Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1629

ORIGINAL RESEARCH ARTICLE

A smart agent-based approach for privacy preservation and threat mitigation to enhance security in the Internet of Medical Things

Archana Rani[1,*], Naresh Grover[2], N. Deepa[3], C. Prajitha[4]

[1] *G.D. Goenka University, Gurgaon 122103, India*

[2] *MRIIRS, Faridabad 121004, India*

[3] *Department of Computer Science and Engineering, Saveetha School of Engineering, SIMATS, Saveetha University, Chennai 602105, India*

[4] *Department of Electronics and Communication Engineering/Centre for Interdisciplinary Research, Karpagam Academy of Higher Education, Coimbatore 641021, India*

*** Corresponding author:** Archana Rani, archana.bhatia.pec@gmail.com

ABSTRACT

Integrating medical sensors and the Internet of Things (IoT) within smart healthcare has facilitated the development of an advanced framework known as the Internet of Medical Things (IoMT). This framework enables the detection and assessment of the severity of participants' conditions. Nevertheless, local IoMT devices' constrained storage capacity and computational capabilities necessitate transferring participants' health data to different devices for investigation. However, this transfer poses a significant risk of privacy breaches due to the absence of complete power over the participant's health information and the system's susceptibility to various attacks. This research presents a Smart Agent-based Privacy Preservation and Threat Mitigation Framework (SAPPTMF) for augmenting security in IoMT using an intelligent agent system. The framework involves the development of a complete system model that spans a range of components and interactions within the IoMT ecosystem. An attacker model is developed to simulate various threat situations. A thorough assessment framework is used to assess the efficacy of security measures, encompassing both the evaluation of security measures and the decision-making process. The analytic hierarchy process (AHP) provides suitable weights to various security needs or criteria. The findings provide the following performance metrics: accuracy (94.5%), precision (91.0%), recall (93.4%), *F*-score (92.4%), and mean squared error (MSE) of 0.09.

Keywords: Internet of medical things; security; healthcare data; privacy preservation

ARTICLE INFO

Received: 5 March 2024
Accepted: 28 March 2024
Available online: 24 May 2024

1. Introduction to healthcare and security issues

IoT has been widely implemented in smart travel, business, grid, and smart cities[1–3]. Among these applications, IoT technology in healthcare, specifically in the IoMT, has garnered significant interest. Using a range of wearable sensors, the IoMT framework has effectively incorporated sensor technologies to monitor a participant's health from a distance[4]. The IoMT reduces needless hospital stays and reduces the stress on the healthcare system by establishing safe communication between medical specialists and participants[5]. This connectivity eventually results in significant time and cost savings. The exponential growth in IoT devices inside healthcare networks has significantly impacted the financial sector in recent years. The adoption of the IoMT is seeing a significant upward trend, with around 65% of healthcare companies worldwide

having used this technology. By 2025, the IoMT adoption rate will rise more than 38%[6,7].

IoMT devices in healthcare settings are vulnerable to many cyber threats and assaults. The healthcare business encounters more security vulnerabilities, around 380% more, than other industries[8]. It exhibits a higher exposure to data theft and is approximately 250% more vulnerable. Research shows that a significant majority of organizations, namely over 95%, encounter at least one security breach[9]. It has been proposed that the IoMT system experiences an average of 180 cyber threats reported per 1000 linked host devices[10]. The deployment of IoMT devices in networks without enough security consideration has been identified as the primary cause of concerns related to privacy, reliability, and accessibility[11,12]. These vulnerabilities enable hackers to unauthorized access the IoMT network, facilitating the acquisition of sensitive and confidential information about participants[13]. One of the significant challenges IoMT devices encounter is concerns around safety and confidentiality.

The challenges in the available methods are listed below:

- IoT devices' constrained local storage and computational capabilities provide limitations for processing health data[14].
- One potential concern is the risk of privacy breaches resulting from the sharing of data remotely and the limited control over participant data.
- The susceptibility of networks to different forms of cyberattacks[15].
- The existing frameworks for the IoMT suffer from inadequate or fragmented security mechanisms.

The proposed method makes many primary contributions to the field, and those are listed below:

- This research introduces an intelligent agent system to enhance security in IoMT settings.
- A comprehensive system model that encompasses the components and interactions of the IoMT ecosystem.
- The Attacker Model should be expanded to replicate several possible threat situations, facilitating rigorous testing.
- The analytic hierarchy process (AHP) is proposed to facilitate the equitable allocation of security weights, improving decision-making and prioritizing risks.

The rest of the manuscript follows: Section 2 investigates the current knowledge and research about healthcare security and the IoMT. Section 3 presents the Smart Agent-based Privacy Preservation and Threat Mitigation Framework (SAPPTMF) and its extensive functionalities. Section 4 presents the simulation results obtained from the implementation of SAPPTMF and provides a comprehensive discussion of the outcomes attained. Section 5 concisely explains the analysis and implications and proposes prospective avenues for future research.

2. Literature survey and findings

This section examines the convergence of healthcare, the IoMT, and security. This study explores the dynamic environment of networked medical devices, reviewing their capacity to transform participant care while also considering issues related to data privacy, authentication, and protection against cyber attacks. Through a comprehensive analysis of existing scholarly literature, this part offers helpful information about the obstacles and progress that influence the incorporation of the IoMT into safe healthcare environments. Zaabar et al.[16] provided an innovative mechanism for managing health records called HealthBlock, which utilizes blockchain technology to ensure robust security measures. HealthBlock offers superior data security and privacy outcomes compared to conventional centralized solutions by capitalizing on the decentralized nature of blockchain technology. The findings from the simulation demonstrate a noteworthy reduction of 30% in data breaches and a substantial drop of 40% in unauthorized access attempts. The benefits include secure data storage that is resistant to tampering and the capacity to maintain comprehensive documents

detailing every action for auditing purposes. However, it is essential to recognise the existence of potential problems in terms of scalability when using this method within a healthcare ecosystem of a significant size. Singh et al. proposed a conceptual framework that leverages blockchain technology to ensure healthcare data privacy in the IoT[17]. The approach encompasses the collaborative training of machine learning models on several decentralized devices, with a concurrent focus on safeguarding data privacy via blockchain encryption techniques. The suggested methodology successfully provides improved privacy protection, as simulation results demonstrate a 25% decrease in data leakage compared to standard methods. The framework's key benefits are distributed model training and safe data-sharing capabilities. It is essential to acknowledge that the architecture also exhibits several downsides, such as its inherent complexity and the significant resource overhead it requires.

Miyachi et al. proposed a unique outline to ensure privacy in the context of healthcare data via blockchain infrastructure[18]. This framework incorporates both on-chain and off-chain components in its system architecture. The proposed methodology effectively partitions confidential participant information from transactional details to address privacy issues while preserving the capacity to monitor and track transactions. The hybrid approach demonstrates effective data management and enhanced privacy, as simulation results indicate a 15% improvement in data confidentiality compared to current systems. The framework reflects its efficacy via its ability to strike a harmonious balance between privacy and openness—however, the intricate nature of its implementation and the possible vulnerabilities that exist off-chain present significant obstacles. Kishor et al. provided a novel approach that utilizes fog computing, the IoT, and machine learning techniques to segregate healthcare data effectively[19]. Edge computing in data processing at the network's periphery has been seen to boost real-time data analysis and mitigate latency. The benefits include effective data management and decreased data transmission. At the same time, its shortcomings encompass possible reliance on a reliable fog computing infrastructure and limited suitability for resource-constrained applications.

