Incident Response and Threat Intelligence in Healthcare: A Study on Cybersecurity Incident Management

Rajesh Keshavrao Deshmukh[1], Mohit Shrivastav[2]

[1]*Assistant Professor, Department of CS & IT, Kalinga University, Raipur, India*
[2]*Research Scholar, Department of CS & IT, Kalinga University, Raipur, India.*

KEYWORDS

Cyber Security, Health, Security, Privacy

ABSTRACT

India and other Asian nations are seeing an unparalleled pace of advancement in the modernisation of their healthcare systems. In this endeavour, information technology is crucial. Though the healthcare industry has made great progress, information security is still lagging behind the protection requirements attained in technologically developed nations such as the United States and the United Kingdom. This study is an honest attempt to pinpoint vulnerabilities and dangers in the field of cybersecurity and offers a few targeted remedies in three main domains: risks, vulnerabilities, and IoMT. Using a qualitative research methodology, this research culminates in the creation of a security maturity model for Indian healthcare. Furthermore, in light of these attacks, the well-known National Institute of Standards and Technology (NIST) risk assessment system and its guiding principles are examined. Evaluating the risks intrinsic to these hacks analytically becomes crucial given the comparatively low information risk management maturity levels in Asian healthcare organisations. While several nations in Asia and throughout the world are battling the COVID-19 outbreak, cybercriminals have been attempting to spread misinformation about vaccines. Additionally, some people and organisations are attempting to undermine specific vaccines in order to promote their COVID-19 treatments. Hacking research data, virus testing, and clinical studies that reveal side effects or possible issues are of particular interest to profit-seeking businesses. The secure methodology for identifying network attacks is suggested by this study.

1. Introduction

Cyber risk, also known as information technology (IT) risk, is the sum of the probability and impact of an unfavourable event. The US National Institute of Standards and Technology, or NIST, defines risk as a function of the likelihood that a specific threat source would exploit any conceivable vulnerability and the subsequent effect of that unfavourable occurrence on the organisation. Cybersecurity risks are defined as any threats that compromise the cybersecurity posture. IT risk is defined as the possibility that an attacker could take advantage of weaknesses in an organization's assets and cause harm to it by the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC) [1]. It is assessed in terms of an event's impact and probability of happening. Information security risk consists of three main elements: an asset, a threat, and a vulnerability. Risk is calculated using the formula in the Open-Web Application Security Project (OWASP) testing guide: likelihood multiplied by impact, where likelihood and impact have numerical values specified [2]. Risk is defined differently depending on the risks and vulnerabilities that are taken into account. The Common Vulnerability Scoring System (CVSS) developed by NIST provides a vulnerability-centric definition of cyber risk. Risk severity is calculated using a 10-point rating system. Researchers look into how two professional groups—cybersecurity specialists and ontology creatorsconceptualize cyber hazards and express them [11]. Both parties emphasise the idea of vulnerability and how an attacker can take advantage of it.

2. Literature Review

There have been several high-profile reports of healthcare data breaches recently. Out of the 2216 data breaches that occurred in 65 countries overall in 2018, 536 of them involved healthcare data, with the healthcare sector suffering the most harm [4]. There were 505 global healthcare data breaches in 2019 that resulted in the exposure of 41.2 million medical records [5]. Furthermore, 157.40 million people were impacted by healthcare data breaches during the course of the previous five years [12]. The desire for healthcare data has made it a target for hackers [6]. There are various kinds of healthcare data, including clinical, administrative, and electronic health record data [3]. On the illicit market, medical data is worth more than credit card information [7]. A comprehensive evaluation of the literature on cyber risk in the healthcare industry, as reported in [8], finds that there are little research contributions in the literature to address the issues of cyber risk management in the healthcare industry. It also emphasises the lack of attention paid by the scientific community to this issue. Medical data breaches are most commonly caused by cyberattacks [13]. Patient data is gathered and stored by healthcare systems using databases, order communication systems (OCS), electronic medical record (EMR) systems, and picture archiving and communication systems (PACS). Since data security is a fundamental component of cybersecurity, patient data is seriously at risk from these cybersecurity threats, which could result in patient mistreatment, incorrect diagnoses, and data leakage [10]. Nearly 60% of hospital officials and healthcare IT experts in the US stated that email was the most frequent point of information compromise, according to the Healthcare Information and Management Systems Society's (HIMSS) Cybersecurity Survey [9]. Hackers frequently use email fraud, including phishing scams. The number of people affected by healthcare attacks increased from 34 million in 2023 to 45 million in 2024. Based on breach data that healthcare organisations reported to the U.S. Department of Health and Human Services (HHS), the figure has tripled in only three years, From 14 Million In 2018.

