International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 1s,2025
https://theaspd.com/index.php

Cybersecurity Measures For Protecting Medical Data

Naina Bhoyar[1],Aakansha Soy[2],Dr. Monica Verma[3],
[1]Assistant Professor, Department of Pharmacy, Kalinga University, Raipur, India.
ku.nainabhoyar@kalingauniversity.ac.in, 0009-0000-0999-8741
[2]Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India.
ku.aakanshasoy@kalingauniversity.ac.in, 0009-0002-1955-6909
[3]Professor, New Delhi Institute of Management, New Delhi, India.,monica.verma@ndimdelhi.org,
https://orcid.org/0000-0003-2789-1117

Abstract
The advancement of the healthcare sector in India and other Asian nations is occurring at an extraordinary pace. Information technology is a crucial component of this transformation. Nevertheless, despite notable progress in healthcare, information security has not yet reached the protective standards established in more technologically advanced nations such as the United States and the United Kingdom. This study aims to identify vulnerabilities and risks within the realm of Cybersecurity and to propose targeted solutions in three key areas: risks, vulnerabilities (IoMT). The outcome of this research is the creation of a security maturity model tailored for healthcare in India, utilizing a qualitative research methodology. Cyberattacks on healthcare facilities are increasing globally, with Asian hospitals recently becoming frequent targets. Asian countries are lagging behind Western nations, such as the United States, which have implemented laws, rules, standards, and other safeguards against healthcare cyberattacks. People in Asia are starting to realize how important electronic health records, or EHRs, are. One type of healthcare data that many hospitals and healthcare systems successfully preserve is sensitive patient data. However, because of the high value of the data involved, protecting healthcare data requires a sophisticated, technology-driven, and compliance-focused strategy.
Keywords: *Cyberattacks, Information technology, Cybersecurity*

INTRODUCTION

Computer networks and Information Communications Technology (ICT) systems are the dynamic backbone for the fast development in today's field of science and technology in the world. With a wide emergence of communication patterns and an exponential increase in the devices of network in quantity, cyber security has become a crucial imperative for protecting valuable data and information that are extremely vulnerable to intruder attacks. Detection of intrusion is the central role in guaranteeing information integrity and security of precious data, and the key technology is to properly identify different threats in the network[1]. The attacks can be manual or automated and always enhance their capability, leading to stealthy data breaches. Many large companies defend themselves with traditional security technologies against network assaults by firewalls, anti-spam methods and anti-virus programs. Unfortunately, these technologies fail to identify the threats of new or sophisticated one. To ensure secure transmission, security measures have to fight against threats and need counter developments to the changing security risk [2]. Although networks are protected by firewalls, intrusion detection in network is an uphill task. Possible intruders introduce a new intrusion pattern of attacks and intrusion in a day to day fashion and an effective intrusion detection method should be able to identify the intrusion. In recent decades, the spread of intrusion targeting devices and network-based services grew exponentially, and cyber security became a necessity subject for protection of systems from threats at local and global levels [3].

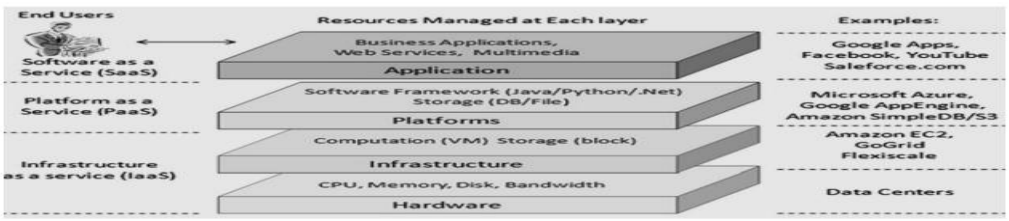

Figure 1: Service Model of Cloud Computing

The methods of machine learning and deep learning became prevalent in the assessment of Intrusion Detection Systems (IDS) that have the capability to quickly and independently detect and classify cyber-attacks on hosts and networks [4]. Machine learning-based Intrusion Detection Systems (IDSs) show strong detection performance when they are given sufficient training data, enabling them to generalize well and detect different attack variants, including new attacks. In addition, such IDSs possess the benefit of not depending greatly on domain knowledge and thus can be designed and constructed easily [5].