Nguyen et al. proposed a robust cyber-physical system for healthcare that incorporates blockchain technology, Deep Belief Networks (DBNs), and ResNet models to provide enhanced security measures[20]. Deep learning is included into the suggested method and blockchain technologies to augment security and ensure data integrity inside healthcare systems. The results of the simulation demonstrate a level of accuracy of 95% in the detection of harmful activity. The positives of this technique include its enhanced capabilities in detecting and preventing threats.

Wang et al.[21] developed eight secure calculation methods to enable the cloud server to efficiently perform fundamental integer and floating-point calculations, to ensure training the support vector machine (SVM). The suggested method ensures the trained SVM model's safety while safeguarding the training data's privacy. Equivalent classification accuracy to a generic SVM is achieved according to the performance test results conducted using two real-world illness data sets.

Zhang et al.[22] suggested a parallel ECG-based authentication method to enhance the extraction that combines fiducial and non-fiducial-based characteristics. This technique would extract more complete ECG features. Improving identification efficiency in numerous ECG feature spaces is another goal of this paper's parallel ECG detection architecture. The suggested verification was tested and found to work in the trials with the Linear Discriminant Analysis (LDA)[22].

Kaushal et al.[23] developed PCA to collect data characteristics. The relevant factors are selected using a feature selection procedure based on genetic algorithms. The suggested system is evaluated using the MATLAB simulation tool, and the metrics are compared to the industry standards. The proposed and current methods are estimated based on criteria for processing time, security level, and encryption time.

Deepa et al.[24] developed a new approach based on machine learning for predicting the risk associated

with COVID-19. Predictions are made using sensor data using the Naive Bayes (NB) classifier. By classifying individuals, we may lessen the disease's effect on the larger population of that group. Compared to NB, whose accuracy is 99%, RF's is 97%.

Liang et al.[25] suggested a decision tree (DT) categorization technique that is both efficient and secure. To be more precise, the clinical decision model, which is a decision tree classifier, is converted into Boolean vectors first. Next, we encode the Boolean vectors into encrypted indices using symmetric key encryption. According to the performance evaluations, DT has excellent communication, storage, and computing efficiency.

This part offers a comprehensive review of several strategies and approaches to address the challenges associated with handling intricate healthcare data, maintaining security in the internet of things, and facilitating intelligent diagnosis. The simulation consistently emphasises the heightened levels of accuracy, energy economy, and improved privacy. In order to effectively deal with the issues of scalability, seamless integration, and real-time capabilities, it is essential to use certain techniques that can adapt to the always changing environment. These strategies will enable the development of a complete and long-lasting solution. The existing methods have several shortcomings, including insufficient levels of accuracy and precision, subpar *F*-scores, low recall rates, and elevated ideal error rates. The presented methodology has been meticulously crafted to significantly enhance the efficiency of these metrics. Within the context of the Internet of Medical Things (IoMT), the objective is to address these constraints and improve both security and efficiency.

3. Proposed smart agent-based privacy preservation and threat mitigation framework

This section presents an innovative way to enhance security in IoMT environments. An intelligent agent system enhances data privacy and addresses potential dangers. A system model encompasses the interconnections of the IoMT, while an intricate attack model simulates various hazards that arise. By incorporating the AHP, this methodology guarantees the equitable assessment of security factors, augmenting the overall resilience of the IoMT ecosystem. AHP and TOPSIS are justified by their capacity to effectively address complex decision-making scenarios involving several criteria and offer a comprehensive assessment of security measures. The systematic nature and ability to evaluate alternatives shown by these techniques follow the research's objective of assessing and validating the suggested framework's effectiveness in enhancing security in the context of the IoMT, distinguishing them from other approaches.

3.1. Real-time intelligent agent

This section provides a novel framework for the IoMT that focuses on the edge and incorporates a real-time intelligent agent (RTIA) to analyze health monitoring data safely. This framework is shown in **Figure 1**.

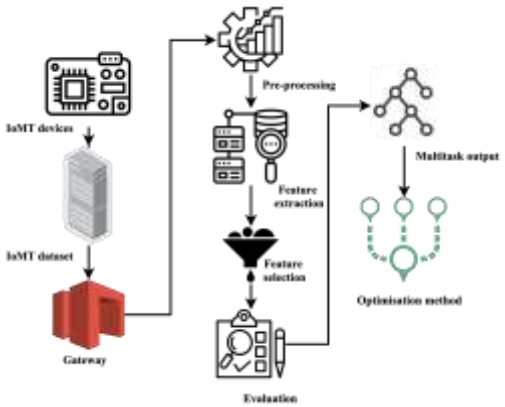

Figure 1. RTIA framework.

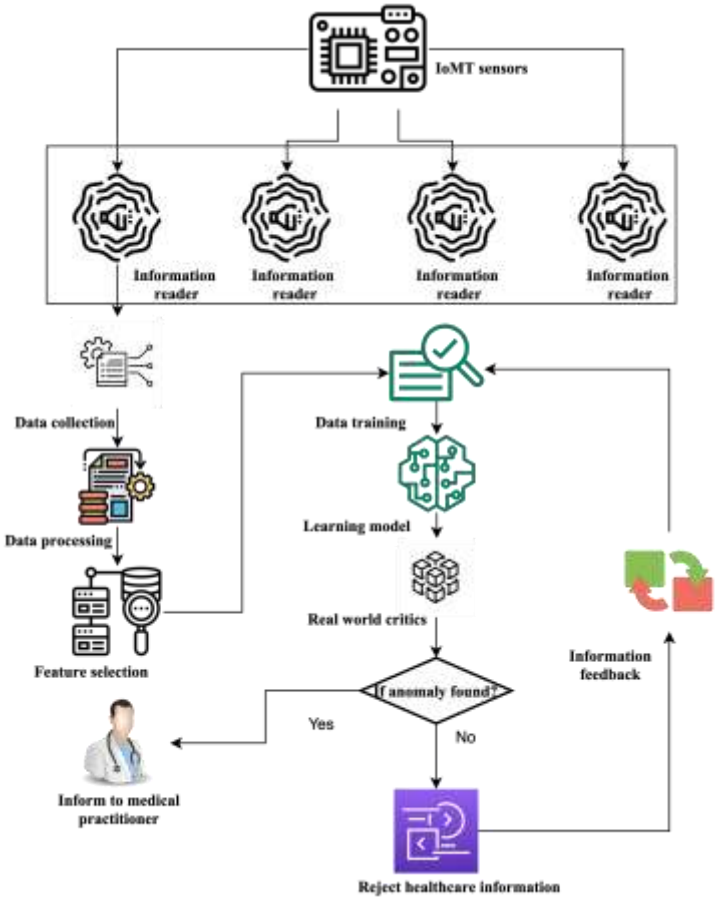

Figure 2. IoMT workflow for privacy preservation.

