data interchange in

the IoHT network, therefore, these protocols can address the issue of transport interoperability.

4.4 IETF standards

The IETF standardization provides services in security and interoperability without the consideration of internet standards. For the scenario where the level is evaluated as high, the provisions of RFC (Request for Comments) are converted into the desired description of the internet. First, we conducted a conventional track analysis of the RFC series. The RFC-8323 provides the protocol definition for IoT through TLS, WebSocket, and TCP in the form of Constrained application protocol (CoAP). Limited devices can connect via CoAP because it was built for constrained devices. Additionally, CoAP can be used to connect devices in low-power, lossy networks, and other restricted networks.

4.5 *ISO*/IEC standards

A paradigm for interoperability inside IoHT systems and an understanding of interoperability for IoHT systems were the main issues of ISO/IEC 21823-1:2019. As a result, ISO/IEC 21823-1:2019 offers many components and traits enabling IoHT interoperability. An aspect model for interoperability is provided by the standard, and it is categorized into five types: transport type, syntactic type, semantic, behavioral, and policy. The shared communication infrastructure that allows IoT units to exchange data is the transport interoperability component.

4.6 ITU-T standards

International Telecommunication Union—Telecommunication (ITU-T) Standardization Sector arranged its standards into a series from A to Z under several headings. Series Y, in particular, is a collection of suggestions for the Internet of Things (IoHT as the case study), Internet protocol characteristics, and next-generation networks. Moreover, series X (security, data communication network, communication framework in an open system) and series F (services offered by communication in a non- telephonic environment) are linked with the guidelines of the IoHT communication environment. ITU-TY.4000/Y.2060 refers to the standardization of IoHT and IoT in ITU-T. The scope, concept, reference, and high-level requirements in IoT are present in this version of the standard. The standard ITU-TY.4000/Y.2060 defines the two fundamental conditions including interoperability and security in IoT and IoHT.

4.7 OCF standards

In February 2020, the Open Connectivity Foundation (OCF) published the most recent internal standards (specification vide 2.1.1), which includes sixteen various complications. The OCF specification provides the foundation for ISO/IEC 30118-1:2018. All devices using the OCF framework must adhere to the OCF Core Specifications (OCF-CS), which encompasses the whole OCF framework. The standard includes some interoperability elements because it specifies the fundamental architecture, user interfaces, communication protocols, network, framework of resources, and offered services for OCF execution in IoT contexts including IoHT.

4.8 M2M standards

The Machine-to-Machine (M2M) technology is a core component of the IoHT system, therefore M2M standards are also analyzed. In Technical Specification 0003, Version 3.11.0 (TS-0003V3.11.0), appropriate security-associated solutions for oneM2M-based systems are described. The standard goes into great detail to describe security-related factors, such as security schematic, authorization, security offered services and security affiliated interaction, security-related parameters, algorithms, protocols, and privacy protection architecture. The secure communication scenario is expressed in TS-0003-V3.11.0 and is further abstracted in TS-0016-V3.0.2. A secure environment offers a logical entity that provides a connection to the sensitive functionalities and the corresponding data to be approved in one M2M entity and protects them against tampering, unauthorized monitoring, or execution. The abstraction standard, in particular, concentrated on the declaration of the corresponding interfaces and mechanisms in a secured communication scenario with the direct technical schematic.

4.9 *ISO* 25237:2017, *ISO*/IEC 27701, *ISO*/IEC 27002

The International Organization for Standardization (ISO) standard referenced offers several methods, such as pseudorandomization, of the data to anonymous data in the healthcare industry. By modifying the criteria, healthcare organizations can share medical records for research without endangering patient privacy, and patients can trust them.

5 Open challenges in the security of IOHT

There are various challenges identified in the security of the IoHT network that are required to be addressed [7, 71, 72,

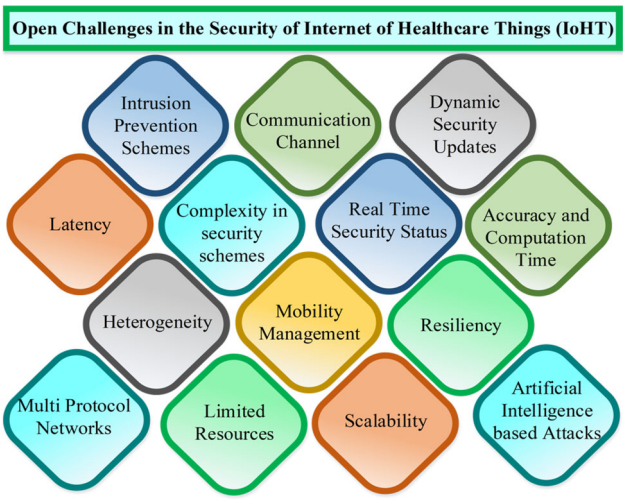


Fig. 4 Open key security challenges in IoHT network

84–90]. The list of open key challenges in the security of IoHT is shown in Fig. 4. These challenges are discussed below:

5.1 Latency

The huge healthcare data volume creates a drastic impact on the factor of latency. Moreover, the systems of IoHT involve end-to-end processing and transmission which increases the delay in the network. Several security enhancement mechanisms were defined in IoHT. Besides, creating a balance between latency and security is still an open challenge. Therefore, security schemes especially for time-critical applications such as telesurgery are required to fulfill the demand for security with minimum latency.

5.2 Complexity in security schemes

Complexity is one of the challenging parameters in IoHT. Moreover, the employment of security methodologies such as cryptographic techniques in IoHT increases the complexity of the network. The complexity affects the storage capacity, resource consumption, availability, quality of service, and process management of the IoHT network. Therefore, an efficient security mechanism for the IoHT with low complexity is required to be developed.

5.3 Real-time security status

The security of the IoHT network is required to be examined continuously such that the status of the security remains up-to-date. However, continuous examination of the whole network is a cumbersome process and requires more battery consumption. Besides, determining the security status of the network at regular intervals can pose a security threat to the IoHT network. Therefore, real-time security examination of the IoHT network is an open issue and required to be optimized.

5.4 Accuracy and computation time

It is considered one of the primary parameters of the security mechanisms based on artificial intelligence. It defines the correctness of the security mechanism such as in intrusion detection schemes appropriateness of distinction between the valid node and an invalid node is defined by the accuracy. Maintaining a high accuracy with a large volume of data for the existing attacks is a considerable threat that needs to be addressed.

5.5 Limited resource

The IoHT involving body area network relies on limited power such that the energy incorporated during processing is less. The wearable IoHTs are required to have sufficient power to execute for a longer duration. Especially for IoHT-based implants, the required active time is preferably longer as the replacement of them is painful and costlier. Moreover, the size of the IoHT is comparatively small with restricted memory and limited power. Security mechanisms are required to execute with small power and memory. The current security schemes are large and to operate well with constraints is quite challenging.

5.6 Heterogeneity

The IoHT involves a wide variety of applications. These applications encompass a wide variety of device classes. The devices vary in properties and exhibit different regulatory requirements. Applying the same security mechanism on different classes of devices is likely to create an adverse impact on the security of the network. Therefore, specific application-based security schemes are required to be suggested.

5.7 Mobility management

The devices in IoHT are operated in a dynamic environment. Mobility plays an important role in the security of the communication network. The interferences due to mobility create distracted communication which ultimately affects the security of the network. Furthermore, the IoHT occupies a diverse nature of mobility speeds. Considering different mobility speeds while analyzing security is an important challenge and is required to be addressed. Therefore, Security schemes with the consideration of the varying mobility in the IoHT network are desirable.

5.8 Resiliency

The security schemes are required to be resilient such that the errors in the mechanism are not able to create a drastic impact on the decision. The schemes are required to be able to recover the error at a high pace without any effect on the network of IoHT. Designing the security schemes with the property of resiliency is an open challenge.

5.9 Artificial intelligence-based attacks

Artificial Intelligence (AI) based attacks in the IoHT network is a new research direction that requires immense attention. The application-specific attacks based on AI in IoHT can create a serious threat wherein minute disturbances devised by the attacker on the devices of the network can prove extremely catastrophic. Therefore, countermeasure strategies for such attacks are required to be formulated.

5.10 Intrusion prevention schemes

The security of the IoHT can be improved by the methodology of intrusion prevention schemes. These schemes are required to be able to eliminate the effect of the attacker and continue the function of the system without failure. Moreover, a security mechanism must be capable of enhancing the security of the network and counter-attacking the detected intruder. However, based on the tiny protocol stack the adaptation of the intrusion prevention or security enhancement schemes is an open challenge.

5.11 Communication channel

The communication medium in IoHT is the wireless channel incorporating a diverse range of wireless technologies such as Zigbee, WiFi, Bluetooth, Worldwide Interoperability for Microwave Access (WiMax), Global System for Mobile Communications (GSM), Z-Wave, etc. Due to the wireless nature of the technology, traditional security methods become obsolete. Building a complete security mechanism or protocol that will work for both wired and wireless technologies while meeting strict security criteria is quite challenging. Additionally, the wireless channel inhibits the broad nature and, therefore is vulnerable to security attacks.

5.12 Dynamic security updates

The security protocol must be regularly updated to offer adequate security in IoHT infrastructure. Executing an advanced and adaptive security model is a challenging task. The security models that are capable of fulfilling the security requirements of the latest and upcoming IoHT systems are a matter of concern.

5.13 Scalability

The number of sensors employed in IoHT or smart healthcare systems is rapidly increasing. Therefore, more massive proportion of devices will interface with the global network. As a result, it is difficult to implement an enormously scalable security mechanism while meeting complex security criteria.

5.14 Multi-protocol networks

The communication network in the infrastructure of IoHT involves the interconnection of several smart devices while operating a proprietary network protocol. It includes the connection of smart IoHT devices over IP networks. Therefore, with the existing protocol network, satisfying all the security requirements for the diverse and dynamic IoHT system is quite challenging.

