Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 8, No. 5, August : 2023

A SURVEY ON SECURITY IN IOT HEALTHCARE

Mohammed Ismail Research Scholar, Dept. of Computer Science, Chaitanya deemed University, Hanamkonda, Telangana, India & Associate Professor, MCA Dept, Auroras PG College, Ramanthapur, Hyderabad, Telangana, India
Dr A Ramesh Babu Professor & HoD, Dept. of Computer Science, Chaitanya deemed University, Hanamkonda, Telangana, India.

Abstract
The proliferation of Internet-of-Things (IoT) technologies in the healthcare sector has ushered in a new era of efficient patient care and monitoring. However, it has also brought to the forefront critical concerns regarding data security and privacy. This survey paper comprehensively explores the multifaceted landscape of security in IoT healthcare, addressing three key domains: secure data access and device authentication, data encryption, and intrusion detection and prevention. The objective is to provide a comprehensive overview of the current state of security measures in IoT healthcare and to highlight emerging trends, challenges, and future directions. Through an extensive analysis of existing literature and case studies, this paper equips stakeholders in the healthcare domain with valuable insights to fortify the security of IoT-enabled healthcare systems, ensuring the confidentiality, integrity, and availability of sensitive patient data.

Keywords: Security in IoT Healthcare, Secure Data Access, Device Authentication, Data Encryption, Intrusion Detection, Intrusion Prevention

1. INTRODUCTION

Because of the growing number of linked devices and technologies being used in the medical field, there is an urgent need for security in the Internet of Things (IoT) healthcare industry. Real-time monitoring, data collecting, and remote patient management are now all possible thanks to the integration of these technologies, which has also brought about a shift in healthcare practices. Nevertheless, this ease of use is coupled with a large increase in both vulnerabilities and hazards. The idea of security in Internet of Things (IoT) healthcare centers on the protection of the linked network of medical equipment, software applications, and data exchanges from possible dangers and illegal access.

The sensitive nature of the data involved and the possible repercussions of a security breach make it very necessary to include security measures in IoT healthcare systems. These Internet of Things ecosystems allow for the transmission and storage of patient records, medical histories, diagnostic information, and even data pertaining to real-time patient monitoring. A compromise of security might result in invasions of patient privacy, the theft of personal information, the manipulation of medical records, and could even put the health of patients in jeopardy. In addition, Internet of Things devices that have been infiltrated might serve as entry points for assaults that target bigger parts of the healthcare infrastructure, such as hospital networks and essential pieces of medical equipment.

There is a wide range of potential applications for security measures within the IoT healthcare industry. It includes not only the tangible gadgets, but also the communication channels, which are what make the flow of data possible. In order to protect data while it is being sent and stored, implementing security protocols requires the use of encryption methods, authentication mechanisms, and intrusion detection systems. Encryption protects data during transmission and storage; authentication ensures the validity of devices and users; and intrusion detection systems identify and react to possible threats. In addition, it is essential to do routine software maintenance such as updating and patching in order to address newly found vulnerabilities.

In the medical industry, Internet of Things (IoT) security encompasses a wide range of devices and components, such as wearable health trackers, medical imaging equipment, insulin pumps, and even

hospital facilities management systems. As the number of Internet of Things devices in use increases, so does the potential attack surface available to cybercriminals; thus, it is essential to implement stringent security measures. It is imperative that governments, regulatory organizations, healthcare practitioners, and device makers work together to set and enforce standards that put an emphasis on the safety of these networked systems.

In conclusion, the fast integration of networked devices and technology in the medical area has made it imperative for there to be security measures in place for the Internet of Things (IoT) in healthcare. The idea is on safeguarding sensitive patient data and maintaining the continuity of medical procedures while operating within the context of the internet of things ecosystem. The potential dangers that might be incurred as a result of illegal access, data breaches, and cyberattacks make the need for security glaringly obvious. Because the area of application encompasses such a broad variety of medical equipment and systems, it is necessary to implement extensive security measures in order to effectively reduce risks.

2. Literature

2.1 Secure Data Access and Device Authentication in IoT Healthcare

Jafar A. Alzubi et al [1] proposed a system that utilizes blockchain technology to enhance the security of medical Internet of Things (IoT) devices. This system incorporates the Lamport Merkle Digital Signature (LMDS) as a means of ensuring robust security measures. The first stage is the verification of IoT devices using the Lamport Merkle Digital Signature Generation (LMDSG) framework. This includes the creation of a tree structure, where the hash function of confidential patient medical information is assigned to the leaf nodes. Furthermore, the identification of the LMDSG root is conducted by a Centralized Healthcare Controller (CHC), using the Lamport Merkle Digital Signature Verification (LMDSV) procedure.

