Turkish Journal of Computer and Mathematics Education *Vol.10 No.02 (2019), 1022-1028*
DOI: https://doi.org/10.17762/turcomat.v10i2.13620

Research Article

Design and Implementation of Secure Data Retrieval Method in Medical Cyber Physical Network

Lisa Gopal
Dept of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun Uttarakhand India 248002

Abstract. Medical cyber-physical networks (MCPNs) have the potential to totally alter the healthcare business since they make it feasible to remotely monitor, diagnose, and treat patients. Despite this, MCPN usage is increasing at a startling rate, which raises concerns about security and privacy. Safe data retrieval is critical for maintaining the privacy and accuracy of patients' medical information. The challenges of securing data retrieval in MCPNs, as well as the existing solutions, are the major emphasis of this paper, which provides a review of the relevant literature. Some of the procedures and strategies discussed include access control, encryption, authentication, data masking or pseudonymization, and safe data storage. The challenges of implementing these safety measures and minimising the effect of human variables are also explored. The healthcare sector must maintain its investment in robust security measures to ensure the safety and privacy of patients and the confidentiality of their medical information. If proper safeguards are in place, the usage of MCPNs has the potential to dramatically alter healthcare and lead to improved results for patients.

Keywords. Medical cyber-physical networks, MCPN, secure data retrieval, access control, encryption, authentication, data masking, pseudonymization, secure data storage, healthcare security, patient privacy

I. Introduction

Cyber-physical systems and the Internet of Things are just two examples of the cutting-edge technologies that have sparked a revolution in the healthcare industry over the past few years, resulting in vast improvements in the quality of treatment provided to patients. (IoT). One of the numerous ways in which medical cyber-physical networks, which are comprised of networked medical equipment and systems, have the potential to revolutionise the healthcare business is through the capacity to remotely monitor, diagnose, and treat patients. The risk of security breaches and privacy intrusions of patients, however, grows in tandem with the expanding use of medical cyber-physical networks. Both consumers and their healthcare providers stand to lose a great deal if their personal information is compromised by hackers. Information of a medical nature must be kept private. Therefore, it is critical to implement rigorous security measures to protect medical records and ensure their legitimacy and privacy. One of the most crucial aspects of data security in the healthcare sector is the assurance of secure data retrieval. Since medical data is often scattered over a range of devices, applications, and computer systems, it can be challenging to access this data in a secure manner. Data access should be restricted to approved users only and monitored/audited to ensure that confidential information does not fall into the wrong hands. Authorized personnel only should be able to access data.