3. Methodology

Designing trust-based internal attack (DoS, DDoS) detection systems is the main goal of the proposed research project. This would enable large-scale networks to transmit data quickly and securely. Large-scale networks that serve a variety of applications are typically the most susceptible to various security threats. As a result, maintaining secure communication in expansive networks is seen as a very difficult undertaking. For the most part, cryptography-based solutions were used to ensure secure data transmission. However, this is not very effective against insider threats, and in large-scale delay-sensitive networks, it necessitates an extra delay for data sharing among reliable neighbours. The only way to overcome and be free from these limitations is to build a trust-based routing protocol that enables nodes to respond as fast as possible to attacks from both the inside and the outside. In this context, the MAP-DRP, TLTGWI, and T-DARF ideas are embodied by robust designs that target insider attackers, who are capable of launching a wide range of attacks, mostly related to service availability. Three methodologies are used in the proposed research project, as shown in Figure 1:

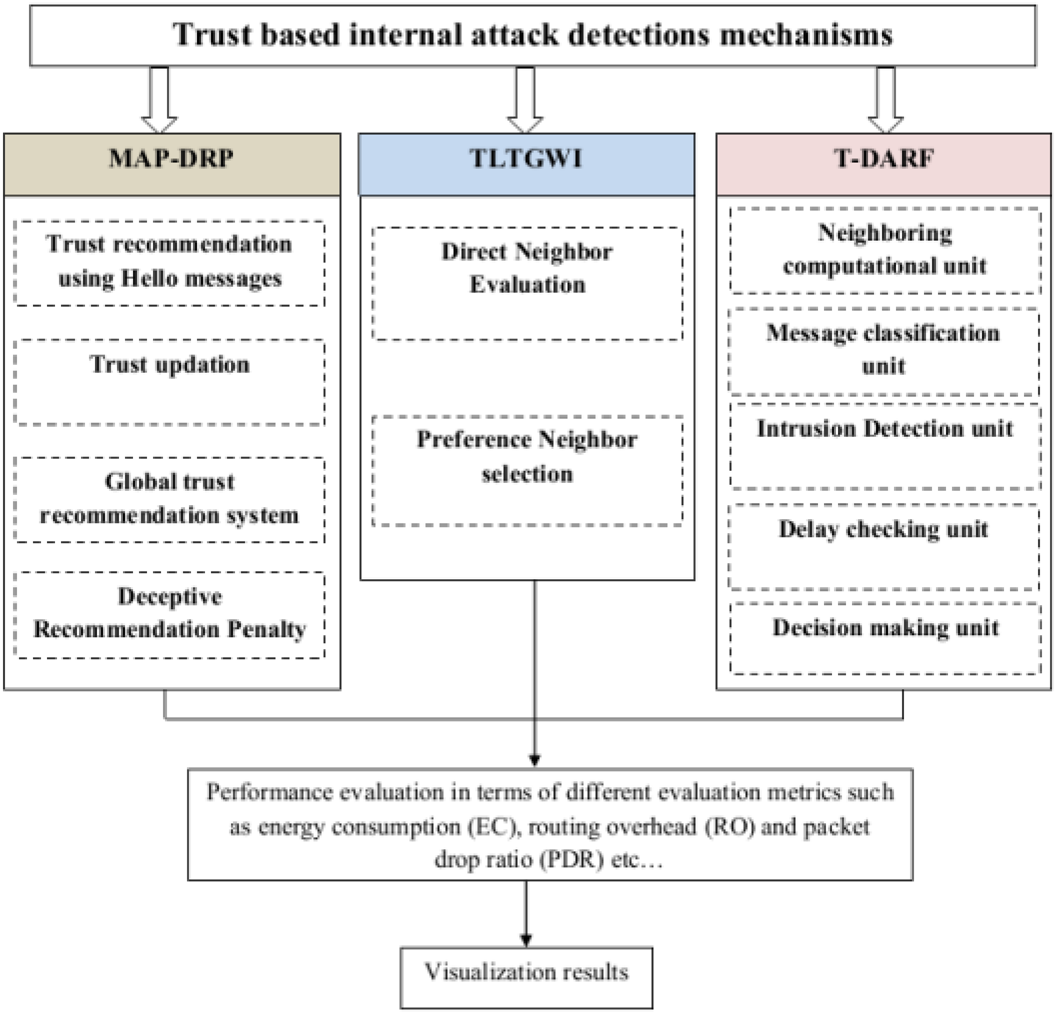
Trust based internal attack detections mechanisms
MAP-DRP
TLTGWI
T-DARF
Trust recommendation using Hello messages
Trust updation
Global trust recommendation system
Deceptive Recommendation Penalty
Direct Neighbor Evaluation
Preference Neighbor selection
Neighboring computational unit
Message classification unit
Intrusion Detection unit
Delay checking unit
Decision making unit
Performance evaluation in terms of different evaluation metrics such as energy consumption (EC), routing overhead (RO) and packet drop ratio (PDR) etc…
Visualization results