Asad Abbas et al [2] introduced a framework, referred to as the blockchain-assisted safe data management framework (BSDMF), which aims to enhance the security of data management in the healthcare sector. The methodology presented herein is designed to address health information management within the specific context of the Internet of Medical Things (IoMT). The primary objective of this system is to enhance the safe transmission of patient information, while simultaneously solving issues related to scalability and data accessibility within the healthcare sector. The proposed BSDMF (Biomedical safe Data Management Framework) aims to develop a robust framework for the safe management of data transmission between implanted medical devices and personal servers, as well as between personal servers and cloud servers. The security framework used in the Internet of Medical Things (IoMT) incorporates the use of blockchain technology to guarantee the secure transfer and administration of data across networked nodes.

Moustafa Mamdouh et al [3] presented a comprehensive analysis of the Internet of Medical Things (IoMT) or IoHT, with a particular emphasis on the IoT perception layer as the primary area of interest. This study discusses the present trends and unsolved issues pertaining to authentication techniques for Internet of Health Things (IoHT) devices. Specifically, it focuses on two approaches: the physically unclonable function (PUF) and blockchain-oriented methods. Moreover, the article integrates Internet of Things (IoT) simulators and validation tools.

Parminder Singh et al [4] proposed a centralized cloud-based cross-domain data sharing platform that runs on a number of security gateways. These security gateways make use of blockchain technology to make it easier to store information in the centralized cloud. In the case that harmful behavior inside the application is detected, the centralized cloud verifies the issue from the blockchain. Then, further steps are taken against the entity in charge of the harmful behavior inside the security gateways. The framework includes the construction of authentication and data transaction algorithms. The recommended architecture has the capacity to safely move data across several global domains.

Sarada Prasad Gochhayat et al [5] proposed a revolutionary strategy for key management in the Internet of Things (IoT) ecosystem. The suggested system aims to enhance the security of IoT devices

by delegating resource-intensive cryptographic operations to a local entity, hence effectively granting protection to these devices. The collaboration between this organization and other similar organizations leads to the establishment of a decentralized key and an authentication mechanism for network devices. The suggested approach effectively utilizes the advantages of mobile agents, which are strategically placed inside different subnetworks as required. The primary objectives of their deployment include two key functions: firstly, to perform cryptographic operations for Internet of Things (IoT) devices, and secondly, to act as a local authenticated entity for expediting authentication processes.

Mahdi Fotouhi et al [6] proposed a new strategy for distributed key management in the Internet of Things (IoT) ecosystem. In the aforementioned architecture, security is efficiently conferred onto Internet of Things (IoT) devices through the process of delegation. This study presents a unique authentication technique that leverages hash chains and forward security for implementation in wireless body area networks (WBANs) within the health-care Internet of Things (IoT) domain. The devised technique has been specifically engineered to effectively resist a variety of well-known assaults that are often directed at Wireless Body Area Networks (WBANs). In addition, a comprehensive security analysis is conducted using the Real-or-Random (ROR) paradigm, along with an informal assessment of the newly suggested approach's security. The authentication of the scheme's security is conducted by the use of the ProVerif tool. Furthermore, the functionality of the scheme is simulated using the OPNET network simulator. A comparative evaluation is then performed, considering security and performance requirements, versus many modern approaches. The allocation of resource-intensive cryptographic processing to a local entity. The collaboration between this entity and other similar entities leads to the establishment of a distributed key and an authentication mechanism for network devices. The suggested strategy effectively utilizes mobile agents to harness their advantages, deploying them inside different subnetworks as necessary. The primary objectives of their implementation include two key functions: firstly, the execution of cryptographic operations for Internet of Things (IoT) devices, and secondly, the provision of a local authenticated entity to facilitate efficient authentication processes.

Within the sphere of the Internet of Things (IoT), Soumya Banerjee et al [7] have presented a novel and effective way for establishing secure and anonymous user-authenticated session key agreements. This strategy makes use of a system that requires authentication from three different sources, including the smart card, password, and individual biometric data of the user. Notably, the gateway node does not have to be used as a storage location for any user-specific data in order for this technique to be used.

Geeta Sharma et al [8] have come up with an innovative user authentication system for remote patient monitoring that guarantees both safety and effectiveness. It has been suggested that this approach, which is distinguished by its toughness, its lightweight construction, and its resistance against a variety of security risks, be used. Additionally, this method is lauded for the little burden it places on a computer's resources. An innovative and lightweight method for generating anonymous user-authenticated session key agreements has been proposed for usage in the context of the internet of things (IoT). This strategy makes use of a three-factor authentication method, which includes a user's smart card, password, and personal biometric data in addition to other identifying information. It is important to note that using this method does away with the need of storing user-specific data at the gateway node.