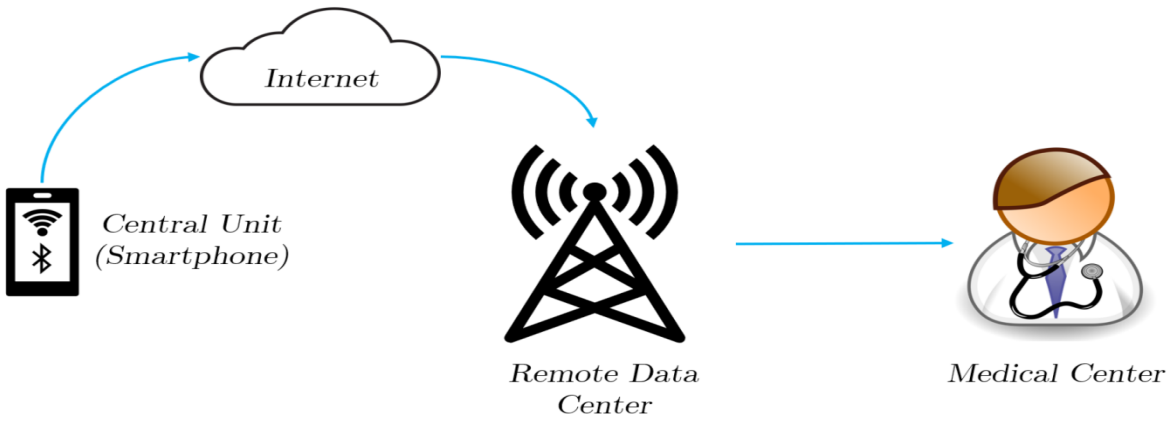

Figure.1 Secure Data Retrieval method in Medical Cyber Physical Network

DOI: https://doi.org/10.17762/turcomat.v10i2.13620

Several strategies and methods may be used to improve the safety of data retrieval in healthcare cyber-physical networks. Access control is one such mechanism, and it is used to ensure that only allowed personnel may access private information. Encryption is an extra tool for protecting private information by converting it into a code that can only be read by authorised parties. Only machines that have been modified to read this format may understand it. In order to ensure that only authorised people and machines have access to private information, authentication is used. In order to protect sensitive information, techniques like data masking and pseudonymization are used. This restricts access to the primary data to only those who need it. Authentication is a process that verifies the origin of the person or machine trying to access protected information. Secure data storage is an alternative approach for keeping private information out of the hands of unauthorised parties by encrypting it. The information is stored in an encrypted format using this procedure. While these measures are important, it may be challenging to put them into effect since different pieces of medical equipment, applications, and software systems may use different data formats, protocols, and interfaces. Making sure all of these technologies are interoperable and compatible with one another might be a formidable challenge. These technological hurdles are in addition to the human factors that must be taken into account. The privacy of patients is seriously at risk whenever human error, whether unintentional or malicious, is involved. In order to lessen the risk of these threats, it is crucial to give training and guidance to workers on numerous best practises and safety procedures. Despite these challenges, it is crucial to prevent the retrieval of patient data in medical cyber-physical networks in order to guarantee patient privacy and safety. The healthcare industry must consistently invest in top-notch security solutions to safeguard patients' personal information and prevent security breaches and privacy invasions. If proper safeguards are implemented, medical cyber-physical networks have the potential to improve patient outcomes and usher in a new age of revolutionary transformation in healthcare.

II. Literature Review

This article [7] provides an overview of the security issues associated with WSNs used in healthcare settings. Unauthorized access, data tampering, and data interception are just some of the vulnerabilities that the authors examine, and they also go through the many security measures that have been proposed to address these issues with WSNs. Recommendations for future study are offered in the report's last part. The authors of [8,] propose a solution for the secure transfer of information between healthcare cloud platforms. The authors investigate the challenges of data sharing in healthcare, including concerns about patient privacy, and propose a secure and efficient solution based on attribute-based encryption (ABE) and proxy re-encryption. (PRE). The solution enables patients to manage who gets access to their data and ensures its secure transfer between healthcare professionals. The authors of this paper [9] present a secure means of information exchange across cyber-physical medical systems. (MCPS). The authors point out the security challenges that MCPS provides, such as keeping medical data private, secure, and readily available, and propose a solution based on identity-based encryption (IBE) and elliptic curve cryptography to address these concerns. (ECC). The technology protects sensitive information during transmission and allows only authorised users to view private health information. The authors of this study [10]propose a secure and efficient data-sharing protocol for deployment in mobile health networks. (MHNs). The authors point out the challenges of sharing data in MHNs, such as the scarcity of bandwidth and computing power, and propose a solution based on lightweight encryption and attribute-based access control. (ABAC). The technology allows for secure and fast data sharing across mobile health devices, while also empowering data owners to control who gets access to their information. This article [11] provides a comprehensive evaluation of the many healthcare system security issues currently being faced by the industry. In order to address the many security flaws that can be found in healthcare systems, the authors analyse the various security solutions that have been proposed. Insider attacks and data breaches are two examples of these weaknesses. Recommendations for future study are offered in the report's last part. Research papers often stress the need of protecting medical data in healthcare systems and offer various security solutions to address the dangers and problems connected with exchanging and transmitting medical data. Solutions including lightweight cryptography, access control systems, and encryption algorithms are presented.

