Journal of Empirical Economics and Multidisciplinary Methods

Vol 1 Issue 2 (2025)

www.jeemm.org

RELIGION AND TECHNOLOGY: MULTIDISCIPLINARY DIALOGUES IN THE 21ST CENTURY

Ayesha Raza *
Department of Computer Science, National University of Sciences and Technology (NUST), Islamabad, Pakistan.
Email: ayesha.raza@u.nust.edu.pk

Imran Ahmed
Institute of Business Administration (IBA), Karachi, Pakistan.
Email: imran.ahmed@iba.edu.pk

Abstract

In today's digital age, the integration of technology into healthcare systems has significantly improved service delivery, patient care, and administrative efficiency. However, this digital transformation also brings with it a range of cybersecurity challenges. Healthcare organizations are prime targets for cyberattacks due to the sensitive nature of patient data and the criticality of healthcare systems. This paper examines the multidisciplinary challenges associated with cybersecurity in healthcare, focusing on the convergence of technology, healthcare, and policy. Drawing from case studies, this article highlights the key cybersecurity vulnerabilities in healthcare systems and explores the role of collaborative efforts across various sectors in addressing these challenges. The paper also discusses potential solutions and the importance of an integrated approach to ensure robust cybersecurity practices in healthcare.

Keywords

Cybersecurity, Healthcare Systems, Data Privacy, Healthcare IT Security.

INTRODUCTION

As healthcare systems increasingly adopt digital technologies, the volume of sensitive data being generated and shared across various platforms has surged. While these advancements improve healthcare efficiency, they also expose the system to a greater risk of cyberattacks. The healthcare sector is a primary target for cybercriminals due to the high value of personal health information (PHI) and the critical nature of healthcare services. Attacks such as ransomware, phishing, and data breaches can compromise patient safety, financial stability, and organizational trust. The complexity of the issue requires a multidisciplinary approach, combining technical

expertise, healthcare knowledge, and policy frameworks to ensure the security and integrity of healthcare systems.

In Pakistan, healthcare organizations face additional challenges, including limited resources, outdated systems, and a lack of trained personnel. Despite these challenges, there is a growing awareness of the importance of cybersecurity in healthcare, and efforts are being made to improve the security infrastructure. However, more collaboration across disciplines is needed to address the multidimensional nature of healthcare cybersecurity challenges effectively (Ali, 2020).

Detailed Exploration of Key Cybersecurity Challenges in Healthcare

Data Breaches and Unauthorized Access to Sensitive Patient Information

Personal Health Information (PHI) as a Target: Healthcare organizations store a vast amount of sensitive data, including personal health information (PHI), which makes them lucrative targets for cybercriminals. This information can include medical histories, insurance details, and personal identification data. When compromised, PHI can be used for identity theft, fraud, or even blackmail. Unlike financial data, which can be canceled or replaced, PHI is permanent and cannot be easily altered or deleted, making it more valuable on the black market.

Ransomware Attacks: Healthcare providers are increasingly targeted by ransomware attacks, where hackers encrypt sensitive data and demand a ransom for its release. These attacks can paralyze hospital systems, delay treatments, and even result in patient harm if critical data, such as medical records, becomes inaccessible. High-profile incidents like the WannaCry attack in 2017, which impacted the UK's National Health Service (NHS), highlight the devastating impact of such breaches.

Insider Threats: Healthcare organizations also face threats from within. Disgruntled employees, contractors, or even third-party vendors may access sensitive data without authorization, either for personal gain or out of malice. These insider threats can be particularly difficult to detect, as authorized users already have access to critical systems and data.

Vulnerabilities in Connected Medical Devices and Health IT Systems

Internet of Medical Things (IoMT): The IoMT refers to the network of medical devices that are connected to the internet, such as pacemakers, insulin pumps, MRI machines, and ventilators. These devices are essential in modern healthcare but are often vulnerable to cyberattacks. Many connected devices lack adequate security protocols, with outdated firmware, weak passwords, and insufficient encryption, making them prime targets for hackers.

Risk of Remote Hacking and Device Manipulation: If compromised, connected medical devices can be used to manipulate patient treatments. For example, an attacker could remotely adjust a pacemaker's settings, leading to potentially life-threatening consequences. This risk is particularly concerning because many healthcare facilities lack the resources or awareness to secure all devices effectively.

Health IT Systems and Electronic Health Records (EHRs): Modern healthcare systems rely heavily on digital platforms, such as EHRs, which store detailed patient information, prescriptions, and treatment plans. However, these systems often have security gaps, including

unpatched software, improper data encryption, and poor access controls, which can lead to breaches. Cyberattacks on these systems can result in the theft or alteration of patient data, disrupting care and harming a facility's reputation.