Gautam Srivastava et al [9] examined the potential benefits of these implementations, the drawbacks of current designs, and the difficulties that this new field of study will face. This chapter examines the most recent efforts in the area, offering an unbiased viewpoint to help academics move ahead in navigating this new area for Healthcare, IoT, and Blockchain Technology.

A remedy has been proposed by Saurabh Shukla et al [10] in order to overcome the problem that was discussed before. The implementation of both fog computing (also known as distributed computing) and blockchain technology is part of their plan. An analytical model, a mathematical framework, and

an Advanced Signature-Based Encryption (ASE) algorithm are included in this strategy along with a three-tier architecture that is constructed upon FC. The key goals of this algorithm are to simplify the authentication of healthcare equipment connected to the Internet of Things (IoT), carry out verification procedures, and guarantee the integrity of Patient Health Data (PHD). The primary purpose is to improve the data transmission security inside healthcare IoT systems so that consumers who depend on real-time services may reap major advantages. This architecture and algorithm that has been developed has the capacity to provide safe transaction and transmission services in close proximity to the edge of the network.

An new approach that is specifically designed for the e-Health cloud has been presented by Minahil et al [11]. This protocol is able to efficiently combat a wide variety of key security concerns, such as breaches in user anonymity, offline password guessing assaults, impersonation occurrences, and theft of smart card data.

The use of a decentralized healthcare system that is augmented by artificial intelligence (AI) is something that Vikram Puri et al [12] have advocated for as an alternative. This architecture is intended to enable access to and authentication of Internet of Things (IoT) devices while also fostering confidence and transparency in patient healthcare records (PHR). This system is built on top of a public blockchain network, and it makes use of smart contracts that are equipped with artificial intelligence functionality. In addition to this, the framework does an active search for any Internet of Things nodes that may be dangerous inside the system.

Table 1: Analysis of secure data access and device authentication in IoT healthcare

Ref. No.	Proposed Method	Parameter
[1]	Lamport Merkle Digital Signature (LMDS).	accuracy
[2]	Blockchain-assisted secure data management framework (BSDMF)	Accuracy Precision Less response time Latency ratio
[3]	Discussed blockchain-based techniques	
[4]	Centralized cloud-based cross-domain data sharing platform	Accuracy
[5]	Distributed key management scheme	Correctness and effectiveness
[6]	Lightweight hash-chain-based and forward secure authentication	Performance
[7]	Lightweight anonymous user authenticated session key agreement, Real-Or-Random (ROR) model	Performance Cost
[8]	user authentication scheme	Cost Time
[9]	overview of IoT health technologies	
[10]	Three-tier FC-based blockchain, Advanced Signature-Based Encryption (ASE)	Accuracy Time
[11]	Lightweight authentication protocol	Efficient, reliable
[12]	Artificial intelligence (AI)-enabled decentralized healthcare framework	Energy consumption, time, throughput, average latency, transaction fee.

2.2 Data encryption in IoT Healthcare

Sangjukta Das et al [13] presented a new encryption system is, within an IoT-enabled healthcare infrastructure, which makes use of elliptic curve cryptography, the Advanced Encryption Standard (AES), and Serpent. The objective of this scheme is to improve the data protection provided to patients' medical records. The combination of both symmetric and asymmetric-based encryption algorithms into this newly proposed hybrid encryption method contributes to an increase in the level of data security that is afforded to the healthcare industry. In addition, the suggested system makes use of digital signatures that are based on elliptic curves, which guarantees the system's ability to maintain the data's integrity.

Mohammad Ayoub Khan et al [14] suggested secure framework, the procedure is started with patient authentication and then the sensor device attached to the patient is turned on. The readings from the patient sensor are then sent to the cloud server. Along with the login and password, the authentication procedure gains an extra component when the patient's biometric data is used. The SHA-512 algorithm is used for authentication, and it was selected for its integrity-assuring capabilities.

M. Vedaraj et al [15] introduced an innovative approach, known as Homomorphic Encryption with Random Diagonal Elliptical curve cryptography integrated with Multi-nomial smoothing Naive Bayes (HERDE-MSNB), for ensuring robust security and disease prediction capabilities for patient data within the IoT Health Cloud system. Within the proposed architecture, the cryptic framework takes center stage, encompassing both patient data and keywords, and operates through the utilization of the HERDE algorithm for encryption and decryption processes. The decryption task and subsequent prediction utilizing the MSNB model are carried out by the medical personnel involved.

Wenchao Li et al [16] suggested proxy re-encryption with equality test (PRE-ET) by combining proxy re-encryption (PRE) and PKE-ET. By combining the benefits of both PKE-ET and PRE, data that is protected with different public keys can be decrypted to get specific information from a healthcare record. At the same time, the named healthcare record can be shared without compromising security or flexibility, while the secret key and data remain hidden.