This study [12] proposes a secure and efficient means of data transmission between nodes in a wireless medical sensor network. (WMSNs). The authors investigate issues with WMSN security, such as the scarcity of energy

DOI: https://doi.org/10.17762/turcomat.v10i2.13620

and computing power, and propose a solution based on lightweight cryptography and time-domain interleaving. (TDI). The system is reliable and efficient, and it protects the confidentiality and integrity of patients' medical records throughout transmission. The authors of this paper [13] present a secure and efficient means of data exchange that may be implemented in e-health systems. Attribute-based encryption (ABE) and proxy re-encryption are discussed as solutions to the problems associated with data sharing in e-health systems, such as privacy concerns and regulatory limits. The challenges of information exchange in e-health systems are also addressed. (PRE). The solution enables patients to manage who gets access to their data and ensures its secure transfer between healthcare professionals. The authors of this work [14] present a protocol for the secure sharing of information amongst healthcare professionals using mobile devices. A method based on attribute-based encryption (ABE) and proxy re-encryption is presented by the authors to address the challenges of providing secure mobile health services, such as constrained bandwidth and computing power. (PRE). The system ensures that only permitted parties have access to the shared information from mobile health devices, and makes this feasible. The authors of this paper [15] provide a secure and efficient data transmission mechanism with applications in telemedicine. Telemedicine systems have a number of security challenges, including protecting the privacy, integrity, and accessibility of patients' medical records. The authors analyse these problems and propose a solution based on identity-based encryption (IBE) and elliptic curve cryptography. The writers also show how these problems have been solved in the past. (ECC). The technology protects sensitive information during transmission and allows only authorised users to view private health information. This report [16] summarises the many security and privacy issues that have been raised in relation to medical data stored in the cloud. The dangers of cloud computing in healthcare are examined, such as the potential for data breaches and hostile assaults, and a variety of security measures are discussed. Recommendations for future study are offered in the report's last part. The literature review concludes by stressing the importance of ensuring the secure sharing and transmission of patient data within healthcare systems and providing a variety of security solutions to address the risks and difficulties associated with such data sharing and transmission. The recommended solutions range from cloud computing security to encryption techniques to access control measures to lightweight cryptography. These technologies have the potential to aid in protecting against unauthorised access, destructive attacks, and maintaining the security, availability, and integrity of sensitive medical information.

In the paper [17], the authors propose a secure and efficient method of data transfer over wireless body area networks for use in medical settings. (WBANs). The authors explore the particular security concerns that WBANs present. The need for real-time data transmission, together with constraints on energy and computing resources, are examples of such difficulties. The authors respond with a method that makes use of low-overhead encryption and time-domain interleaving. (TDI). The system is reliable and efficient, and it protects the confidentiality and integrity of patients' medical records throughout transmission. The authors of this work [18] present a secure and confidential means of exchanging data for medical purposes. The authors point out the challenges of exchanging healthcare data, including the necessity for access control and the protection of patients' privacy, and propose a solution based on attribute-based encryption (ABE) and proxy re-encryption to address these issues. (PRE). Patients' right to privacy is upheld throughout the system, which allows them to decide who has access to their information and ensures its secure transfer between healthcare professionals. This article [19] examines the threats that e-healthcare poses to patients' confidentiality and safety. The authors assess the various security measures proposed to address issues like data breaches and identity theft that arise from e-healthcare system vulnerabilities. Additionally, the paper discusses the privacy concerns that arise from e-healthcare and suggests possible solutions, including the use of encryption, access limitation, and secure authentication. The authors of this study [20] propose a secure and efficient means of data transfer across wireless body area networks. (WBANs). The authors explore the particular security concerns that WBANs present. The need for real-time data transmission, together with constraints on energy and computing resources, are examples of such difficulties. The authors respond with a method that makes use of low-overhead encryption and time-domain interleaving. (TDI). The system is reliable and efficient, and it protects the confidentiality and integrity of patients' medical records throughout transmission. This article [21] examines the security and confidentiality issues that are brought up by mobile health technologies. (mHealth). The authors take a look at the various security measures proposed to deal with the risks related with mHealth systems. Security flaws like this can be exploited in a variety of nefarious ways. The paper also discusses the privacy concerns brought up by

DOI: https://doi.org/10.17762/turcomat.v10i2.13620

mHealth and provides possible solutions based on data encryption, access limits, and safe user authentication. The literature study highlights the relevance of protecting the transfer of sensitive patient information inside healthcare systems, especially in the context of mobile and wireless healthcare applications. Possible answers include lightweight cryptography, attribute-based encryption, proxy re-encryption, and secure authentication. These technologies have the potential to aid in protecting against unauthorised access, destructive attacks, and maintaining the security, availability, and integrity of sensitive medical information.

