*International Journal of Scientific Research and Engineering Development-– Volume X Issue X, Year*

*Available at www.ijsred.com*

LITERATURE REVIEW OPEN ACCESS

# Securing Health Care Infrastructure

Tosheet Hedaoo*, Ashish Sangolkar**, Shreya Ranjan Porwal***

*(Computer Science and Engineering, D Y Patil International University, Akurdi, Pune
Email: tosheethedaoo@gmail.com)

** (Computer Science and Engineering, D Y Patil International University, Akurdi, Pune
Email: ashishsangolkar99@gmail.com)

***(Computer Science and Engineering, D Y Patil International University, Akurdi, Pune
Email: ranjanshreya413@gmail.com)

---

## Abstract:

**This literature review aims to analyse the current state of healthcare infrastructure security and identify key issues and challenges related to the protection of sensitive patient information. With the increasing adoption of digital Electronic Health Records (EHR) and the advancement of high-speed wireless networking, hospitals are facing a growing number of cybersecurity threats. The review examines various security techniques and measures being implemented in healthcare organisations, including administrative, physical, and technical safeguards. Furthermore, the review identifies the need for advanced security techniques that can cover the vast array of threats present in healthcare systems. The researchers conducted a search of online databases to collect and analyse relevant literature, including studies, reviews, and journals. The findings of this review will provide a foundation for future research in healthcare infrastructure security and help healthcare organisations better understand the risks and challenges associated with protecting patient information in a rapidly evolving technological landscape.**

*Keywords* — **Electronic Health Record (EHRs), Medical Internet of Things (MIoT), Security, Encryption, IDS/IPS, VPN**.

---

## 1. INTRODUCTION

The healthcare industry is experiencing a rapid digital transformation, with hospitals and healthcare facilities adopting new technologies to enhance patient care and improve operational efficiency. [1] As technology becomes increasingly integrated into healthcare infrastructure, concerns about the security of sensitive patient data have also become more pronounced. The importance of protecting patient privacy and data security cannot be overstated, as data breaches in the healthcare industry can have serious consequences for patient safety and well-being. With the increased use of electronic health records, mobile health apps, and medical Internet of Things (MIoT) devices, hospitals and healthcare facilities have become prime targets for cybercriminals looking to steal patient data for financial gain or to disrupt healthcare operations.

To address these concerns, healthcare organisations must invest in modern security measures that can safeguard patient data and prevent unauthorised access. [2] However, the healthcare industry faces unique challenges when it comes to securing data, as healthcare data is among the most sensitive and

  

private data types. [3] Healthcare data often contains personally identifiable information (PII), such as patient names, addresses, and medical histories, which can be exploited by hackers to commit identity theft or medical fraud. Healthcare data breaches can also cause reputational damage to healthcare providers, resulting in a loss of trust among patients and stakeholders.

The purpose of this literature review is to explore the current state of healthcare infrastructure security and the challenges faced by healthcare organisations in securing sensitive patient data.

## 2. ELECTRONIC HEALTH RECORDS

Electronic Health Records (EHRs) are digital versions of a patient's medical information, including their medical history, medications, allergies, test results, and other important clinical information. [4] The adoption of EHRs has become increasingly prevalent in healthcare institutions due to their potential to improve patient care, reduce medical errors, and increase efficiency. However, EHRs also present significant security challenges, as sensitive patient information is stored electronically and vulnerable to cyber-attacks.

However, despite the benefits of EHRs in securing medical infrastructure, there are also limitations and challenges. [5] One limitation is the cost associated with implementing EHRs and related security measures, which can be a significant financial burden for healthcare institutions, particularly for smaller institutions. Moreover, EHRs can be complex to implement and maintain, requiring specialised technical expertise and training for healthcare professionals.

In conclusion, the use of EHRs in securing medical infrastructure presents both opportunities and challenges for healthcare institutions. While EHRs have the potential to improve patient care and increase efficiency, they also pose significant security challenges. The implementation of multi-factor authentication, encryption, data backup, and access control mechanisms can enhance EHR security, but healthcare institutions must carefully consider the cost and complexity of implementing and maintaining these solutions.