Using homomorphic encryption, Xuancheng Guo et al [17] have developed a unique method that they name Mutual Privacy-Preserving K-Means (M-PPKS). The fundamental objective is to keep the privacy of the members' personal data as well as the information contained inside the cluster centers a secret at all times. The M-PPKS method includes partitioning each iteration of the k-means algorithm into two discrete phases in order to do the analysis. In the first phase, it is necessary to locate the center of the cluster that is geographically closest to each participant. In the second step, it is necessary to locate a new center for each cluster. During these first and second stages, the cluster center implements strict privacy protections to ensure the safety of its users. It is important to note that researchers do not have access to any sensitive information that may pertain to specific individuals. It is important to note that M-PPKS makes use of a cloud platform hosted by a third party, which helps to reduce the communication needs necessary for homomorphic encryption.

Within the context of a blockchain and Internet of Things (IoT)-based architecture, Pratima Sharma et al [18] have suggested using Identity-Based Encryption (IBE) as a method for making healthcare data more secure using Identity-Based Encryption (IBE). A smart contract is used to govern the core operations of the healthcare system in this method. This technique offers a solution that is helpful for all of the parties who are involved. Extensive testing to determine the efficacy of this strategy that was recommended has been carried out.

Ravi Raushan Kumar Chaudhary et al [19] proposed a new block cipher method was, to make sure that data from the IoT devices described above is sent safely. The most important thing to think about when saving a patient's record is keeping it safe from possible mistreatment and illegal data changes, since it can be tracked by outside devices. Using advanced secure methods to protect data is made more difficult by the fact that IoT devices have their own limits.

Ata Ullah et al [20] presented a plan for putting together healthcare data with the help of Fog (FoG) in a safe and effective way. Between healthcare tracking devices and gadgets, peer-to-peer contact is set up so that sensitive data can be shared with an aggregation point. After that, this aggregation machine talks to the FoG server. In this case, the scenario includes situations where a collector is far away from a FoG computer, making it hard to send data directly. In these situations, the aggregator uses private data sharing with a nearby aggregator, which adds the data to its own set of already-aggregated data. Then, the FoG service gets this info that has been changed. The FoG server pulls the necessary values from the data it receives and stores them in a local repository. Cloud files can be updated later if necessary. To make these tasks easier, two methods are introduced: one for receiving messages at the aggregator level and the other for extracting messages at the FoG server level.

K. Sowjanya et al [21] proposed a novel key management method for the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme. The system utilizes Elliptic Curve Cryptography (ECC) to provide a lightweight solution. One notable characteristic of this methodology is that, irrespective of the semi-trusted authority's generation of secret keys, which is conducted by an honest entity with a curiosity regarding confidential information, said authority is unable to decrypt any messages utilizing these keys unless it also possesses an extra private key from the intended recipient. In the specific setting of the Internet of Things (IoT), the CP-ABE technique has two main challenges: complex decryption processes and the issue of key escrow. Therefore, the current work aims to develop a simplified CP-ABE (Ciphertext-Policy Attribute-Based Encryption) method for a healthcare system focused on the Internet of Things (IoT), using Elliptic Curve Cryptography (ECC). The key management mechanism included into the CP-ABE framework demonstrates the avoidance of key-escrow and a significant decrease in the decryption overhead experienced by the receiver of the data.

Andreou Andreas et al [22] presented a novel encryption architecture that revolves on the concept of data fragmentation. Furthermore, this study introduces a novel optical encryption technique that relies on fundamental principles of mathematics and is implemented in a deterministic way using greyscale. The objective is to use encryption as the primary method to make data less readily understandable, while also using fragmentation to break down complex relationships between features. Consequently, discrete and sensitive data is distributed across several data repositories, enabling later processes of decryption and reassembly. The aforementioned objective is accomplished by using interpolation techniques, which include the use of polynomial coefficients obtained via a systematic process, as well as specific data collected from the Database Management System (DBMS).

Yaru Liu et al [23] proposed an innovative DSSE strategy, with a specific emphasis on safeguarding privacy in Industrial Internet of Things (IIoT) healthcare systems. This signifies the commencement of a DSSE (Dynamic Searchable Symmetric Encryption) method designed for databases that store personal health record (PHR) files, while also including the idea of forward security. The establishment of the secure index is achieved via the utilization of a hash chain, while the incorporation of trapdoor updates has been incorporated to bolster resistance against file injection assaults. Additionally, the successful implementation of a sophisticated search feature in an encrypted database of personal health record (PHR) files, organized in an attribute-value format, has been accomplished.

Sangjukta Das et al [24] proposed a unique technique, which utilizes CP-ABE, as a solution to tackle the issue of attribute revocation. The proposed methodology entails the integration of numerous attribute authorities, which helps alleviate the operational challenges often encountered in traditional CP-ABE systems that rely on a single authority. In addition, the suggested technique involves assigning the task of decryption to a separate entity known as the decryption helper. This allocation of responsibilities effectively decreases the amount of decryption-related tasks that end-users are required to do.