The overall challenges in the security of IoHT are specified in Table 2. This table provides the overview of prominent security challenges in IoHT network. It involves authentication vulnerabilities of IoHT network, data privacy concerns, data integrity threats, and overall network security attacks in IoHT. Each of the challenge is defined with its possible effect on the network of IoHT.

6 Proposed system model

There are various security-challenging parameters required to be fulfilled in the IoHT network as mentioned in the previous section. To provide an improvement in the security of IoHT while considering these challenges we have proposed a trust assessment framework for IoHT. The proposed framework achieves the security prerequisites required by the network of IoHT. The security issues addressed by the proposed trust level mechanism are illustrated as follows:

- Trust management decreases the vulnerabilities due to services offered by the vulnerable nodes.
- Intrusion detection based on the signal strength, communication channel variation, and communication overload can be easily detected.
- The allocation of services according to the degree of trust enables security by enhancing the decision-making process between the nodes of the communication network.
- The security issues due to the trust on the connecting nodes or in other words, mismanagement of the trust are well addressed by the proposed model. The estimation of degree of trust enhances the security of the overall network by managing the degree of trust among the devices.

The proposed system model is shown in Fig. 5. The proposed framework is divide into three phases.

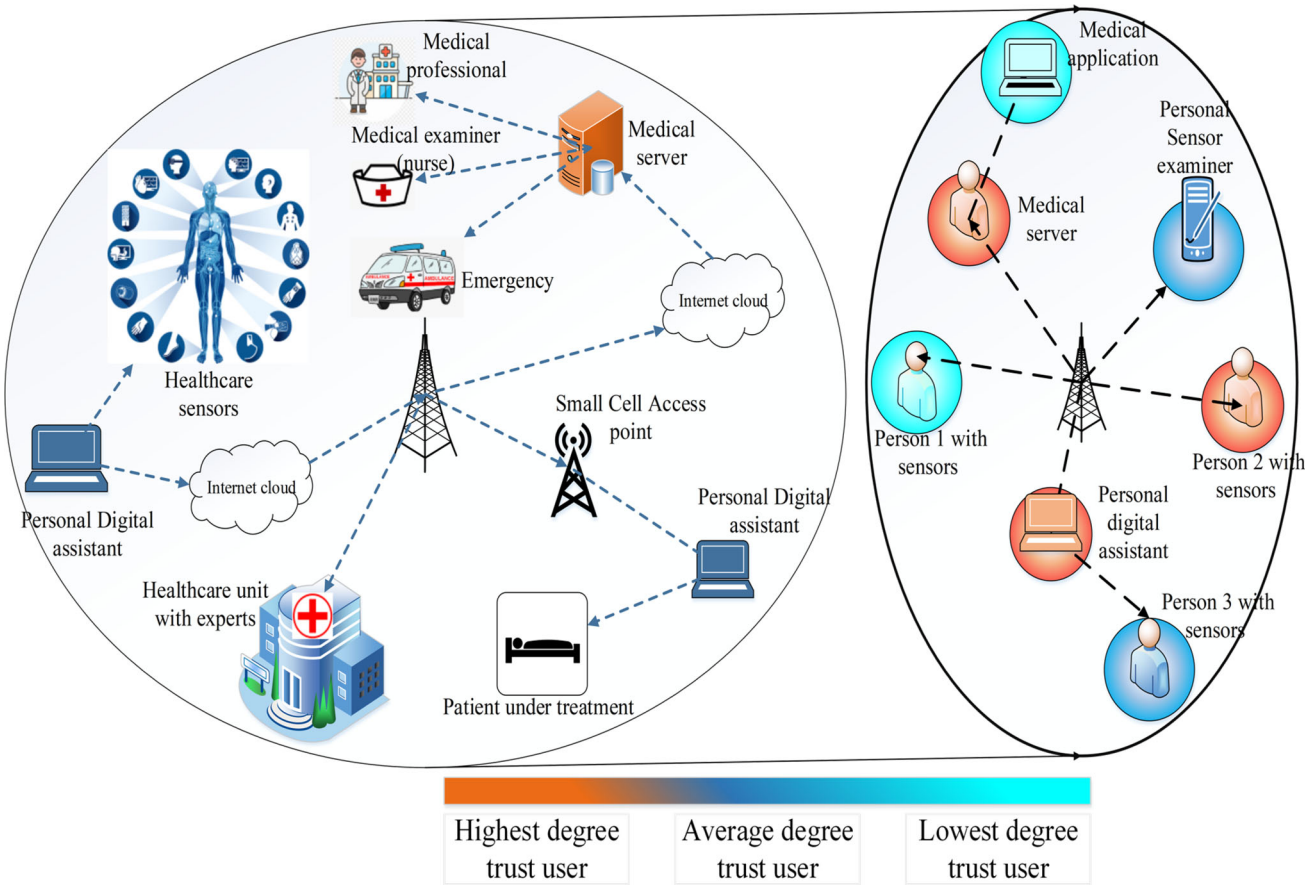


Fig. 5 Proposed system model with trust level security framework

6.1 Parameter estimation

This phase provides the estimation of security parameters for the nodes participating in the network of IoHT. As far as the data of the patient is concerned, the node interaction is required to be trustworthy. Trustworthiness is defined by three.

parameters such as breach history, secrecy capacity, and energy efficiency.

Illustration The process of estimating the parameter values of the model from the different feature data is called parameter estimation. Different features that significantly impact trust and overall security are taken into consideration. Based on the data estimated for the IoHT network various parameter values are estimated such that the trust model is trained as per the estimated data.

6.1.1 Breach history

It is defined as the violation of the security requirements such as the availability of confidential information to the untrustworthy user or spoofing of ID or resources. In the network of IoHT, possible breach sites have tremendously increased due to the improvisation of the cloud network, multi-cooperative communication, and personal user information availability. In 2020 COVID-19 has severely affected security in every part of the world. Due to multiple registrations for medical attention, scams were increased by 400% in March. Breach history depends on the number of registrations done by the patients at any portal with open access.

Illustration The parameter of breach history at time t for the k^{th} node is defined as:

$$B_h[k,\ t] = \sum P_n(n[k,\ t] \in [0,\ 1]) \tag{1}$$

where n is the registrations of nodes having breach history, P_n as the probability for n number of registered nodes. Therefore, for the kth node, the breach history is evaluated as:

$$B_h = \{B_h(1,\ 1),\ B_h(2,\ 1),\ B_h(3,\ 1),\ \ldots,\ B_h(n,\ t)\} \in [0,\ 1] \tag{2}$$

The 0 value denotes the node without breach history while 1 denotes the user with breach history.

Table 2 Recent and prominent challenges in the security of IoHT

Challenge	Interpretation
Hijacking telesurgery robots	A teleoperated surgical robot was the target of cyberattacks by security researchers, who were able to take control of the teleoperated robot during surgery and conduct a denial-of-service attack that brought the robot to a halt and prevented a surgeon from operating.remotelyb
Communication Latency	Medical network of internet things are expected to have minimum tolerance to communication latency as far as end to end processing, data transmission, and operation execution is concerned. Latency on the other hand, in time critical application creates a threat to the security of the IoHT
Interoperable Telesurgery Protocol (ITP)	In telesurgical robots, defining particular specifications related to security and interoperability is still a major challenge in IoHT. However, research on interoperable telesurgery protocol for medical network of internet things is required to be enhanced to develop the secure protocols
AI based Security attacks	The artificial intelligence based security attacks in IoHT creates a serious threat on the parameter of security. These attacks possess the capability to execute adaptively and therefore can compromise and risk lives and health of the people. Research efforts must be carried out effectively to counteract these attacks in IoHT effectively
Limited resources	The sensing level devices in IoHT are associated with limited power resources to execute the operation. More energy efficient security schemes are required to be formulated with the specification of IoHT
Lack of security updates	The security models in IoHT are required to be updated with the capability against the latest possible attacks. Updation of the security models, protocols are required to be regularly followed in the communication network of IoHT
Trust management	Various trust management schemes were developed to enhance the security of IoHT network. However, specific roles or the trust levels or the trusting categories have not been completely addressed for the different types of devices in the network such as device type, trust level, device role
Real-time security status	Real- time security status of the IoHT is of crucial importance as far as various applications such as telesurgery is concerned. However, due to power constraint in the devices of IoHT continous security monitoring is a challenging task to be executed
Accuracy	The correctness of the security mechanism in terms of accuracy in authorization and accuracy in authentication is one of major challenge in IoHT
Computation time	Computational time with the balance of accuracy of the security mechanisms is one of the primary requirement in the fulfillment of security in IoHT networks
Heterogeneity	Using different variety of applications in the communication network of IoHT incorporates various types of devices that exhibit varying characteristics. The execution of security mechanism applicable to these different classes is quite challenging

Table 2 (continued)

Challenge	Interpretation
Resiliency	Resilient, error free security mechanism especially in the IoHT applications such as telesurgery is of primary importance. However, considering various constraints such as low power availability, accuracy, light weight security schemes, achieving an error free response is one of the major challenge that requires immense attention
Intrusion prevention schemes	The approach of intrusion prevention systems can increase the security of IoHT. These strategies are necessary to be able to stop the attacker's impact and keep the system operating without interruption. A security system should also be able to strengthen network security and launch a counterattack on any intruders that are discovered. The adoption of intrusion prevention or security enhancing systems is still a challenge with the current protocol framework
Scalability	Smart healthcare systems are using an increasing number of sensors. As a result, a larger percentage of devices will connect to the global network. Therefore, it is challenging to create a hugely scalable security system while yet adhering to intricate security requirements
Multi-protocol networks	Multiple smart devices are connected to one another as part of the IoHT communication network, which utilizes a proprietary network protocol. It entails the IP network connection of intelligent IoHT devices. Therefore, it is difficult to meet all the security criteria for the diversified and dynamic IoHT system with the current protocol network
Lightweight security schemes	Due to the constraints in computations and power requirements, the security provided by the lightweight security mechanisms is compromised
Remote identity verification	Authorization and authentication in the network of IoHT such as telesurgery requires remote identity verification over an insecure communication channel is a huge challenge in the security of IoHT
Data anonymity	Data anonymity prevents the direct association of the information between the data and the system thereby, enhances the security of the network. However, providing the data anonymity alotng with the encryption is a challenges in the IoHT network
Data collection policies	The data collection policies are required to defined as a complete standard. These policies involve the data access control and monitoring to ensure privacy
Malware detection framework	Malware detection in the current architectural operating systems of IoHT is one challenge in the security that is required to be addressed. Conventional malware detection framework requires updation according to the latest architectural standards of the internet of health care things

6.1.2 Secrecy rate

It is considered as one of the important parameters of security. The security of the network is compromised if the capacity of the intruder is more as compared to the capacity of the valid node. The secrecy rate of the participating node(s) is estimated. The secrecy outage probability for the respective node is defined to evaluate the trustworthiness of the participating node of the IoHT network.

