Journal of Cognitive Computing and Cybernetic Innovations(JCCCI)
Research Article
Received: 2025-04-28 **Reviewing:** 2025-05-21 **Accepted:** 2025-06-29 **Online:** 2025-07-26 **Issue Date:** 2025-07-27
Year: 2025, **Volume:** 01, **Issue:** 02, **Pages:** 27-33, **Doi:** https://doi.org/10.21276/jccci.2025.v1.i2.5

Ransomware in Healthcare: Reducing Threats to Patient Care *

Nasar Mohammed
Valparaiso University, IN, USA

Abdul Faisal Mohammed
Trine University, MI, USA

Sruthi Balammagary
University of the Cumberlands, KY, USA

***Abstract*—Healthcare has become a prime target for ransomware attacks, a type of malicious program that encrypts sensitive information and requires ransom in exchange for its release. Beyond disrupting hospital operations, these cyberattacks become serious threats to patient care, undermining safety and confidentiality. The distinctive character of health care—where unbridled access to electronic health records (EHRs), image machines, and clinical equipment is essential—contributes to the severity of ransomware's effect. A succession of high-profile attacks, including the WannaCry attack on the United Kingdom's National Health Service and the Ryuk attack on Universal Health Services in the United States, illustrate the very real effects of such attacks, including delayed treatment, data breaches, and even death. This article discusses the root explanations for the vulnerability of the health care industry to ransomware attacks, including legacy IT systems, inadequate cybersecurity education, and negligible financial investments in cyber protections. It further delves into the wider implications regarding data protection, business resilience, and adherence to regimes such as HIPAA and GDPR. As a reaction, the article presents a multi-faced mitigation strategy of technical, organizational, and human factor solutions. Technological controls like network segmentation, endpoint detection and response (EDR), and multi-factor authentication (MFA) are advised in addition to proper data backup and incident response planning. Additionally, cybersecurity education and awareness need to become healthcare culture so that frontline workers can identify and report suspicious behaviour. Cooperation with national cybersecurity organizations and industry-specific organizations like Health-ISAC is also critical for real-time sharing of threat intelligence and coordinated response. By meeting the looming threat of ransomware with a robust defence strategy, medical facilities can not only protect their IT systems but also the quality and integrity of patient care. This paper reasserts the timely need for health providers to invest in cybersecurity as an integral aspect of contemporary clinical practice.**

Keywords*—*ransomware, healthcare cybersecurity, patient safety, data breaches, electronic health records (EHRs), legacy systems, HIPAA, GDPR, endpoint detection, network security, incident response, Health-ISAC, WannaCry, Ryuk, medical infrastructure, cyber resilience

I. Introduction

With the advent of the digital age, health care organizations have embraced technology on a big scale to improve patient care, automate administrative work, and optimize overall efficiency. From Electronic Health Records (EHRs) and telemedicine to networked devices, health care delivery is becoming more dependent on digital systems [1]. But this technology revolution has also let loose the health care sector to an ever-increasing list of cyber security threats, the largest one being ransomware.

Ransomware is a criminal software that encrypts the files or computer systems of a victim so they cannot be used except for the payment of a ransom, most often in the form of cryptocurrency [2]. What differentiates ransomware in the health care context is that it has an immediate and direct effect on human life. While in most other sectors, cyberattacks would only lead to financial loss or business disruption, ransomware attacks on healthcare institutions can lead to a delay in receiving essential treatment, disrupt life-supporting equipment, and even endanger patients' lives.

The frequency and level of sophistication of ran-

*Cite (APA): Nasar Mohammed1, Abdul Faisal Mohammed, Sruthi Balammagary (2025). Ransomware in Healthcare: Reducing Threats to Patient Care *Journal of Cognitive Computing and Cybernetic Innovations, Volume 01* (IssueNo 02), 27-33. https://doi.org/10.21276/jccci.2025.v1.i2.5

somware attacks on healthcare have grown over the past few years. Cybercriminals are now more and more targeting vulnerabilities in the industry [3]. legacy IT systems, old software, weak security processes, and tight cybersecurity budgets. In addition, healthcare providers tend to possess a huge repository of sensitive personal data, rendering them a target-rich environment for cyber extortion. All of these coupled with the urgency nature of medical services tend the healthcare staff to pay ransoms promptly to get back to work—thus instigating further attacks.