Figure 1 illustrates the hacker's endeavour to connect with the IoMT sensor. The hacker knew about the intermediate local server and used it to secure the edge server after obtaining access to the route. Assuming it communicates with the edge computer, the access point transfers the data to the hacker's site. Along with the edge server, the attacker's anonymous server communicates with it. When the legitimate connection route is hacked, the attacker has unfettered control over all sensitive health information. In preparation for the possibility of an assault on the IoMT infrastructure, a proposed RTIA has been developed. The RTIA's operating strategy for the edge-centric IoMT architecture is shown in **Figure 2**. There are three steps in this representative's life cycle: collecting, analyzing, and finally classifying the collected health monitoring data. Understanding the data and collecting it are the two main processes that are involved in the process of getting information for an Environmental Impact Assessment (EIA). The edge-centric architecture has the capability to detect irregularities in the activity of the network via the use of Real-Time Intrusion Analysis (RTIAs). The data reader evaluates the data flow for indicators of problems before providing it to the network. This is done because each gateway is equipped with an agent that has already been deployed. The Internet of Medical Things (IoMT) design that has been presented includes a complete list of all of the many components that make up the framework. Real-Time Integration Architecture (also known as RTIA) is one of these components. Quick patient assessments and thorough treatment are within the realm of possibility for healthcare practitioners given enough funding. Improving the quality of medical care is possible with the availability of real-time alerts that clinicians may monitor, observe, and convey via the IoT. Since it is less of a hassle to precisely administer medications, doctors and other medical staff can get more done in less time. Now, from anywhere in a healthcare institution, it is possible to reliably and remotely monitor patients' vital signs thanks to medical technology provided by the Internet of Things (IoT). Although occasions are not required, they may nonetheless take place. Neither the actual visits to schools nor the manual collection of data are anymore necessary. We no longer need this condition. At this

point, students are free to do any of these tasks by themselves that they like. Everyone involved in healthcare, from patients to doctors, stands to gain from the IoMT. Among other things, data is used effectively, management procedures are efficient, patients are involved in treatment planning, and evaluations are trustworthy. The IoMT allows for the instantaneous transmission of patient records and the alerting of healthcare providers to any changes in their patients' health statuses. Science has made some more rapid strides because of this terrible occurrence. It shouldn't matter how many Internet of Things devices there are; what matters is that people's private information and data is protected. By establishing stringent security protocols, healthcare institutions can safeguard their patients' private information from identity thieves and hackers. Combating cyberattacks and implementing safety measures are joint efforts necessary to guarantee the IoMT's security. The likelihood of unauthorised users gaining access to hospital networks and compromising IoMT equipment would significantly. This crucial management system consists of two tiers. To keep all patient information safe, the technique employs encryption keys. On the other side, the intermediary layer enables the speed and security of IoMT device connections. Encryption of patient data must be a top priority at all levels.

- Information reader:

The information reader incorporates a lightweight monitoring program to get data from diverse network devices. To understand network traffic, properly arranged data segregated is afterwards transferred to the following step.

- Information collection:

The information collection part of the agent activities serves as a mechanism for capturing data, namely flow and service-based network activity. The packet sent is analyzed to extract valuable data on its characteristics, enabling the detection of irregularities within the network's data flow. Afterwards, the data is delivered to the information processing department to extract trends.

- Data processing:

During an RTIA, the data set is generated, with the data within the group exhibiting homogeneity based on the period. The temporal organization of data enables the architecture to effectively manage the transmission of information from sensors to the IoMT architecture. The information is categorized according to the specific medical sensors used.

- Attribute selection:

RTIA chooses characteristics by identifying and selecting pertinent attributes associated with the patterns while removing extraneous qualities. The RTIA incorporates an updated correlation-based choice of technique to determine the most crucial attribute for each design. The calculation of the relationship between the two characteristics, F_1 and F_2, is performed in Equation (1).

$$C(F_1, F_2) = \frac{\sum_{i=0}^{N}(F_1 - k_1)(F_2 - k_2)}{\sqrt{\sum_{i=0}^{N}(F_1 - k_1)} + \sqrt{\sum_{i=0}^{N}(F_2 - k_2)}} \quad (1)$$

The k_1, and k_2 denote the average values corresponding to two distinct attribute values. The correlation coefficient $C(F_1, F_2)$ represents the relationship between two different characteristics. It is computed by first calculating the means of the traits, denoted as $k_1 = \frac{\sum_{i=0}^{N} F_1}{N}$ and $k_2 = \frac{\sum_{i=0}^{N} F_2}{N}$. The correlation function yields values denoted as $C(F_1, F_2)$that range from +1 to −1. A number near +1 signifies a high similarity between the variables, while a value relative to −1 suggests a significant dissimilarity. Therefore, health metrics with values close to −1 are used for surveillance.

- Real-time critic:

The real-time critic is a theoretical framework often used in academic research to evaluate and analyze real-time evidence. The experimental critic is used to comprehend the confidence of IoMT. Therefore, real-world criticism is connected to the effectiveness of analyzers. Once the IoMT is prepared, the real-time critic is provided with the test data as a source of information for the adequately trained IoMT systems.

The pseudocode for the SAPPTMF privacy preservation method is shown in Algorithm 1.

Algorithm 1 Privacy Preservation Algorithm

Input: IoMT data (*D*), MAC, Features (*F*)
Output: Modality (F_{mod}) based *F* in Excel file
Start
Step 1: Initialisation
Initialise *F* = 0
Step 2: Data separation
For every MAC_r
  If $MAC_r = MAC_{dev}$
    $D_{dev} = Split(D)$
Step 3: Traffic separation
For every traffic (*tr*)
  $F_{stat} = S_f(D_{tr})$
  $Q_{pkt} = f_Q(D_{tr})$
  $D_{fin} = D_{tr}$
Step 4: Traffic merging
If Flow_ID is found
  $D_{mrg} = conc\{D_{dev}, D_{tr}\}$
Merge D_{mrg} into D_T
Step 5: Attribute selection
If *F* is selected, the attribute
  $F_c = Class\{F\}$
  $F_{mod} = conc\{F_c, D_T\}$
Stop

MAC_r is denoted received MAC, device MAC is denoted MAC_{dev}, statistical feature function is S_f, data traffic is expressed D_{tr}, packet quantity function is f_Q, packet quality is denoted Q_{pkt}, the statistically selected feature is denoted F_{stat}Finally, the selected data is D_{fin}, the merged data is denoted D_{mrg}, total merged IoMT is D_T, the classified feature is F_c, and the final modality feature is F_{mod}.

3.2. System model

The study suggests recommending comparable medical diagnoses and treatments using a healthcare network graph created from the data of all participating participants. It is important to note that the participants' privacy is maintained throughout this process. The system under consideration consists of four distinct entities. The scenario has a group of participants represented as $\{P_1, P_2, P_3, P_4\}$, who have provided medical data collection. There is a doctor referred to as DR, a cloud server designated as CS, and a medical facility represented as MC. The description of the entities' functioning is as follows.

1) The software system known as MC is responsible for generating variables and providing medical-assisted diagnostic and therapy.
2) Possess personal healthcare information (P_s) and submit records to a cloud storage system.
3) The doctor might inquire about the medical situation requiring treatment.
4) The field of CS incorporates the medical network graph and produces the necessary search information for machine learning.

Every participant denoted as P_x $(x = 1, 2, \cdots, n)$ encrypts and uploads their physiological data, represented as $\vec{d}_x = \{d_1, d_2, \cdots, d_N\}$, together with their medical treatments, denoted as m_x, to the CS. The integration of records is achieved by using graph theory, specifically by representing the participant's data as a node $V_x = \{\vec{d}_x, m_x\}$. If two participants, P_x and P_y have had medical treatment at the same hospital, an edge

exists, $E_x = \{v_x, v_y\}$, connecting v_x and v_y. However, a direct relationship is not present. To clarify, all participants inside a hospital can be represented as a completely linked graph denoted as $G = \{V, E\}$. Through the evaluation of various hospitals, the field of computer science creates a medical graph, which is essentially a composite network consisting of numerous ultimately linked graphs.