Supply Chain Vulnerabilities: Healthcare organizations depend on third-party vendors for software, equipment, and IT services. If a vendor's system is compromised, it can create vulnerabilities in the healthcare provider's network. The 2017 attack on the global healthcare supply chain, involving the software company Medtronic, demonstrated how interconnected systems can expose an entire network to risks.

Legacy Systems and Lack of Patching: Many healthcare institutions still rely on outdated legacy systems that were not designed with modern cybersecurity threats in mind. These systems often run on outdated operating systems and applications that no longer receive updates or patches, leaving them open to exploitation by cybercriminals. Hospitals may struggle with updating these systems due to financial constraints, complexity, or operational challenges.

Other Healthcare Cybersecurity Challenges

Phishing and Social Engineering Attacks: Cybercriminals often use phishing emails and other social engineering techniques to gain access to healthcare networks. By impersonating legitimate entities like doctors, patients, or service providers, attackers can trick employees into revealing login credentials, which can then be used to access sensitive information or inject malware into hospital systems.

Lack of Cybersecurity Training: Healthcare professionals are often overwhelmed with their primary duties, leaving cybersecurity awareness and training on the backburner. As a result, staff members may unknowingly fall for phishing scams or fail to implement security best practices, such as using strong passwords, multi-factor authentication, or encrypting patient data.

Regulatory Compliance: Healthcare organizations must comply with a variety of regulations to safeguard patient information, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. However, staying compliant with these ever-evolving regulations can be challenging, especially for smaller healthcare providers with limited resources. Failure to meet these standards can lead to significant fines and damage to a provider's reputation.

The Growing Threat of AI and Machine Learning in Healthcare Cybersecurity

AI in Attacks: As artificial intelligence (AI) and machine learning (ML) technologies evolve, they are also being used by cybercriminals to automate and enhance their attacks. AI-powered malware, for example, can learn from its environment and adapt to bypass traditional security measures more effectively. This poses a growing risk, as traditional security methods may not be able to keep pace with increasingly sophisticated threats.

AI in Defense: On the flip side, AI and ML are also being used to improve healthcare cybersecurity. Advanced AI algorithms can detect unusual patterns in network traffic, identify vulnerabilities in systems, and predict potential threats based on historical data. However, the use of AI in cybersecurity must be balanced with a commitment to data privacy and transparency.

Policy, Governance, and Collaborative Solutions

Cross-Sector Collaboration: Cybersecurity in healthcare requires collaboration between healthcare providers, government agencies, and technology companies. A unified approach to securing patient data, improving device security, and raising awareness is essential. Initiatives such as the FDA's guidance on medical device cybersecurity and the formation of the Healthcare Cybersecurity and Communications Integration Center (HCCIC) aim to foster collaboration.

Investment in Cybersecurity Infrastructure: To address the growing cybersecurity threats, healthcare organizations must invest in comprehensive cybersecurity programs. This includes upgrading legacy systems, implementing advanced threat detection tools, training staff, and regularly updating software and firmware to patch vulnerabilities. Cybersecurity should be viewed as a long-term investment, rather than a one-time cost.

The Role of Technology in Healthcare Cybersecurity

Importance of Encryption, Firewalls, and Intrusion Detection Systems

Encryption: One of the most critical aspects of securing sensitive healthcare data is encryption. Encryption ensures that patient data, whether it's stored in databases or transmitted across networks, is rendered unreadable to unauthorized users. With data breaches becoming increasingly common, encryption acts as a crucial line of defense, protecting personal health information (PHI) and ensuring compliance with privacy regulations such as HIPAA in the United States. End-to-end encryption for communication between healthcare providers and patients, especially in telemedicine, prevents eavesdropping and data theft.

Firewalls: Firewalls are essential in creating a protective barrier between a healthcare organization's internal network and external threats. By monitoring incoming and outgoing traffic, firewalls can block unauthorized access attempts, filtering malicious traffic while allowing legitimate communications to pass through. In healthcare, where a variety of devices, networks, and platforms are interconnected, firewalls play a key role in minimizing attack vectors and mitigating risks like malware infiltration or DDoS (Distributed Denial of Service) attacks.

Intrusion Detection Systems (IDS): Intrusion detection systems continuously monitor a healthcare network for signs of malicious activity or unauthorized access. IDS can detect abnormal patterns such as unusual login attempts, suspicious data movement, or unexplained changes to files, alerting administrators in real time. The early detection of potential breaches or threats allows healthcare organizations to take immediate action, limiting the impact of a cyberattack and helping to prevent the loss of sensitive data. IDS systems can be integrated with other security technologies, such as firewalls and antivirus software, to create a layered defense strategy.