History has borne out the destruction of ransomware in healthcare in the real world. The WannaCry incident in 2017, for example, created wholesale disruption to the UK National Health Service (NHS) by rescheduling surgery and refusing access to patients [4]. In 2020, the ransomware attack on the Universal Health Services resulted in system downtime at more than 400 of this large US healthcare provider's facilities, impacting care and increasing risk to patient safety. This report aims to analyse the range and impact of ransomware attacks in the health sector, establish the root vulnerabilities that enable the attacks, and propose a range of mitigation actions that are viable and effective. Through case study, technical analysis, and policy recommendations, this research aims to provide further knowledge on how the health sector can better defend itself against one of the most critical cybersecurity threats to our time [5].

II. The Scope of the Problem

The health care industry has been among the major victims of ransomware attacks, with increasing signs that such attacks are increasingly occurring on a regular basis, in greater sophistication, and with increased severity [6]. The next subsection defines the main facts of the problem: the increase in the frequency of attacks, the effect on patient care, and the far-reaching financial impact on health care organizations.

A. Ransomware Attack Growth

The frequency of ransomware attacks on healthcare has grown exponentially in the past decade [7]. Cyber attackers have evolved from targeting single systems to launching complex, multi-stage attacks that compromise entire hospital networks. In a 2023 Sophos report, 66 percentage of healthcare organizations globally indicated that they had been affected by a ransomware attack in the past year, a sharp increase from 34 percentage just three years prior. In addition, the healthcare industry ranks highest among all industries in terms of the percentage of ransomware-related data breaches. This is due to several contributing factors, such as the industry's behind-the-times cybersecurity position, the cost of healthcare services, and the value of medical records on the black market.

B. Impact on Patient Care

Unlike ransomware attacks on other industries, medical facility attacks have tangible impacts on human lives [8]. When systems are encrypted and rendered useless, hospitals can lose patient files, diagnostic software, imaging devices, and scheduling software. Such disruption can result in: a. Delayed or cancelled surgeries and treatments b. Redirection of emergency patients to a different hospital c. Loss of access to medication histories or writing prescriptions d. Higher likelihood of medical errors A 2021 JAMA Network Open study discovered that the hospitals that were victims of ransomware had increased wait times for patients and more deaths during and shortly following the period of the attack [9].

C. Financial Costs

The financial burden of ransomware to healthcare is double: immediate costs like ransom payment and back-end costs like recovery efforts, legal fees, reputation loss, and regulatory penalties [10]. In 2022, the Ponemon Institute approximated the cost of a healthcare data breach at an average of USD 10.1 million, and ransomware attacks covered a major portion of that. Organizations are often left with the difficult question of whether or not to pay the ransom, which does not guarantee data restoration and may be contrary to national legislation or statutory obligations. Recovery time, even when paid for, can extend to weeks or months, meaning weeks or months of business downtime.

D. Comparative Data Table

To place in context the extent of the ransomware threat in healthcare, the following table compares incident rates and costs across various relevant sectors: Table I: Ransomware Impact by Industry Sector (2023)

Industry Sector	Ransomware Incidents (2023)	Average Cost per Breach	Average Downtime
Healthcare	66%	$10.1 million	21 days
Financial Services	45%	$5.9 million	14 days
Education	56%	$3.2 million	30 days
Government	38%	$2.5 million	15 days
Retail	42%	$3.8 million	12 days

The statistics unequivocally indicate that healthcare organizations not only have the highest incidence rate of ransomware attacks but also carry the greatest financial and operational cost [11]. This highlights the critical necessity for healthcare systems to improve their cybersecurity resilience.

III. Case Studies

Real-life instances of ransomware attacks on healthcare organizations provide insight into the ruinous impact of such attacks on patient safety, data security, and business continuity [12]. The following case studies provide an insight into how ransomware has been used, against which vulnerabilities, and the extent of the damage caused.

A. WannaCry Attack on the NHS (2017)

The WannaCry ransomware attack in May 2017 was one of the most publicized cyber-attacks to affect the healthcare industry [13]. The malware used a previously known Windows vulnerability (EternalBlue) to rapidly spread between networks. The UK's National Health Service (NHS) was hit hardest, with more than 80 hospitals and 595 general practices being affected. Those critical systems such as radiology and pathology labs, scheduling software, and EHRs went down [14]. A total of approximately 19,000 surgeries and appointments were cancelled. No ransom was paid, but the attack cost the NHS £92 million to recover and lost productivity. The attack emphasized the risks of unpatched systems and the need to patch outdated infrastructure.