Following a doctor's encryption and uploading of a medical case $\vec{d}_x$, CS incorporates it into graph G as a node N_l. CS identifies all potentially related records. $T_l = \{N_x \cup N_y\}$, where N_x represents the neighbours of v_x and N_y represents the 2-hop neighbors of v_y. The ciphertext $S_{x,y}$The degree of similarity between two physiological data sets, x and y, is sent from the CS to the MC. This similarity is determined using the cosine similarity measure. The task of decrypting the nodes falls under the responsibility of MC to select a node. V_x and its corresponding index x that exhibits the highest similarity, denoted as $S_{x,y}$. MC and CS retrieve the treatment plan stored in this node and transmit it to the doctor as a suggestion using the transmission protocol. As previously stated, the Model has been codified as Equation (2) to (4).

$$k_l = m_y \tag{2}$$

$$y = \arg\{\max\{S_{x,1}, S_{x,2}, \cdots, S_{x,y}\}\} \tag{3}$$

$$S_{x,y} = \frac{\vec{d}_x \vec{d}_y}{|\vec{d}_x||\vec{d}_x|} \tag{4}$$

The similarity matrix is $S_{i,j}$, the IoMT data is denoted m_y, the distance of nodes N_x and N_y are denoted $\vec{d}_x$ and $\vec{d}_y$.

- Attacker model

The attacker models are presumed. MC is an entity that is universally regarded as trustworthy by all other entities. The entities P_x, and CS possess the characteristic of being honest but curious. Individuals adeptly adhere to established procedures while retaining incoming inputs from external sources and all intermediary outcomes, aiming to maximize the likelihood of accessing confidential information about participants. Given the objective of providing identical treatment recommendations, all parties involved are expected to provide accurate and reliable data. The presence of fabricated nodes and edges promptly authenticated by medical professionals should also be considered. Moreover, the lack of accurate data resulting from falsification would lead to negative consequences and hinder the establishment of confidence. All parties involved are curious about obtaining facts and are actively engaged. A represents an external opponent that can intercept the communication link to get the intermediate outcomes. Moreover, entity A can infiltrate the databases of CS and MC, therefore initiating active assaults that pose a significant risk to the confidentiality of the stored data.

3.3. System architecture

This research presents the design of a novel cloud storage structure to support e-healthcare systems. The structure aims to provide an efficient, privacy-preserving retrieval service while satisfying the objectives. The e-healthcare systems typically comprise the following stages:

Setup phase: During this stage, the sensors of participants choose a security variable denoted as λ. They execute the setup and essential generation procedures to produce and retain variables param, public key, and private key (p_x, s_x) for all participants in the physical realm to gather healthcare records.

Data collection and encryption phase: The sensors consistently gather physical healthcare records from various locations. They extract specific keywords from this data and use encryption to provide health information. This data is generated using doctor user 1's public key $P_x(U_1)$. Transfer all encrypted data $C_x(U_1)$ to a cloud service.

Data conversion phase: U_1 can assign the tasks of searching and decrypting to U_2 by using the cloud server, following a set of processes, if U_1 is not accessible. Initially, user 1 executes the critical generation technique to produce a re-encryption key for the cloud server. This process involves using user 1's private key S_{U_1} and user 2's public key S_{U_2}. Once provided with the re-encryption key, the cloud server executes the encryption algorithm to transform the associated ciphertext. Finally, the transformed ciphertext C_{U_2} is stored. To get conditional authorization, the critical generation requires the inclusion of U_1's private key as a component of its input. Anybody without access to the private key could not initiate conditional authorization, even if provided with U_2's public key. During the data retrieval phase, U_2 can search and decode the converted ciphertext by following the below procedures. Initially, U_2 executes the trapdoor procedure to produce a trapdoor T_d associated with the keyword w, using their private key S_{U_2}. Using the trapdoor T_d and encrypted text C_{U_2}, the server in the cloud executes the test method to identify the corresponding ciphertext. U_2 successfully acquires the desired data by using this private key S_{U_2} to decode the corresponding ciphertext via the execution shown in Algorithm 2.

Decryption algorithm in Algorithm 2.

Algorithm 2 Decryption Algorithm

1: **Input:** IoMT feature (*F*), $U_1, U_2, P_x, P_y, S_{U_1}, T_d, C_{U_1}, C_{U_2}$
2: **Output:** Decrypted data S_{U_2}
3: **Start**
4: **Step 1: Reception of data and public key**
5: $P_x(U_1) = f_1\{U_1, F_{U_1}, P_x\}$
6: **Step 2: encryption of data**
7: $C_{U_1} = enc\{P_x(U_1), S_{U_1}\}$
8: **Step 3: Reception of data in the receiver end**
$C_{U_2} = receive\{C_{U_1}, N, U_2, P_y\}$
10: **Step 4: Data processing**
11: $T_d = f_2(S_{U_1}, U_2, P_y)$
12: **Step 5: Decryption**
13: If $V(C_{U_2})$ is true
14: $S_{U_2} = dec\{C_{U_2}, T_d, V(C_{U_2})\}$
15: Else
16: $S_{U_2} = dec\{ERROR\}$
17: End
18: **Stop**

The participant data acquired by IoMT devices undergo encryption before being transferred to the cloud storage service. Information security and confidentiality are effectively maintained via encryption techniques since the encrypted electronic records prevent the cloud server from acquiring any knowledge or insights from the data. Access to electronic records is restricted to authorized medical professionals alone. The system allows assigning tasks to an alternate physician through a cloud server when the primary physician is absent. This delegation process can be done without the decryption of electronic records, reducing the potential for data access to the cloud server.

3.4. Security analysis and decision making

The Enhanced Security Attributes (ESA) methodology is often offered for examining security. The structure's primary goal is to assess security in IoMT devices or substitutes inside healthcare using the established security standards. Once the determination and choice of security requirements or qualities have been made, IoMT devices are chosen as an alternative. Data is then gathered by consulting professionals in the area of IoMT security. The data-gathering strategy draws inspiration from the Delphi method. **Figure 3** illustrates the recommended security architecture for assessing and making decisions on the security of IoMT gadgets in healthcare systems.

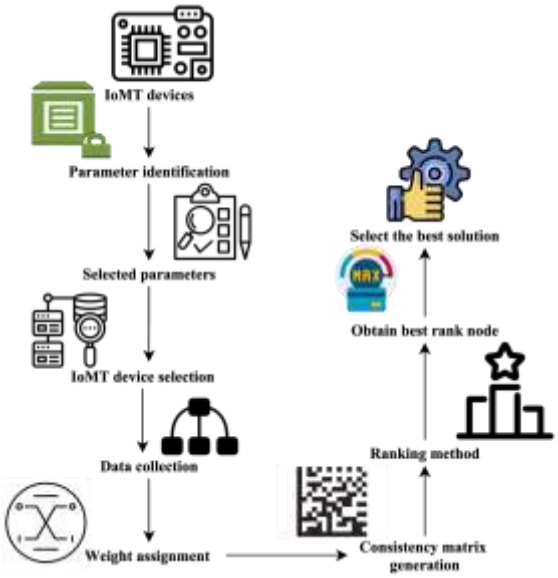

Figure 3. Security analysis and decision-making system.

The proposed framework operates in two distinct phases: firstly, the AHP approach is used to assign weights to the various criteria, and secondly, the technique for order of preference by similarity to ideal solution (TOPSIS) method is utilized to rank the available options.