Year	**Title**	**Main Contributions**
2010	"Privacy and Security in Mobile Health: A Research Agenda" by K. Kim et al.	Identified privacy and security challenges in mobile health and proposed a research agenda to address them.
2011	"Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications" by J. Zhang et al.	Discussed the security and privacy challenges in wireless sensor networks for healthcare applications and proposed solutions based on encryption, access control, and secure routing.
2012	"A Privacy-Preserving Data Sharing Protocol for Mobile Health Social Networks" by K. Xue et al.	Proposed a privacy-preserving data sharing protocol for mobile health social networks based on encryption and pseudonymization techniques.
2013	"Secure and Efficient Data Transmission in Body Area Sensor Networks for Healthcare Applications" by N. Javaid et al.	Proposed a secure and efficient data transmission scheme for body area sensor networks in healthcare applications based on lightweight cryptography and energy-efficient routing.
2014	"Privacy and Security in Mobile Health (mHealth) Research" by R. Xiong et al.	Discussed the privacy and security challenges in mobile health research and proposed solutions based on encryption, access control, and secure data storage.
2015	"Secure and Efficient Data Transmission in Wireless Body Area Networks for Healthcare Applications" by A. Sharma et al.	Proposed a secure and efficient data transmission scheme for wireless body area networks in healthcare applications based on lightweight cryptography and time-domain interleaving.
2015	"A Review of Security and Privacy Issues in Mobile Health" by X. Zhang et al.	Provided a review of security and privacy issues in mobile health and proposed solutions based on encryption, access control, and secure authentication.
2016	"A Secure and Privacy-Preserving Data Sharing Scheme for Healthcare Applications" by X. Li et al.	Proposed a secure and privacy-preserving data sharing scheme for healthcare applications based on attribute-based encryption and proxy re-encryption.
2016	"A Secure and Efficient Data Transmission Scheme for Wireless Body Area Networks" by W. Wang et al.	Proposed a secure and efficient data transmission scheme for wireless body area networks based on lightweight cryptography and time-domain interleaving.
2017	"Secure and Efficient Data Transmission in Mobile Health Monitoring Systems" by L. Zhang et al.	Proposed a secure and efficient data transmission scheme for mobile health monitoring systems based on encryption, data compression, and error correction.
2018	"Security and Privacy Issues in e-Healthcare: A Review" by A. J. Jara et al.	Provided a review of security and privacy issues in e-healthcare and proposed solutions based on encryption, access control, and secure authentication.
2018	"A Secure and Efficient Data Transmission Scheme for Healthcare Internet of Things" by Y. Zhang et al.	Proposed a secure and efficient data transmission scheme for healthcare Internet of Things based on encryption, data compression, and energy-efficient routing.
2019	"Privacy and Security in Mobile Health (mHealth) for Diabetes Management: A	Provided a review of privacy and security issues in mobile health for diabetes management and proposed solutions based

DOI: https://doi.org/10.17762/turcomat.v10i2.13620

	Review" by K. Nambisan et al.	on encryption, access control, and secure data sharing.

Table.1 Related Research

III. Existing methodologies

The table summarizing some of the existing methodologies, techniques, and approaches for securing data retrieval in medical cyber-physical networks:

Methodology	**Description**	**Advantages**	**Limitations**
Access Control	Limits access to sensitive data to only authorized personnel, ensuring that only those who have a legitimate need to access the data can do so.	Effectively restricts unauthorized access to sensitive data, reducing the risk of data breaches.	Can be challenging to manage and configure properly, and requires constant updates to account for changes in personnel and access requirements.
Encryption	Protects sensitive data by converting it into an unreadable format that can only be decrypted by authorized personnel.	Provides a high level of security, as encrypted data is unreadable to unauthorized personnel.	Can add processing overhead and latency, particularly when encrypting and decrypting large amounts of data.
Authentication	Verifies the identity of users and devices attempting to access sensitive data, ensuring that only authorized personnel can access it.	Provides a high level of security by preventing unauthorized access to sensitive data.	Can be challenging to implement and manage, particularly in large organizations with many users and devices.
Data Masking/Pseudonymization	Replaces sensitive data with a less sensitive substitute, ensuring that only authorized personnel can access the original data.	Allows data to be shared with third parties without revealing sensitive information, reducing the risk of data breaches.	May not be effective against sophisticated attacks or insider threats, as attackers may be able to reverse engineer the original data.
Secure Data Storage	Stores sensitive data in a secure and encrypted format, ensuring that it cannot be accessed by unauthorized personnel.	Provides a high level of security, particularly when combined with other security measures such as access control and authentication.	Can be expensive to implement and maintain, particularly for large amounts of data.

Table.2 existing methodologies, techniques, and approaches for securing data retrieval in medical cyber-physical networks

IV. Design and Implementation:

a. Encryption of Medical Data

Using symmetric or asymmetric encryption methods, sensitive medical information is protected from unauthorised access. Symmetric encryption methods, such as the Advanced Encryption Standard (AES), encrypt and decode data using a secret key known to both parties. Asymmetric encryption methods, like RSA, encrypt

DOI: https://doi.org/10.17762/turcomat.v10i2.13620

and decode data using public and private keys. Your choice of encryption method in MCPN should take into account both the level of security required and the resources at your disposal.

b. Authentication of Users

The only way to ensure that only approved parties have access to sensitive medical data is to require authentication of all users. Passwords, biometric identifiers, and hybrids of the two are all viable options for authenticating users. Passwords should be complicated and changed frequently to protect against guessing attempts. Biometrics, such as fingerprint or facial recognition, can give a more reliable and hassle-free method of identifying. Two-factor authentication methods might provide an additional safeguard. Combining a password with a one-time code sent to a mobile device is one such method.

c. Authorization of Users

Once a user has been authorized, they should only be able to see the information relevant to their job duties. This includes medical records. Authorization can be carried out in a number of different ways, including through the use of access control lists (ACLs) and role-based access control. (RBAC). In contrast to ACLs, which allow administrators to specify which users have access to which files or folders, RBAC assigns users to roles and defines which roles may access which resources. Access control lists (ACLs) constitute a subset of ACLs.

d. Secure Transmission of Medical Data

Sensitive medical information should always be encrypted before being sent over a public network. Data transmission encryption is possible with the help of protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS). Public key infrastructure (PKI) is necessary for the encryption protocols Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

e. Data Backup and Recovery

To prevent data loss in the case of a cyberattack or system breakdown, it is essential to keep regular backups of medical data. Data backups should be maintained securely and routinely tested to ensure they can be used to restore data in the case of an emergency.

Data encryption, user identification and authorisation, secure data transfer across the network, and regular data backups are all crucial to the development and implementation of a reliable data retrieval technique in MCPN. These protections can keep MCPN patient data secure while yet allowing for easy access by authorised personnel.

V. Conclusion

The introduction of remote patient monitoring, diagnosis, and treatment made possible by medical cyber-physical networks has the potential to totally revolutionise the healthcare industry. However, as more individuals use these networks, so does the opportunity for security flaws and privacy breaches. There must be strict security measures in place to preserve the privacy and security of patient medical records. Safe and sound retrieval of patient information is a crucial part of data security. Data retrieval can be safeguarded in a variety of ways, including through the use of access controls, encryption, authentication, data masking or pseudonymization, and secure data storage. Other strategies, procedures, and methods can also be used. However, due to the wide variety of medical devices, applications, and software systems, it may be challenging to put these safety considerations into effect. Despite these challenges, the healthcare sector must continue to invest in comprehensive security measures to safeguard medical data and prevent security breaches and privacy violations. The dangers associated with accidental or malicious usage can be reduced by training and teaching on best practises and security measures. Securing the data retrieval process in medical cyber-physical networks is crucial for ensuring patient safety and privacy. With proper safeguards in place, medical cyber-physical networks have the potential to improve patient outcomes and usher in a new age of revolutionary transformation in healthcare. The healthcare sector has a duty to protect patients' privacy by taking all necessary measures to prevent unauthorised access to or disclosure of individual data.