Figure 1. overall proposed framework

A new Multi-Level Authentic Propagation Model with a Deceptive Recommendation Penalty (MAP-DRP) strategy is developed by combining QoS and social trust. This scheme's primary objective is to prevent packet forwarding misbehaviour nodes while also utilising the trust mechanism to guarantee dependable and strong communication during path discovery. This technique determines the best forwarding node based on packet forwarding behaviour and QoS measures (link quality, quality of the channel, and residual energy).

4. Results And Discussion

Experiments were carried out for the suggested mechanism by changing the node density in the network from 10 to 40. The NS2 platform is used for the experimental analysis of MAP-DRP mechanisms to analyse the performance. The Random Waypoint mobility model is the one used to detect node movement inside the network. The nodes are arranged in a field measuring 1000 by 1000 meters at random. By changing the number of nodes with a packet delivery ratio, malicious node, the effectiveness of the MAP-DRP technique is examined. Three protocols, including Ad Hoc On-Demand Distance Vector (AODV), Enhanced Trusted Routing system with Pattern Discovery (ETRSPD), and Trust-based secure QoS routing system (TSQRS), were tested in order to demonstrate the effectiveness of the suggested technique (MAPDRP). The PDR for the MAP-DRP, AODV, ETRS-PD, and TSQRS protocols is shown in Figure 2. Compared to the suggested MAP-DRP method, the current protocols have demonstrated poor packet transmission to the intended destination when the mobility rate is increased from 4 to 20 m/s. The process of evaluating the interaction among the nodes collectively in a group with increased node speeds is the reason behind this cause, which is that there is a greater link drop with these current protocols. However, compared to the other current methods, the suggested MAP-DRP methodology has demonstrated superior PDR. Due to the fact that the suggested MAP-DRP system has taken into account both the secured route from source to destination and the link quality before choosing the next forwarding nodes.