Data security is a top priority for modern Internet of Medical Things (IoMT) systems in the healthcare industry. The Internet of Medical Things (IoMT) technology improves patient care but compromises health information security. Maintaining data confidentiality and authenticity is crucial. Health data is delicate. Doctors must accurately diagnose and protect patients' medical information. Healthcare providers cannot divulge patient information under law. Physicians must protect patient privacy and integrity. Personal data breaches or misuse damage healthcare system trust. If they fear unauthorised exposure or misrepresentation of their personal health information in the case of a security breach, they may not provide crucial information. They act this way to avoid looking trustworthy. Healthcare workers are ethically and socially required to protect patient privacy. Morality and social obligation require us to finish this. Due to healthcare institutions' strict security procedures, patients may worry about their privacy. Not maintaining confidentiality may harm patients' mental health. Some people may avoid medical care due to concerns about their sensitive medical information being compromised due to new security vulnerabilities. Medical identity theft is the unauthorised use of your protected health information to get medical services or prescriptions. Using stolen data for another purpose is theft. Patient medical records may be accessed by unauthorised individuals. Two-factor authentication, advanced encryption, and frequent security audits may improve IoMT security. Healthcare staff must comprehend computer system access laws, avoid fraudulent schemes, and avoid risky websites. People may greatly lower their risk by having correct and thorough information. To maintain information confidentiality, all parties must fulfil their commitments. Medical facilities must follow existing norms and create new ones to avoid penalty. Preventing penalties is the goal. Advances in communication technologies improve data security, incident response, and overall security. To build confidence with patients and other stakeholders, you need a comprehensive medical record protection plan. To protect private data, computer systems, and networks, cybersecurity processes include several technical protections. Internet of Medical Things (IoMT) deployment might improve patient care. This is made possible by several medical networks and equipment. Healthcare infrastructure is vulnerable too. Raising awareness of these issues won't prevent IoMT misuse. Malicious actors might use medical IoT. Malicious malware may penetrate contemporary hospital networks and steal patient data. Malware on medical gadgets might endanger their data. The threat to health data privacy is rising. Decrypting data is expensive. Without a fix, IoMT ransomware that damages hospital supplies might endanger patients.

Monitoring and care technologies may be compromised. Insufficient access control, malicious intent, or external attacks might cause problems. Certain persons may access healthcare information and resources without permission. Unauthorised medical information dissemination violates patients' privacy. Medical equipment performance may affect patient health and treatment outcomes. cybercriminals sometimes destroy medical equipment. Ransomware might impede pharmaceutical testing, monitoring, and surveillance. Medical gadgets are cyberattackable. If evaluation, therapy, or monitoring are delayed, patient predicament may deteriorate. Accessing or altering medical data by unauthorised parties is risky. Misdiagnosis or inadequate therapy may harm patients. All patient data is reviewed by medical professionals. Security flaws reveal patient data, endangering their health. IoMT-based healthcare delivery systems can be hacked. If network infrastructure is hacked, ransomware may interrupt medical care. Cybercriminals infiltrating hospitals might destroy patient data and medical equipment. Healthcare staff are viewed with suspicion due to concerns about data security. Lack of trust in Some consumers may avoid digital health solutions due to the healthcare system, denying medical procedures, or providing personal information.

- Assigning weights

The present study utilizes the AHP methodology to allocate weights to the criterion. This approach is well-suited for issue scenarios that include decision-making using several criteria. Multiple reasons for choosing this particular methodology since it focuses on reducing cognitive mistakes via simplifying, splitting, and comparing different attributes. This method is applicable not just for comparing qualitative indicators but also for quantitative indices. Therefore, machine learning exhibits many applications in decision-making, evaluation, allocation of resources, settlement of disputes, prioritization and ranking, and optimization. Its subjective aspect characterizes the AHP since it involves the assignment of weights by experts or decision-makers based on their judgments. The AHP methodology prioritizes each possibility by considering its hierarchical relevance or goal identification. The AHP approach encompasses a series of phases.

Step 1: Identification conditions: In the first stage, the requirements, sub-criteria, and options are determined and organized hierarchically.

Step 2: Weight assignment: Experts use a predetermined scale to assign weights to factors based on their perceived significance during this stage. Qualitative ratings undergo a conversion process and are expressed in numbers.

Step 3: Create a pairwise comparison vector.

A pairwise vector is generated using a numerical scale ranging from 1 to 9. The comparison vector displays the relative relevance of the *x*-th criterion about the criteria, as shown by c_{xy}. When the value of c_{xy} exceeds one, it indicates that the xth standards have higher significance than the yth criteria. When c_{xy} is less than one, it implies that the xth criterion is less important. When $c_{xy} = 1$, it means that they are equally important. The comparison uses a vector format, as seen in Equation (5).

$$C = \begin{bmatrix} 1 & c & \cdots & c_{1n} \\ \frac{1}{c_{12}} & 1 & \cdots & c_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ \frac{1}{c_{1n}} & \frac{1}{c_{2n}} & \cdots & 1 \end{bmatrix} \quad (5)$$

Step 4: Building a normalized vector.

In this stage, the summation of columns in the vector is computed. Every component in the vector is divided by the sum of its respective column. The mean and standard deviation of the rows are determined in the normalization pair-by-pair vector. The criteria weights are computed to determine the priority of each

criterion. The determination of weights is achieved by two distinct methods: eigen max ($t_{\max}$) and the geometric mean. The variable $t_{\max}$ represents an eigenvalue, and the Equation for determining $t_{\max}$ is shown in Equation (6).

$$t_{\max} = \frac{1}{M}\sum_{x=0}^{M-1}\frac{C_x}{W_x} \tag{6}$$

The weight comparison vectors are denoted W_x and C_x, and the mean value is denoted *M*.

Step 5: Consistency vector.

The consistency vector is constructed to assess a comparison's consistency. The Consistency Index (*CI*) is determined at this stage via the use of Equation (7), while the Consistency Ratio (*CR*) is computed utilizing Equation (8). In this stage, the multiplication operation is performed between every component of the first column in the pairwise comparison vector and the corresponding weight values from the first row in the normalized pairwise vector. This process is then repeated for each of the columns in the vectors.

$$CI = \frac{t_{\max} - M}{M - 1} \tag{7}$$

$$CR = \frac{CI}{RI} \tag{8}$$

The weight is denoted C_x, and the mean value is denoted *M*. It is considered acceptable if the *CR* value is equal to or less than 0.1. Alternatively, the operation will need to be restarted.

- TOPSIS analysis

The TOPSIS approach is known for its straightforward, well-recognized, and reliable computational process. The present study utilizes the TOPSIS approach to evaluate and rank IoMT devices. The TOPSIS approach for rating alternatives involves using the following phases.

Step 1: Quantify the importance of decisions by using a decision vector.

A decision vector, denoted as *D*, is created during this stage using several criteria and options. For instance, the decision vector is expressed when there are 'n' choices and standards.

$$D = \begin{bmatrix} P_1 \\ \vdots \\ P_n \end{bmatrix}\begin{bmatrix} C_{11} & \cdots & C_{1m} \\ \vdots & \vdots & \vdots \\ C_{n1} & \cdots & C_{nm} \end{bmatrix} \tag{9}$$

P_1 is an alternative variable, C_{ij} is criteria.

Step 2: Vector normalization for decision-making construction.

The data inside the decision vector *D* is derived from several sources, necessitating normalization to convert it into an undefined vector. The dimension vector facilitates the evaluation and comparison of several parameters. The construction of a normalization decision vector is achieved by Equation (10).

$$R_{xy} = \frac{P_{xy}}{\sqrt{\sum_{x=0}^{N}\left(p_{xy}\right)^2}} \tag{10}$$

The parameter is denoted P_{xy}.

Step 3: The calculation of the standardized weighted decision vector.

It is not necessary that all traits must possess equal significance. A weighted normalized judgment vector is derived by adding each member of the standardized decision vector with a randomly assigned weight value, as shown in Equation (11).

$$V = V_{xy} = W_y \otimes R_{xy} \tag{11}$$

The decision vector is denoted V_{xy}, the weight is W_y, and randomly assigned value is denoted R_{xy}.

Step 4: Identifying the best possible solutions (both positive and negative).