REVIEW OF LITERATURE

In a Defend–assault scenario, for example, a sequential choice game is depicted in which the attacker chooses an assault plan (a) and the defender chooses a defense strategy (d). In this instance, the attack's success or failure is indicated by the outcome S [6]. Therefore, the success of one player's attacking move determines the outcome for both players. At a given project level, the Cyber Security Game (CSG) provides a framework for statistically assessing digital security threats and using the results to decide how best to apply security solutions for particular systems [7].

One of the main characteristics of non-cooperative games is that participants cannot enforce their contracts with one another, which means that no other authority (like the courts) may enforce the agreements [8]. In this case, players' cooperation only becomes an equilibrium or solution proposal when it serves their own interests [9].

MATERIALS AND METHODS

All organizational assets are subject to hazards, which are identified, estimated, and prioritized as part of the Cyber Risk Assessment Process. There are unique features to every risk assessment approach. In this regard, our goal is to investigate a number of current risk assessment frameworks, the particular techniques they use, and whether or not they are suitable for assessing IoT threats.

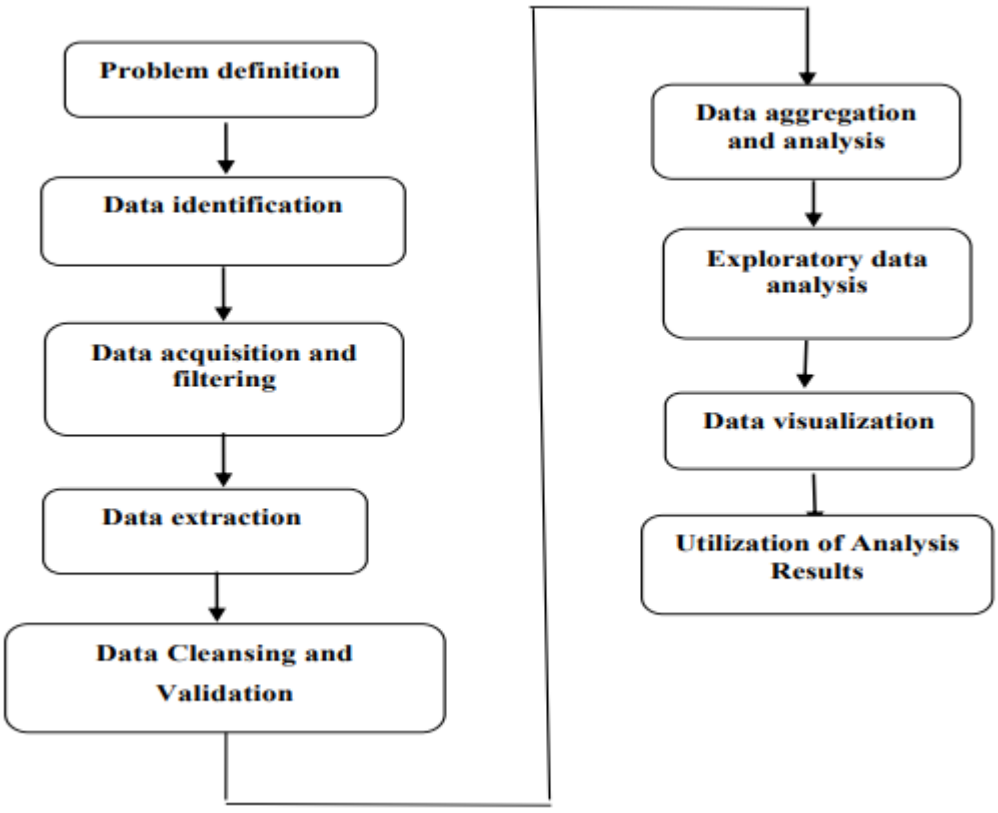

Figure 2: Big Data Analytics Lifecycle

Similar to earlier approaches, OCTAVE Allegro can be conducted in a collaborative workshop environment, supplemented by guidance, worksheets, and questionnaires found in the appendices of this