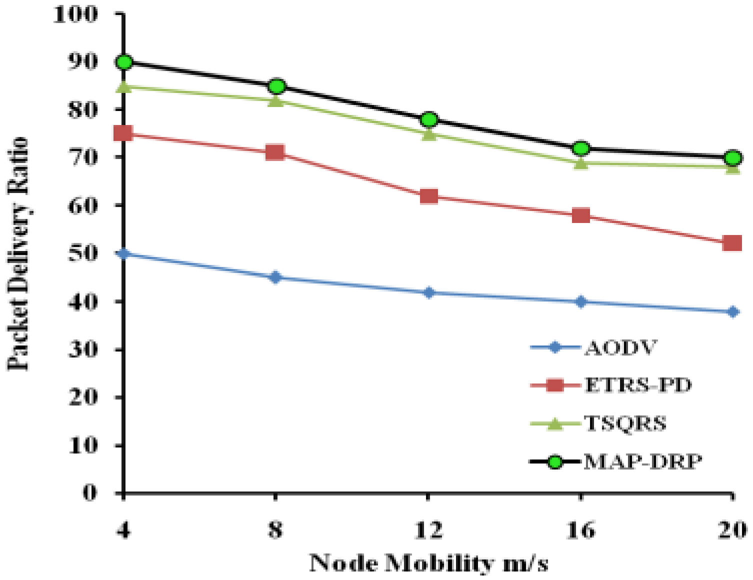

Figure 2. Node mobility Vs. packet delivery ratio (PDR)

The MAPDRP scheme's performance against routing overhead is shown in Figure 3, along with comparisons to other protocols currently in use. The reduced connection failure during the routing route discovery process has resulted in fewer RO for the proposed MAP-DRP method. In the MAP-DRP method, the intermediate nodes are also chosen according to the QoS parameters. However, every other current technique has demonstrated a higher RO in conjunction with a faster node.

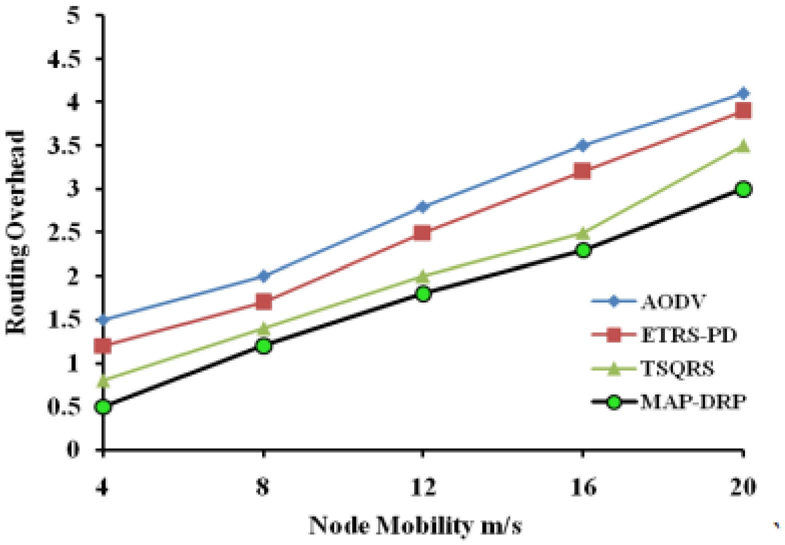

Figure 3. Node mobility Vs. Routing overhead (RO)

The performance of the suggested MAP-DRP strategy against energy usage is shown in Figure 4 in comparison to other protocols that are currently in use. Typically, nodes' energy consumption is calculated based on the total number of packets delivered and received to the targeted destination nodes. Because the suggested MAP-DRP technique takes into account the nodes' residual energy and link quality prior to initialising procedure, it has therefore consumed less energy throughout data transmission. However, the current protocols, TSQRS, ETRSPD, and AODV, require more energy to transmit data and have a higher connection failure rate.