## 3. EXISTING SOLUTIONS AND TECHNOLOGIES

### *3.1 FIREWALL*

They are designed to control access to a network, protecting it from unauthorised access and potential cyber attacks. Firewalls can be implemented in different ways, such as hardware, software, or a combination of both. In a health care setting, firewalls can be used to protect patient data, prevent unauthorised access to medical devices, and block malicious traffic.

[6] Firewalls can provide a range of security features, such as packet filtering, stateful inspection, and application-level filtering. Packet filtering examines packets of data as they pass through the firewall and blocks traffic that does not meet specified criteria. Stateful inspection goes a step further, analysing the context of the packets to determine whether they are part of a legitimate communication stream. Application-level filtering adds another layer of protection, examining the content of the traffic and blocking any traffic that does not match a set of rules.

### *3.2 INTRUSION DETECTION SYSTEM/ INTRUSION PREVENTION SYSTEM*

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have become a popular solution in the healthcare industry to detect and prevent cyber attacks. IDS monitors network traffic for suspicious activity and alerts administrators when potential threats are detected. IPS is an enhanced version of IDS that not only detects suspicious activity but also takes automated action to prevent the intrusion. The implementation of IDS and IPS can significantly improve the security of healthcare infrastructure by providing real-time monitoring and protection against threats.

[7] The study also revealed that the system was able to detect previously unknown threats through the use of machine learning algorithms. Another study investigated the use of an IDS/IPS system in a cloud-based healthcare environment. The researchers found that the system was effective in detecting and preventing various types of cyberattacks, including denial-of-service (DoS) and man-in-the-middle (MITM) attacks. They also noted that the system was able to provide

  

real-time alerts to administrators, allowing for rapid response and mitigation of cyber threats.

However, some studies have highlighted potential limitations of IDS/IPS in healthcare infrastructure security. For example, one study found that IDS/IPS systems can generate a high number of false positives, which can result in increased workload for security personnel and potential delays in responding to actual cyber threats. Another study noted that IDS/IPS systems may be vulnerable to evasion techniques used by sophisticated cyber attackers.

## 4.WIRELESS ATTACKS

### *4.1 EAVESDROPPING*

Eavesdropping is a form of cyber attack in which an unauthorised user intercepts and listens to network communication between two parties, such as a healthcare provider and a patient.[8] In healthcare, this can be particularly damaging because the information being communicated may be sensitive, confidential, and protected by regulations like HIPAA.

In healthcare, eavesdropping can result in the exposure of sensitive patient data such as medical history, diagnoses, medications, and other personal information. The attacker may then use this information for financial gain, identity theft, or other malicious purposes.

To prevent eavesdropping attacks, healthcare organisations can use encryption technologies like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) to protect sensitive information in transit. Encryption scrambles the information in a way that can only be deciphered by the intended recipient, making it unreadable to any unauthorised users who may be listening in.

### *4.2 MASQUERADING ATTACKS*

Masquerading attacks, also known as impersonation attacks, are a common type of cyber attack that involves a hacker assuming the identity of a trusted user or system in order to gain unauthorised access to sensitive information or resources. [9] In the context of healthcare infrastructure security, masquerading attacks can have serious consequences as they can be used to access and manipulate electronic health records (EHRs), steal sensitive patient information, or cause other types of damage.

One common type of masquerading attack is phishing, in which an attacker sends an email or message that appears to be from a trusted source, such as a healthcare provider, and asks the recipient to provide sensitive information or click on a malicious link. Another type of masquerading attack is known as spoofing, in which an attacker creates a fake network address or identity in order to impersonate a trusted device or system.

To prevent masquerading attacks, healthcare organisations should implement strong authentication and access control mechanisms, such as multi-factor authentication, to verify the identity of users and devices accessing sensitive information or resources. Regular security awareness training for employees can also help to prevent phishing attacks by teaching them how to identify and avoid suspicious emails or messages.