Table 2: Analysis of data encryption in IoT Healthcare

Ref. No.	Proposed Method	Remarks

[13]	Elliptic curve cryptography, Advanced Encryption Standard (AES), and Serpent	Effectiveness
[14]	SHA-512, Substitution-Ceaser cipher and improved Elliptical Curve Cryptography (IECC)	Cost Time Performance
[15]	Homomorphic Encryption with Random Diagonal Elliptical curve cryptography	Effectiveness Accuracy Cost Time
[16]	proxy re-encryption with equality test (PRE-ET).	Performance
[17]	Mutual privacy-preserving k-means strategy (M-PPKS)	Performance
[18]	Identity-Based Encryption (IBE)	Efficiency
[19]	ARX(Addition-Rotation-XOR) based lightweight block ciphers	Memory Performance
[20]	Efficient healthcare data aggregation (EHDA)	Storage, communication, transmission ratio, energy consumption and resilience.
[21]	Ciphertext Policy-Attribute Based Encryption (CP-ABE) using ECC	Effective
[22]	Encryption frame based on data fragmentation	Performance
[23]	Dynamic searchable symmetric encryption (DSSE)	Security and efficiency
[24]	Ciphertext policy attribute-based encryption (CP-ABE)	Effectiveness

2.3 Intrusion Detection and Prevention in IoT healthcare networks

Tanzila Saba et al [25] introduced a methodology that utilizes Convolutional Neural Networks (CNN) for the purpose of anomaly-based intrusion detection systems (IDS). This technique takes use of the Internet of Things (IoT) to provide a thorough examination of all IoT traffic in a highly efficient manner.

Anar A. Hady et al [26] constructed a real-time testbed known as the Enhanced Healthcare Monitoring System (EHMS) facilitated the monitoring of patients' biometrics and the collection of network traffic data. The observed data was communicated to a remote server in order to ease later diagnostic assessments and treatment-related choices. In this particular context, man-in-the-middle cyber-attacks were used, resulting in the creation of a dataset consisting of more than 16,000 examples including both regular healthcare information and instances exhibiting abnormalities caused by cyber-attacks.

Eman Ashraf et al [27] implemented FIDChain IDS, which incorporates lightweight artificial neural networks (ANN) inside a federated learning (FL) architecture. The objective of this strategy is to guarantee the safeguarding of privacy in healthcare data. The integration makes use of improvements in blockchain technology, which enables a distributed ledger approach for combining local weights. Afterwards, the revised global weights are distributed through broadcasting following a process of averaging. This approach efficiently mitigates the risk of poisoning attacks while simultaneously ensuring extensive transparency and immutability throughout the distributed system. The use of the detection model occurs at the periphery, functioning to protect the cloud in the case of a security breach. This involves the use of measures that hinder the timely transmission of data to its designated

gateway, resulting in a decrease in the time required for detection, a reduction in computational resources needed, and a drop in processing capacity. The use of the FL approach offers notable benefits as it demonstrates proficiency in handling reduced data sets, consequently augmenting its efficacy in safeguarding data.

Blockchain Assisted IoT Healthcare System with Ant Lion Optimizer and Hybrid Deep Learning (BHS-ALOHDL) is the name given to the novel technique that was developed by Hayam Alamro et al [28]. This strategy is intended to detect and identify any unwanted access or breaches inside the system while also allowing for the safe transmission of medical data within the healthcare industry through Internet of Things (IoT) devices. The goals of the BHS-ALOHDL approach are accomplished by the use of an Ant Lion Optimizer (ALO)-based strategy for the selection of feature subsets. This strategy is referred to as ALO-FSS. A collection of feature vectors is produced by using this method. In order to simplify the process of intrusion detection, a combination of the properties of convolutional neural networks (CNNs) and the long short-term memory (LSTM) model has been included into the high-level design (HDL) model.

An novel machine learning assistance system that combines a genetic algorithm with Random Forest (RF) has been described by Celestine Iwendi et al [29]. This system is intended to optimize characteristics and develop superior intrusion detection systems, ultimately leading to increased detection rates as well as more accurate false alarm rates. A weighted genetic algorithm and Random Forest (RF) are merged in their approach in order to improve the efficacy of their technique. This results in the generation of an ideal subset of features, which in turn leads to a considerable improvement in detection rates while simultaneously retaining a minimum false alarm rate. Within the context of machine learning, the research made use of the NSL-KDD dataset to carry out a simultaneous classification of RF, Naive Bayes (NB), and logistic regression classifiers.