B. Ryuk Ransomware Attack on UHS (2020)

In September 2020, Universal Health Services (UHS) with more than 400 sites became a victim of the Ryuk ransomware [15]. The incident took down EHR access, phone networks, and internal messaging for weeks. UHS workers were forced to use manual documentation, which bogged down patient treatment and helped create the risk of clinical errors. Though the ransom payment isn't quantified, recoupment had been costing the company USD 67 million. It evidenced the kind of interruption, by scale, that may be done to a distributed health network if the central infrastructure is breached.

C. Conti Attack on Ireland's Health Service Executive (2021)

Ireland's Health Service Executive (HSE) in May 2021 was also affected by a huge ransomware attack perpetrated by the Conti group [16]. The attack put the national healthcare IT system of the country in a frozen state, comprising appointment booking, diagnostics, lab systems, and payroll processing. The attackers also requested a ransom of USD 20 million, which was not met by the Irish government. The systems were months in recovery, with recovery and cybersecurity expenses over the long term estimated to be USD 600 million [17]. The HSE attack highlighted the difficulty of defence against nation-state-level attackers and the cost of delay in system upgrade.

D. Pie Chart: Breakdown of Major Healthcare Ransomware Incidents' Impact

Below is a pie chart illustrating the dissemination of primary effects suffered in the highlighted major ransomware attacks mentioned above:

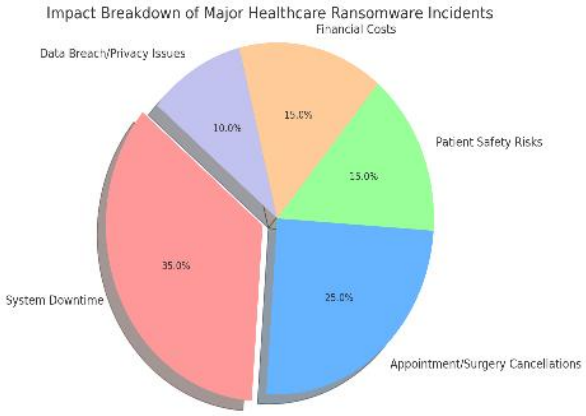

Figure I: Impact Breakdown of Major Healthcare Ransomware Incidents

Table II: Impact Breakdown of Major Healthcare Ransomware Incidents

Impact Type	Percentage
System Downtime	35%
Appointment/Surgery Cancellations	25%
Patient Safety Risks	15%
Financial Costs	15%
Data Breach/Privacy Issues	10%

Percentages are based on cumulative analysis of reported consequences from the case studies. Case examples above not only reflect the prevalence of the impact of ransomware in healthcare but also to typical vulnerabilities on which attackers have succumbed—namely, old systems, poor network segmentation, and untrained staff. Awareness of such attacks guides future resilience planning and guides prioritized security spend.

IV. Why Healthcare is Vulnerable

Healthcare organizations became one of the most frequently attacked industries by ransomware. In comparison to other sectors, combined life-dependent services, legacy gear, regulatory haste, and lucrative data render healthcare uniquely susceptible to ransomware attacks. The ensuing section addresses hidden vulnerabilities that leave healthcare systems exposed to ransomware [18].

A. Legacy Systems and Legacy Technology

A vast majority of medical staff continue to operate legacy systems with no contemporary security features or vendor support. These also include older versions of Windows, older medical imaging equipment, and legacy hospital information systems [19]. These systems are un-patchable or un-updatable since they present backward compatibility problems with proprietary software or hardware. Legacy systems present a large attack surface and are regularly targeted by cybercriminals employing standard exploits [20]. The WannaCry attack of

2017 took advantage of a vulnerability that had already been patched but not yet installed in most hospitals.

B. Limited Cybersecurity Budgets

Compared to defence or finance units, healthcare organizations allocate relatively lower percentages of their budgets to cybersecurity [21]. This budget constraint at times manifests as under-resourced IT staffs, inadequate security tools, and delayed infrastructure updates. Clinical operations are given priority in hospitals, with cybersecurity relegated to a secondary priority. In small or rural healthcare organizations, cybersecurity positions are combined with other IT tasks, often leading to monitoring and late response to threats [22].