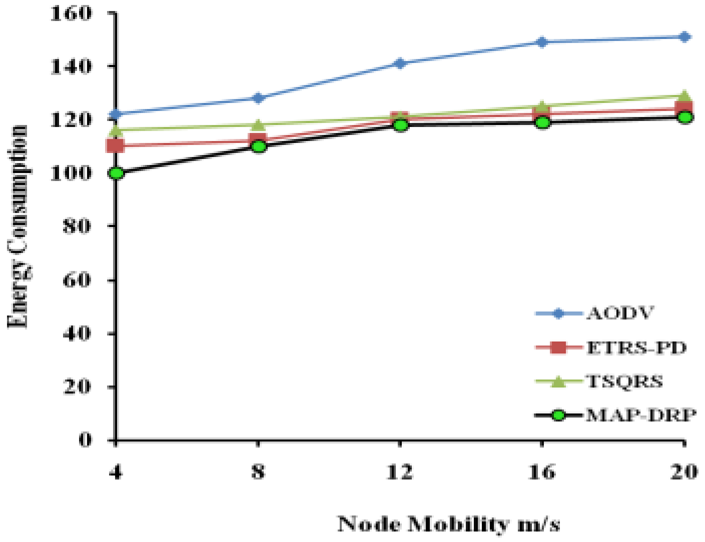

Figure 4. Node mobility Vs. Energy consumption

The network overhead of the suggested MAP-DRP strategy is shown in Figure 5 for different numbers of malicious nodes. The figure shows that, in comparison to other current protocols, the suggested MAP-DRP approach has only used a smaller amount of network overhead when the number of malicious nodes is adjusted. The suggested MAP-DRP system exhibits this goodness because there are fewer control packet retransmissions and fewer link failures during the route establishment phase.

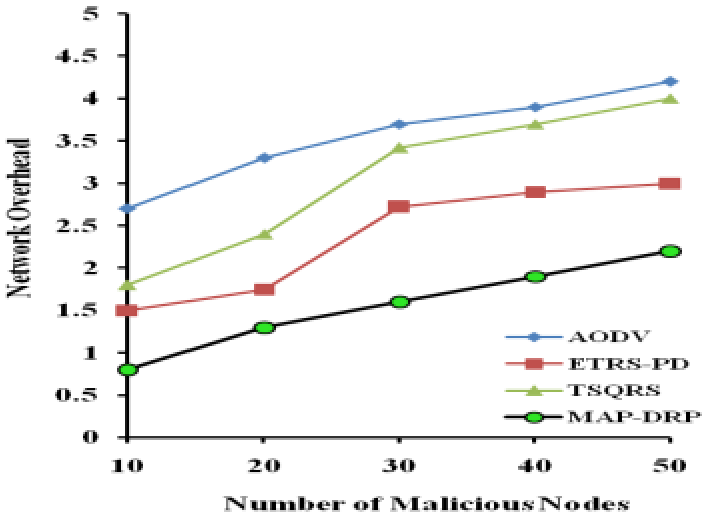

Figure 5. Number of Malicious Nodes Vs Network Overhead

Creating a Multi-Level Authentic Propagation Model with Deceptive Recommendation Penalty (MAP-DRP) strategy for DDoS attack mitigation and prevention is the primary goal of this module. Here, a trust-based mechanism was developed by combining social trust and quality of service. The three most important factors in a wireless environment remaining energy, link quality, and channel quality are taken into account throughout the route discovery phase to ensure dependable communication. Also, using intimacy level, DFR, and CFR values, the hostile nodes (i.e., DDOS attacked nodes) were eliminated during the trust update procedure.

5. Conclusion

Through the prism of risk frameworks, relevant theories, sectors, risk vectors, and a unique risk score computational model, this book offers thorough coverage of the IoT risk area. The cyber-security risk assessment frameworks appropriate for Internet of Things systems are critically examined and provided. To illustrate the maturity of the IoT risk area, applications of IoT risk assessment frameworks in the banking and healthcare sectors are presented. These frameworks' IoT risk considerations are described, along with their advantages, disadvantages, and areas of emphasis. In order to raise important risk issues related to the IoMT domain, a thorough treatment of the IoMT risk domain is given. Additional parameters pertaining to the clinical observations can be used into the assessment of IoMT risk. It is possible to create an IoMT risk computation model that, given the necessary parameters, would calculate the risk level automatically. The cyber risk framework that is most suited for the healthcare systems in India should be modified in light of the various characteristics of current cyberattacks and data breaches in the Indian healthcare environment.

