International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 20s, 2025
https://theaspd.com/index.php

Cybersecurity Methods To Safeguard Healthcare Data

Namrata Bathli[1], Vanishri Sataraddi[2], Shrati Bothgi[3], Nagaratna Yaligar[4], Shruti M Patil[5], Shruti Modi[6]
[1]Assistant Professor, Computer Science, Department, P C Jabin Science College Hubballi, Karnataka, India.
namratakottursheettar@gmail.com
[2]Assistant Professor, Computer Science and Engineering, RNS Intitute of Technology, Bengaluru, Karnataka, India.
vanishrisataraddi@gmail.com
[3]Assistant Professor, Computer Science Department, P C Jabin Science College Hubballi, Karnataka, India.
shrativbothgi@gmail.com
[4]Assistant Professor, Computer Science and Engineering, KLE Technological University, Hubballi, Karnataka, India.
nagaratna.yaligar@kletech.ac.in
[5]Assistant Professor, Computer Science and Engineering, SUK University, Kalburgi, Karnataka, India.
shrutimnpatil@gmail.com
[6]Assistant Professor, CSE, Lingrajappa Engineering, College, Bidar, Karnataka, India.
modi21shruti@gmail.com
*Corresponding Author: namratakottursheettar@gmail.com

Abstract: *With the increasing digitization of medical records and the adoption of electronic health information systems, healthcare data security has grown more demanding in order to ensure patient privacy, data integrity, and regulatory compliance. In this paper we are discussing different cybersecurity techniques which are used to strengthen healthcare organizations security posture and protect private patient data. Important strategies include thorough employee training, incident response planning, network segmentation, intrusion detection systems, and strict access controls and multi-factor authentication to prevent unauthorized access. Encryption can be used for both protecting data and in transit at rest. The cybersecurity architecture in healthcare settings is further strengthened by compliance with pertinent rules, such as GDPR and HIPAA. Healthcare companies can enhance patient data security by putting these cybersecurity precautions into practice.*

Keywords: *Healthcare Data, Cybersecurity techniques, patient privacy, Encryption, Access Control, Data Breaches.*

1. INTRODUCTION

The healthcare industry has experienced a notable digital revolution in recent times, owing to the extensive use of electronic health records (EHRs), telemedicine platforms, and other technologically advanced solutions. Although these developments have increased productivity and enhanced patient care, they have also sparked worries about the safety of private medical information. Protecting medical records from online attacks has emerged as a top concern for healthcare institutions across the globe. Ensuring patient confidentiality, data integrity, data availability and regulatory compliance face significant issues as a result of the digitization of healthcare data. Cybercriminals may take advantage of holes in systems and networks to obtain unauthorized access, steal patient data, or interfere with healthcare services. Healthcare data is very important to them. Furthermore, a data breach in the healthcare industry can have serious repercussions, including diminished patient safety, legal responsibilities, and financial losses as well as harm to one's reputation.

Aspects	Description
Patient Confidentiality	It is about preventing the disclosure of sensitive information about patient data to unauthorized parties.
Data Integrity	Integrity assures that healthcare data is accurate, consistent, and dependable. Putting safeguards in place to stop unauthorized additions, deletions, or tampering with patient records is part of maintaining data integrity.
Data Availability	Availability assures that authorized people or systems can access and use healthcare data as needed.

Regulatory Compliance	In the healthcare industry, regulatory compliance is the act in which healthcare organizations adhering to laws, rules, and guidelines that are designed to protect patient privacy, security, and integrity, as well as the calibre and safety of healthcare services.

2. BACKGROUND

Cybersecurity in Healthcare: A History

Due to lengthy purchase cycles, stringent regulations, and historical delayed adoption of new technology, healthcare practitioners have an easier time continuing to use outdated systems even after they become insecure. However, in the last several years, the landscape of healthcare cybersecurity has quickly transformed. Following many notable data breaches, the Cybersecurity Act of 2015 (CSA) was created specifically to enhance cybersecurity in the healthcare sector. Since then, the importance of cybersecurity has grown, both for the regular operation of healthcare institutions and as a fundamental element of high-quality patient care. Additionally, healthcare cybersecurity is becoming a viable and necessary investment due to the rising costs of patient data breaches.