Illustration Consider an IoHT network with k number of users, such that the secrecy rate for the k^{th} node is given by:

$$S_r(k) = \begin{Bmatrix} S_{cv}(k) - S_{ce}(k) & S_{cv}(k) \geq S_{ce}(k) \\ 0 & elsewhere \end{Bmatrix} \tag{3}$$

where $S_{ci} = B_i \log(1+SNR_i), i = validuser, intruder$, S_r is the secrecy rate, S_{cv} is the capacity of the valid user, B is the operating bandwidth, S_{ce} is the capacity of the eavesdropper.

The secrecy outage probability for the respective greater than or equal to 0.7 is taken as 1 and below 0.7 is taken as 0.

$$S_p[k] = P(S_r(k) \in [0,\ 1]) \tag{4}$$

where S_p is the secrecy outage probability.

In other words, secrecy rate is a parameter of data confidentiality. It is a critical parameter of security because it involves protecting sensitive information from unauthorized access and ensuring that only intended parties can view or use it. In the context of network security, especially in the Internet of Health Things (IoHT) framework, secrecy is vital for several reasons such as: maintaining trust, data confidentiality, prevention of data breaches.

6.1.3 Energy efficiency

The trustworthiness of the node is evaluated by the parameter of energy efficiency. The maximum and minimum possible energy efficiency of the respective node at the time instant t is defined. If the node lies in the range, it is considered trustworthy, and if the node does not lie in the range then it is specified as an untrustworthy node.

Illustration The energy efficiency (bps/watt) of the node is defined as the ratio of the capacity of the user to the power consumed as:

$$EE(n) = \frac{S_{cv}(k)}{P_c} \tag{5}$$

The maximum energy efficiency is estimated without the inclusion of additional propagation losses while the minimum energy efficiency is estimated with the inclusion of propagation loss. If the estimated lies in the range between the maximum and minimum energy efficiency, the user is allocated with the value 1 otherwise is allocated with 0 value.

Energy efficiency is the parameter based on capacity and power consumed. It is a crucial security parameter because it helps prevent potential vulnerabilities associated with resource depletion and device failures. In the IoHT network, energy-efficient devices are less likely to suffer from rapid battery depletion, which could be exploited by attackers through resource exhaustion attacks. Efficient energy use also ensures stable device operation, reducing the risk of unauthorized access and disruptions caused by frequent shutdowns or reboots. Additionally, by optimizing energy consumption, network stability is maintained, supporting reliable performance and resilience against multiple attacks. Thus, energy efficiency contributes to overall security by enhancing device longevity, maintaining network reliability, and mitigating potential security risks associated with energy constraints.

6.2 Trust estimation

Trust is the primary parameter of network security. Secure communication is established if the nodes are trustworthy. The proposed framework defines three trust levels for the users. The lowest trust level users are not allowed for active communication with other participating nodes of IoHT. Active communication is defined as the participation in data collection from the sensors of the patient or transmission of the collected data or the allocation of the medical application or the availability of the patient's information. The average trust level users take part in the communication processes such as the availability of patient information, and allocation of medical applications but are not allowed to participate in time-critical communication networks such as telesurgery and are not allowed to participate in decision-making processes such as health care application unit. The highest level of trust users actively participate in the network of IoHT and can take part in multi-cooperative communication. These nodes are highly suitable for time-critical healthcare applications (Table 3).

The 0 indicates that the breach history for the particular node is not present and 1 indicates that the breach history of the node is present. For secrecy rate, 1 indicates that the user lies in the range of minimum and maximum secrecy rate and 0 specifies that the secrecy rate for the user does not lie in the estimated range of maxima and minima. Similarly, for energy efficiency 0 designates the user does not lie in the range of minima and maxima while 1 indicates that the energy efficiency of the user does lie in the calculated range of minima and maxima. The trustworthiness of the nodes is defined by the parameters given in Table 4.

6.3 Updation and monitoring

For every time instant t, the parameter for each participating node is updated such that the evaluation of the trustworthiness is revised. Further, the parameters are continuously monitored for change. If any of the parameters shows a change such that the change in the trust level is observed, the corresponding parameter for the node is updated, and therefore, in the consecutive next iterations, security attacks can be detected and removed from the communication network based on trust management. The frequency of updation

Table 3 Trust prediction analysis using different algorithms for 6G network

Rank type	False negative rate (%)				
	Decision tree	Discriminant	KNN	Ensemble	SVM
First trust rank	0.3	0	0	0.3	0
Second trust rank	0.3	1.1	0	0.3	0.8
Third trust rank	0	1.2	3.5	0	0
Fourth trust rank	0.3	8.1	0	0.3	0.3
Fifth trust rank	0	0	0	0	0
Rank type	False discovery rate (%)				
First trust rank	0.3	0.5	0	0.3	0
Second trust rank	0.3	0	3	0.3	0
Third trust rank	0.3	0.6	0	0.3	1.2
Fourth trust rank	0	1.2	0.3	0	0
Fifth trust rank	0	7.2	0	0	0
Model false discovery rate (%)	0.18	1.9	0.6	0.18	0.24
Model false negative rate (%)	0.18	2.08	0.7	0.18	0.22
Model true positive rate (%)	99.82	97.92	99.3	99.82	99.78
Model accuracy (%)	99.8	98	99.3	99.8	99.8

Table 4 Parameter definitions to determine the trustworthiness

Breach history	Secrecy rate	Energy efficiency	Trust level
0	0	0	Untrustworthy
1	0	0	Untrustworthy
0	1	1	Highest level trust
1	1	1	Average level trust
0	1	0	Lowest level trust
1	0	1	Untrustworthy

is executed based on the type of the network applications and the change of the security parameters corresponding to each node of the network. In time-critical applications such as telesurgery, updation must be of shorter duration to ensure alertness and security in the network for any subsequent changes in the behavior of the node. However, for less critical applications, the updation can occur at regular intervals of time with the consideration of the balance between the security and efficiency of the model. The computational overhead with respect to the proposed scheme is essential for balancing the efficiency of the network while maintaining security. One of the prominent impacts on the computational overheads is the analysis of the limited number of security parameters. Secondly, is the frequency of updation and monitoring of the security status of the network. A balance is required to be maintained to ensure security with low computational overheads.

The overall methodology of the proposed framework nvolves the enhancement of the security in the IoHT network. The proposed scheme involves the three step process. The first first process is the parameter estimation. This process incorporates all nodes present in the network such that the security parameters are determined. These parameters are breach history, secrecy rate and energy efficiency. The second process is the estimation of the trust levels determined for the nodes of the network. The trust levels are allocated based on the values of security parameters. This process is followed by the allocation of the services corresponding to the respective levels. If the node is determined to be untrustworthy, it is removed from the network. The lowest trust level users are not allowed for active communication (both transmission and reception). The average level trust nodes take part in active communication, however, time critical applications and multi-cooperative communication is restricted to these users. The high level trust users participate in the multi-cooperative communication wherein nodes can provide the services to other users as well and can be used for time critical applications such as telesurgery. The proposed framework for the IoHT network can be well understood by the step by step process flow given in the flowchart Fig. 6.

6.3.1 Case study of the 6G network

This case study is about the 6G wireless communication network where trust ranking model can be incorporated. This