### *4.3 DUMPSTER DIVING*

Dumpster diving is a type of attack that involves physically searching through an organisation's trash or recycling to find sensitive or confidential information. This type of attack is particularly dangerous for healthcare organisations, as medical records contain a large amount of personal and sensitive information, such as patient names, addresses, social security numbers, and medical history.

Attackers who use dumpster diving as a tactic will typically go through the garbage of medical facilities, including hospitals, clinics, and doctor's offices, in search of physical documents or electronic devices that may contain valuable information. [10] They may also search through recycling bins to find items that have been improperly discarded.

Once attackers find documents or devices that contain sensitive information, they can use that information for identity theft, financial fraud, or other malicious purposes. For example, they may use patient information to obtain prescription drugs or to file fraudulent insurance claims. They may also sell the information on the dark web, where it can be used for a variety of criminal purposes.

### *4.4 BLUE BUGGING*

[15] Blue bugging is a type of cyber attack that targets Bluetooth-enabled devices, such as smartphones, laptops, and tablets. The goal of a blue bugging attack is to gain unauthorised access to a device and its data, including confidential information. This type of attack can be particularly dangerous in healthcare settings, where medical devices and equipment often rely on Bluetooth connectivity to communicate with each other and with electronic health records (EHR) systems.

Blue bugging attacks typically begin with the attacker discovering a vulnerability in the Bluetooth protocol used by the targeted device. The attacker then uses specialised software tools and techniques to exploit this vulnerability and

  

gain access to the device's Bluetooth stack, which controls its Bluetooth connectivity. Once access has been gained, the attacker can eavesdrop on communications between the targeted device and other Bluetooth-enabled devices, or even take control of the device remotely.

In healthcare settings, blue bugging attacks can be particularly devastating. For example, an attacker could potentially gain control of a patient monitoring device and manipulate the readings to cause harm to the patient. Additionally, an attacker could gain access to a healthcare provider's smartphone or tablet and steal sensitive patient data, such as medical records and prescription information.

### *4.5 MEDJACKING*

[16] Medjacking is a type of cyberattack that targets medical devices and equipment that are connected to the internet. The term "medjacking" is a portmanteau of "medical device hijacking" and is used to describe the process of taking control of a medical device and using it to gain access to sensitive patient data or to cause harm to a patient.

Medjacking attacks are becoming increasingly common as more and more medical devices are connected to the internet. These devices can include everything from pacemakers and insulin pumps to MRI machines and other diagnostic equipment. While the internet connectivity of these devices can offer many benefits, such as real-time monitoring of patient health, it also exposes them to a range of security threats.

The most common way that medjacking attacks occur is through the use of malware. Hackers can create custom malware that is specifically designed to target a particular medical device or type of device. Once the malware is installed on the device, the hacker can take control of it remotely and use it to perform a variety of nefarious actions.

## 5.POSSIBLE COUNTERMEASURES FOR SECURITY

### *5.1.TOKEN-BASED SECURITY*

Token-based security is a type of security measure that is commonly used in securing healthcare infrastructure.[11] It is a method of authentication that involves the use of a token to gain access to a system or resource. In the healthcare industry, this is often used to secure electronic health records (EHRs), patient data, and other sensitive information.

The most common type of token-based security is the use of smart cards or tokens that are issued to healthcare professionals. These tokens contain a unique identifier that is linked to the user's account, and they are required to be presented each time the user accesses the system. This ensures that only authorised users are able to access the system and prevents unauthorised access.

Another type of token-based security is the use of one-time passwords (OTPs). These are typically sent to the user's mobile device or email address and are required to be entered each time the user logs in to the system. This provides an added layer of security, as the user must have physical access to their device in order to gain access to the system.

This is highly effective in securing healthcare infrastructure, as it provides a high level of authentication and access control. It ensures that only authorised personnel are able to access sensitive information, and it helps prevent data breaches and other security incidents.

