Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 12, 2025

SECURING GOVERNMENT INFORMATION SYSTEMS AGAINST EMERGING CYBER THREATS

Waqar Younis[*1], Mariam Nayab[2], Waqar Ahmad[3], Iqra Fazilat[4], Dr. Jawaid Iqbal[5]

[*1,3]*Master of Science in Software Engineering from Riphah International University, Islamabad.*
[2]*Master of Science in Computer Science, from Riphah International University, Islamabad.*
[4]*Master of Science in Computer Science, from Riphah International University, Islamabad.*
[5]*Associate Professor, Faculty of Computing, Riphah International University, Islamabad.*

[*1]sardarwaqar819@gmail.com,[2]khanmaryam8584@gmail.com,[3]waqar.ahmad9960@gmail.com,
[4]iqrafazilat2000@gmail.com, [5]jawaid.iqbal@riphah.edu.pk

DOI: https://doi.org/10.5281/zenodo.18058568

Keywords
Government Information Systems, Emerging Cyber Threats, Zero Trust Security, Data Protection, Cybersecurity Policy, National Security

Article History
Received: 11 October 2025
Accepted: 21 November 2025
Published: 26 December 2025

Corresponding Author: *
Waqar Younis

Abstract
The increasing threats and zero-day vulnerabilities might pose a significant risk to the GIS-Government Information System which is the foundation of the power of the state. Such systems facilitate vital services such as the provision of public services, national security operations, financial, healthcare, and policy development. With the digitalization and interconnection of such systems by governments, they are becoming vulnerable to advanced and pervasive cyber-attacks. The development of new attack vectors, including advanced persistent threats (APTs), ransomware, supply-chain attacks, AI-enabled phishing and zero-day exploits pose significant threats to the privacy, sanctity and readability of sensitive government information. The present paper explores the currently changing cyber-threat environment that attacks government information systems and considers effective measures to mitigate it. The current research identifies the major weaknesses of the outdated infrastructure, poor security policies, human error, and limited incident-response capabilities to highlight ways in which the country could be more susceptible to them after reviewing the case studies in the world and situating them into the context of Pakistan, which is a developing nation. The proposed study is a mixed-methods/single-method research because it seeks to obtain quantitative data concerning cyber-incidents, as well as qualitative data, based on expert interviews and reviews of policy documents. Such a two-tier approach provides a full understanding of both technical and socio-organizational aspects of GIS security. This Paper studies suggest that such things as transitioning to zero-trust architecture, having continuous monitoring of your network, increasing the protection on endpoints, establishing a robust encryption protocol, and conducting regular security awareness training to governmental staff.

INTRODUCTION

Online systems are quite popular and handy in any sphere of life, but at the same time, they have disturbing sides to them. On the one hand, digital tools simplify our life and on the other hand, we simply upload the most valuable information online without second thoughts and

it can become a significant threat. Cyber-bullying, spoofing and others are ubiquitous, and, in that case, it is especially important that government systems should be locked down due to the sensitivity and confidentiality of the data. GIS is not just vulnerable, but vulnerability is a socio-technical problem with a variety of factors that affect it. Old, outdated legacy infrastructure, insufficient financing of cybersecurity, lack of personnel in the field of skilled security professionals, laxity in policy implementation, and human error all combine to create a factor that an attacker can use up both technical and non-technical vulnerabilities. In such countries as Pakistan, those difficulties become even larger, due to incoherent cybersecurity policies, reduced cross-agency interactivity, and absent of a consistent national incident response system. This is the reason the paper had suggested a multi-layered security model that could be utilized to guarantee that systems are stronger with technical, procedural and policy controls.