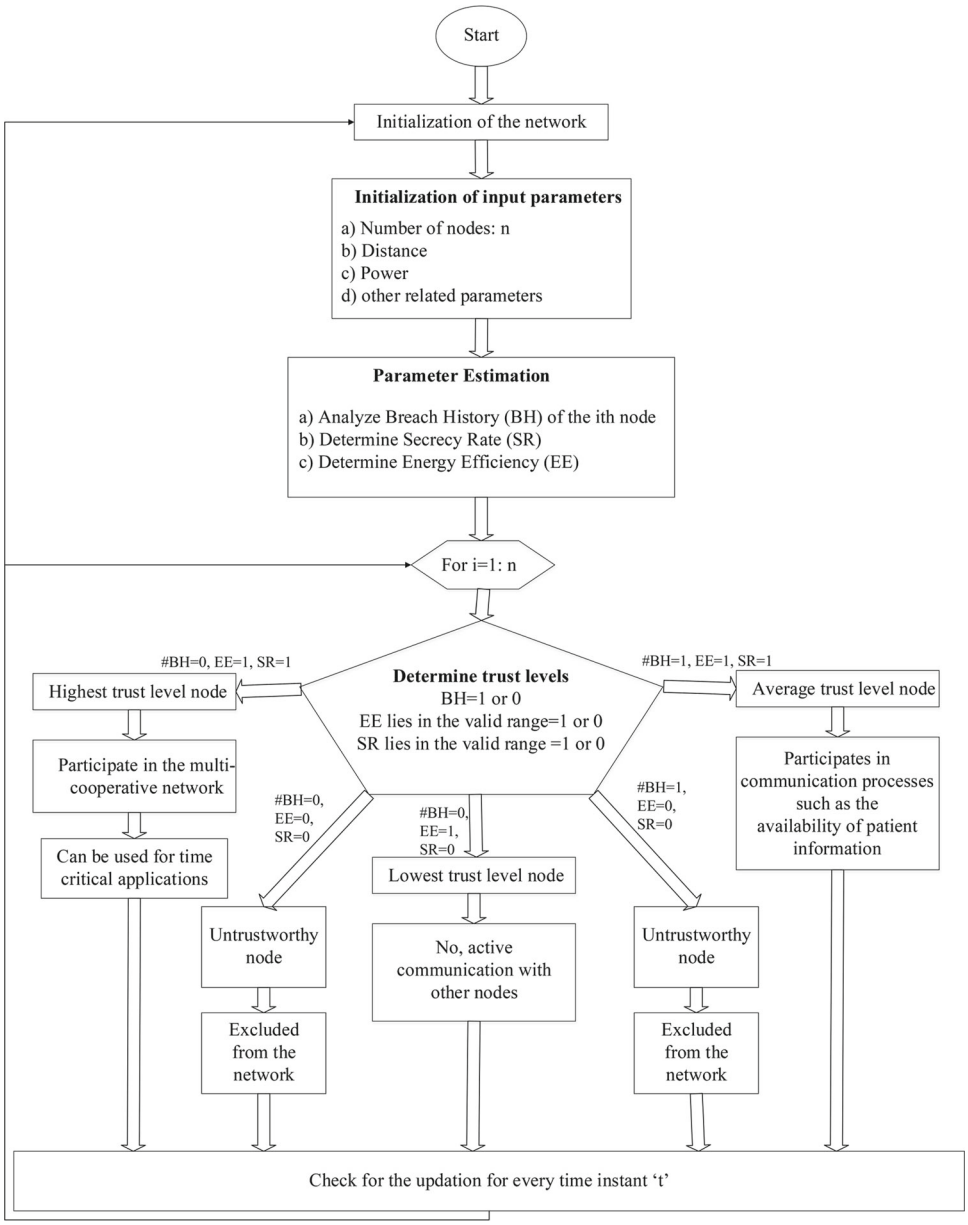


Fig. 6 Flowchart of the proposed mechanism of trust level mechanism

trust ranking model consists of supervised machine learning model. The model is used to predict the trust ranks based on various attributes. Five trust ranks are considered for the model. The fifth rank shows the highest trust, fourth rank shows above moderate trust, third rank as the moderate trust, second rank as the below moderate trust and first rank defines the lowest trust. Based on the ranks of the trust services can be allotted to the users. For highly confidential services fifth rank is followed. The trust ranking model involves the training of the prediction model using the data attributes based on security parameters of the 6G network. After the preprocessing of the data, the training of the model is followed, such that the model is able to predict the rank of the node present in the 6G network. This allows the security enhancement of the network by allowing the services to the users as per the trust rank achieved. For high trust users confidential services are applicable where as for low trust ranks any possible security vulnerable service is not applicable and transmission of artificial noise is initiated for that user to counteract the possible vulnerability. The overall scenario can be show in Fig. 7. below.

The Table 3 shows the results of case study for 6G network, in which whole communication users are identified in the form of different trust ranks using prediction models. The performance of these prediction models for 5 trust ranks are evaluated in this table. Accurate prediction of the trust rank

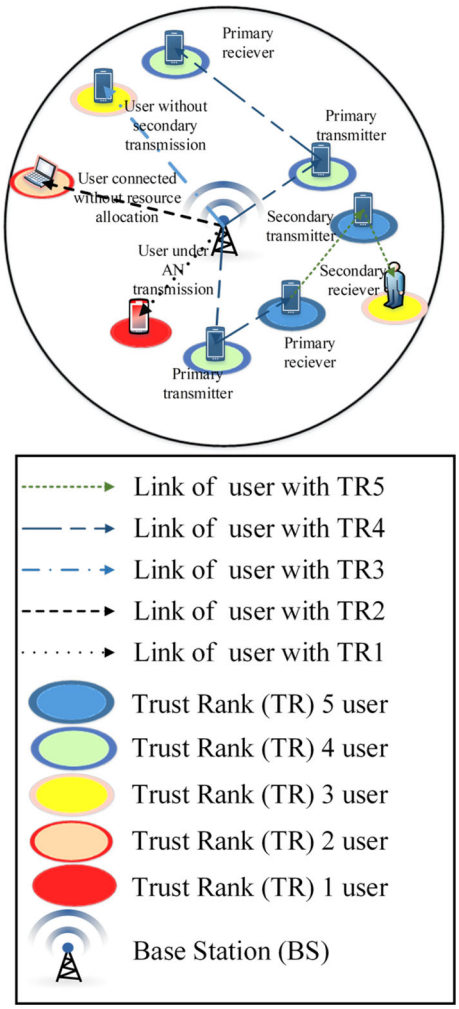


Fig. 7 Trust ranking mechanism in 6G network for 5 trust ranks

defines the security of the network as the services are offered based on the allotted trust rank of the user. Similarly, with the same analogy trust levels can be predicted for the IoHT network.

In view of future research three primary considerations can be incorporated to enhance the security of the IoHT network. The first is the consideration of multiple security attributes of the IoHT network such as time complexity, computational complexity, resource availability, non-repudiation, auditability and other relevant possible security attributes. The second consideration of the future research direction in IoHT network is the number of trust levels. More number of trust levels, more will be the bifurcation of the specific services allotted to the users. However, increasing number of trust levels also increases the complexity of the security model. The third consideration is the involvement of deep learing and machine learning prediction models, optimization models, and the environment based reinforcement learning models.

7 Future research directions in security enhancement of IoHT system

The review on the security of IoHT highlights future research directions in various areas of security. Security in wearable healthcare systems is an emerging field and requires more advancement. Security in the data acquisition and storage based on cloud technologies is another research direction in IoHT. Data processing, algorithm efficiency, and artificial intelligence for the enhancement of the security of IoHT can prove extremely valuable. The research directions listed below are a few examples that can be used to improve the security of IoHT systems [7, 78, 91, 92]. The overall visualization and the other possible future directions in the security enhancement of the IoHT system are shown in Fig. 8.

7.1 Artificial intelligence

Artificial intelligence is one of the prominent and latest research topics inculcated in the various fields including the security of IoHT. Machine learning, deep learning, and reinforcement learning are the primary approaches to artificial intelligence. The different algorithms of machine learning and deep learning are executed in the form of intrusion detection schemes and intrusion prevention schemes. The whole security network in the IoHT can be further improved by optimizing the artificial learning procedures. The security at various levels of the IoHT system can be enhanced by incorporating security examination at the edge level using the schemes of artificial intelligence.

7.2 Security assessment

The proper standard and implementation to ensure security measurement is not present in the literature. Different research directions focused on the areas of security parameter optimization. Various tools such as adversarial analysis were executed to estimate the security level of the IoHT system. However, these mechanisms do not follow the same level of standards, rules, theories, and assumptions. Therefore, the comparison of these varying mechanisms is not a suitable criterion. Security assessment standard is the latest research direction to analyze the levels of security and privacy in the network of the IoHT system. Security assessment in the literature involves the input of the users using a web-based IoHT system evaluated to assess the security. Though, cryptographic solutions are security enhancement mechanisms these schemes do not provide any benchmark for the security assessment. Thus, vast research is required for the development of efficient security assessment schemes in the IoHT system.

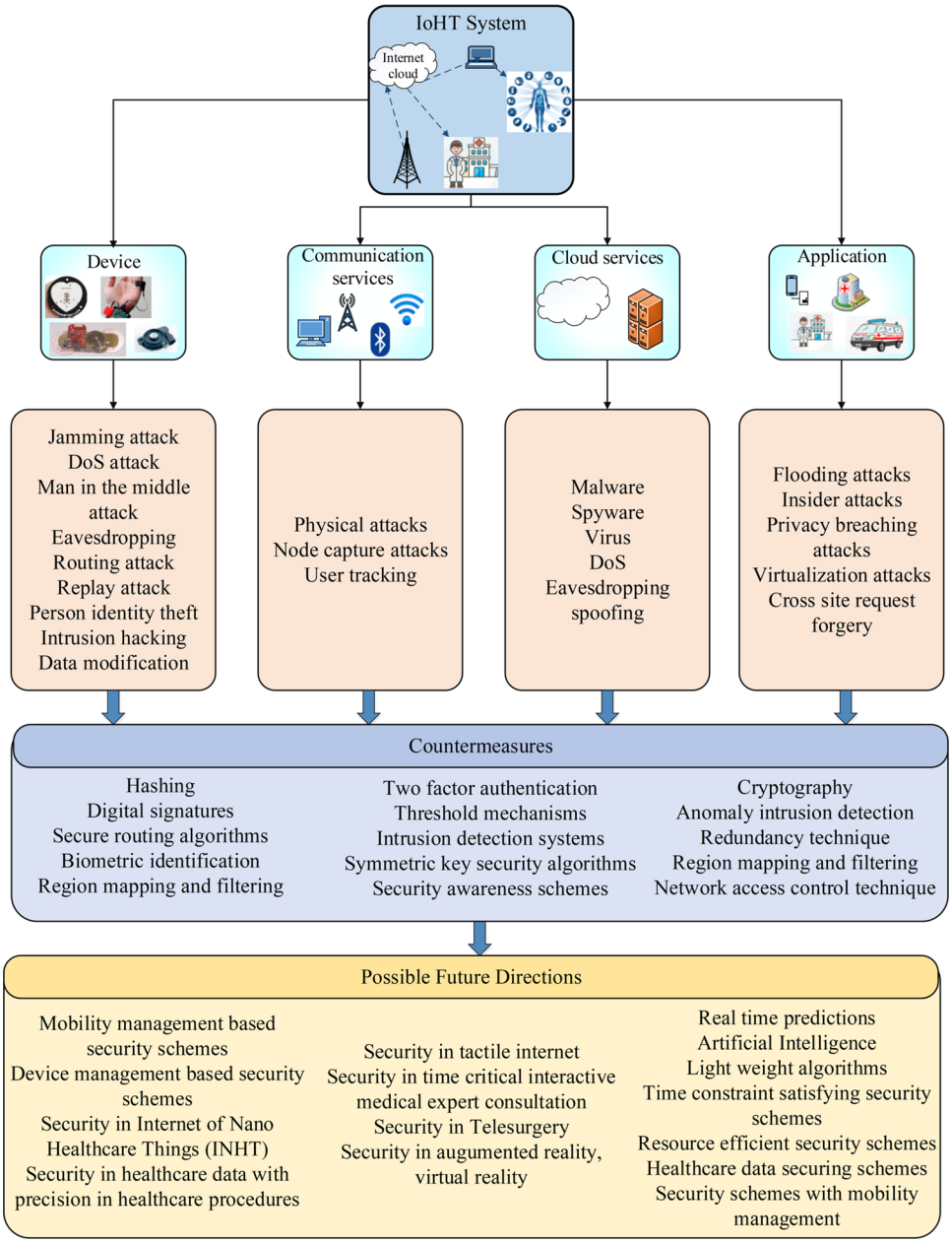


Fig. 8 Security based visualization in IoHT representing IoHT network based security threats, countermeasures and pssible future directions