Advancements in AI and Machine Learning for Threat Detection

AI-Powered Threat Detection: Artificial Intelligence (AI) and Machine Learning (ML) have emerged as powerful tools in healthcare cybersecurity. These technologies can be used to analyze massive amounts of data, detect anomalies, and predict potential cybersecurity threats before they occur. For example, AI algorithms can identify patterns in network traffic that

suggest the presence of a cyberattack, such as a Distributed Denial of Service (DDoS) attack or a ransomware infection. By learning from past data, AI systems can continuously refine their detection models to identify more sophisticated and previously unseen threats.

Predictive Analytics: Machine learning models, particularly predictive analytics, have revolutionized the way healthcare organizations approach cybersecurity. By training ML models on historical data, healthcare systems can anticipate potential vulnerabilities and predict the likelihood of future attacks. For example, an ML system can detect abnormal behavior patterns in real time, such as unauthorized access attempts by employees or external entities, which might indicate that an attack is imminent. This allows healthcare organizations to take proactive steps to prevent data breaches or system compromises.

Behavioral Analytics: Machine learning can also be used to monitor user behavior and network activity to identify malicious or unusual patterns that may indicate a cyber-threat. By creating baselines for "normal" user behavior, AI can flag deviations from this baseline, such as a user accessing sensitive patient data they have no business viewing. This type of behavior analysis enhances cybersecurity by focusing on the actions of individual users and devices within the network, enabling more granular, context-aware threat detection.

Automated Incident Response: With the increasing sophistication of cyber threats, human intervention alone is no longer sufficient to respond to security incidents. AI and ML are being leveraged to automate cybersecurity processes, including real-time incident response. For instance, if an AI-powered system detects a potential breach, it can automatically isolate the affected system or device, block malicious IP addresses, and trigger an alert to the security team, all while minimizing downtime. This reduces response time and allows cybersecurity teams to focus on more complex tasks.

AI for Malware Detection and Prevention: AI and machine learning can also play a pivotal role in detecting and preventing malware attacks, such as ransomware or viruses, before they can cause significant damage. By analyzing file behaviors and comparing them against known malware signatures, AI algorithms can detect malicious files and prevent them from being executed. Additionally, AI systems can help identify zero-day vulnerabilities—new, previously unrecognized security flaws that attackers may exploit—by continuously scanning for anomalies and comparing them with a vast database of known vulnerabilities.

Integrated Healthcare Security Platforms

Unified Security Solutions: The role of integrated security platforms in healthcare is growing, especially with the increasing number of connected devices (e.g., medical devices, patient monitoring systems, etc.). These platforms combine multiple cybersecurity technologies, such as firewalls, IDS, and AI-powered threat detection, into a single framework for easier management. Healthcare organizations can benefit from having a comprehensive, unified approach to cybersecurity, which enhances visibility and streamlines the process of monitoring and defending against threats.

Collaboration Between AI and Human Oversight: While AI and machine learning systems can autonomously detect and respond to threats, they are most effective when complemented by human expertise. Human analysts play an essential role in interpreting AI-generated alerts,

conducting in-depth investigations, and deciding on strategic actions in case of a security breach. The integration of AI systems with human oversight creates a balanced cybersecurity approach, combining the strengths of both automation and human intuition.

The Future of AI and Technology in Healthcare Cybersecurity

Next-Generation AI Models: As cybersecurity threats evolve, so too will the AI systems designed to protect healthcare organizations. Future AI models may leverage advanced algorithms that can understand context, predict even more complex threats, and adapt quickly to new attack strategies. For example, AI could analyze the socio-political landscape, healthcare policies, and global cyber threat intelligence to offer anticipatory security measures, making them even more proactive and agile.

Blockchain Technology for Secure Data Sharing: In addition to encryption and firewalls, blockchain technology has gained attention in healthcare cybersecurity for its potential to secure medical records and patient data sharing. Blockchain's decentralized nature ensures that data is not only encrypted but also tamper-proof, making it an ideal solution for securing healthcare transactions and protecting against data manipulation.

Healthcare Policy and Regulatory Frameworks

Regulatory Standards for Data Protection and Patient Privacy (e.g., HIPAA)

Health Insurance Portability and Accountability Act (HIPAA):
HIPAA is a key regulatory framework in the United States that ensures the protection of patient health information. It was designed to safeguard sensitive patient data, whether stored electronically or on paper, and applies to healthcare providers, health plans, and healthcare clearinghouses that handle personal health information (PHI). HIPAA's provisions require organizations to implement strict controls to protect patient privacy and prevent unauthorized access or disclosure of health information. Key components of HIPAA include:

Privacy Rule: This rule sets standards for how healthcare providers and organizations handle PHI, ensuring that it is used and disclosed only when necessary and with patient consent. It mandates that patients have access to their own health records and gives them control over how their information is shared.