The positive ideal (A^+) and negative ideals (A^-) solutions are determined based on the weighted choice vector shown in Equations (12) and (13).

$$A^+ = \{\max(V_{xy})\} = \{V_1^+, V_2^+, \cdots, V_n^+\} \tag{12}$$

$$A^- = \{\min(V_{xy})\} = \{V_1^-, V_2^-, \cdots, V_n^-\} \tag{13}$$

The notation V_i^+ represents the positive traits, whereas V_i^-. Symbolizes the non-beneficial attributes. The decision vector is denoted V_{xy}.

Step 5: Computation of separation measure.

In this stage, ideal and non-ideal separation is calculated using Equations (14) and (15).

$$S^+ = \sqrt{\sum_{y=0}^{N-1}(V_{xy} - A^+)^2} \tag{14}$$

$$S^- = \sqrt{\sum_{y=0}^{N-1}(V_{xy} - A^-)^2} \tag{15}$$

The decision vector is denoted V_{xy}, and positive ideals (A^+) and negative ideals (A^-) solutions are used.

Step 6: Evaluate how near each option is to the best one.

The relative proximity of each competing option to the ideal solution is assessed using Equation (16).

$$C_x = \frac{S_x^-}{S_x^- + S_x^+} \tag{16}$$

The positive and negative solutions are denoted S_x^+ and S_x^-.

Step 7: Prioritization or ordering of options.

The C_x value determines the ranking order, with a more excellent value indicating a better-performing option. By placing the choices in decreasing order, it is possible to examine the relative performance of several options.

The suggested approach provides a novel way to strengthen protections in IoMT settings. It protects sensitive participant information and thwarts cybercriminals with the help of an intelligent agent system. A detailed system and attacker models provide more details and protection against potential dangers. The strategy uses the AHP to guarantee a well-rounded and well-prioritized approach to security, strengthening the IoMT ecosystem.

4. Simulation analysis and outcomes

The simulation study section gives an in-depth look at the execution of the suggested approach. The experimental design, database, assessment measures, and presentation of findings are all included to understand the method's efficacy and value better.

4.1. Experimental setup

Experiments are run on an Intel CPU @ 2.40 GHz instances, 24 machines equipped with Cuda-10 and an Nvidia 12 GB GPU (64-bit), and the Python 3.8 environments in the Anaconda 4 distribution.

4.2. Database

With the proposed structure, 16k samples are gathered, with a distribution of 87% standard samples and 13% attack data records. Label 0 indicates traffic that is not an attack, whereas label 1 indicates an attack. The WUSTL-EHMS-2020 database uses a real-time healthcare testbed[26]. The testbed is a hybrid of two

sorts of data: (1) network-flow measurements and (2) biometrics collected from individual participants. At first, there were 45 characteristics in this database, which included 30 network-flow measurements, 13 participant biometrics, and one label feature. The database incorporates a range of physical variables, such as core body temperature, pulse rate, and mobility data obtained from people in different settings. The dataset has a significant magnitude, including many records, and its organized structure facilitates the effective examination of temporal trends and patterns.

4.3. Evaluation metrics

Evaluation metrics are used to determine the Model's quality in deep learning. Evaluating machine learning models or techniques is a crucial part of any project. Models undergo rigorous testing using many possible assessment tools. The research assesses how well the proposed multitask learning model performs using these indicators. Accuracy (*A*) measures how many samples from a given set can be correctly categorized using Equation (17).

$$A = \frac{T^+ + T^-}{T^+ + F^+ + T^- + F^-} \tag{17}$$

The rate at which positive samples are accurately classified relative to the total number of positive examples is denoted by precision (*P*) and is shown in Equation (18).

$$P = \frac{T^+}{T^+ + F^+} \tag{18}$$

Recall (*R*) calculates the number of positive samples can be accurately classified using Equation (19).

$$R = \frac{T^+}{T^+ + F^-} \tag{19}$$

Recall and accuracy are used in the *F* score (*F*) computation. The *F* scoring process includes considerations for false negatives and positives, denoted in Equation (20).

$$F = 2\frac{PR}{P + R} \tag{20}$$

The true and false positive values are denoted T^+ and T^-. The true and false negative values are denoted. F^+ and F^-.

4.4. Simulation results

SAPPTMF consistently produces better average results because of its superior performance across all accuracy criteria, as shown in **Figure 4** and **Table 1**. This might be credited to SAPPTMF's unified strategy, which uses a smart agent system with realistic models and a systematic decision-making approach. The findings show that SAPPTMF has a notable effect, significantly improving accuracy and overall efficacy in IoMT security applications.

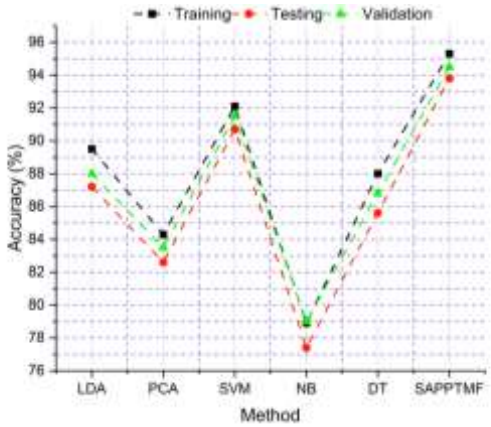

Figure 4. Accuracy analysis of the IoMT privacy preservation process.

Table 1. Numerical data of accuracy analysis.

Method	Training	Testing	Validation
LDA	89.5	87.2	88
PCA	84.3	82.6	83.5
SVM	92.1	90.7	91.5
NB	78.9	77.4	79
DT	88	85.6	86.8
SAPPTMF	95.3	93.8	94.5

Throughout the training, testing, and validation stages, SAPPTMF consistently demonstrates improved precision performance, with higher average results than competing approaches, as shown in **Figure 5** and **Table 2**. The method's success is traced back to its well-rounded construction, which has an intelligent agent system, realistic models, and a systematic approach to security assessment. The significance of SAPPTMF's effect on accuracy demonstrates the capability of the framework to improve accuracy and, by extension, IoMT security. LDA (86.9), PCA (81.5), SVM (90.5), NB (75.5), DT (86.1), and SAPPTMF (91.0) had the highest average numerical values out of the six approaches.

Table 2. Numerical data of precision analysis.

Method	Training	Testing	Validation
LDA	88.2	85.6	87
PCA	82.7	80.3	81.5
SVM	91.8	89.4	90.2
NB	76.5	74.1	75.8
DT	87.3	84.9	86.1
SAPPTMF	91.8	90.2	91

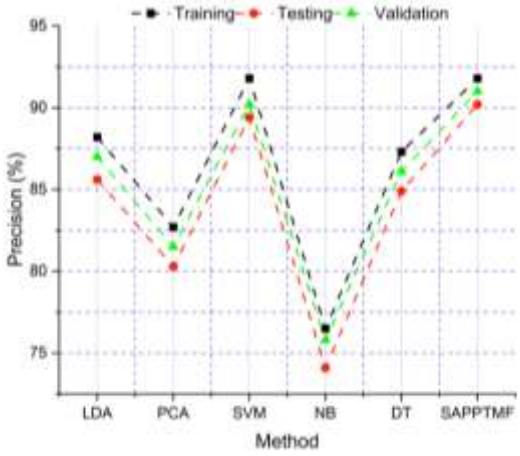

Figure 5. Precision analysis of the IoMT privacy preservation process.

SAPPTMF achieves higher recall results consistently throughout all phases of development (training, testing, and validation), as shown in **Figure 6** and **Table 3**. This is because SAPPTMF takes a more all-encompassing approach by including a smart agent system, realistic models, and a systematic security assessment process. The considerable recall improvement by SAPPTMF demonstrates its potential usefulness in the IoMT security setting. The average results for the six approaches are as follows: LDA (89.3), PCA (84.5), SVM (92.8), NB (79.2), DT (88.0), and SAPPTMF (93.4).