7.3 Blockchain

In the literature, blockchain has been developed for the security of financial records such that the decentralized mechanism is followed. The mechanism involves the dependency of the blocks on one another. The incorporation of the blockchain mechanism in the IoHT system leads to an extensive enhancement in security. The blockchain scenario can be applied to the server level of the IoHT system to provide decentralized data security. One of the fundamental limitations of the blockchain mechanism is that it requires vast resources for computation and, therefore cannot be operated at the sensor level. To counteract such disadvantages, optimization methods are required, and thus can be adapted at the server level to secure the health data and medical records. Permission management given the blockchain mechanism is one of the schemes evolving in the research field of the IoHT system.

7.4 Smart gateways

Considering entry points of the IoHT system as one of the primary aspects of security authorization and authentication. Smart gateway is the new research direction that proves an enhancement of data security. These gateways are impervious

to different attacks such as denial of service attacks, man-in-the-middle attacks, black hole attacks, routing attacks, and other attacks on the data. A smart gateway is a potential solution for the improvement of data security. More efficient mechanisms are required for the security enhancement in IoHT using smart gateways.

7.5 5 Protocol standardization

Communication in the IoHT network is critical and, therefore requires a balance between content and speed. Various communication protocols were evaluated for different types of sensors used at the sensor level. Protocol standardization is required to generalize the communication in the IoHT system while using different types of sensors to execute the operation seamlessly. Protocol standardization can be further optimized for the time management of data transmission such that the network is optimized without network congestion.

7.6 Trust management

Trust management is one of the latest research directions in the field of security in IoHT systems. The security of the IoHT network can be improved by the incorporation of a trust mechanism on the nodes such that only trusted nodes are capable of communicating in the IoHT network. One of the major advantages of trust management is that the nodes that are identified as trusted nodes are allowed to process and transmit the data in the network. Optimizing trust management in the IoHT using artificial intelligence is one of the ways to advance security adaptability.

7.7 Optimizing energy

The resources at the sensor level are quite limited. Therefore requirement of resources at the sensor level of the IoHT system is required to be optimized. The solution of optimization involves lightweight security enhancement mechanisms, intelligent priority based communication systems, and optimized design algorithms.

7.8 Need for robust health dataset

The availability of the data in healthcare applications is required to be validated whether in the form of numerical data, images, or videos. The acquisition of the data for example, the data on blood type, sugar level, blood pressure, etc. to form the healthcare dataset consists of different information. The procedures of security enhancement in IoHT that depend on artificial intelligence are critical. Therefore, more updated and robust healthcare datasets are required for the advancement of security in the IoHT system.

7.9 Reliability of 6G with IoHT networks

The latest wireless communication network in the form of 6G has gained great recognition. Many communication researchers are working on the development of technologies that can be adopted in the 6G network. Considering 6G as the prominent part in different fields of application, IoHT networks are required to be made reliable with the architecture of 6G.

7.9.1 Data fidelity and data limitation

The introduction of mobile health could solve the limitation of data fidelity. The acquisition of multimodal data collection due to variation of data in terms of time series, system operation, and sensor sampling creates a deterioration in the performance of the IoHT system as a whole. The current IoHT network lacks the potential to manage heterogeneous data efficiently. Therefore, transfer learning is one of the possible techniques to handle the variations in the data. The data reliability issues due to the biased data lead to false or misleading conclusions. Thus, verifying the data fidelity is one of the important aspects that is worthy of exploration.

Overall, in different areas of IoHT network, immediate research is required to enhance the security. Artificial intelligence based models are requisite to be optimized for the advancements in intrusion detection and prevention schemes in IoHT network. Enhancing security standards in the IoHT are of critical importance to deliver uniform and reliable benchmarks. As far as the technology of blockchain in IoHT network is concerned, optimization at the server level, smart gateway mechanisms are the possible security enhancement solutions. Protocol standardization is another primary aspect to advance trust management in the varied sensor network using artificial intelligence based mechanisms. Considering IoHT as the source limited network, energy efficient solutions with latest attributes of security. By incorporating advanced measures in these areas security, reliability and efficiency of the IoHT network can be enhanced.

8 Conclusion

The Internet of Healthcare Things (IoHT) is a network of sensors, servers, and the corresponding medical services where the essential heath data is processed, communicated, and analyzed. The evaluated data is observed for the inconsistencies in providing specific services in terms of medical attention. The advancement such as the involvement of cloud servers, and big data in the technology of IoHT has created a big challenge in the security framework. This work provides a systematic survey of the security of IoHT. To identify the possible security attack, IoHT architecture with the security

visualization is well elaborated in the paper. The recent security concerns in IoHT along with countermeasures have been presented. Incorporating intelligence in the security mechanism of IoHT proves an effective approach. These approaches involve the methodology of machine learning, deep learning, and reinforcement schemes. However, considering the limitations of computational time, complexity, and resource availability, we have proposed a trust evaluation framework for the IoHT network. The whole network is divided into three types of users. The first type is the highest degree trust user. The second type is the average degree trust user and the third type is the lowest degree trust user. The proposed scheme provides security enhancement in the network of IoHT.

It is essential for practitioners to effectively implement the proposed mechanism involving integration of continuous assessment of security parameters in the IoHT network such as breach history, secrecy rate, and energy efficiency in the form of routine security parameter estimations. The dynamicity of the proposed security framework must be maintained such that real time updates of the trust levels with respect to the user must be facilitated with correct service allocations. This ensures confidentiality maintained by the high trust nodes and low trust nodes are restricted to such services. It is recommended, that policymakers create and implement guidelines for trust-based security measures and stimulate research projects that progress IoHT security solutions involving more and more security attributes affecting security of IoHT network. While technology manufacturers should concentrate on creating safe, interoperable products that adhere to these security solutions. Healthcare providers should embrace these frameworks and perform frequent security assessments to guarantee compliance.

Appendix A

Table 5 provides the recent security attacks in the IoHT network. It includes description, strategy of the attack, and consequences of the attack targeting vulnerabilities in IoHT network.

Table 5 Possible security attacks in Internet of Healthcare Things

Citation	Attack	Definition	Strategy of the attack	Consequences of the attack
[11]	Collision attack	In the attack, two input strings for a hash function are analyzed if they yield the same hash value. The hash value being generated by malicious input as by genuine input	It follows the strategy of generating hash values	Attack on confidentiality, authentication
[25]	Ciphertext attack	In this attack, attacker only gets access to a limited number of encrypted communications. The primary goal is to find as many plaintext messages in order to estimate the secret. The subsequent information that have been encrypted with this key can be decrypted once the encryption key has been found	It follows the strategy of estimating the key to convert the ciphertext into plaintext	Attack on the confidentiality
[27]	Impersonation attack	The attack is a spoofing attack where the attacker acts as a legitimate user or group of valid users	It follows the strategy of identity spoofing mechanism and performs active eavesdropping	Attack on confidentiality, integrity, availability, and authentication
[28]	Insider attack	The attack is defined as the malicious attack executed on the network by the authenticated system	The attack follows the strategy of utilizing the inside vulnerabilities using authorized access instead of external attacks	Attack can target the confidentiality, availability, and integrity of the network in the form of perceiving the sensitive information, changing the information or overloading the network

Table 5 (continued)

Citation	Attack	Definition	Strategy of the attack	Consequences of the attack
[29]	Identity spoofing attack	The attack is defined as, spoofing the identity of the valid user and using that identity to get the authenticated access	The attack follows the strategy of using the authenticated identity to perform the desired execution	Attack on confidentiality, authentication, and authorization
[38]	Differential attack	The attack involves the comparison to estimate the required key or plaintext by comparing differences between the input and encrypted output	It involves the estimation of the secret key by involving the comparison between the plaintext and ciphertext	Attack on the confidentiality
[39]	Traffic analysis attack	The attack defines, the attacker modifies the timings of a flow of packets in accordance with a predetermined pattern and searches for that pattern on the opposing side of the network	It follows the strategy of analyzing the flow of packets	Attack on confidentiality
[53]	Quantum attack	Deciphering the techniques that underlie the encryption keys used to protect our data	It makes use of quantum computing to perform the calculations in the form of units called qubits to break the encryption	Attack on confidentiality
[54]	Dictionary attack	By repeatedly inputting every word in a dictionary as a password, a dictionary attack is a technique for accessing a password-protected computer, network, or other IT resource	It follows the strategy of brute force attack	Attack on authentication
[55]	U2R (User to Root) attack	Attackers first acquire access to a regular user account before using system flaws to eventually take control of the root	It follows the strategy of accessing the regular user account and acquires knowledge of the root access details of the system	Attack on authentication
[56]	Machine learning attack	The attack involves the misclassification of inputs and data poisoning	It follows the strategy of misleading the trained model	Security violation, attack on authentication
[57]	MIM (Man in the Middle) attack	The attack involves the eavesdropping between the transmitter and the receiver without the knowledge of the two	It follows the strategy of secretly intercepting the information between the users	Attack on confidentiality and integrity
[61]	Routing attack	A hack against an internet service provider intended to lower uptime or deny users access to a web-enabled system	The attack incorporates the strategy of separating the communication network into parts such that the communication between these is interrupted	Attack on confidentiality, and authentication
[26]	Replay attack	The attack involves the retransmission of the information such that accurate information can be retrieved from the valid user	It follows the strategy of retransmission and interception	Overloading, fraudulent delays, threat to the integrity

Appendix B

Table 6 represents the overview of ongoing projects in IoHT network. It involves brief details of the projects including direct link of the project as well. It provides insights into the current state of IoHT advancements and the attempts being made to address obstacles and innovate in the field by providing a summary of these initiatives.