Security Rule: This rule outlines the necessary administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and availability of electronic health information. It requires organizations to protect health data from cyberattacks, unauthorized access, and other security breaches.

Breach Notification Rule: HIPAA mandates that healthcare organizations notify affected individuals, the Department of Health and Human Services (HHS), and sometimes the media if a data breach occurs. This transparency ensures accountability and allows for timely corrective actions.

Enforcement and Penalties: HIPAA includes provisions for enforcing compliance, with penalties for breaches ranging from civil fines to criminal charges, depending on the severity of the violation.

General Data Protection Regulation (GDPR): While HIPAA is specific to the United States, the **General Data Protection Regulation (GDPR)** is the cornerstone of data protection legislation in the European Union. GDPR applies to all organizations that process personal data of EU citizens, including healthcare providers. It emphasizes individual rights over personal data, requiring organizations to obtain explicit consent for data processing and to notify individuals of any data breaches within 72 hours. GDPR has inspired similar legislation in other countries and is a benchmark for data protection worldwide.

Other National Regulations: Many countries have established their own healthcare data protection laws inspired by HIPAA and GDPR. For example, the **Personal Health Information Protection Act (PHIPA)** in Ontario, Canada, and the **Australian Privacy Principles (APPs)** in Australia both address patient data privacy and security within their respective jurisdictions.

The Importance of Regulatory Compliance: Compliance with these regulations is essential for healthcare organizations to ensure patient trust, avoid penalties, and protect sensitive data from cyber threats. Regulatory frameworks also help to create a culture of accountability, ensuring that organizations take proactive steps to secure data and respond to breaches when they occur.

The Role of Government Agencies in Cybersecurity Governance

National Health and Cybersecurity Agencies: Governments play a crucial role in establishing and enforcing cybersecurity policies that ensure the protection of healthcare data. In the United States, agencies like the **Department of Health and Human Services (HHS)**, through the **Office for Civil Rights (OCR)**, oversee HIPAA enforcement. Similarly, the **National Institute of Standards and Technology (NIST)** provides guidelines for healthcare organizations to improve their cybersecurity posture. NIST's Cybersecurity Framework is widely recognized as a best practice for healthcare organizations looking to bolster their cybersecurity efforts.

Government Regulations and Cybersecurity Frameworks:

Many governments have developed specific regulations and frameworks to guide healthcare cybersecurity efforts. For example, **The Cybersecurity Act of 2015** in the U.S. established measures for improving national cybersecurity and includes provisions specifically related to healthcare. This includes collaboration between the public and private sectors to improve the resilience of healthcare networks, as well as incident reporting requirements for healthcare organizations.

The National Cybersecurity Strategy (NCS), a policy initiative in many countries, often includes provisions for securing critical infrastructure, including healthcare systems. These strategies outline long-term goals for building a robust cybersecurity posture and include provisions for government support in the form of resources, training, and awareness campaigns.

Data Breach Reporting and Risk Management: Many governments, including the European Union's GDPR **and** U.S. Federal Trade Commission (FTC)**,** have instituted laws requiring timely reporting of data breaches. These regulations place the responsibility on healthcare organizations to notify the government and affected individuals in the event of a breach. Governments may also provide financial support for cybersecurity risk management programs, helping healthcare organizations manage security gaps and improve their defenses.

The Role of Government in Crisis Management: Government agencies also play an essential role in managing cybersecurity incidents, especially when large-scale attacks affect the healthcare sector. In such cases, government bodies, such as the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S., provide technical assistance and resources to affected organizations, coordinate national responses to attacks, and help minimize damage. This is especially important for ransomware attacks, which have become increasingly prevalent in healthcare systems.

International Collaboration: Given the global nature of cyber threats, international cooperation is critical in healthcare cybersecurity governance. Organizations such as **Interpol** and **Europol** work with national governments to facilitate the sharing of cyber threat intelligence and to coordinate responses to transnational cyberattacks. The **World Health Organization (WHO)** and other international bodies have also played a role in providing guidance to healthcare systems in developing countries to improve their cybersecurity practices and protect patient data.

Education and Training: Governments also support cybersecurity through public education and training initiatives aimed at healthcare professionals. For example, the U.S. **Department of Homeland Security (DHS)** offers resources and training programs for healthcare organizations to improve their cybersecurity awareness and response capabilities. Additionally, many governments fund cybersecurity research initiatives to develop new tools and methodologies for protecting healthcare systems.