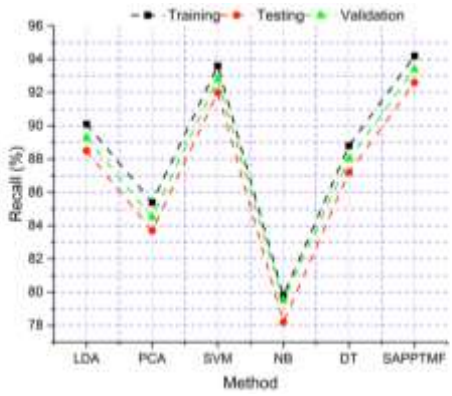

Figure 6. Recall analysis of the IoMT privacy preservation process.

Table 3. Numerical data of recall analysis.

Method	Training	Testing	Validation
LDA	90.1	88.5	89.3
PCA	85.4	83.7	84.5
SVM	93.6	92	92.8
NB	79.8	78.2	79.5
DT	88.8	87.2	88
SAPPTMF	94.2	92.6	93.4

SAPPTMF shows superior F-score performance compared to competing approaches in all three phases of development (training, testing, and validation), as shown in **Figure 7** and **Table 4**. Incorporating a smart agent system, realistic models, and a structured method for security review, SAPPTMF achieves this result. SAPPTMF considerably affects the *F*-score, demonstrating its ability to substantially improve *F*-score levels and overall IoMT security results. LDA (88.0%), PCA (82.8%), SVM (91.9%), NB (77.5%), DT (86.5%), and SAPPTMF (92.4%) are the median numerical values across all six approaches.

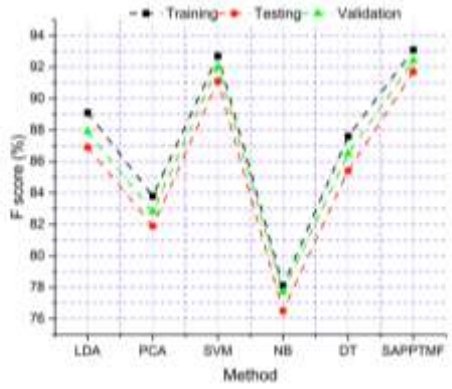

Figure 7. F score analysis of the IoMT privacy preservation process.

Table 4. Numerical data of *F*-score.

Method	Training	Testing	Validation
LDA	89.1	86.9	87.9
PCA	83.8	81.9	82.8
SVM	92.7	91.1	92
NB	78.1	76.5	77.7
DT	87.6	85.4	86.5
SAPPTMF	93.1	91.7	92.4

SAPPTMF consistently outperforms other approaches regarding Mean Squared Error (MSE) during training, testing, and validation stages, as shown in **Figure 8** and **Table 5**. SAPPTMF takes a holistic approach to evaluating security by including an intelligent agent system, realistic models, and an organized assessment framework. SAPPTMF considerably affects MSE reduction, demonstrating its capacity to reduce prediction errors and reliably improve IoMT security. Averaging across all six approaches yields the following numerical values: LDA = 0.13, PCA = 0.20, SVM = 0.10, NB = 0.27, DT = 0.16, and SAPPTMF = 0.09.

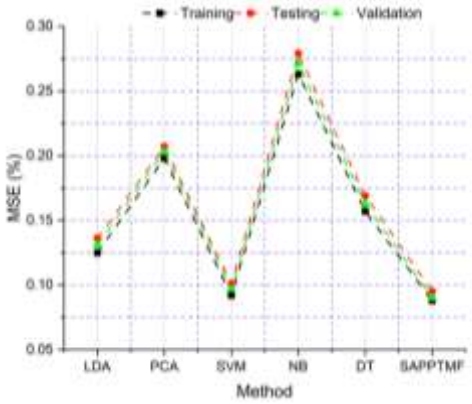

Figure 8. MSE analysis of the IoMT privacy preservation process.

Table 5. Numerical data of MSE.

Method	Training	Testing	Validation
LDA	0.125	0.136	0.131
PCA	0.198	0.207	0.203
SVM	0.092	0.101	0.097
NB	0.263	0.279	0.271
DT	0.157	0.169	0.163
SAPPTMF	0.088	0.095	0.09

SAPPTMF delivers lower Root Mean Squared Error (RMSE) values than competing methods throughout all three phases of the development process: training, testing, and validation. The RMSE results of all methods are shown in **Figure 9** and **Table 6**. This is because of the well-rounded nature of SAPPTMF, which includes an intelligent agent system, realistic models, and a standardized procedure for evaluating security. SAPPTMF considerably reduces RMSE, indicating its potential to minimize prediction errors and improve IoMT security in general. Across all six approaches, the mean numerical values are as follows: LDA = 0.36, PCA = 0.45, SVM = 0.31, NB = 0.52, DT = 0.40, and SAPPTMF = 0.30.

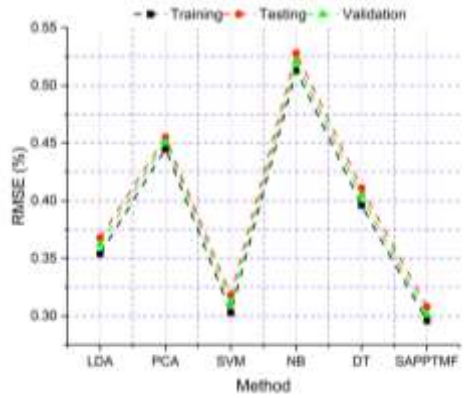

Figure 9. RMSE analysis of the IoMT privacy preservation process.

Table 6. Numerical data of RMSE.

Method	Training	Testing	Validation
LDA	0.354	0.368	0.362
PCA	0.445	0.455	0.451
SVM	0.303	0.318	0.311
NB	0.513	0.528	0.52
DT	0.396	0.411	0.404
SAPPTMF	0.296	0.308	0.301

The SAPPTMF significantly outperforms the state-of-the-art techniques like Support Vector Machine (SVM)[21], Linear Discriminant Analysis (LDA)[22], Principal Component Analysis (PCA), Naive Bayes (NB)[24], and Decision Tree[25]. Integrating a smart agent system, realistic models, and systematic security assessment in a complete strategy dramatically strengthens the security of the IoMT. The results of the technique emphasize its capacity to continuously enhance accuracy, precision, and recall while reducing prediction mistakes, thereby demonstrating its efficacy in bolstering the IoMT ecosystem.

5. Conclusion and future scope

Within the healthcare domain, the significance of security issues has become more prominent due to the widespread use of digital technology. With the advent of IoMT devices, remote monitoring, diagnosis, and treatment have become possible, completely transforming healthcare. Additionally, security concerns have arisen as a result of this paradigm shift, and they need robust and efficient remedies. In this research, we provide SAPPTMF, a new privacy preservation and threat mitigation framework based on smart agents. An organised procedure for evaluating safety precautions is included in this system, which furthermore includes a set of intelligent agents and realistic models. Internet of Things security issues are addressed by SAPPTMF's comprehensive approach. Data privacy, attack susceptibility, and lack of control over participant data are all well handled by the proposed approach. Based on the extensive simulation findings, SAPPTMF worked admirably on many different measures.