One of the primary concerns is the risk of lost or stolen tokens. If a healthcare professional loses their token or it is stolen, an unauthorised person may be able to gain access to sensitive information

It can be time-consuming and inconvenient for healthcare professionals. Having to carry and present a token each time they access the system can be a burden, and the use of one-time passwords can be cumbersome.

### *5.2. VPN ENCRYPTION*

[12] VPN encryption can be used to protect sensitive medical information transmitted between healthcare providers, patients, and other authorised personnel that provides a secure communication tunnel between two endpoints, such as a remote user and an enterprise network. It works by creating a tunnel which is established between a VPN client & VPN server over a public network such as the internet. The VPN client is usually set up on a remote user's device while a VPN server is set up in the healthcare institute's network. Once the connection is established, all communication between VPN client & VPN server is encrypted using strong encryption algorithms.

There are several benefits of VPN encryption, for e.g. accessing patients data & other medical resources from outside the healthcare institute's network. One healthcare institute can share medical information with other medical institutes without risking data breaches or any other security threats. However, it should be noted that VPN encryption is not foolproof & can be vulnerable to attacks, like man-in-the-middle (MITM) attacks or other forms of network-based attacks.

### *5.3 GAIT BASED TECHNIQUES*

In gait-based techniques, a type of biometric authentication method is used to verify a specific individual's identity. For

  

e.g. unique walking style, which is determined by various factors such as weight, height, length of legs & posture. In the context of securing healthcare infrastructure, gait-based techniques can be used to enhance physical security measures. [13] For instance, hospitals & health Care institutions can use gait recognition to monitor the movement of people within the institution & detect any abnormal activity.

Gait-based technique involves usage of specialised sensors or cameras that can capture an individual's walking pattern. The data captured through these sensors is then analysed & compared to pre-registered gait patterns in the database to verify the individual's identity.

On the other hand, gait-based techniques do have some limitations. For e.g. They may not be as accurate as other biometric methods such as fingerprint recognition, particularly if the individual being authenticated has a medical condition that affects their gait.

### *5.4 HOMOMORPHIC ENCRYPTION*

Homomorphic encryption is a type of encryption technique that allows computations to be performed on encrypted data without decrypting it first. This makes it an ideal tool for securing healthcare infrastructure, where sensitive patient data must be protected from unauthorised access.

[17] Homomorphic encryption can help mitigate this risk by allowing computations to be performed on encrypted data. For example, if a researcher wants to analyse the data to identify patterns and trends, they can encrypt the data using a homomorphic encryption scheme and perform the computation on the encrypted data. The results of the computation will also be encrypted, and only the authorised personnel with the correct decryption key can access the results.

[18] Homomorphic encryption has several advantages for securing healthcare infrastructure:

Privacy: Patient data remains encrypted at all times, even during computation, ensuring that it cannot be accessed by unauthorised personnel.

Security: Homomorphic encryption uses mathematical algorithms that are difficult to break, making it highly secure against cyberattacks.

Efficiency: Homomorphic encryption allows computations to be performed on encrypted data without the need for decryption, which can save time and resources.

One of the biggest challenges is the computational complexity of homomorphic encryption algorithms, which can slow down the computation and make it less efficient. Additionally, the use of homomorphic encryption may require specialised hardware or software, which can add to the cost of implementing the system.

## 6.LIMITATIONS OF EXISTING SYSTEM

Firewalls have a number of limitations that can impact their effectiveness in protecting healthcare networks. One major limitation is that they are typically designed to block incoming traffic, but are less effective at identifying and blocking outbound traffic. This means that if an attacker gains access to a healthcare network, they may be able to exfiltrate sensitive data by bypassing the firewall's outbound rules. [6] Another limitation of firewalls is that they are typically static and unable to keep pace with the rapidly evolving threat landscape. New attack techniques and vulnerabilities are constantly emerging, and traditional firewalls may not be able to keep up with these developments. Additionally, many firewalls are designed to protect against known threats, but may be less effective at identifying and blocking zero-day attacks.