C. Healthcare Data to Criminals

Healthcare data is very high-value on the dark web—10–20 times higher in value than credit card data. It has personally identifiable information (PII), insurance information, and even financial information, so they are perfect for identity theft and fraud [23]. Therefore, they are of interest to attackers to hit healthcare providers since the stolen data can be sold in many various ways. Also, hospitals are high-risk organizations where information access literally can be a question of life and death. Such urgency predisposes them more towards the payment of a ransom under urgency to resume operations.

D. Lack of Cybersecurity Training

Frontline healthcare workers are rarely provided any or a lot of cybersecurity education, therefore they are exposed to phishing attacks and social engineering [24]. Overemphasizing patient care does not enable many healthcare workers to even think about digital hygiene, thereby sabotaging systems unknowingly. Phishing is the most prevalent ransomware attack mechanism in healthcare. One careless mistake, for instance, clicking on a suspicious link or downloading a contaminated attachment, can taint an entire network.

E. Networked Devices and Systems

Higher numbers of IoMT devices, including networked infusion pumps, monitoring devices, and intelligent diagnostic devices, offer additional entry points for attackers [25]. Most of these devices were not designed with security and do not have simple protection like encryption or authentication controls. They run on closed or proprietary platforms and are not easily patchable or monitorable. Line Chart: Healthcare Cybersecurity Spending vs. Ransomware Attack Rate (2018–2023) Below is a line chart showing the inverse correlation between healthcare cybersecurity spending and ransomware attack rate over the last six years:

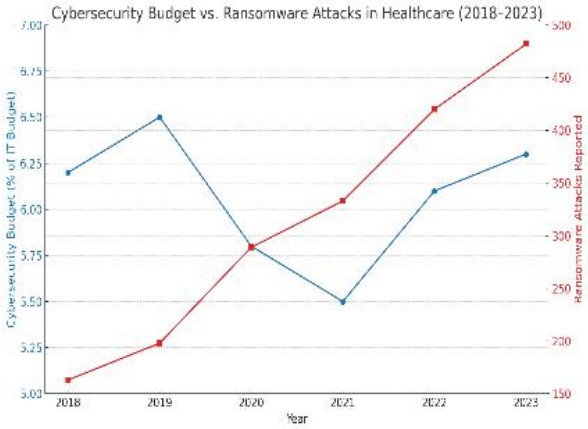

Figure II: Cybersecurity Budget vs Ransomware Attack in Healthcare (2018-2013)

Table III: Cybersecurity Budget vs Ransomware Attacks in Healthcare (2018–2023)

Year	Budget (% of IT Budget)	Ransomware Attacks Reported
2018	6.2%	163
2019	6.5%	198
2020	5.8%	289
2021	5.5%	333
2022	6.1%	420
2023	6.3%	482

Source: HIMSS Cybersecurity Survey, Sophos Reports (2018–2023) This point emphasizes that the vulnerability of the healthcare industry is not only technological—it is cultural, economic, and structural too. Mitigation involves a change of heart where cybersecurity is considered an integral part of patient safety [26].

V. Mitigation Strategies

Successful mitigation of ransomware threat in healthcare needs a multi-dimensional approach that integrates technology, policy, education, and partnership. In contrast to purely reactive models, proactive and participatory security models are needed for safeguarding critical health infrastructure. The chapter describes essential mitigation controls in five core areas [27].

A. Technical Defences

The cornerstone of any ransomware defence is a solid technical foundation [28]. Healthcare organizations need to adopt a defence-in-depth approach that entails: a. Endpoint Detection and Response (EDR) software to detect and isolate suspicious activity in real time. b. Multi-Factor Authentication (MFA) for all logins, particularly administrative and remote access accounts. c. Regular patch management to remedy known vulnerabilities for operating systems, applications, and medical devices. d. Network segmentation to contain infections and prevent lateral movement within hospital networks. Also, using zero-trust architecture means no device or user should be trusted by default, thereby lowering the internal compromise risk.