Table 6 Current Internet of healthcare Thing projects

S.no	Project name	Aim of project	HTTP location
1	Transforming healthcare with 5G	Advancement of remote diagnosis and the development of robotic-assisted surgery	https://www.ericsson.com/en/cases/2016/5gtuscany/transforming-healthcare-with-5g
2	Healthcare IoT solutions	To develop energy-efficient healthcare IoT based systems	https://www.se.com/in/en/work/solutions/for-business/healthcare
3	A.I. Powered Synchronized Stroke Care (Viz pager)	Artificial intelligence-based healthcare monitoring system	https://www.viz.ai/ischemic-stroke
4	Reimagining the possible in the Indian healthcare ecosystem with emerging technologies	To upgrade the healthcare industry in coordination with the emerging networking systems	https://www.pwc.in/industries/healthcare/reimagining-the-possible-in-the-indian-healthcare-ecosystem-with-emerging-technologies.html
5	Smart e-health gateway	To develop IoT based Healthcare systems	https://www.skyfilabs.com/project-ideas/smart-e-health-gateway
6	Deliver intelligent, connected healthcare	To provide real-time based healthcare using cloud technology	https://www.nokia.com/networks/industries/healthcare/
7	Smart autonomous robotic assistant surgeon	To develop a surgical robotic system based on next generation communication to implement robotic minimally invasive surgery	https://saras-project.eu/
8	Medtronic-Robotic assisted surgery	To develop a digital robot-assisted surgery system	https://www.medtronic.com/covidien/en-gb/robotic-assisted-surgery.html?sfdcid=7014O000001JF3G&cid=PPC:GOOG:%2Bsurgical%20%2Brobot:rashug
9	DOBOT magician	To develop a lightweight intelligent robotic arm	https://www.dobot.cc/dobot-magician/product-overview.html?gclid=CjwKCAjwtpGGBhBJEiwAyRZX2n8l3Wec7btI9Dh7HZef6cLce63kcemgBp7CKb7SaazBXQ-aTI4HZRoCFJEQAvD_BwE

Acknowledgements The authors gratefully acknowledge the support provided by SDCSS, ISRO, Central University of Jammu, Jammu and Kashmir, India.

Author's contribution Misbah: Conceptualization, Methodology, Data curation, Writing—Original draft preparation. Rakesh: Formal analysis, Investigation, Visualization, Writing—Review & Editing. Sanjeev: Supervision, Writing—Review & Editing. Mantisha: Editing and review Zeenat: Validation, Resources, Software, Writing—Review & Editing.

Funding The authors have not disclosed any funding.

Data availability No datasets were generated or analysed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

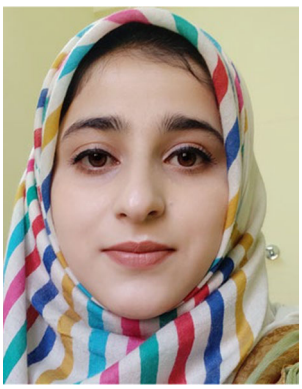
References

1. Meng, W., Cai, Y., Yang, L. T., & Chiu, W.-Y. (2021). Hybrid emotion-aware monitoring system based on brainwaves for Internet of Medical Things. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3079461
2. Awaisi, K. S., Hussain, S., Ahmed, M., Khan, A. A., & Ahmed, G. (2020). Leveraging IoT and fog computing in healthcare systems. *IEEE Internet of Things Magazine, 3*(2), 52–56. https://doi.org/10.1109/IOTM.0001.1900096
3. Chin, W., Chang, C., Tseng, C., Huang, Y., & Jiang, T. (2019). Bayesian real-time QRS complex detector for healthcare system. *IEEE Internet of Things Journal, 6*(3), 5540–5549. https://doi.org/10.1109/JIOT.2019.2903530
4. Bhuiyan, M. N., Rahman, D. M. M., Billah, M. M., & Saha, D. (2021). Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security and market opportunities. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3062630
5. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2021). Recent advances in the Internet-of-Medical-Things (IoMT) systems security. *IEEE Internet of Things Journal, 8*(11), 8707–8718. https://doi.org/10.1109/JIOT.2020.3045653
6. Sun, Y., Lo, F. P., & Lo, B. (2019). Security and privacy for the Internet of Medical Things enabled healthcare systems: A survey. *IEEE Access, 7*, 183339–183355. https://doi.org/10.1109/ACCESS.2019.2960617
7. Algarni, A. (2019). A survey and classification of security and privacy research in smart healthcare systems. *IEEE Access, 7*, 101879–101894. https://doi.org/10.1109/ACCESS.2019.2930962
8. Alladi, T., & Chamola, V. (2021). HARCI: A two-way authentication protocol for three entity healthcare IoT networks. *IEEE Journal on Selected Areas in Communications, 39*(2), 361–369. https://doi.org/10.1109/JSAC.2020.3020605
9. Xu, L., Zhou, X., Tao, Y., Liu, L., Yu, X., & Kumar, N. (2022). Intelligent security performance prediction for IoT-enabled healthcare networks using improved CNN. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2021.3082907
10. Luo, E., Bhuiyan, M. Z. A., Wang, G., Rahman, M. A., Wu, J., & Atiquzzaman, M. (2018). privacyprotector: privacy-protected patient data collection in IoT-based healthcare systems. *IEEE Communications Magazine, 56*(2), 163–168. https://doi.org/10.1109/MCOM.2018.1700364
11. Tao, H., Bhuiyan, M. Z. A., Abdalla, A. N., Hassan, M. M., Zain, J. M., & Hayajneh, T. (2019). Secured data collection with hardware-based ciphers for IoT-based healthcare. *IEEE Internet of Things Journal, 6*(1), 410–420. https://doi.org/10.1109/JIOT.2018.2854714
12. Tang, W., Ren, J., Deng, K., & Zhang, Y. (2019). Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives. *IEEE Internet of Things Journal, 6*(5), 8714–8726. https://doi.org/10.1109/JIOT.2019.2923261
13. Ding, R., Zhong, H., Ma, J., Liu, X., & Ning, J. (2019). Lightweight privacy-preserving identity-based verifiable IoT-based health storage system. *IEEE Internet of Things Journal, 6*(5), 8393–8405. https://doi.org/10.1109/JIOT.2019.2917546
14. He, D., Ye, R., Chan, S., Guizani, M., & Xu, Y. (2018). Privacy in the Internet of Things for smart healthcare. *IEEE Communications Magazine, 56*(4), 38–44. https://doi.org/10.1109/MCOM.2018.1700809
15. Wang, L., Ali, Y., Nazir, S., & Niazi, M. (2020). ISA evaluation framework for security of Internet of Health Things system using AHP-TOPSIS methods. *IEEE Access, 8*, 152316–152332. https://doi.org/10.1109/ACCESS.2020.3017221
16. Islam, A., & Shin, S. Y. (2020). A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things. *Computers & Electrical Engineering, 84*, 10662. https://doi.org/10.1016/j.compeleceng.2020.106627
17. Tsafack, N., et al. (2020). A new chaotic map with dynamic analysis and encryption application in Internet of Health Things. *IEEE Access, 8*, 137731–137744. https://doi.org/10.1109/ACCESS.2020.3010794
18. Awan, K. A., Din, I. U., Almogren, A., Almajed, H., Mohiuddin, I., & Guizani, M. (2021). NeuroTrust—artificial neural network-based intelligent trust management mechanism for large-scale Internet of Medical Things. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2020.3029221
19. Singh, O. P., Anand, A., Agrawal, A. K., & Singh, A. K. (2022). Electronic health data security in the Internet of Things through watermarking: An introduction. *IEEE Internet of Things Magazine, 5*(2), 55–58. https://doi.org/10.1109/IOTM.001.2100122
20. Egala, B. S., Pradhan, A. K., Badarla, V., & Mohanty, S. P. (2021). Fortified-chain: A blockchain-based framework for security and privacy-assured Internet of Medical Things with effective access control. *IEEE Internet of Things Journal, 8*(14), 11717–11731. https://doi.org/10.1109/JIOT.2021.3058946
21. Zheng, Y., Lu, R., Zhang, S., Guan, Y., Shao, J., & Zhu, H. (2022). Toward privacy-preserving healthcare monitoring based on time-series activities over cloud. *IEEE Internet of Things Journal, 9*(2), 1276–1288. https://doi.org/10.1109/JIOT.2021.3079106
22. Zhang, M., Chen, Y., & Susilo, W. (2020). PPO-CPQ: A privacy-preserving optimization of clinical pathway query for E-healthcare systems. *IEEE Internet of Things Journal, 7*(10), 10660–10672. https://doi.org/10.1109/JIOT.2020.3007518
23. Liu, J., Wang, L., & Yu, Y. (2020). Improved security of a pairing-free certificateless aggregate signature in healthcare wireless medical sensor networks. *IEEE Internet of Things Journal, 7*(6), 5256–5266. https://doi.org/10.1109/JIOT.2020.2979613
24. Deebak, B. D., & Al-Turjman, F. (2021). Smart mutual authentication protocol for cloud based medical healthcare systems using Internet of Medical Things. *IEEE Journal on Selected Areas in Communications, 39*(2), 346–360. https://doi.org/10.1109/JSAC.2020.3020599
25. Zhang, Y., He, D., Obaidat, M. S., Vijayakumar, P., & Hsiao, K.-F. (2021). Efficient identity-based distributed decryption scheme for electronic personal health record sharing system. *IEEE Journal*