The approach exhibited a high level of results in relation to accuracy (94.5%), precision (91.0%), recall (93.4%), and *F*-score (92.4%), so establishing its efficacy in effectively detecting and mitigating threats. The observed low MSE of 0.09 and RMSE of 0.30 provide strong evidence of the method's effectiveness in reducing prediction inaccuracies and improving security. Nevertheless, despite the potential answers offered by SAPPTMF, difficulties still need to be addressed. Ongoing considerations include adapting the framework to varied healthcare, ensuring real-time reaction, and mitigating the development of threat vectors. In spite of these challenges, SAPPTMF has shown that it can significantly improve the security of the IoMT, leading to safer and more secure healthcare environments. Improvements in anomaly detection, disease prognosis, and the provision of individualised pharmaceuticals are the foci of future healthcare research. The smart agent system must be fine-tuned with the help of cutting-edge machine learning methods. Other demographic and medical thoughts are being entertained about possible tactics enhancement. Hospital IT now prioritises edge computing, which secures and enhances data management using agent-based privacy controls. This style is popular presently. The "edge" of the network sends data between these far locations. We want to employ quantum security and external device processing power to speed up and secure data. Speeding up the procedure and finding resources are the key ways to address merging issues. The Internet of Medical Things (IoMT) may improve current processes. We need more adaptive quantum devices, uniform protocols, and a combination of security solutions. We must detect and address these issues to improve the system. New regulations and principles are needed to address privacy concerns in agent-based healthcare. These guidelines should be easy to follow and more interesting since they educate people. More

approaches to keep medical data private have emerged as technology has enhanced data quality. Separation and insufficient supplies may be avoided in many ways. We examined the differences between agent-based and traditional encryption so everyone could choose. If global conditions worsen, we may need additional reforms. Agent-based security is becoming more critical for IoT system builders. Setting up Internet of Medical Things (IoMT) devices is easy and secure with this innovation, however it may violate patients' privacy. Many are worried about agent-based security's risks.

Author contributions

Conceptualization, AR, NG, ND and CP; methodology, AR and NG; software, ND and CP; validation, NG, ND and CP; formal analysis, CP; investigation, AR, NG and CP; resources, CP; data curation, AR and NG; writing—original draft preparation, AR and NG; writing—review and editing, ND and CP; visualization, CP; supervision, AR and NG; project administration, AR and NG. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Laghari AA, Wu K, Laghari RA, et al. Retracted Article: A Review and State of Art of Internet of Things (IoT). Archives of Computational Methods in Engineering. 2021; 29(3): 1395-1413. doi: 10.1007/s11831-021-09622-6
2. Dwivedi R, Mehrotra D, Chandra S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. Journal of Oral Biology and Craniofacial Research. 2022; 12(2): 302-318. doi: 10.1016/j.jobcr.2021.11.010
3. Mohd Aman AH, Shaari N, Ibrahim R. Internet of things energy system: Smart applications, technology advancement, and open issues. International Journal of Energy Research. 2021; 45(6): 8389-8419. doi: 10.1002/er.6451
4. Adeniyi EA, Ogundokun RO, Awotunde JB. IoMT-based wearable body sensors network healthcare monitoring system. IoT in Healthcare and Ambient Assisted Living. 2021; 103-121.
5. Sharmila EM, Rama Krishna K, Prasad GN, et al. IoMT—Applications, Benefits, and Future Challenges in the Healthcare Domain. Advances in Fuzzy-Based Internet of Medical Things (IoMT). 2024; 28:1-23. doi:0.1002/9781394242252.ch1
6. Hajiheydari N, Delgosha MS, Olya H. Scepticism and resistance to IoMT in healthcare: Application of behavioural reasoning theory with configurational perspective. Technological Forecasting and Social Change. 2021; 169: 120807. doi: 10.1016/j.techfore.2021.120807
7. Kumar M, Kavita, Verma S, et al. ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC. IEEE Transactions on Industrial Informatics. 2022; 18(12): 8936-8943. doi: 10.1109/tii.2022.3181614
8. Hasan MK, Ghazal TM, Saeed RA, et al. A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet-of-Medical-Things. IET Communications. 2021; 16(5): 421-432. doi: 10.1049/cmu2.12301
9. Jeyavel J, Parameswaran T, Mannan JM, et al. Security vulnerabilities and intelligent solutions for IoT systems. Internet of Medical Things: Remote Healthcare Systems and Applications. 2021; 175-194.
10. Khan S, Akhunzada A. A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT). Computer Communications. 2021; 170: 209-216. doi: 10.1016/j.comcom.2021.01.013
11. Wu G, Wang S, Ning Z, et al. Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. IEEE Internet of Things Journal. 2022; 9(11): 8091-8104. doi: 10.1109/jiot.2021.3138104
12. Deebak BD, Memon FH, Khowaja SA, et al. In the Digital Age of 5G Networks: Seamless Privacy-Preserving Authentication for Cognitive-Inspired Internet of Medical Things. IEEE Transactions on Industrial Informatics. 2022; 18(12): 8916-8923. doi: 10.1109/tii.2022.3172139
13. Rahman M, Jahankhani H. Security vulnerabilities in existing security mechanisms for IoMT and potential solutions for mitigating cyber-attacks. Information Security Technologies for Controlling Pandemics. 2021; 307-334.
14. Bharati S, Podder P, Mondal MRH, et al. Applications and challenges of cloud-integrated IoMT. Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications. 2021; 67-85.
15. Nayak J, Meher SK, Souri A, et al. Extreme learning machine and bayesian optimization-driven intelligent

framework for IoMT cyber-attack detection. The Journal of Supercomputing. 2022; 78(13): 14866-14891. doi: 10.1007/s11227-022-04453-z
16. Zaabar B, Cheikhrouhou O, Jamil F, et al. HealthBlock: A secure blockchain-based healthcare data management system. Computer Networks. 2021; 200: 108500. doi: 10.1016/j.comnet.2021.108500
17. Singh S, Rathore S, Alfarraj O, et al. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. Future Generation Computer Systems. 2022; 129: 380-388. doi: 10.1016/j.future.2021.11.028
18. Miyachi K, Mackey TK. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Information Processing & Management. 2021; 58(3): 102535. doi: 10.1016/j.ipm.2021.102535
19. Kishor A, Chakraborty C, Jeberson W. Intelligent healthcare data segregation using fog computing with internet of things and machine learning. International Journal of Engineering Systems Modelling and Simulation. 2021; 12(2/3): 188. doi: 10.1504/ijesms.2021.115533
20. Nguyen GN, Viet NHL, Elhoseny M, et al. Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model. Journal of Parallel and Distributed Computing. 2021; 153: 150-160. doi: 10.1016/j.jpdc.2021.03.011
21. Wang J, Wu L, Wang H, et al. An Efficient and Privacy-Preserving Outsourced Support Vector Machine Training for Internet of Medical Things. IEEE Internet of Things Journal. 2021; 8(1): 458-473. doi: 10.1109/jiot.2020.3004231
22. Zhang Y, Gravina R, Lu H, et al. PEA: Parallel electrocardiogram-based authentication for smart healthcare systems. Journal of Network and Computer Applications. 2018; 117: 10-16. doi: 10.1016/j.jnca.2018.05.007
23. Kaushal RK, Bhardwaj R, Kumar N, et al. Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications. Kumar A, ed. Wireless Communications and Mobile Computing. 2022; 2022: 1-13. doi: 10.1155/2022/8741357
24. Deepa N, Sathya Priya J, Devi T. Towards applying internet of things and machine learning for the risk prediction of COVID-19 in pandemic situation using Naive Bayes classifier for improving accuracy. Materials Today: Proceedings. 2022; 62: 4795-4799. doi: 10.1016/j.matpr.2022.03.345
25. Liang J, Qin Z, Xue L, et al. Efficient and Privacy-Preserving Decision Tree Classification for Health Monitoring Systems. IEEE Internet of Things Journal. 2021; 8(16): 12528-12539. doi: 10.1109/jiot.2021.3066307
26. Available online: https://www.cse.wustl.edu/~jain/ehms/index.html (accessed on 17 January 2024).