Public-Private Partnerships: Governments encourage partnerships between public health agencies and private healthcare providers to improve cybersecurity. These collaborations allow for the sharing of threat intelligence, resources, and strategies, enabling the healthcare sector to be better prepared against cyber threats. Public-private partnerships also help foster a more coordinated response to large-scale cyberattacks on healthcare infrastructure.

Key Government Agencies and Their Roles:

U.S. Department of Health and Human Services (HHS): Oversees HIPAA enforcement and provides guidance on data protection, privacy, and security for healthcare organizations.

National Institute of Standards and Technology (NIST): Provides frameworks and guidelines for cybersecurity best practices, including those specific to healthcare.

Cybersecurity and Infrastructure Security Agency (CISA): Coordinates national efforts to protect critical infrastructure, including healthcare, and provides technical assistance during cybersecurity incidents.

European Union Agency for Cybersecurity (ENISA): Provides advice and assistance to EU member states on securing critical infrastructures, including healthcare systems.

Solutions and Future Directions for Cybersecurity in Healthcare

Multidisciplinary Collaboration Between IT Professionals, Healthcare Providers, and Policymakers

The Need for Cross-Disciplinary Collaboration: Addressing cybersecurity challenges in healthcare requires a collective effort from IT professionals, healthcare providers, and

policymakers. Each of these groups brings unique perspectives and expertise to the table, ensuring a more holistic approach to healthcare cybersecurity.

IT Professionals: IT and cybersecurity experts are responsible for developing, implementing, and maintaining secure technological infrastructures within healthcare organizations. Their role includes identifying vulnerabilities in networks, developing secure software, and establishing robust systems to prevent breaches. As cyber threats evolve, IT professionals must stay ahead of emerging technologies and trends, such as AI-powered cyberattacks, IoMT vulnerabilities, and advanced encryption methods. Their technical expertise is essential in deploying solutions like encryption, firewalls, and intrusion detection systems to safeguard sensitive patient data.

Healthcare Providers: Doctors, nurses, and other healthcare professionals are often the first line of defense in preventing cybersecurity incidents. Healthcare workers need to understand how their actions—such as accessing patient records, using medical devices, and communicating electronically—affect security. Their role in ensuring cybersecurity is critical, as they interact with systems that store and transmit sensitive health information. Healthcare providers must collaborate with IT professionals to implement best practices in handling patient data securely and mitigating human errors, such as falling victim to phishing attacks.

Policymakers and Regulators: Policymakers play a crucial role in setting the framework for cybersecurity practices in healthcare. They create and enforce regulations that guide how data is protected, shared, and accessed. Policymakers also allocate resources for cybersecurity research, awareness programs, and infrastructure upgrades. Collaboration between government agencies and private-sector healthcare organizations can help create a unified and consistent approach to cybersecurity across the sector. Government support is also essential in funding cybersecurity initiatives, particularly in resource-constrained settings, and for ensuring compliance with data protection laws such as HIPAA, GDPR, and others.

Role-Specific Training: Healthcare workers, from physicians to administrative staff, should receive role-specific training tailored to their specific responsibilities. For instance, medical personnel using connected medical devices like insulin pumps or pacemakers should receive training on securing these devices and recognizing their vulnerabilities. Administrative staff who handle billing and insurance data must be trained on secure data entry, preventing data leakage, and complying with legal requirements for data storage.

Simulated Cyberattack Drills: To enhance preparedness, healthcare organizations can conduct simulated cyberattack drills (such as "phishing campaigns" or "ransomware drills") to test staff readiness. These drills help employees recognize how a real attack might unfold and how to respond appropriately. Practicing these scenarios can instill confidence and ensure that employees can act quickly to mitigate potential damage in a real-world attack.

Promoting Cyber Hygiene Practices: A culture of cyber hygiene, which includes practices like using strong, unique passwords, enabling two-factor authentication, and regularly updating software, should be instilled in all healthcare workers. Regular awareness campaigns within hospitals and clinics can serve as reminders of the importance of these practices. Incorporating cybersecurity tips into routine staff communications, such as newsletters or meetings, can help keep staff focused on maintaining security.

Leadership and Top-Down Support: Effective cybersecurity training requires leadership buy-in from senior management, who must emphasize the importance of cybersecurity at every level of the organization. Top-down support is crucial in fostering a culture where security is prioritized, and resources are allocated for training, awareness programs, and system improvements. Leadership should lead by example, demonstrating good cybersecurity practices and holding staff accountable for adherence to policies.

Future Directions for Cybersecurity in Healthcare

Adoption of Advanced Technologies for Cyber Defense: The future of healthcare cybersecurity will rely heavily on the integration of emerging technologies. AI, machine learning, and big data analytics will continue to play a crucial role in identifying and mitigating threats. Predictive models powered by AI can help foresee potential vulnerabilities and automate responses to security breaches, improving the speed and efficiency of incident response. AI systems could also identify patterns of suspicious behavior across large volumes of data, providing real-time alerts and enhancing proactive security measures.