B. Planning for Data Backup and Recovery

It is required to have a robust and detailed backup plan in order to be resistant to ransomware [29]. Backups must be: a. Regular (hourly or daily, based on importance). b. Offline or in immutable cloud storage so ransomware can't encrypt the backups. c. Trained with regular restoration exercises to guarantee timely and efficient recovery in case of an actual emergency. Incident response plans should define roles, escalation steps, and communications clearly. Speed counts during a ransomware attack—preparation can drastically minimize recovery times and impact.

C. Cybersecurity Awareness and Training

Healthcare personnel—receptionists to surgeons—can be the first line of defence against ransomware. Repeated cybersecurity training ensures the establishment of a security-aware culture [30]. Training on the following is focused: a. Phishing email and suspicious link identification b. Authentication of unusual requests or file attachments c. Reporting suspect activity in timely manner Simulated phishing test can also be used to determine staff preparedness and vulnerabilities.

D. Policy, Compliance, and Governance

Cybersecurity policy must be informed by regulatory frameworks like: a. HIPAA (Health Insurance Portability and Accountability Act) b. GDPR (General Data Protection Regulation) c. NIST Cybersecurity Framework Policies can establish data access controls, passwords, device management, and cybersecurity requirements minimum across the departments [31]. Accountability and continuous evaluation of risks are the benefits of having a cybersecurity governance committee.

E. Industry Collaboration and Threat Intelligence Sharing

Healthcare ecosystem cooperation boosts mutual resilience. Information sharing with entities such as Health-ISAC (Health Information Sharing and Analysis Center) gives real-time threat information, early warning on developing threats, and playbooks for response in collaboration [32]. Partnerships with national cyber agencies enhance access to sophisticated tools, training materials, and collective responses against mass attacks. Ransomware prevention in healthcare is not an event, but an ongoing evaluation, improvement, and alignment [33]. With the convergence of technical defences, staff preparedness, sound governance, and inter-organization cooperation, healthcare organizations are capable of establishing a secure cyber environment that not only safeguards their systems but also patients' lives.

VI. Future Direction

As ransomware becomes more sophisticated and widespread, healthcare organizations will need to develop forward-looking strategies to remain competitive against future threats. The healthcare cybersecurity future will rely on proactively innovating, collaborating across industries, and ongoing investment in digital resilience [34]. This section highlights the most impactful future trends affecting anti-ransomware efforts in healthcare.

A. Artificial Intelligence and Machine Learning in Threat Detection

Using Artificial Intelligence (AI) and Machine Learning (ML) capabilities in cybersecurity products has the potential to change the game in detecting and responding to threats [35]. These capabilities can: Scan enormous volumes of network traffic in real time Identify anomaly behaviour patterns resulting in ransomware Isolate affected devices automatically and initiate containment processes Predictive analytics using AI can enable security teams to react ahead of an attack, reducing response time and impact by a great deal. With ever-evolving algorithms, they will take the lead in proactive threat hunting.

B. Blockchain for Data Integrity and Secure Sharing

Blockchain technology holds the promise of solutions to ensuring data integrity and improving secure communication among healthcare systems [36]. By distributing data storage and employing cryptographic validation, blockchain is able to: a. Prevent unauthorized access and tampering. b. Secure patient data exchange between organizations c. Improved data auditing and access logs transparency Although already in its early days of uptake, blockchain arguably can be part of secure health information exchanges (HIEs) of the future.

C. Development of Cybersecurity Skills and Workforce Expansion

Healthcare cyber threat sophistication's increased growth created a humongous healthcare cyber skills gap [37]. To address it, future plans must include: a. Investments in new cutting-edge training courses for cybersecurity experts b. Facilitating partnerships with universities to build healthcare-focused cyber curricula c. Reorganization of existing IT personnel for handling emerging threats Healthcare organizations will also find advantages in possessing cybersecurity leadership positions (such as Chief Information Security Officers, or CISOs) that are solely dedicated to risk management and incident response.

D. Adoption of Zero Trust Architecture

The "trust but verify" ethos of the past is not enough in the world of remote work, mobile computing, and networked systems. The future of cybersecurity is to implement a Zero Trust Architecture (ZTA)—an architecture in which no user or system within or without the network is trusted by default [38]. Some of the primary ZTA tenets are: a. Continuous identity verification b. Least-privilege access controls c. Microsegmentation of networks Zero Trust, complemented with robust identity and access management (IAM) capabilities, minimizes the attack surface for adversary lateral movement and enables highly controlled access to sensitive systems and data [39].