IDS/IPS systems also have several limitations. One limitation is that they can generate a high volume of alerts, many of which may be false positives. This can lead to alert fatigue, where security personnel become overwhelmed by the number of alerts and are unable to effectively identify and respond to real threats. Another limitation of IDS/IPS systems is that they may be prone to evasion techniques. Attackers may be able to bypass detection by using sophisticated techniques such as fragmentation, tunnelling, or encryption. Additionally, IDS/IPS systems may not be effective at detecting attacks that are designed to exploit specific vulnerabilities in healthcare software or hardware.

Tokens can be easily lost or stolen, and this poses a significant risk to the security of healthcare infrastructure.[19] If a token falls into the wrong hands, it can be used to gain unauthorised access to

  

sensitive data. The implementation of token-based security requires the purchase of tokens for every user, which can be expensive. The cost of replacing lost or stolen tokens can also add to the overall expense. Tokens need to be carried by users to gain access to healthcare infrastructure, which can be limiting in terms of mobility. Users may forget their tokens or lose them while on the go, making it difficult to access healthcare infrastructure remotely. Token-based security relies on technology, and technical issues can arise, leading to system downtime or reduced efficiency. The implementation of token-based security requires user training to ensure proper usage, and this can be time-consuming and expensive. Users may also need to be trained on how to properly handle tokens to prevent loss or theft. Token-based security typically uses single-factor authentication, which may not be enough to provide adequate security. Multiple factors of authentication may be required to ensure the security of healthcare infrastructure.

Encrypting and decrypting data takes processing power, which can slow down the network and increase latency. In healthcare, where real-time data exchange is critical, this delay can be problematic. Some VPNs are not compatible with certain applications or devices, which can lead to connectivity issues or the need for multiple VPNs. VPNs require regular maintenance and management, including updates and patches to address security vulnerabilities. This can be time-consuming and resource-intensive. VPNs are vulnerable to tunnel breaches, where an attacker gains access to the network by intercepting or compromising the VPN tunnel. This can be particularly concerning in healthcare, where sensitive patient data is at risk. VPNs rely on internet connectivity, which can be unreliable or disrupted, leading to interruptions in service or security breaches.

Gait can be affected by various environmental factors such as the surface on which a person is walking, the shoes they are wearing, and weather conditions. These factors can make it difficult to capture and analyse a person's gait accurately. Gait can also be influenced by a person's health conditions, such as arthritis, injuries, or disabilities. These conditions can affect a person's walking pattern and make it difficult to use gait as a reliable biometric authentication method. Current gait-based authentication systems have limitations in terms of accuracy and reliability. Some systems may not be able to distinguish between similar gaits or may have difficulty identifying people walking at different speeds. Gait-based authentication requires capturing and analysing personal biometric data. This raises privacy concerns and the potential for misuse or unauthorised access to this sensitive information. Gait-based authentication requires users to walk in a specific manner, which may be uncomfortable or unnatural for some people. This could lead to user reluctance or non-compliance with the authentication process.

One of the main limitations of homomorphic encryption is its computational complexity. The process of performing computations on encrypted data is much more complex and resource-intensive than performing the same computations on unencrypted data. This can lead to significant performance issues, particularly when dealing with large amounts of data. Another limitation of homomorphic encryption is the limited range of computations that can be performed on encrypted data. While some operations, such as addition and multiplication, can be performed on encrypted data, more complex computations may not be possible. This can limit the usefulness of homomorphic encryption in certain applications.

## 7. CONCLUSION

Hospitals are facing significant cyber security threats due to the adoption of digital Electronic Health Records (EHRs) and the lack of necessary infrastructure and personnel to defend their networks, putting patients' data at risk. The adoption of electronic health records in the

  

healthcare industry requires strong security measures to ensure patient privacy and data security. This review analysed and discussed various security techniques for healthcare organisations seeking to adopt secure electronic health records systems. The study found that administrative, physical, and technical safeguards are the most frequently mentioned security measures and techniques.