Reference

[1] Agarwal, Reshu, and Mukul Kumar. "Cyber Security for Handling Threats in Healthcare Devices." In *Healthcare Systems and Health Informatics*, pp. 217-233. CRC Press, 2022.

[2] Sharma, Durgansh, Tarun Kumar Singhal, and Deepak Singh. "Threat Intelligence Model to Secure IoT Based Body Area Network and Prosthetic Sensors." ECS Transactions 107, no. 1 (2022): 15417.

[3] S. Neelima, Manoj Govindaraj, Dr.K. Subramani, Ahmed ALkhayyat, & Dr. Chippy Mohan. (2024). Factors Influencing Data Utilization and Performance of Health Management Information Systems: A Case Study. Indian Journal of Information Sources and Services, 14(2), 146–152. https://doi.org/10.51983/ijiss-2024.14.2.21

[4] Chaudhary, Sachi, Riya Kakkar, Nilesh Kumar Jadav, Anuja Nair, Rajesh Gupta, Sudeep Tanwar, Smita Agrawal et al. "A taxonomy on smart healthcare technologies: Security framework, case study, and future directions." Journal of Sensors 2022, no. 1 (2022): 1863838.

[5] Purohit, Soumya, Roshan Neupane, Naga Ramya Bhamidipati, Varsha Vakkavanthula, Songjie Wang, Matthew Rockey, and Prasad Calyam. "Cyber threat intelligence sharing for co-operative defense in multi-domain entities." IEEE Transactions on Dependable and Secure Computing 20, no. 5 (2022): 4273-4290.

[6] Choudhary, A., Choudhary, G., Pareek, K., Kunndra, C., Luthra, J., & Dragoni, N. (2022). Emerging Cyber Security Challenges after COVID Pandemic: A Survey. Journal of Internet Services and Information Security, 12(2), 21-50.

[7] Rajamäki, Jyri, Dominik Jarzemski, Jiri Kucera, Ville Nyman, Ilmari Pura, Jarno Virtanen, Minna Herlevi, and Laura Karlsson. "Implications of GDPR and NIS2 for Cyber Threat Intelligence Exchange in Hospitals." (2024).

[8] Mojail, N. Disages K., et al. "Understanding Capacitance and Inductance in Antennas." *National Journal of Antennas and Propagation* 4.2 (2022): 41-48.

[9] Bou-Harb, Elias, and Nataliia Neshenko. Cyber threat intelligence for the internet of things. New York: Springer, 2020.

[10] Kotenko, I.V., Saenko, I., & Kushnerevich, A. (2017). Parallel big data processing system for security monitoring in Internet of Things networks. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 8(4), 60-74.

[11] Al-Hawawreh, Muna, Nour Moustafa, and Jill Slay. "A threat intelligence framework for protecting smart satellite-based healthcare networks." Neural Computing and Applications 36, no. 1 (2024): 15-35.

[12] Shamshad, Salman, Khalid Mahmood, Shafiq Hussain, Sahil Garg, Ashok Kumar Das, Neeraj Kumar, and Joel JPC Rodrigues. "An efficient privacy-preserving authenticated key establishment protocol for health monitoring in industrial cyber–physical systems." IEEE Internet of Things Journal 9, no. 7 (2021): 5142-5149.

[13] Soldatos, John, James Philpot, and Gabriele Giunta. Cyber-physical threat intelligence for critical infrastructures security: a guide to integrated cyber-physical protection of modern critical infrastructures. Now Publishers, 2020.

[14] Ghazal, Taher M. "Internet of things with artificial intelligence for health care security." Arabian Journal for Science and Engineering (2021).