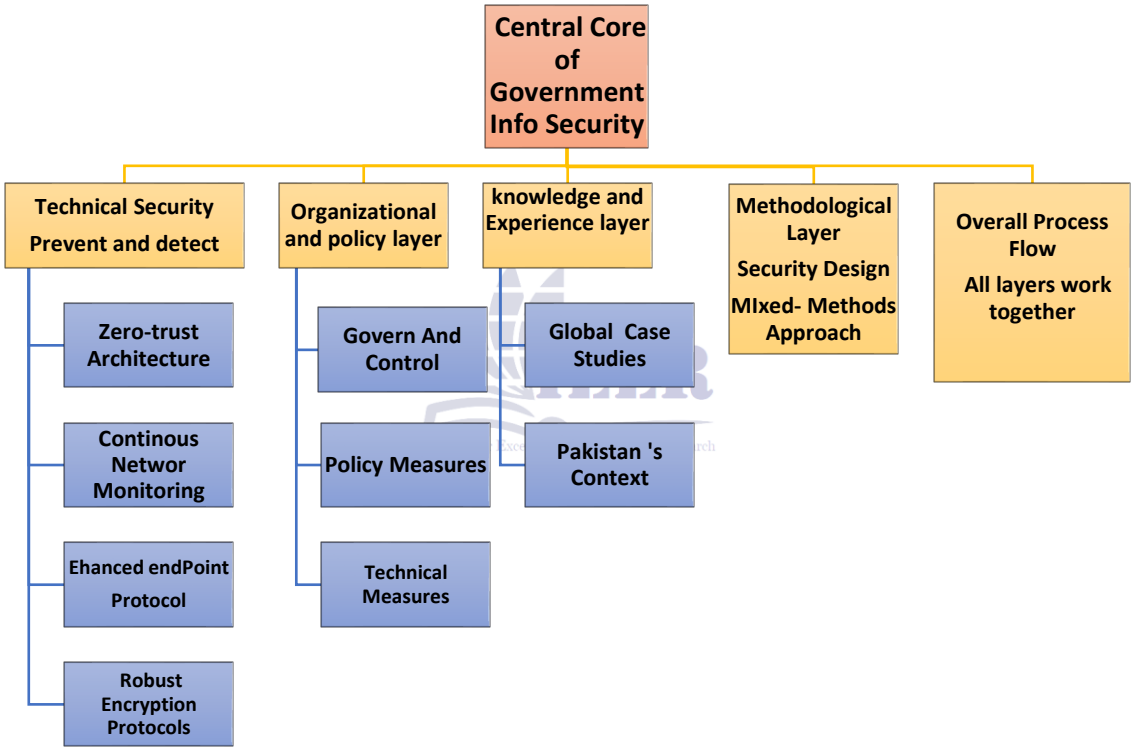

Figure 1: Government Information System Protection Scenarios

The need to move beyond is essential to guarantee the security of the government information systems. an outmoded, heavily restrictive models to one that is initiative-taking, multi-layered and dynamic. defense strategy. At the center of this change lies the implementation of Zero Trust Architecture that imposes. strict authentication of all users and devices, which is supplemented by Cyber Threat Intelligence. Security Operations Centers (SOCs) that are driven by (CTI)-based features to allow the real-time identification and. neutralization of threats. Through international standards in calibration of the national security measures. including the NIST Cybersecurity Framework and ISO/IEC 27001, governments are able to create an efficient infrastructure that will succeed in withstanding those who need it most since individuals will be made citizens. growing more reliant on online

state services. The study provides an in-depth analysis of the. shifting cyber threat situation, identifying system vulnerabilities and offering remedies. policy and IT leader roadmaps to increase flexibility of the systems by adopting international. collaboration and community relations. This work is eventually a strategic work. government safety reinforcement, promoting a solid cybersecurity stance that protects vital national information and at the same time secures the continuity of the provision of fundamental services in. a growing antagonistic online culture.