document. However, OCTAVE Allegro is also a great option for those who want to perform risk assessments on their own without a lot of organizational support, knowledge, or feedback. The collaborative nature of the OCTAVE method offers an interdisciplinary viewpoint on the processes of risk identification, assessment, and mitigation [9]. The workshop-based data collection and subsequent analysis inherent in existing OCTAVE methods unite various groups within the organization towards a shared objective.

RESULT AND DISCUSSION

Besides emphasizing the connection between these levels and an organization's appropriate cybersecurity expenditure, this research illustrates how such analysis can assist companies in selecting the most suitable NIST Implementation Tier level [10]. The report, however, does not delve into the working specifics of spending decisions or the optimal method of distributing funds across various cybersecurity initiatives [11]. The extent to which an organization's cybersecurity management practices are aligned with its stated cybersecurity capabilities is indicated by the implementation levels. Companies can use the framework profile to identify where their cybersecurity posture must be improved by comparing a "Current" and "Target" profile [12].

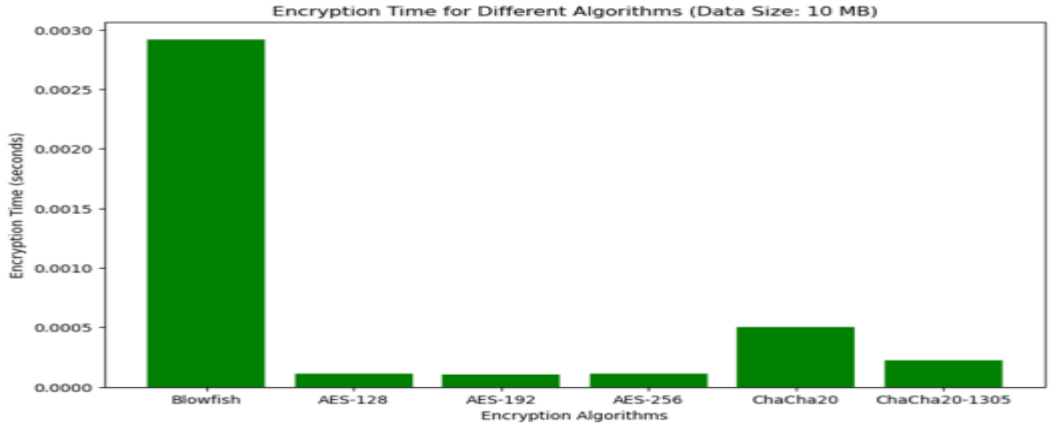

Figure 3: Encryption Time For 10 MB Data

The NIST Cybersecurity Framework only briefly touches on risk management issues, although acknowledging that each organization's cybersecurity risk management practices are distinct. Some examples of cybersecurity risk management procedures are those described by the International Organization for Standardization [13].