E. Policy Innovation and International Cooperation

Emerging policy trends will include governments collaborating with healthcare organizations and global agencies. Possible initiatives are: a. Compelled ransomware incident reporting b. Incentivization schemes for cybersecurity uptake among small or rural hospitals c. Global pacts to curb ransomware groups operating transnationally Harmonizing legislation and enforcing compliance will be essential, particularly as ransomware groups continue to take advantage of legal and jurisdictional loopholes [40].

VII. Conclusion

Ransomware is an increasingly pressing issue for the global health sector, with implications far more critical than financial loss. From the disruption of clinical workflows and patient safety, to reputational harm and harm to public trust, the effects of such attacks are far-reaching and severe. With cybercrooks ongoing exploitation of weaknesses within health systems—ranging from aging infrastructure to a lack of cybersecurity training—the need for a coordinated, strategic, and visionary response has never been greater. This study has analysed the scope of the ransomware issue in healthcare using real-world case studies, analysis of industry-specific risks, and an assessment of available and emerging mitigation methods. The facts are undeniable: healthcare is uniquely at risk based on its reliance on networked infrastructure, legacy infrastructure, and the sensitive nature of health data. Concomitantly, the health care mission of safeguarding and preserving lives makes the cost of inaction so catastrophic. Thankfully, there is more and more recognition of the need for cybersecurity as a part of patient safety and institutional resilience. Mitigation measures like the implementation of multi-factor authentication, increased network segmentation, frequent practice of backups, and improved staff training are becoming more mainstream. Meanwhile, technical innovation in artificial intelligence, machine learning, and blockchain is on the horizon to redefine the digital defence landscape in healthcare. But technology alone isn't enough. An effective defence against ransomware needs to be a holistic effort-one involving policy reform, international cooperation, investment, and developing an effective cybersecurity workforce. Cybersecurity also needs to be everyone's responsibility at every level of a healthcare organization, including IT, clinical staff, executives, and policy makers. In summary, the danger of ransomware is real, but it is not impossible to overcome. Through vigilance, through compliance, through cooperation, and through an unwavering dedication to safeguarding healthcare networks, we can make healthcare's future secure, resilient, and dedicated to doing what matters most: delivering quality, uninterrupted care to every patient.

Competing interests

The authors declare no competing interests.

Ethical Statement

In this article, the principles of scientific research and publication ethics were followed. This study did not involve human or animal subjects and did not require additional ethics committee approval.

Declaration Of AI Usage

No AI tools were used in the creation of this manuscript.

References

[1] Bastarache, L. (2021). Using phecodes for research with the electronic health record: from PheWAS to PheRS. *Annual Review of Biomedical Data Science*, 4(1), 1-19.

[2] Lubin, A. (2022). The law and politics of ransomware. *Vand. J. Transnat'l L.*, 55, 1177.

[3] Mohammed, S., DDS, Dr. S. T. A., Mohammed, N., & Sultana, W. (2024). A review of AI-powered diagnosis of rare diseases. *International Journal of Current Science Research and Review*, 07(09). https://doi.org/10.47191/ijcsrr/v7-i9-01

[4] Filip, R., Puscaselu, R. G., Anchidin-Norocel, L., Dimian, M., & Savage, W. K. (2022). Global challenges to public health care systems during the COVID-19 pandemic. *Journal of Personalized Medicine*, 12(8), 1295.

[5] Balammagary, S., Mohammed, N., Mohammed, S., & Begum, A. (2025). AI-Driven Behavioural Insights for Ozempic Drug Users. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 10-13.

[6] Karatas, M., Eriskin, L., Deveci, M., Pamucar, D., & Garg, H. (2022). Big Data for Healthcare Industry 4.0. *Expert Systems with Applications*, 200, 116912.

[7] Begum, A., Mohammed, N., & Panda, B. B. (2024). Leveraging AI in health informatics.

IARJSET, 11(12), 71–79. https://doi.org/10.17148/iarjset.2024.111205

[8] Mohammed, A., Sultana, G., Aasimuddin, F. M., & Mohammed, S. (2025). Leveraging NLP in Capital Markets. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 14-18.