Common Threats in Cybersecurity

1. Phishing Emails

An email that looks to be from a reliable source is sent to employees as part of an email phishing attack. The email will deceive medical personnel into revealing personal data, including system login credentials, or clicking on a link that infects the machine with malware.

2. Ransomware Assaults

Ransomware is a type of malware that encrypts files or stops users from using their computers until a ransom is paid. Because their operations are so essential, healthcare organizations are especially liable to ransomware assaults. These attacks have the potential to impair patient treatment, compromise private information, and cause monetary losses.

3. Hardware Theft or Loss

This is among the more frequent reasons why there are breaches in healthcare data. Laptops and other devices that have access to medical data can occasionally be lost or stolen, giving thieves access to them. In other instances, improper disposal of computers with sensitive data results in a data breach.

4. Attacks on Healthcare Equipment

Cyberattacks of this kind pose a particularly dangerous risk to healthcare providers because they give hackers access to their computer network and give them the ability to seize control of smart medical devices, such heart monitors, and disable them altogether until a ransom is paid.

3. Methods of Cybersecurity to Protect Healthcare Data

Encrypting the Data

To avoid unwanted access, healthcare data must be encrypted while it is in transit and at rest. Sensitive data kept on servers, portable devices, and databases should be encrypted using robust encryption techniques. Additionally, use encryption technologies to secure data while it is being transmitted over networks, such as TLS/SSL.

Access Control

Use strong access controls to limit access to medical records according to user roles and authorization. Use role-based access control (RBAC) techniques to ensure that only authorized individuals can read, edit or remove patient records. Endpoint Protection

Endpoint Protection

Endpoint protection software are used to safeguard mobile, laptop, and desktop computers. Install firewalls, intrusion detection/prevention systems (IDS/IPS), and antivirus software to find and eliminate threats targeting endpoint devices. Enable features like device encryption, multi-factor authentication (MFA), and remote wipe capabilities to enhance endpoint security.

Firewall and Intrusion Protection System

Hospitals should make sure they have the most recent software to seal and patch any potential points of intrusion since hackers will try to locate and exploit any weak spots in a computer network. SonicWall Firewall devices were affected by one of the most recent widespread vulnerabilities, known as URGENT/11.

In order to eliminate the possibility of an attacker exploiting this vulnerability, SonicWall promptly produced a patch for SonicOS.

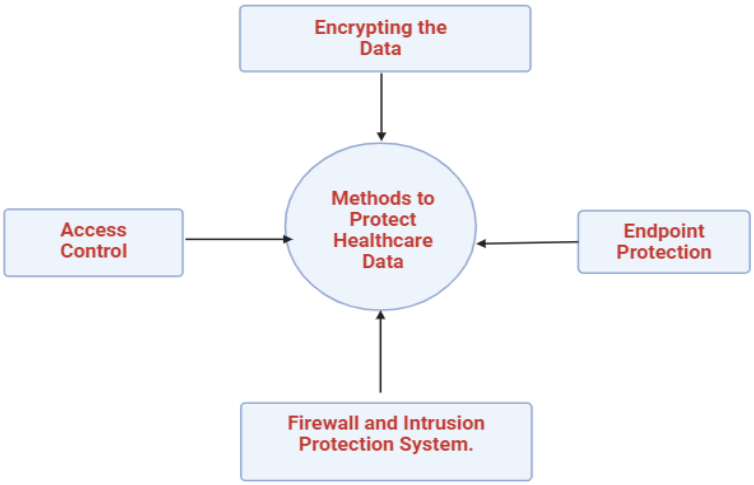

Fig 1. Cybersecurity for Healthcare Data

4. LITERATURE REVIEW

Cybersecurity Analysis and Evaluation for Intrusion Detection Systems

In order to counter the growing threat of cyberattacks, proactive security solutions are becoming more and more important, as this study [1] highlights the importance of machine learning in cybersecurity. Analytical Hierarchy Process (AHP) and Technique for Order of Preference by Similarity to Ideal-Solutions (TOPSIS) are two examples of Multi-Criteria Decision Making (MCDM) methodologies that can be used to evaluate the effectiveness of machine learning-based intrusion detection systems in fuzzy situations.