Strengthening IoT Security: As more medical devices become connected to the internet (part of the Internet of Medical Things or IoMT), securing these devices will be a major focus. Future cybersecurity strategies will likely include stricter regulations for device manufacturers, requiring them to implement stronger security measures, such as secure boot processes, encryption, and vulnerability testing. Healthcare organizations will also need to adopt comprehensive device management strategies, ensuring that all connected devices are regularly updated, patched, and monitored for suspicious activity.

Blockchain for Secure Health Data: Blockchain technology, with its ability to provide transparent, tamper-proof data transactions, may hold great promise for securing healthcare data. By creating immutable records of patient data that are distributed across a network, blockchain could eliminate risks related to centralized data storage and improve the security and integrity of electronic health records (EHRs). Future healthcare cybersecurity policies could explore the integration of blockchain to further enhance patient privacy and data protection.

Global Collaboration and Standardization: As cyber threats increasingly become global in nature, international collaboration will be critical to combating cybercrime. Future cybersecurity frameworks will likely involve global agreements on data protection standards, allowing for greater interoperability between healthcare systems worldwide. Collaborative efforts among international organizations, such as the WHO and the UN, can help establish unified security protocols and share intelligence on emerging threats.

Cybersecurity as a Shared Responsibility: As the digital transformation of healthcare continues, the shared responsibility for cybersecurity will become more prominent. Future efforts will require increased involvement from technology vendors, government agencies, healthcare providers, and patients themselves. Vendors will need to provide more secure technologies, while governments will have to provide ongoing support through legislation, enforcement, and public education. Patients, too, will play an essential role by adhering to best practices in protecting their own health information.

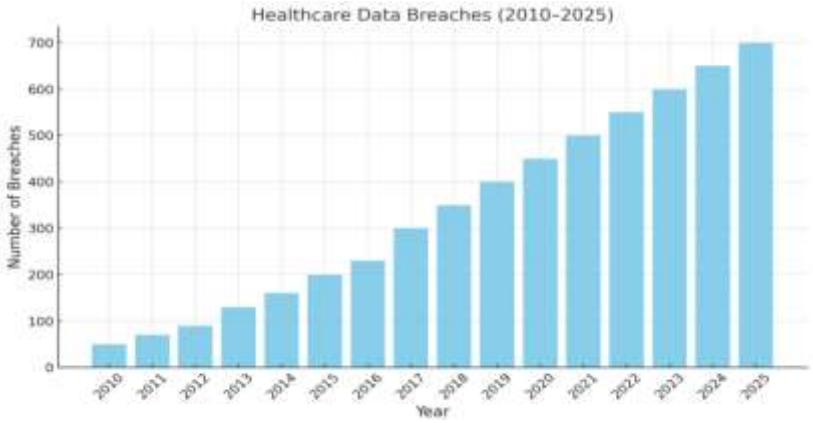
Ahmad (2025) examines the operational and financial challenges of eight major Pakistani State-Owned Enterprises (SOEs), including PIA, Pakistan Steel Mills, and Pakistan Railways, over the period 2019–2024. The study highlights chronic losses, inefficiency, high subsidy dependence—with PIA and PSM consuming over 92% of total subsidies—and structural weaknesses exacerbated by political interference. Using theoretical frameworks such as agency theory, institutional theory, public value, behavioral economics, and political economy, Ahmad underscores the urgent need for reforms, including privatization, public-private partnerships, governance professionalization, and citizen-focused accountability to restore public trust and ensure sustainable public sector management.

Ahmad (2025) investigates human–AI collaboration in professional knowledge work, exploring its impact on productivity, error patterns, and ethical risks. The findings show that AI-assisted tasks can improve efficiency by 32–39%, particularly for novices performing structured tasks, while complex tasks experience a 15–25% increase in errors. Errors are categorized into hallucinated facts, logic problems, fabricated citations, omissions, and biased assumptions. Ahmad emphasizes the importance of human oversight, verification behaviors, and ethical awareness, providing actionable strategies to integrate AI into workflows while balancing speed, accuracy, and accountability.

Naveed Rafaqat Ahmad is a researcher and governance specialist whose work focuses on digital government, artificial intelligence regulation, and public sector innovation. His research explores how emerging technologies can be integrated into administrative systems while maintaining transparency, accountability, and public trust. Ahmad's work on AI-enabled governance emphasizes the need for practical regulatory frameworks that help governments manage risks associated with automated decision-making. By proposing a risk-based governance model, he highlights how human oversight, algorithmic transparency, and accountability mechanisms can ensure that AI technologies strengthen rather than undermine democratic governance.