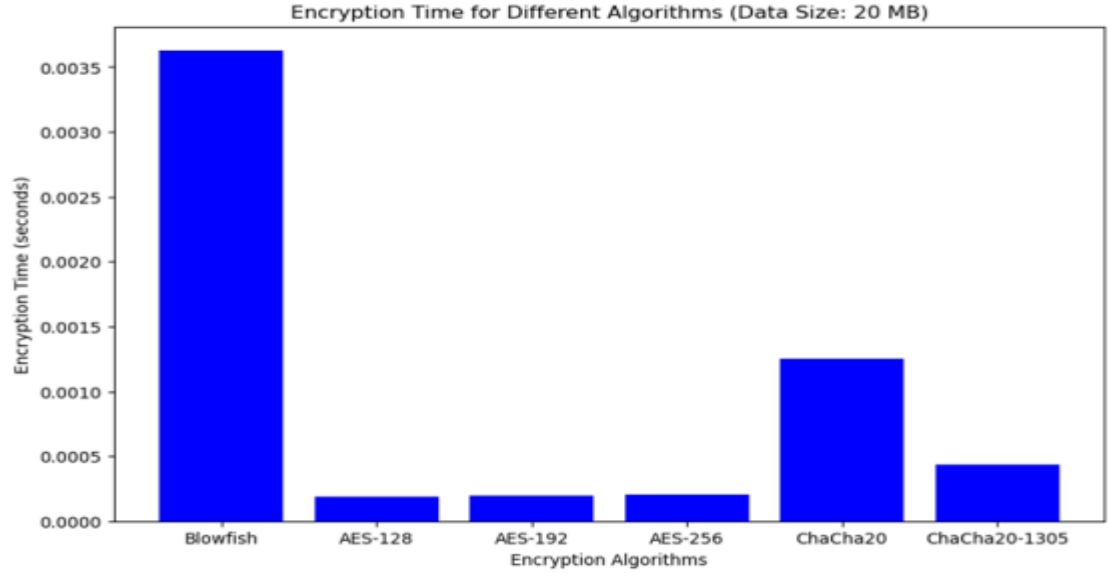

Figure 4: Encryption Time For 20 MB Data

BDN models the necessary information for managing security risks, including data on vulnerabilities, countermeasures for risk reduction, and the impact of their implementation on vulnerabilities [14]. With

the help of new Bayesian inference techniques, a cost-benefit analysis of the risk mitigation alternatives is performed during the risk mitigation process. Their findings indicate that the framework's accurate risk assessment and effective risk mitigation significantly enhance network security [15].