Adel Binbusayyis et al [30] investigated the use of several machine learning methods for the purpose of detecting intrusions inside Internet of Medical Things (IoMT) networks. The analytical investigation comprises machine learning methods, including K-nearest neighbor, Naïve Bayes, support vector machine, artificial neural network, and decision tree. In order to assess the effectiveness of the ML models stated earlier, the Bot-IoT benchmark dataset, which is publically accessible and includes a wide variety of assaults, was used for both the training and testing phases. In addition, a wide range of assessment criteria was used to facilitate the comparison of intrusion detection accuracy in IoMT networks across various machine learning algorithms being studied.

Daojing He et al [31] analysed the security vulnerabilities inherent in the systems is conducted, followed by the proposal of a unique intrusion detection approach that utilizes a stacked autoencoder as its foundation.

Prabhat Kumar et al [32] created an IoT-enabled healthcare system using a Blockchain-orchestrated Deep Learning method for Secure Data Transmission (BDSDT). As part of the strategy, a brand-new, scalable blockchain architecture is suggested with the goal of assuring both data integrity and safe data transfer. By using the Zero Knowledge Proof (ZKP) technique, this is accomplished. To efficiently handle issues related to data storage costs, integration with the off-chain storage solution InterPlanetary File System (IPFS) is also carried out. To address problems with data security, integration with an Ethereum smart contract is also done. Following these steps, a deep learning architecture is built using the authenticated data that was produced. This design is used to identify intrusions into the network of the healthcare system.

Abdallah Ghourabi et al [33] offered a brand new intrusion and malware detection system as a means of improving the network security across the whole healthcare system. The proposed solution is comprised of two essential elements: an intrusion detection system that is developed for the medical devices that have been incorporated into the healthcare network, and a malware detection system that is customized for the data servers and the computers that are used by medical professionals. Both of these systems are meant to protect the network from unauthorized access. Establishing network security that is not reliant on the individual devices and computers that are in use is the major objective

of this project. The system that is being suggested is constructed using an enhanced version of the LightGBM model as well as a Transformer-based model. These models have been trained using four different datasets, which has ensured that a thorough knowledge of the many sorts of assaults that have the potential to damage the healthcare industry has been achieved.

Faisal Hussain et al [34] offered a framework for making IoT security solutions that are aware of context and can spot harmful data in different IoT situations. IoT-Flock, a new open-source tool made to create IoT data, is a part of the system. With the IoT-Flock tool, you can create an IoT use case that includes both good and bad IoT devices and generates network data to match.

Gia Nhu Nguyen et al [35] proposed a safe intruder detection system with blockchain-based data transfer and a classification model for use in the Cyber-Physical Systems (CPS) of the healthcare field. In this suggested method, monitor devices are used to collect data, and a deep belief network (DBN) model is used to find attacks. A multiple share creation (MSC) model is also used to make several copies of the picture that was taken. The goals of both private and security are met by the model provided because of these tactics.

Raja Waseem Anwar et al [36] provided a full review and best practices for all types of firewalls, including their pros and cons. This may help to define a full set of rules for smart medical devices and settings.

Table 3: Analysis of intrusion detection and prevention in IoT healthcare networks

Ref. No.	Proposed Method	Remarks
[25]	Convolutional Neural Network (CNN)	Accuracy
[26]	Enhanced Healthcare Monitoring System (EHMS)	Performance Robustness Accuracy
[27]	FIDChain	Accuracy
[28]	Blockchain Assisted IoT Healthcare System using Ant Lion Optimizer with Hybrid Deep Learning	Performance
[29]	Random Forest (RF) and a genetic algorithm	Detection rate Average precision Average F1-score
[30]	Investigate K-nearest neighbor, Naïve Bayes, support vector machine, artificial neural network and decision tree.	
[31]	Simultaneous Authentication of Equals (SAE)	Effectiveness Time
[32]	Blockchain-orchestrated Deep learning approach for Secure Data Transmission (BDSDT)	Accuracy
[33]	LightGBM model and a Tranformer-based model.	Accuracy
[34]	IoT-Flock	Performance
[35]	Deep belief network (DBN) Multiple share creation (MSC)	Effectiveness
[36]	comprehensive review on firewall types	

Conclusion

In the evolving landscape of IoT healthcare, security remains a paramount concern, and this survey paper has endeavored to shed light on the key aspects of securing these transformative systems. Secure data access and device authentication mechanisms are vital for controlling access to IoT healthcare networks. Authentication protocols like OAuth and device fingerprinting have shown promise in ensuring only authorized entities interact with these systems. Data encryption, both at rest and in transit, is essential to protect sensitive patient information. Techniques such as homomorphic encryption and blockchain-based approaches hold potential in enhancing data security. Furthermore, intrusion detection and prevention mechanisms play a pivotal role in identifying and mitigating threats in IoT healthcare networks. Machine learning-based intrusion detection systems and anomaly detection algorithms have demonstrated their effectiveness in safeguarding these critical systems. However, challenges like resource constraints and the dynamic nature of IoT environments must be addressed. As IoT healthcare continues to advance, the security landscape will evolve in tandem. Future research directions should explore the integration of Artificial Intelligence and Machine Learning for real-time threat detection, the development of lightweight encryption algorithms for resource-constrained devices, and the adoption of standardized security frameworks. Through continued vigilance and innovation, the healthcare industry can harness the full potential of IoT while ensuring the highest levels of data security and patient privacy.