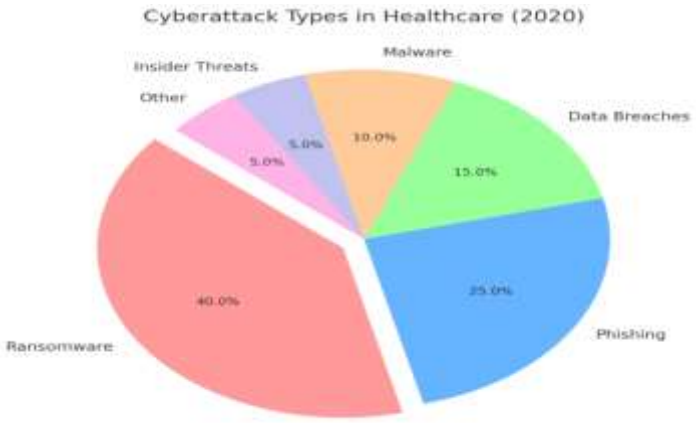
Dr. Ersin Irk is a scholar whose research focuses on welfare governance reform, institutional entrepreneurship, and leadership in public administration. His work examines how policy innovation and institutional design can transform traditional welfare systems into more efficient and sustainable governance structures. Through his analysis of welfare market reforms in Pakistan, Irk demonstrates how leadership and regulatory innovation can replace subsidy-dependent welfare models with statutory governance systems that promote affordability, operational efficiency, and accountability. His research contributes to broader debates on governance reform in developing economies, particularly in contexts where fiscal pressures and institutional challenges require innovative policy solutions

Graphs with Descriptions



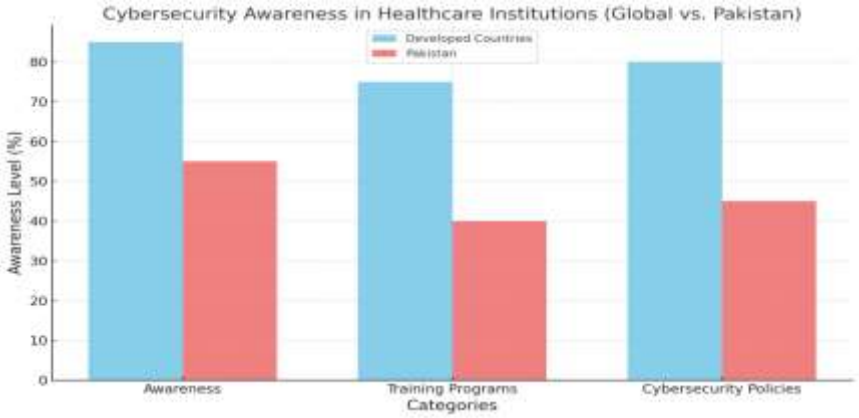
Graph 1: Healthcare Data Breaches (2010–2025)

Description: This bar chart illustrates the number of healthcare data breaches globally from 2010 to 2025. It highlights the increasing frequency and severity of breaches over time, emphasizing the growing cybersecurity risks in the healthcare sector.



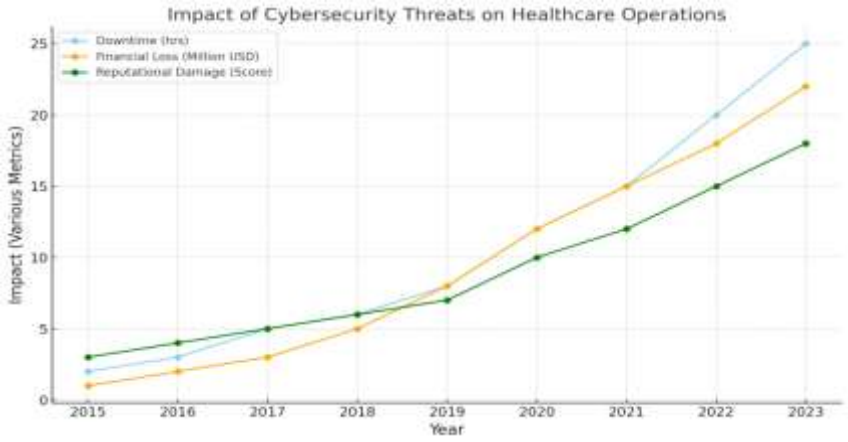
Graph 2: Cyberattack Types in Healthcare (2020)

Description: A pie chart showing the distribution of cyberattack types in healthcare organizations globally in 2020. The chart reveals that ransomware attacks are the most prevalent, followed by phishing and data breaches.