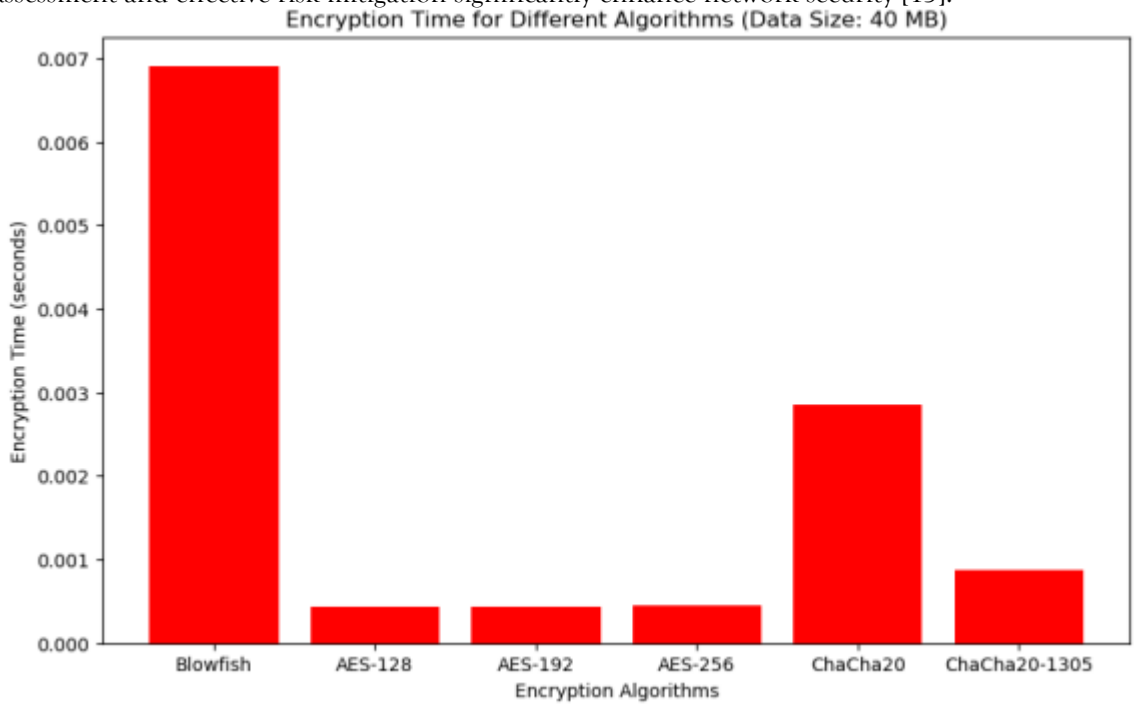

Figure 5: Encryption Time For 40 MB Data

Recognizing that the NIST Cybersecurity Framework does not provide an effective financial methodology for justifying cybersecurity initiatives, a cost-benefit analysis has been incorporated into the framework.

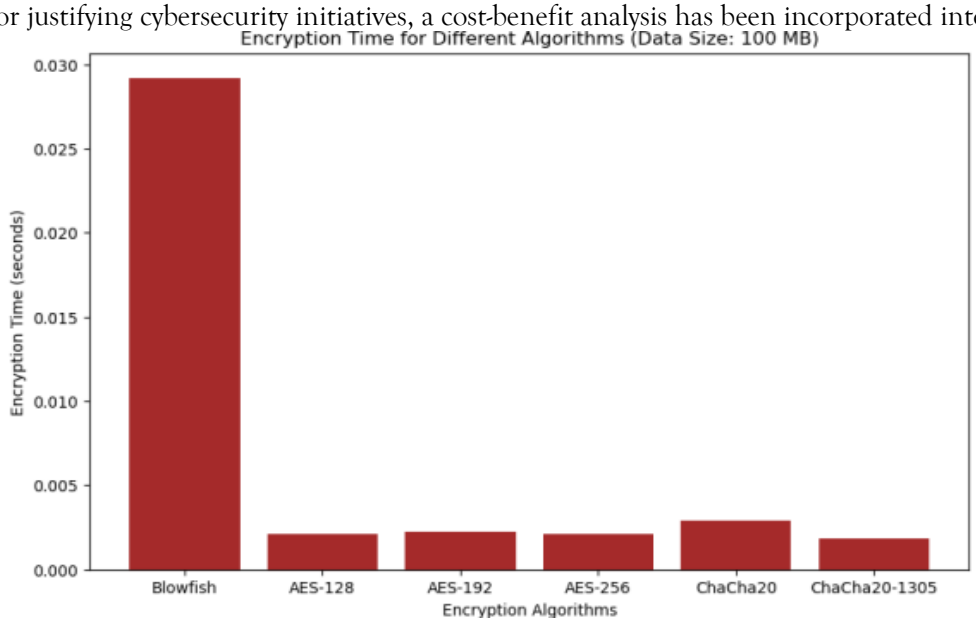

Figure 6: Encryption Time For 100 MB Data

The repercussions of malevolent actors taking advantage of weaknesses in a medical facility can be disastrous. Healthcare services could be disrupted, patient privacy could be jeopardized, and lives could be in danger. Access to patient data from electronic health records by malicious actors can seriously damage a patient's credit and have a negative impact on the financial viability of the participating healthcare organizations. It is not possible to overemphasize the significance of cybersecurity in medicine. In order to avoid cyberattacks, the healthcare industry has to detect and fix vulnerabilities as well as implement preventive measures.

CONCLUSION

This paper provides an exhaustive analysis of the IoT risk ecosystem through a variety of risk models, applicable theories, industries, risk vectors, and a new computational risk scoring model. In order to convince the audience that a unique method for calculating IoT risk is required, the explored. This study could stimulate more investigation into the cybersecurity threats associated with IoT and IoMT. Deep learning, a branch of machine learning, is superior to attaining impressive performance. Deep learning methods surpass conventional machine learning methods in processing large-scale data. Deep learning models also have the capability of learning spontaneously the feature description from raw data and generating results in an end-to-end fashion, making them extremely practical. The deep structure of deep learning, which is described by multiple hidden layers, is one of its significant characteristics.