References

[1] Alzubi, Jafar A. "Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare." *Computer Communications* 170 (2021): 200-208.

[2] Abbas, Asad, Roobaea Alroobaea, Moez Krichen, Saeed Rubaiee, S. Vimal, and Fahad M. Almansour. "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things." *Personal and ubiquitous computing* (2021): 1-14.

[3] Mamdouh, Moustafa, Ali Ismail Awad, Ashraf AM Khalaf, and Hesham FA Hamed. "Authentication and identity management of IoHT devices: achievements, challenges, and future directions." *Computers & Security* 111 (2021): 102491.

[4] Singh, Parminder, Mehedi Masud, M. Shamim Hossain, and Avinash Kaur. "Cross-domain secure data sharing using blockchain for industrial IoT." *Journal of Parallel and Distributed Computing* 156 (2021): 176-184.

[5] Gochhayat, Sarada Prasad, Chhagan Lal, Lokesh Sharma, D. P. Sharma, Deepak Gupta, Jose Antonio Marmolejo Saucedo, and Utku Kose. "Reliable and secure data transfer in IoT networks." *Wireless Networks* 26 (2020): 5689-5702.

[6] Fotouhi, Mahdi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S. Morteza Pournaghi, and Mohammad-Ali Doostari. "A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT." *Computer Networks* 177 (2020): 107333.

[7] Banerjee, Soumya, Vanga Odelu, Ashok Kumar Das, Jangirala Srinivas, Neeraj Kumar, Samiran Chattopadhyay, and Kim-Kwang Raymond Choo. "A provably secure and lightweight anonymous user authenticated session key exchange scheme for Internet of Things deployment." *IEEE Internet of Things Journal* 6, no. 5 (2019): 8739-8752.

[8] Sharma, Geeta, and Sheetal Kalra. "A lightweight user authentication scheme for cloud-IoT based healthcare services." *Iranian Journal of Science and Technology, Transactions of Electrical Engineering* 43 (2019): 619-636.

[9] Srivastava, Gautam, Reza M. Parizi, and Ali Dehghantanha. "The future of blockchain technology in healthcare internet of things security." *Blockchain cybersecurity, trust and privacy* (2020): 161-184.

[10] Shukla, Saurabh, Subhasis Thakur, Shahid Hussain, John G. Breslin, and Syed Muslim Jameel. "Identification and authentication in healthcare internet-of-things using integrated fog computing based blockchain model." *Internet of Things* 15 (2021): 100422.

[11] Ayub, Muhammad Faizan, Khalid Mahmood, Saru Kumari, and Arun Kumar Sangaiah. "Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology." *Digital Communications and Networks* 7, no. 2 (2021): 235-244.

[12] Puri, Vikram, Aman Kataria, and Vishal Sharma. "Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0." *Transactions on Emerging Telecommunications Technologies* (2021): e4245.

[13] Das, Sangjukta, and Suyel Namasudra. "A novel hybrid encryption method to secure healthcare data in IoT-enabled healthcare infrastructure." *Computers and Electrical Engineering* 101 (2022): 107991.

[14] Khan, Mohammad Ayoub, Mohammad Tabrez Quasim, Norah Saleh Alghamdi, and Mohammad Yahiya Khan. "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data." *IEEE Access* 8 (2020): 52018-52027.

[15] Vedaraj, M., and P. Ezhumalai. "HERDE-MSNB: a predictive security architecture for IoT health cloud system." *Journal of Ambient Intelligence and Humanized Computing* 12 (2021): 7333-7342.

[16] Li, Wenchao, Chuanjie Jin, Saru Kumari, Hu Xiong, and Sachin Kumar. "Proxy re-encryption with equality test for secure data sharing in Internet of Things-based healthcare systems." *Transactions on Emerging Telecommunications Technologies* 33, no. 10 (2022): e3986.

[17] Guo, Xuancheng, Hui Lin, Yulei Wu, and Min Peng. "A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems." *Future Generation Computer Systems* 113 (2020): 407-417.

[18] Sharma, Pratima, Nageswara Rao Moparthi, Suyel Namasudra, Vimal Shanmuganathan, and Ching-Hsien Hsu. "Blockchain-based IoT architecture to secure healthcare system using identity-based encryption." *Expert Systems* 39, no. 10 (2022): e12915.