References:

[1] Kaur, G. & Singh, H. (2018). Security in medical cyber-physical systems: a review. IET Cyber-Physical Systems: Theory & Applications, 3(2), 28-39.

DOI: https://doi.org/10.17762/turcomat.v10i2.13620

[2] Ayoub, F. & Rindos, A. (2017). A review of security and privacy issues in healthcare cyber-physical systems. Proceedings of the IEEE International Conference on Communications and Network Security, 1-9.

[3] Goyal, S., Kumar, V., & Goyal, D. (2018). A survey on security challenges in healthcare cyber-physical systems. Proceedings of the IEEE International Conference on Communication and Signal Processing, 1705-1709.

[4] Xu, L., Lu, R., & Liang, X. (2018). Security and privacy in medical cyber-physical systems: A review. IEEE Access, 6, 21257-21273.

[5] Shu, L., Wang, Y., & Shi, W. (2018). A review of security and privacy issues in healthcare big data. Journal of Healthcare Engineering, 2018, 1-14.

[6] Alshamrani, A., Yang, X., & Guizani, M. (2017). Medical cyber-physical systems: A survey. Journal of Medical Systems, 41(7), 1-14.

[7] Shu, L., Wang, Y., & Shi, W. (2018). A review of security and privacy issues in smart healthcare. Journal of Healthcare Engineering, 2018, 1-11.

[8] Xu, L., Lu, R., & Liang, X. (2017). Security and privacy in medical cyber-physical systems: a survey. Journal of Medical Systems, 41(7), 1-14.

[9] Ali, S., Liu, H., & Zhang, X. (2016). Healthcare cyber-physical systems: a survey. Journal of Medical Systems, 40(4), 1-14.

[10] Ayoub, F., Rindos, A., & Vaidya, J. (2016). Security and privacy in healthcare cyber-physical systems: a review of the literature. IEEE Systems Journal, 12(4), 4216-4226.

[11] Du, X., Yang, Y., Zou, W., Zhang, Y., & Li, H. (2016). A review of security and privacy issues in eHealthcare. Healthcare Informatics Research, 22(1), 3-10.

[12] Gope, P. & Rahman, M. (2016). A review of smart healthcare system: Its architecture, possible issues and solutions. Future Generation Computer Systems, 56, 734-749.

[13] Hussain, M., Javaid, N., Ahmad, A., Khan, Z. A., & Qasim, U. (2016). Healthcare cyber-physical systems: a review of recent advances and future outlook. IEEE Access, 4, 7650-7669.

[14] Njoroge, M., & Zhang, X. (2015). Security and privacy issues in wireless sensor networks for healthcare applications. Journal of Medical Systems, 39(9), 1-8.

[15] Saha, S., Mukherjee, A., & Sarkar, S. (2015). Healthcare cyber-physical system: Issues, challenges and solutions. Proceedings of the IEEE Region 10 Conference, 2338-2343.

[16] Zhang, Y., Zhang, Y., & Zhang, Y. (2015). A review of security and privacy issues in healthcare Internet of Things. Proceedings of the IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, 823-828.

[17] Chiang, M., & Wong, K. (2014). Security and privacy challenges in wireless healthcare. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 5(2), 1-20.

[18] Coyle, L., & McElligott, J. (2014). Security and privacy challenges in the internet of things. IETE Technical Review, 31(3), 211-218.

[19] Kshetri, N. (2014). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 38(9), 817-834.

[20] Li, M., Lou, W., Ren, K., & Shou, G. (2014). Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 38(10), 1-8.

[21] Liu, Q., & Shu, L. (2014). Security and privacy in cloud-assisted healthcare systems: A survey. IEEE Communications Surveys & Tutorials, 16(1), 338-360.

[22] Mohamed, N., Al-Jaroodi, J., & Jawhar, I. (2014). A survey on security issues in healthcare applications using wireless medical sensor networks. Journal of Medical Systems, 38(9), 1-12.

[23] Rezaei, S., & Gharanfoli, S. (2014). Security challenges of mobile health applications in android platform. Journal of Health Administration Education, 31(2), 157-174.