[9] Rivara, F. P. et al. (2021). Structural racism and JAMA network open. *JAMA Network Open*, 4(6), e2120269-e2120269.

[10] Khadri Syed, W., & Janamolla, K. R. (2023). Fight against financial crimes. *IJARCCE*, 13(1), 59–64. https://doi.org/10.17148/ijarcce.2024.13107

[11] Olden, P. C., & Erwin, C. O. (2023). *Management of Healthcare Organizations: An Introduction*. ACHE Learn.

[12] Mohammed, S. (2024). Telemedicine: Impact on Pharmaceutical Care.

[13] Aljaidi, M. et al. (2022). NHS Wannacry Ransomware Attack. *IEEE EICEEAI*, pp. 1-6.

[14] Mohammed, Z. et al. (2025). AI-Powered Energy Efficient Cloud Networking. *Journal of Cognitive Computing and Cybernetic Innovations*, 1(1), 31-36.

[15] Pandey, N., & Jha, S. (2022). Universal health system in India. *Journal of Health Management*, 24(3), 337-346.

[16] Porcedda, D. M. G. (2024). Ransomware attack against Irish Health Service.

[17] Chittoju, S. R., & Ansari, S. F. (2024). Blockchain in Financial Services. *IJARCCE*, 13(12), 1–5. https://doi.org/10.17148/IJARCCE.2024.131201

[18] Ferreira, J. B. B. et al. (2021). Vulnerability and primary health care. *Journal of Primary Care & Community Health*, 12.

[19] Blessing, E., & Hubert, K. (2024). Technological Infrastructure and Challenges.

[20] Mohammed, S. et al. AI-Driven Automated Malware Analysis.

[21] Khadri, W. et al. (2024, July). Smart Banking Automation. *IEEE AIC*, pp. 686-692.

[22] Syed, W. K. et al. (2024, July). Biometric Authentication Systems in Banking. *IEEE AIC*, pp. 1331-1336.

[23] Mohammed, A. K., & Ansari, M. A. (2024). Impact and Limitations of AI in Power BI. *IJMRAP*, 7(7), 24–27.

[24] Mohammed, A. K. et al. Boosting Decision-Making with LLM in PowerBI.

[25] Shanmugam, B., & Azam, S. (2023). IoMT Devices Risk Assessment. *Technologies*, 11(1), 31.

[26] Janamolla, K. et al. Blockchain Enabled Cybersecurity in FinTech.

[27] Peter, H. (2022). Cybersecurity in Critical Infrastructure.

[28] Manning, L., & Kowalska, A. (2023). Ransomware in Food Supply Chain. *Trends in Organized Crime*, 1–29.

[29] Jane, K. (2025). Backup and Recovery Solutions.

[30] Hijji, M., & Alam, G. (2022). Cybersecurity Awareness Framework. *Sensors*, 22(22), 8663.

[31] Al-Tarawneh, A. et al. (2024). Governance and Legal Compliance. *Corporate Law & Governance Review*, 6(3).

[32] Eltayeb, O. (2024). Cyber Threat Intelligence. *Journal of Ecohumanism*, 3(4), 2422–2434.

[33] Tariq, U. et al. (2022). Ransomware Prevention in IoMT. *Sensors*, 22(21), 8516.

[34] Salama, R. et al. (2024). Healthcare Cybersecurity. *Computational Intelligence and Blockchain in Complex Systems*, 97–111.

[35] Manoharan, A., & Sarker, M. (2023). AI and ML in Cybersecurity. *IRJMETS*, 1. https://doi.org/10.56726/IRJMETS32644

[36] Rahman, M. S. et al. (2022). Blockchain-of-Blockchains. *Journal of Industrial Information Integration*, 30, 100408.

[37] Crumpler, W., & Lewis, J. A. (2022). Cybersecurity Workforce Gap. *CSIS*, p. 10.

[38] Emmanni, P. S. (2024). Zero-Trust Architecture. *IJCTT*, 72(5), 33–39.

[39] Singh, C., Thakkar, R., & Warraich, J. (2023). IAM Identity Access Management. *European Journal of Engineering and Technology Research*, 8(4), 30–38.

[40] Zhukova, . et al. (2021). Innovative Technologies in Higher Education. *Journal of Higher Education Theory and Practice*, 21(14), 153–169.