The Medical Internet of Things (MIoT) is an innovative technology that is transforming the healthcare industry towards a more patient-centric approach. MIoT provides real-time intervention solutions and individualised e-health services. However, they manage sensitive patient information. The security and privacy of data acquired from MIoT devices remain major unsolved challenges that require further research.

## 8.REFERENCES

[1] Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.: The Internet of Things for health care: a comprehensive survey. IEEE Access 3, 678–708, 2015.

[2] Nikhat Akhtar, Saima Rahman, Halima Sadia, Yusuf Perwej, "A Holistic Analysis of Medical Internet of Things (MIoT)", Journal of Information and Computational Science (JOICS), ISSN: 1548 - 7741, Volume 11, Issue 4, Pages 209 - 222, April 2021. DOI:10.12733/JICS.2021/V11I3.535569.31023.

[3] A Review of Medical IoT: Applications, Opportunities, and Security Challenges" by M. A. Hasan, M. H. Z. Shakir, and M. M. Rahman (2019)

[4] Electronic Health Records (EHR) by Dr. Tom Joseph Seymour (2012)

[5] Bey, J.M., and Magalhaes, J.S., Electronic health Records in an Occupational Health Setting—Part II. A global overview. Perspect. Int. Occup. Health Nursing. 61(3):95–98, 2013

[6] Kruse, Clemens Scott et al. "Security Techniques for the Electronic Health Records." Journal of Medical Systems 41.8 (2017): 127. PMC. Web. 29 Sept. 2018

[7] Public Health Infrastructures and National Security - Ian Wardell (2018)

[8] Branley, D. and Coventry, L. (2018, April 22). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward.

[9] Stellios, I.; Kotzanikolaou, P., M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor, 20, 3453–3495, 2018

[10] Security Techniques for the Electronic Health Records by Clemens Scott Kruse & Brenna Smith & Hannah Vanderlinden & Alexandra Nealand (2017)

[11] Kogetsu, S. Ogishima, and K. Kato, "Authentication of patients and participants in health inform. exchange and consent for medical research: A key step for privacy protection, respect for autonomy, and trustworthiness," Frontiers Genet., vol. 9, p. 167, June. 2018

[12] Premarathne, U.S.: Hybrid cryptographic access control for cloud based electronic health records systems. IEEE Cloud Comput. 2, 1–7, 2017

[13] Y. Sun and B. Lo, "An Artificial Neural Network Framework for Gait-Based Biometrics," IEEE Journal of Biomedical and Health Informatics, vol. 23, no. 3, pp. 987-998, 2019

[14] Anatomy of Threats to the Internet of Things Imran Makhdoom, M. Abolhasan, J. Lipman, R. Liu, Wei Ni Published 1 April 2019

[15] Haataja, K.M.J. Box, P.O. Kuopio, F. "Security in Bluetooth, WLAN and IrDA: A comparison Department of Computer Science Security", University of Kuopio: Kuopio, Finland, pp. 1–14, 2006

[16] N. BeNazir, I. Minar, and M. Tarique, "BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY," International Journal of Distributed and Parallel Systems (IJDPS), vol. 3, no. 1, 2012

[17] Z. Brakerski, C. Gentry and V. Vaikuntanathan, "Fully homomorphic encryption without bootstrapping", ITCS'12 Proceedings of the 3rd Innovations in Theoretical Com. Science Conf., pp. 309-325, 2012

[18] J.H. Cheon, A. Kim, M. Kim and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers", International Conference on the Theory and Application of Cryptology and Information Security, pp. 409-437, 2017

[19] C. Easttom and N. Mei, "Mitigating Implanted Medical Device Cybersecurity Risks," in 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pp. 0145-0148, 2019

[20] J. Xu and B. Chen, "Secure coding over networks against noncooperative eavesdropping", IEEE Transactions on Information Theory, vol. 59, no. 7, pp. 4498-4509, July 2013

  