on Selected Areas in Communications, 39(2), 384–395. https://doi.org/10.1109/JSAC.2020.3020656
26. Wang, Z. (2019). Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected health. *IEEE Internet of Things Journal, 6*(6), 9555–9562. https://doi.org/10.1109/JIOT.2019.2929803
27. Li, X., Peng, J., Obaidat, M. S., Wu, F., Khan, M. K., & Chen, C. (2020). A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Systems Journal, 14*(1), 39–50. https://doi.org/10.1109/JSYST.2019.2899580
28. Meng, W., Li, W., & Zhu, L. (2020). Enhancing medical smartphone networks via blockchain-based trust management against insider attacks. *IEEE Transactions on Engineering Management, 67*(4), 1377–1386. https://doi.org/10.1109/TEM.2019.2921736
29. Meng, Y., Huang, Z., Shen, G., & Ke, C. (2020). SDN-based security enforcement framework for data sharing systems of smart healthcare. *IEEE Transactions on Network and Service Management, 17*(1), 308–318. https://doi.org/10.1109/TNSM.2019.2941214
30. Thamilarasu, G., Odesile, A., & Hoang, A. (2020). An intrusion detection system for Internet of Medical Things. *IEEE Access, 8*, 181560–181576. https://doi.org/10.1109/ACCESS.2020.3026260
31. Krall, A., Finke, D., & Yang, H. (2021). Mosaic privacy-preserving mechanisms for healthcare analytics. *IEEE Journal of Biomedical and Health Informatics, 25*(6), 2184–2192. https://doi.org/10.1109/JBHI.2020.3036422
32. Fang, L., Li, Y., Liu, Z., Yin, C., Li, M., & Cao, Z. J. (2021). A practical model based on anomaly detection for protecting medical IoT control services against external attacks. *IEEE Transactions on Industrial Informatics, 17*(6), 4260–4269. https://doi.org/10.1109/TII.2020.3011444
33. Rezaeibagha, F., Yi, M., Huang, K., & Chen, L. (2021). Secure and efficient data aggregation for IoT monitoring systems. *IEEE Internet of Things Journal, 8*(10), 8056–8063. https://doi.org/10.1109/JIOT.2020.3042204
34. Chinaei, M. H., Gharakheili, H. H., & Sivaraman, V. (2021). Optimal witnessing of healthcare IoT data using blockchain logging contract. *IEEE Internet of Things Journal, 8*(12), 10117–10130. https://doi.org/10.1109/JIOT.2021.3051433
35. Sun, Y., Liu, J., Keping, Y., Alazab, M., & Lin, K. (2022). PMRSS: Privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. *IEEE Transactions on Industrial Informatics, 18*(3), 1981–1990. https://doi.org/10.1109/TII.2021.3070544
36. Jan, M. A., Khan, F., Mastorakis, S., Adil, M., Akbar, A., & Stergiou, N. (2021). LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. *IEEE Transactions on Green Communications and Networking, 5*(3), 1202–1211. https://doi.org/10.1109/TGCN.2021.3077318
37. Masud, M., Gaba, G. S., Choudhary, K., Hossain, M. S., Alhamid, M. F., & Muhammad, G. (2022). Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3080461
38. Wang, J., et al. (2021). A multistage blockchain-based secure and trustworthy smart healthcare system using ECG characteristic. *IEEE Internet of Things Magazine, 4*(3), 48–58. https://doi.org/10.1109/IOTM.0101.2000182
39. Radoglou-Grammatikis, P., et al. (2022). Modeling, detecting, and mitigating threats against industrial healthcare systems: A combined software defined networking and reinforcement learning approach. *IEEE Transactions on Industrial Informatics, 18*(3), 2041–2052. https://doi.org/10.1109/TII.2021.3093905
40. Pradhan, M., & Mohanty, S. (2024). A blockchain-assisted multi-factor authentication protocol for enhancing IoMT security. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2024.3422242
41. Awan, K. A., Din, I. U., Almogren, A., & Rodrigues, J. J. P. C. (2024). MediTwin: A web 3.0-integrated digital twin for secure patient-centric healthcare in the metaverse. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2024.3409845
42. Zukaib, U., Cui, X., Zheng, C., Hassan, M., & Shen, Z. (2024). Meta-IDS: Meta-learning-based smart intrusion detection system for Internet of Medical Things (IoMT) network. *IEEE Internet of Things Journal, 11*(13), 23080–23095. https://doi.org/10.1109/JIOT.2024.3387294
43. Reddi, S., et al. (2024). Privacy-preserving electronic medical record sharing for IoT-enabled healthcare system using fully homomorphic encryption, IOTA, and masked authenticated messaging. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2024.3397343
44. Rahman, M. Z. U., Akunuri, S., Nagabhushana Babu, D., Ramprasad, M. V. S., Mohammed Shareef, S., & Bayleyegn, M. D. (2024). Proof of trust and expertise (PoTE): A novel consensus mechanism for enhanced security and scalability in electronic health record management. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3424685
45. Yang, N., Tang, C., Xiong, Z., & He, D. (2024). RCME: A reputation incentive committee consensus-based for matchmaking encryption in IoT healthcare. *IEEE Transactions on Services Computing*. https://doi.org/10.1109/TSC.2024.3387691
46. Saha, S., Das, A. K., Wazid, M., Park, Y., Garg, S., & Alrashoud, M. (2024). Smart contract-based access control scheme for blockchain assisted 6G-enabled IoT-based big data driven healthcare cyber physical systems. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2024.3391667
47. Chen, C.-M., Chen, Z., Kumari, S., Obaidat, M. S., Rodrigues, J. J. P. C., & Khan, M. K. (2024). Blockchain-based mutual authentication protocol for IoT-enabled decentralized healthcare environment. *IEEE Internet of Things Journal, 11*(14), 25394–25412. https://doi.org/10.1109/JIOT.2024.3396488
48. Alferaidi, A., et al. (2024). A novel hybrid, BERT and deep learning model network intrusion detection system for healthcare electronics. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2024.3412199
49. Almogren, A., Mohiuddin, I., Din, I. U., Almajed, H., & Guizani, N. (2021). FTM-IoMT: Fuzzy-based trust management for preventing sybil attacks in Internet of Medical Things. *IEEE Internet of Things Journal, 8*(6), 4485–4497. https://doi.org/10.1109/JIOT.2020.3027440
50. Shim, K.-A. (2019). Universal forgery attacks on remote authentication schemes for wireless body area networks based on Internet of Things. *IEEE Internet of Things Journal, 6*(5), 9211–9212. https://doi.org/10.1109/JIOT.2019.2922701
51. Mishra, N., & Pandya, S. (2021). Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access, 9*, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408
52. Saheed, Y. K., & Arowolo, M. O. (2021). Efficient cyber attack detection on the Internet of Medical Things-smart environment based on deep recurrent neural network and machine learning algorithms. *IEEE Access, 9*, 161546–161554. https://doi.org/10.1109/ACCESS.2021.3128837
53. Fernández-Caramés, T. M. (2020). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. *IEEE Internet of Things Journal, 7*(7), 6457–6480. https://doi.org/10.1109/JIOT.2019.2958788
54. Masud, M., Gaba, G. S., Choudhary, K., Hossain, M. S., Alhamid, M. F., & Muhammad, G. (2022). Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare.