Challenges

- As mentioned, the primary goal of this work was to evaluate intrusion detection systems' optimality using integrated fuzzy-based AHP-TOPSIS techniques.
- The components that were included in this estimation were selected and identified using expert judgement in conjunction with recently published, relevant research findings.
- In AHP, the accuracy feature has been assigned the highest weight under fuzzy logic settings.
- Systems for detecting anomalies, abuse, malware, DoS attacks, phishing, spam, and implementation complexity come next.

This work well communicates the study subject, which is assessing machine learning-based intrusion detection systems in fuzzy situations using MCDM approaches. In my opinion, in terms of its importance, it provides a methodical way to tackling this problem and clearly highlights the necessity for proactive cybersecurity measures in light of growing cyber threats.

Ensuring Network Security with a Robust Intrusion Detection System Using Ensemble-Based Machine Learning

An article that advances intrusion detection systems (IDS) with ensemble-based machine learning algorithms is highlighted in this research study [2]. It offers an innovative solution to these restrictions while acknowledging the drawbacks of conventional IDSs that rely on signature-based detection.

Challenges

- The objective of this research is to develop and evaluate an ensemble-based machine learning methodology for intrusion detection that performs better than existing methods in terms of accuracy and false positive rate (FPR).
- A range of public datasets and numerous ensemble methods, including Random Forest, Gradient Boosting, Adaboost, Gradient XGBoost, Bagging, and Simple Stacking, will be utilised to assess the proposed methodology.

I believe that this research paper effectively addresses a significant cybersecurity challenge, enhancing intrusion detection systems via the use of ensemble-based machine learning methods. The paper outlines the need for a rigorous development and evaluation of the proposed technique. This is a critical step in the advancement of the profession. The thoroughness of the evaluation process, which includes using a variety

of evaluation measures and testing the suggested approach on numerous public datasets, has really impressed me. This thorough assessment guarantees that the findings are solid and trustworthy, offering insightful information about how well the method works.

Prevention and Mitigation Measures Against Phishing Emails: A Sequential Schema Model

In the field of cybersecurity, the growing frequency of phishing emails is a serious concern since they take advantage of flaws in information technology systems and put people and businesses at danger. Professionals in cybersecurity have created a variety of mitigation techniques in response to these risks. The situational crime prevention strategy serves as the model for the sequential schema that this study [3] suggests to classify these mitigation activities into. Cybersecurity experts may create more planned and strategic reactions to phishing situations by using this approach, which enables a systematic examination of both environmental and human vulnerabilities.

Challenges

- Complexity of Situational Crime Prevention strategy: Although insightful, the situational crime prevention strategy could be difficult for cybersecurity experts who aren't familiar with criminological theories to understand. To guarantee that these ideas are widely understood and used, it could be required to simplify and turn them into workable tactics.
- Vulnerability assessment subjectivity: Depending on the situation, evaluating environmental and human vulnerabilities may be arbitrary. The way that the sequential schema is applied can vary depending on how various companies view and rank vulnerabilities.
- Cyber threats are dynamic in nature: They are always changing, and phishing attacks are no exception. As attackers evolve their strategies, mitigation solutions that work today might not work tomorrow. Constant modification and updating will be necessary to keep the suggested schema current and relevant.

This research suggests a step-by-step framework for classifying phishing mitigation techniques to be a promising addition to the cybersecurity community. Utilizing the situational crime prevention strategy offers a novel viewpoint on handling the intricate problem of phishing attempts, taking into account both environmental and human vulnerabilities. Cybersecurity experts may find the paper's organized framework useful in developing more potent protection tactics against phishing attacks, as it provides a methodical approach to evaluate and rank mitigation measures. Through its emphasis on comprehending and mitigating vulnerabilities at various phases of an assault, the paper promotes a proactive and comprehensive strategy for cybersecurity.

A Review of Deep Learning Models to Detect Malware in Android Applications

Malware detection in Android applications is a major and expanding cybersecurity threat that is addressed in this research [4]. As people depend more and more on smartphone apps for a variety of tasks, mobile device cyberattacks are becoming a serious concern. In order to improve mobile security, it is crucial to investigate the use of DL models in this situation.