[19] Chaudhary, Ravi Raushan Kumar, and Kakali Chatterjee. "An efficient lightweight cryptographic technique for IoT based E-healthcare system." In *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pp. 991-995. IEEE, 2020.

[20] Ullah, Ata, Ghawar Said, Muhammad Sher, and Huansheng Ning. "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN." *Peer-to-Peer Networking and Applications* 13 (2020): 163-174.

[21] Sowjanya, K., Mou Dasgupta, and Sangram Ray. "A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems." *Journal of Systems Architecture* 117 (2021): 102108.

[22] Andreas, Andreou, Constandinos X. Mavromoustakis, George Mastorakis, Dinh-Thuan Do, Jordi Mongay Batalla, Evangelos Pallis, and Evangelos K. Markakis. "Towards an optimized security approach to IoT devices with confidential healthcare data exchange." *Multimedia Tools and Applications* 80 (2021): 31435-31449.

[23] Liu, Yaru, Jia Yu, Jianxi Fan, Pandi Vijayakumar, and Victor Chang. "Achieving privacy-preserving DSSE for intelligent IoT healthcare system." *IEEE Transactions on Industrial Informatics* 18, no. 3 (2021): 2010-2020.

[24] Das, Sangjukta, and Suyel Namasudra. "MACPABE: Multi-Authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure." *International Journal of Network Management* 33, no. 3 (2023): e2200.

[25] Saba, Tanzila, Amjad Rehman, Tariq Sadad, Hoshang Kolivand, and Saeed Ali Bahaj. "Anomaly-based intrusion detection system for IoT networks through deep learning model." *Computers and Electrical Engineering* 99 (2022): 107810.

[26] Hady, Anar A., Ali Ghubaish, Tara Salman, Devrim Unal, and Raj Jain. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." *IEEE Access* 8 (2020): 106576-106584.

[27] Ashraf, Eman, Nihal FF Areed, Hanaa Salem, Ehab H. Abdelhay, and Ahmed Farouk. "Fidchain: Federated intrusion detection system for blockchain-enabled iot healthcare applications." In *Healthcare*, vol. 10, no. 6, p. 1110. MDPI, 2022.

[28] Alamro, Hayam, Radwa Marzouk, Nuha Alruwais, Noha Negm, Sumayh S. Aljameel, Majdi Khalid, Manar Ahmed Hamza, and Mohamed Ibrahim Alsaid. "Modelling of Blockchain Assisted Intrusion Detection on IoT Healthcare System using Ant Lion Optimizer with Hybrid Deep Learning." *IEEE Access* (2023).

[29] Iwendi, Celestine, Joseph Henry Anajemba, Cresantus Biamba, and Desire Ngabo. "Security of things intrusion detection system for smart healthcare." *Electronics* 10, no. 12 (2021): 1375.

[30] Binbusayyis, Adel, Haya Alaskar, Thavavel Vaiyapuri, and M. Dinesh. "An investigation and comparison of machine learning approaches for intrusion detection in IoMT network." *The Journal of Supercomputing* 78, no. 15 (2022): 17403-17422.

[31] He, Daojing, Qi Qiao, Yun Gao, Jiajia Zheng, Sammy Chan, Jinxiang Li, and Nadra Guizani. "Intrusion detection based on stacked autoencoder for connected healthcare systems." *IEEE Network* 33, no. 6 (2019): 64-69.

[32] Kumar, Prabhat, Randhir Kumar, Govind P. Gupta, Rakesh Tripathi, Alireza Jolfaei, and AKM Najmul Islam. "A blockchain-orchestrated deep learning approach for secure data transmission in IoT-enabled healthcare system." *Journal of Parallel and Distributed Computing* 172 (2023): 69-83.

[33] Ghourabi, Abdallah. "A security model based on lightgbm and transformer to protect healthcare systems from cyberattacks." *IEEE Access* 10 (2022): 48890-48903.

[34] Hussain, Faisal, Syed Ghazanfar Abbas, Ghalib A. Shah, Ivan Miguel Pires, Ubaid U. Fayyaz, Farrukh Shahzad, Nuno M. Garcia, and Eftim Zdravevski. "A framework for malicious traffic detection in IoT healthcare environment." *Sensors* 21, no. 9 (2021): 3025.

[35] Nguyen, Gia Nhu, Nin Ho Le Viet, Mohamed Elhoseny, K. Shankar, B. B. Gupta, and Ahmed A. Abd El-Latif. "Secure blockchain enabled Cyber–physical systems in healthcare using deep belief network with ResNet model." *Journal of parallel and distributed computing* 153 (2021): 150-160.

[36] Anwar, Raja Waseem, Tariq Abdullah, and Flavio Pastore. "Firewall best practices for securing smart healthcare environment: A review." *Applied Sciences* 11, no. 19 (2021): 9183.