IEEE Internet of Things Journal, 9(4), 2649–2656. https://doi.org/10.1109/JIOT.2021.3080461
55. Latif, S., Zou, Z., Idrees, Z., & Ahmad, J. (2020). A novel attack detection scheme for the industrial Internet of Things using a lightweight random neural network. *IEEE Access, 8*, 89337–89350. https://doi.org/10.1109/ACCESS.2020.2994079
56. Gope, P., Millwood, O., & Sikdar, B. (2022). A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for Internet of Medical Things. *IEEE Transactions on Industrial Informatics, 18*(3), 1971–1980. https://doi.org/10.1109/TII.2021.3096048
57. Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A., & Boutaba, R. (2022). Man-in-the-middle attack mitigation in Internet of Medical Things. *IEEE Transactions on Industrial Informatics, 18*(3), 2053–2062. https://doi.org/10.1109/TII.2021.3089462
58. Guo, R., Yang, G., Shi, H., Zhang, Y., & Zheng, D. (2021). O3-R-CP-ABE: An efficient and revocable attribute-based encryption scheme in the cloud-assisted IoMT system. *IEEE Internet of Things Journal, 8*(11), 8949–8963. https://doi.org/10.1109/JIOT.2021.3055541
59. Ke, C., Zhu, Z., Xiao, F., Huang, Z., & Meng, Y. (2022). SDN-based privacy and functional authentication scheme for fog nodes of smart healthcare. *IEEE Internet of Things Journal, 9*(18), 17989–18001. https://doi.org/10.1109/JIOT.2022.3161935
60. Babbar, H., Rani, S., & AlQahtani, S. A. (2022). Intelligent edge load migration in SDN-IIoT for smart healthcare. *IEEE Transactions on Industrial Informatics, 18*(11), 8058–8064. https://doi.org/10.1109/TII.2022.3172489
61. Agiollo, A., Conti, M., Kaliyar, P., Lin, T.-N., & Pajola, L. (2021). DETONAR: Detection of routing attacks in RPL-based IoT. *IEEE Transactions on Network and Service Management, 18*(2), 1178–1190. https://doi.org/10.1109/TNSM.2021.3075496
62. Garg, N., Wazid, M., Das, A. K., Singh, D. P., Rodrigues, J. J. P. C., & Park, Y. (2020). BAKMP-IoMT: Design of blockchain enabled authenticated key management protocol for Internet of Medical Things deployment. *IEEE Access, 8*, 95956–95977. https://doi.org/10.1109/ACCESS.2020.2995917
63. Chen, M., & Lee, T.-F. (2021). Anonymous group-oriented time-bound key agreement for Internet of Medical Things in telemonitoring using chaotic maps. *IEEE Internet of Things Journal, 8*(18), 13939–13949. https://doi.org/10.1109/JIOT.2021.3068489
64. Ebrahimi, M., Haghighi, M. S., Jolfaei, A., Shamaeian, N., & Tadayon, M. H. (2022). A secure and decentralized trust management scheme for smart health systems. *IEEE Journal of Biomedical and Health Informatics, 26*(5), 1961–1968. https://doi.org/10.1109/JBHI.2021.3107339
65. Yang, W., Wang, S., & Mu, Y. (2021). An enhanced certificateless aggregate signature without pairings for E-healthcare system. *IEEE Internet of Things Journal, 8*(6), 5000–5008. https://doi.org/10.1109/JIOT.2020.3034307
66. Liu, Y., Yu, J., Fan, J., Vijayakumar, P., & Chang, V. (2022). Achieving privacy-preserving dsse for intelligent IoT healthcare system. *IEEE Transactions on Industrial Informatics, 18*(3), 2010–2020. https://doi.org/10.1109/TII.2021.3100873
67. Wang, W., et al. (2022). Blockchain and PUF-based lightweight authentication protocol for wireless medical sensor networks. *IEEE Internet of Things Journal, 9*(11), 8883–8891. https://doi.org/10.1109/JIOT.2021.3117762
68. Gouissem, A., Abualsaud, K., Yaacoub, E., Khattab, T., & Guizani, M. (2022). Toward secure IoT networks in healthcare applications: A game-theoretic anti-jamming framework. *IEEE Internet of Things Journal, 9*(20), 19615–19633. https://doi.org/10.1109/JIOT.2022.3170382
69. Ullah, I., Alkhalifah, A., Rehman, S. U., Kumar, N., & Khan, M. A. (2021). An anonymous certificateless signcryption scheme for Internet of Health Things. *IEEE Access, 9*, 101207–101216. https://doi.org/10.1109/ACCESS.2021.3097403
70. Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Islam, A. K. M. N., & Shorfuzzaman, M. (2022). Permissioned blockchain and deep learning for secure and efficient data sharing in industrial healthcare systems. *IEEE Transactions on Industrial Informatics, 18*(11), 8065–8073. https://doi.org/10.1109/TII.2022.3161631
71. Qadri, Y. A., Nauman, A., Zikria, Y. B., Vasilakos, A. V., & Kim, S. W. (2020). The future of healthcare Internet of Things: A survey of emerging technologies. *IEEE Communications Surveys & Tutorials, 22*(2), 1121–1167. https://doi.org/10.1109/COMST.2020.2973314
72. Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of Things for smart healthcare: technologies, challenges, and opportunities. *IEEE Access, 5*, 26521–26544. https://doi.org/10.1109/ACCESS.2017.2775180
73. Amin, S. U., & Hossain, M. S. (2021). Edge intelligence and Internet of Things in healthcare: A survey. *IEEE Access, 9*, 45–59. https://doi.org/10.1109/ACCESS.2020.3045115
74. Firouzi, F., et al. (2022). Fusion of IoT, AI, edge-fog-cloud, and blockchain: challenges, solutions, and a case study in healthcare and medicine. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2022.3191881
75. Akter, M., Moustafa, N., Lynar, T., & Razzak, I. (2022). Edge intelligence: federated learning-based privacy protection framework for smart healthcare systems. *IEEE Journal of Biomedical and Health Informatics*. https://doi.org/10.1109/JBHI.2022.3192648
76. Liu, W., et al. (2022). Lead separation and combination: A novel unsupervised 12-lead ECG feature learning framework for Internet of Medical Things. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2022.3188771
77. Lai, Q. H., & Lai, C. S. (2022). Healthcare with wireless communication and smart meters. *IEEE Consumer Electronics Magazine*. https://doi.org/10.1109/MCE.2022.3181438
78. Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated learning for privacy preservation in smart healthcare systems: A comprehensive survey. *IEEE Journal of Biomedical and Health Informatics*. https://doi.org/10.1109/JBHI.2022.3181823
79. Gupta, B. B., & Lytras, M. D. (2022). Fog-enabled secure and efficient fine-grained searchable data sharing and management scheme for IoT-based healthcare systems. *IEEE Transactions on Engineering Management*. https://doi.org/10.1109/TEM.2022.3143661
80. Mazzocca, C., Romandini, N., Colajanni, M., & Montanari, R. (2022). FRAMH: A federated learning risk-based authorization middleware for healthcare. *IEEE Transactions on Computational Social Systems*. https://doi.org/10.1109/TCSS.2022.3210372.ci
81. Bhuiyan, M. N., Rahman, M. M., Billah, M. M., & Saha, D. (2021). Internet of Things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal, 8*(13), 10474–10498. https://doi.org/10.1109/JIOT.2021.3062630
82. Karunarathne, S. M., Saxena, N., & Khan, M. K. (2021). Security and privacy in IoT smart healthcare. *IEEE Internet Computing, 25*(4), 37–48. https://doi.org/10.1109/MIC.2021.3051675
83. Lee, E., Seo, Y.-D., Oh, S.-R., & Kim, Y.-G. (2021). A survey on standards for interoperability and security in the Internet of Things. *IEEE Communications Surveys & Tutorials, 23*(2), 1020–1047. https://doi.org/10.1109/COMST.2021.3067354

84. Alshehri, F., & Muhammad, G. (2021). A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access, 9*, 3660–3678. https://doi.org/10.1109/ACCESS.2020.3047960
85. Yang, Z., Liang, B., & Ji, W. (2021). An intelligent end-edge-cloud architecture for visual IoT assisted healthcare systems. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3052778
86. Habibzadeh, H., Dinesh, K., Rajabi Shishvan, O., Boggio-Dandry, A., Sharma, G., & Soyata, T. (2020). A survey of healthcare Internet of Things (HIoT): A clinical perspective. *IEEE Internet of Things Journal, 7*(1), 53–71. https://doi.org/10.1109/JIOT.2019.2946359
87. Kumar, M., & Chand, S. (2020). A secure and efficient cloud-centric Internet-of-Medical-Things-enabled smart healthcare system with public verifiability. *IEEE Internet of Things Journal, 7*(10), 10650–10659. https://doi.org/10.1109/JIOT.2020.3006523
88. Somasundaram, R., & Thirugnanam, M. (2020). Review of security challenges in healthcare Internet of Things. *Wireless Networks*. https://doi.org/10.1007/s11276-020-02340-0
89. Egala, B. S., Pradhan, A. K., Badarla, V. R., & Mohanty, S. P. (2021). Fortified-chain: A blockchain based framework for security and privacy assured Internet of Medical Things with effective access control. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2021.3058946
90. Ketu, S., & Mishra, P. K. (2021). Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications, 192*, 103179. https://doi.org/10.1016/j.jnca.2021.103179
91. Wang, Z., et al. (2022). From personalized medicine to population health: A survey of mhealth sensing techniques. *IEEE Internet of Things Journal, 9*(17), 15413–15434. https://doi.org/10.1109/JIOT.2022.3161046
92. Abualsaud, K. (2022). Machine learning algorithms and Internet of Things for healthcare: A survey. *IEEE Internet of Things Magazine, 5*(2), 133–139. https://doi.org/10.1109/IOTM.003.2100061



Misbah Shafi received her B.Tech degree and M.Tech degree in Electronics and Communication Engineering in 2016 and 2018. She has done her Ph.D. degree in Electronics and Communication Engineering from SMVD University, J&K. She is currently associated with SDCSS, ISRO, Central University of Jammu, Jammu and Kashmir. Her research interest includes network security in emerging technologies of 5G, 5GNR, and 6G wireless communication networks, cryptography, optical fiber communication networks, machine learning, and deep learning.

Rakesh Kumar Jha (S'10, M'13, SM 2015) is currently working as an associate professor in the department of Electronics and Communication Engineering, Indian Institute of Information Technology Design and Manufacturing Jabalpur, India. He has also worked as an associate professor at SMVD University, J&K, India. He is among the top 2% of research scientists in the world. He has published more than 55 Science Citation Index Journals Papers including many IEEE Transactions, IEEE Journal, and more than 25 International Conference papers. His area of interest is Wireless communication, Optical Fiber Communication, Computer Networks, and Security issues. Dr. Jha's concept related to the router of Wireless Communication was accepted by ITU in 2010. He received the Young Scientist Author Award from ITU in Dec 2010. He has received an APAN fellowship in 2011, 2012, 2017, and 2018 and a student travel grant from COMSNET 2012. He is a senior member of IEEE, GISFI, and SIAM, International Association of Engineers (IAENG), and ACCS (Advance Computing and Communication Society). He is also a member of, ACM and CSI, with many patents and more than 5100 citations on his credit.

Sanjeev Jain is currently working as a vice chancellor of the Central University of Jammu, Jammu and Kashmir, India. He has worked as a director at Indian Institute of Information Technology Design and Manufacturing Jabalpur, India. He has also worked as a vice chancellor at SMVD University, Katra. He has served as Director, of Madhav Institute of Technology and Science (MITS), Gwalior. Besides teaching, he has the credit of making significant contributions to R&D in the area of Image Processing and Mobile ad hoc Networks. His work on Digital Watermarking for Image Authentication is highly valued in the research field.

Mantisha Gupta (Student Member, IEEE) received her B.E degree in Electronics and Communication Engineering from Jammu University, J&K, India in 2017 and the M.Tech Degree in Electronics and Communication Engineering from Shri Mata Vaishno Devi University(SMVDU), Katra, Jammu, J&K, India in 2019. She is pursuing a PhD in IoT-configured networks in B5G/6G wireless communication systems from the School of Electronics and Communication Engineering(SoECE), at Shri Mata Vaishno Devi University (SMVDU). She is a student member of the Institute of Electrical and Electronics Engineers (IEEE).

Zeenat Zahra received B.Tech degree in information technology and engineering from Baba Ghulam Shah Badshah University Rajouri, Jammu and Kashmir, India, in 2021. She is currently pursuing an M.Tech degree in computer science and information technology at Central University Of Jammu, Jammu and Kashmir. Her research interest includes machine learning and image processing. Currently, she is doing her research on Hybrid and efficient iris vitality detectors.