Challenges

- Data Availability and Quality: Obtaining and maintaining high-quality datasets is a major obstacle to developing deep learning models that are capable of detecting malware. Malware samples are frequently hard to come by, and it might be difficult to gather representative and diverse datasets. Furthermore, malware samples can differ in terms of quality and labeling, which could affect how well trained models work.
- Model Generalization: New and undiscovered malware variants may be difficult for deep learning models trained on current datasets to generalize to. The methods used by malware writers to avoid detection are always changing, making it challenging for static models to stay up to date. A major difficulty is making sure the trained models are resilient and able to identify new threats.

This work contributes significantly and opportunely to the realm of cybersecurity by examining the application of deep learning models for Android application malware detection. It does an excellent job of illustrating both the increasing threat that malware in the mobile arena poses and the potential that deep learning techniques provide for solving this problem.

Towards Insighting Cybersecurity for Healthcare Domains: A Comprehensive Review of Recent Practices and Trends

Given the rising reliance on cutting-edge medical technology and healthcare apps, the study [5] correctly highlights the growing significance of cybersecurity in the field of healthcare. Strong security measures must be put in place in the healthcare sector immediately because of the possible repercussions of cybersecurity breaches, which include ransomware attacks and tampering with medical devices.

Challenges

- Healthcare systems are intrinsically complicated due to their large number of interdependent stakeholders and components. It can be difficult to implement cybersecurity measures across such a wide range of interconnected systems, necessitating close coordination and cooperation between IT specialists, healthcare providers, government agencies, and other stakeholders.
- Regulatory Compliance: Strict laws, such as the Health Insurance Portability and Accountability Act (HIPAA) in the US and the General Data Protection Regulation (GDPR) in the EU, must be followed by the healthcare sector. In order to assure legal compliance, the deployment of cybersecurity measures requires
- Specialised knowledge and introduces an additional degree of complexity.

This study discusses cybersecurity issues in the healthcare industry offers a thorough synopsis of a problem that is becoming more and more important. It does a good job of highlighting the significance of safeguarding private patient data from online attacks and the particular difficulties that healthcare institutions encounter when putting strong cybersecurity measures in place.

Design of Blockchain-Enabled Secure Smart Health Monitoring System and Its Testbed Implementation

This paper [6] presents a novel solution to the security and privacy concerns associated with smart healthcare technologies: the implementation of a blockchain-enabled secure smart health monitoring system (BSSHM). highlights the need of collaboration in enhancing cybersecurity within the healthcare sector.

Challenges

- Complexity of Blockchain Integration: It can be difficult and resource-intensive to integrate blockchain technology into healthcare systems. Infrastructure development for blockchain-enabled data transmission and storage necessitates specialized knowledge and financial investment in technological resources.
- Scalability Issues: Blockchain systems may experience scalability issues when managing substantial amounts of medical data. A major problem is making sure the BSSHM system can scale efficiently to meet the increasing demand for smart healthcare services without sacrificing effectiveness.
- Interoperability with Current Systems: There may be interoperability issues when integrating BSSHM with current healthcare standards and systems. To guarantee seamless data transfer and interoperability with legacy systems, electronic health records (EHRs), and health information exchanges (HIEs), careful planning and coordination are required.

It's a creative and relevant idea to use blockchain technology into smart healthcare systems. Blockchain technology's decentralised and immutable features offer a novel solution to the security and privacy problems that beset traditional healthcare systems. The idea of BSSHM, which combines blockchain technology with real-time health monitoring sensors to transmit safe data, seems to have implications in the healthcare industry for bettering patient care and data security. The study presents the architecture and functionality of BSSHM in an effective manner, indicating that it may be feasible in the future.

Healthcare Data Quality Assessment for Cybersecurity Intelligence

This article [7] proposes the normalised double entropy (NDE) method to assess the quality of picture data in healthcare systems. It tackles issues with indiscriminate data collecting, annotation, and transfer, which can jeopardize healthcare data processing security and efficiency.