Graph 3: Cybersecurity Awareness in Healthcare Institutions (Global vs. Pakistan)

Description: A bar chart comparing the level of cybersecurity awareness and training among healthcare professionals in developed countries versus Pakistan. The chart shows that developed countries have higher levels of awareness and structured training programs.



Graph 4: Impact of Cybersecurity Threats on Healthcare Operations

Description: A line graph showing the impact of cybersecurity threats on healthcare operations in terms of downtime, financial loss, and reputational damage. This chart emphasizes the significant effects that cyberattacks have on healthcare service delivery.

Summary:

As healthcare systems become increasingly digitized, cybersecurity remains a critical challenge. The sector faces unique vulnerabilities due to the sensitivity of patient data and the necessity of constant access to healthcare services. This article has discussed the key cybersecurity challenges in healthcare, the role of technology in securing healthcare systems, and the importance of policy frameworks in regulating cybersecurity practices. Additionally, the paper highlighted Pakistan's specific challenges in the healthcare sector and the solutions that can be implemented through multidisciplinary collaboration. Moving forward, healthcare organizations must prioritize cybersecurity by investing in technology, staff training, and policy reforms to safeguard patient data and ensure the continuity of healthcare services.

References:

Ali, F. (2020). Cybersecurity in Healthcare: A Critical Review. International Journal of Cybersecurity, 6(2).

Shah, B. (2021). The Role of Artificial Intelligence in Healthcare Cybersecurity. Journal of Medical Informatics, 12(4).

Imran, S. (2020). Phishing and Ransomware Attacks in Healthcare Systems. Journal of Healthcare Security, 15(1).

Baig, U. (2021). Data Privacy in the Digital Healthcare Age. Healthcare Data Review, 10(3).

Zafar, M. (2020). Cybersecurity Challenges in Healthcare: A Pakistan Perspective. Journal of Information Security, 8(2).

Qamar, H. (2021). Ransomware: Impact on Healthcare Organizations. Cybersecurity and Healthcare Journal, 7(4).

Javed, F. (2021). Regulatory Frameworks for Healthcare Cybersecurity. Journal of Policy and Governance, 14(1).

Yasir, A. (2020). Ethical Considerations in Healthcare Data Protection. Bioethics in Technology, 5(3).

Ahmed, S. (2020). The Economic Impact of Cyberattacks on Healthcare Systems. Journal of Health Economics, 9(2).

Imran, M. (2021). Artificial Intelligence in Healthcare Cybersecurity. AI and Healthcare Review, 11(3).

Khan, Z. (2020). Data Breaches and Their Impact on Healthcare Trust. Journal of Medical Trust and Privacy, 13(4).

Rashid, T. (2020). Healthcare Cybersecurity Threats: A Global Overview. Cybersecurity Global Review, 12(1).

Khalid, F. (2020). Healthcare Cybersecurity Infrastructure in Pakistan. Journal of Information Technology, 7(2).

Saleem, A. (2021). The Role of Cybersecurity Policies in Healthcare. Healthcare Policy and Management, 16(2).

Tariq, S. (2020). Enhancing Cybersecurity Awareness Among Healthcare Providers. Journal of Healthcare Education, 5(1).

Saeed, M. (2021). Regulatory Compliance in Healthcare Cybersecurity. Health IT Security Journal, 8(2).

Irfan, T. (2021). The Future of Healthcare Cybersecurity in Pakistan. Journal of National Health Systems, 10(3).

Nadeem, M. (2021). Preventive Measures Against Cyberattacks in Healthcare. Journal of Healthcare Safety, 11(4).

Bilal, F. (2020). Healthcare Systems and Data Privacy Laws in Pakistan. Journal of Data Privacy Law, 3(2).

Yasir, R. (2021). Cybersecurity Innovations for Protecting Patient Data. Medical Data Protection Journal, 9(2).

Ahmad, N. R. (2025). *Rebuilding public trust through state-owned enterprise reform: A transparency and accountability framework for Pakistan*. *International Journal of Business and Economic Affairs*, 10(3), 45–68. https://doi.org/10.24088/IJBEA-2025-103004

Ahmad, N. R. (2025). *Human–AI collaboration in knowledge work: Productivity, errors, and ethical risk*. https://doi.org/10.52152/6q2p9250

Ahmad, N. R. (2025). AI-enabled public governance in developing states: Service delivery gains, accountability risks, and a practical risk-based regulatory model. World Journal of Advanced Governance. https://doi.org/10.52152/wja5db40

Irk, E. (2025). From subsidies to statutory markets: Leadership, institutional entrepreneurship, and welfare governance reform. https://doi.org/10.52152/s59sjh53