REFERENCES

1. Ejiofor, Oluomachi, and Ahmed Akinsola. "Securing the future of healthcare: building a resilient defense system for patient data protection." *arXiv preprint arXiv:2407.16170* (2024).
2. Fathima Sapna, P., & Lal Raja Singh, R. (2022). Electrical Load Forecasting Techniques & Methods: An Overview. International Journal of Advances in Engineering and Emerging Technology, 13(2), 254–262.
3. Tariq, Muhammad Usman. "Enhancing cybersecurity protocols in modern healthcare systems: Strategies and best practices." In Transformative approaches to patient literacy and healthcare innovation, pp. 223-241. IGI Global, 2024.
4. Sethi, K., & Kapoor, M. (2024). Data-Driven Marketing in the Age of AI: Reflections from the Periodic Series on Technology and Business Integration. In Digital Marketing Innovations (pp. 7-11). Periodic Series in Multidisciplinary Studies.
5. Prasad, Guru, Praveen Gujjar, HN Naveen Kumar, M. Anand Kumar, and S. Chandrappa. "Advances of cyber security in the healthcare domain for analyzing data." In Cyber Trafficking, Threat Behavior, and Malicious Activity Monitoring for Healthcare Organizations, pp. 1-14. IGI Global, 2023.
6. Pamije, L. K., Havalam, N. K., & Bosco, R. M. (2022). Challenges in wireless charging systems for implantable cardiac pacemakers. National Journal of Antennas and Propagation, 4(1), 14–20.
7. Argaw, Salem T., Juan R. Troncoso-Pastoriza, Darren Lacey, Marie-Valentine Florin, Franck Calcavecchia, Denise Anderson, Wayne Burleson et al. "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks." BMC medical informatics and decision making 20 (2020): 1-10.
8. Madugalla, A. K., & Perera, M. (2024). Innovative uses of medical embedded systems in healthcare. Progress in Electronics and Communication Engineering, 2(1), 48–59. https://doi.org/10.31838/PECE/02.01.05.
9. Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, and Rajiv Suman. "Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends." Cyber Security and Applications 1 (2023): 100016.
10. Marwedel, R., Jacobson, U., & Dobrigkeit, K. (2025). Embedded systems for real-time traffic management: Design, implementation, and challenges. SCCTS Journal of Embedded Systems Design and Applications, 2(1), 43–56.
11. Adeyinka, Kehinde Iyioluwa, and Taye Iyinoluwa Adeyinka. "Cybersecurity Measures for Protecting Data." In Analyzing Privacy and Security Difficulties in Social Media: New Challenges and Solutions, pp. 365-414. IGI Global Scientific Publishing, 2025.
12. Javier, F., José, M., Luis, J., María, A., & Carlos, J. (2025). Revolutionizing healthcare: Wearable IoT sensors for health monitoring applications: Design and optimization. Journal of Wireless Sensor Networks and IoT, 2(1), 31-41.
13. Swede, Marci J., Vincent Scovetta, and Marie Eugene-Colin. "Protecting patient data is the new scope of practice: A recommended cybersecurity curricula for healthcare students to prepare for this challenge." Journal of allied health 48, no. 2 (2019): 148-156.
14. Thomasian, Nicole M., and Eli Y. Adashi. "Cybersecurity in the internet of medical things." Health Policy and Technology 10, no. 3 (2021): 100549.
15. Danh, N. T. (2025). Advanced geotechnical engineering techniques. Innovative Reviews in Engineering and Science, 2(1), 22-33. https://doi.org/10.31838/INES/02.01.03