Challenges

Validation and Generalization: Extensive validation of the NDE method's efficacy across a range of healthcare datasets and imaging modalities is required. For the

- Method to be more broadly applicable and generalizable, it must be guaranteed to function uniformly across a variety of medical image formats and patient demographics.
- Data Quality Definition: It can be difficult and subjective to define what "good" and "bad" data are in healthcare settings. Since the NDE technique depends on these distinctions to assess data quality,

it is imperative to provide precise and consistent standards for defining data quality in order to guarantee the dependability and correctness of the evaluations.

As a significant development in the field, this work proposes the use of the normalised double entropy (NDE) approach to assess the quality of picture data in healthcare systems. Ensuring the quality and reliability of medical photographs is a critical component of healthcare data processing that this study covers. Accurate diagnosis and treatment depend on these images. By taking into account both probability and distance entropies, the NDE technique presents a novel way to analyze data quality. This thorough evaluation can assist in identifying important data while removing noise and artifacts. The paper's experimental results emphasize the NDE method's potential usefulness in healthcare settings by demonstrating how well it can discern between good and bad data.

5. Future Scope

Data sharing, collection, and analysis will become increasingly widespread in the health sector in the future. with this previously unobtainable data, health care firms will be in a position to generate new value by boosting customer engagement and operational efficiencies. organizations will need to update data protection rules and pay more attention to data privacy as this change progresses. they will also be under more pressure to improve cybersecurity threat awareness, detection, and response capabilities in the healthcare industry.

6. CONCLUSION

Two major challenges in the healthcare industry are ensuring patient data security and protecting critical infrastructure. As healthcare systems become more digitized, they face increased cyber threats targeting sensitive data and essential services. Strong cybersecurity measures are crucial to protect patient privacy and maintain uninterrupted care. Healthcare organizations can improve their defences by adopting robust risk management, securing networks with firewalls and monitoring tools, and regularly updating systems. Employee training, data encryption, multi-factor authentication, and frequent security audits further strengthen protection and ensure compliance. As cyber threats continue to evolve, proactive threat detection and incident response strategies are essential. Building a cybersecurity culture across all levels of staff can significantly reduce risks and enhance patient trust.

Ethical Approval and Consent to Participate

Hereby, I Ms. Namrata Bathli and co-authors consciously assure that for the manuscript **Cybersecurity Methods to Safeguard Healthcare Data** does not involve Human, Animals or Plants.

Consent for Publication

I, declare the manuscript does not contain any individual person data.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created.

Author Contribution

All authors have equal contribution in the paper and all authors have read and agreed to the published version of the manuscript.

Funding

Authors declare that they have no funding involved in this paper.

Competing Interests

Declaration of Interests: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

A. Cybersecurity Analysis and Evaluation for Intrusion Detection Systems Yoosef B. Abushark1, Asif Irshad Khan1, *, Fawaz Alsolami1, Abdulmohsen Almalawi1, Md Mottahir Alam2, Alka

1. Agrawal3, Rajeev Kumar4 and Raees Ahmad Khan, Tech Science Press, January 2022
2. Ensuring network security with a robust intrusion detection system using ensemble-based machine learning Md. Alamgir Hossain *, Md. Saiful Islam, Elsevier, 1 July 2023
3. Prevention and mitigation measures against phishing emails: a sequential schema model, Yumi E. Suzuki1 · Sergio A. Salinas Monroy2, Springer to nature, 28 September 2021
4. A review of deep learning models to detect malware in Android applications, Elliot Mbunge a,b,∗, Benhildah Muchemwa a, John Batani c, Nobuhle Mbuyisa, Elsevier, 11 February 2023
5. Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends, Mohd Javaid a, ∗, Abid Haleem a, Ravi Pratap Singh b, Rajiv Suman, Elsevier, 11 March 2023

6. Design of blockchain-enabled secure smart health monitoring system and its testbed implementation, Siddhant Thapliyal a, Shubham Singh a, Mohammad Wazid a,*, D.P. Singh a, Ashok Kumar Das, Elsevier 10 June 2023,
7. Healthcare Data Quality Assessment for Cybersecurity Intelligence, Yang Li, Jiachen Yang, Senior Member, IEEE, Zhuo Zhang, Jiabao Wen, and Prabhat Kumar, IEEE Transactions On Industrial Informatics, Vol. 19, No. 1, January 2023