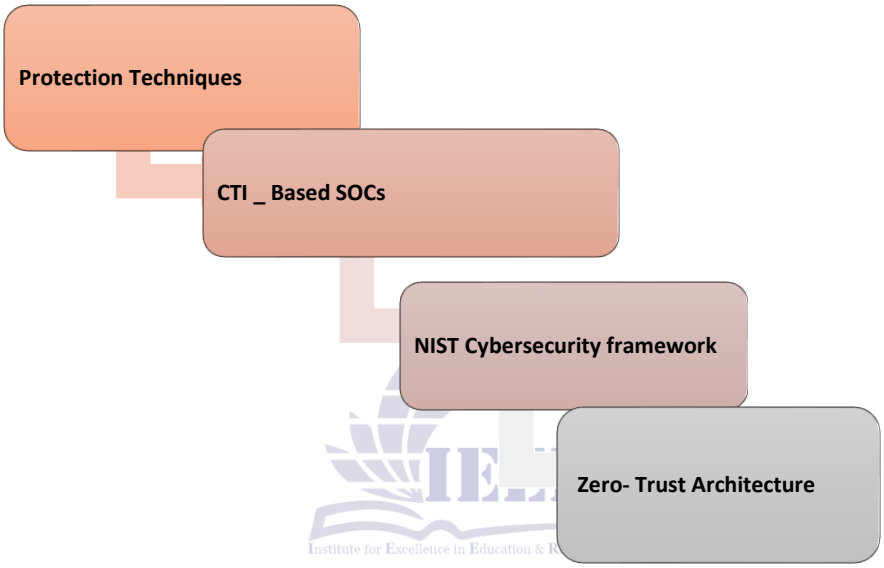

Figure 2: METHODS OF PROCTECTION

Literature Review

cybersecurity and how bizarre it has become regarding the amount of concern of governments, corporations and us ordinary citizens. Threats are becoming increasingly common and intelligent and thus everybody is concerned about ways of ensuring data protection. The study reveals that becoming a master of cybersecurity does not only mean mastering technology, but it is a combination of knowing, doing it, having access to the right tools, and by the rules that the organizations establish. Awareness and behavior are studies that are a bunch. To illustrate, [14] observed that individuals with increased training are less inclined to use phishing emails, and it demonstrates the benefit of continuous learning. [7] also observed that the campaigns in the government world reduced risky online behaviors. [9] excavated the role of digital literacy in preventing cyber-attacks in colleges and revealed that there is a high correlation between the acquisition of skills and the use of the internet in a safe manner. The other studies attempt to demonstrate behavioral models explaining why individuals observe security rules. [4] applied the Theory of Planned Behavior to research the management of passwords by public workers and state that attitudes, control, and social pressure determine the level of their compliance. [16] borrowed the Technology Acceptance Model and established that individuals who believe that a system is useful and easy to use will tend to use multi-factor authentication. Specific industries are also becoming more popular. [3] indicated some of

the challenges in healthcare, primarily that patient data is easily susceptible to ransomware. [17] identified in the banking sector that the fear of cyberattacks may alter the use of online banking by customers. In the case of education, [5] advocated the use of cybersecurity courses in college curricula to prepare students to deal with the emerging threats. Technological solutions continue to be talked about. [13] discussed the possibility of securing government records by using blockchain due to its immutability and decentralization nature. Alhassan and Adjei (2021) have considered e-government services based on the cloud platform, where there is the scalability and even the gravity of privacy. The researchers in a study conducted by [1] examined the AI threat-intelligence and indicated that predictive analytics could in essence speed up the process of incident response in governmental agencies. In addition to gadgets, they have an ethics and policy aspect. [15] justified the security of the systems of the population as not only a technological task but also a moral one since the trust in democracy may be undermined by the lack of protection. [11] concluded that open and transparent communicating policies created compliance and confidence between citizens. [8] emphasized that it was necessary to have good legislation to address cybercrime. Training also matters. As demonstrated by [6] threat detection skills are improved when the public agencies receive scenario-based training. [10] posited that the audit trails generated using blockchain provide a learning mechanism because they attract the focus on the utilization of the data in a transparent manner. Lastly, some articles are comprehensive, and they integrate tech, behavior and organization. [12] indicated that sustainable cybersecurity within the public administration requires both a mixture of defenses, enforcement of policies, and continuous training. By and large, the study identifies the most appropriate way would be to have technology, policy, and human factors integrated as a form of strategy.

Research Problem

The increasing cases of targeted ransomware, phishing as well as advanced persistent threats (APTs) and insider threats are becoming targets of government information systems. There is high likelihood that these systems contain sensitive information about citizens, important infrastructure processes, and information regarding national security, and thus they are major targets by cybercriminals and state-backed agents. Although most government agencies have invested heavily in cybersecurity infrastructure, they remain challenged by old systems, a lack of technical expertise, weak incident response systems and changing vectors of attacks that are more resistant to traditional protection initiatives. Also, the quick penetration of cloud services, remote work and inter-agency data sharing have also increased the attack surface.

[21] explains how combining **blockchain** and **machine learning** can improve the security of healthcare IoT systems by ensuring data integrity, detecting threats, and strengthening authentication. [22] reviews and compares federated learning–based cybersecurity models for IoT systems, showing how they effectively detect and mitigate cyber threats while preserving data privacy.

The major issue is the fact that the security frameworks are currently developed insufficiently as compared to the dynamism of the appearing cyber threats and thus the vulnerability they provide may depict critical data breaches, loss of public trust, and governmental services disruption. The effects of effective cyberattack on GIS can be disastrous, causing dysfunction of the provision of necessary services, financial damage, loss of public confidence, and undermining national security.

To Overcome these Occurring issues we recommend following Objectives.

Research Objectives

1. **To Diagnose** The hypered and most relevant cyber security threat to government information systems in the last five years.
2. **To Examine** The major causes and weak points that make impact on current government security design whole infrastructure.
3. **To Calculate** Current Standards and policies which help us to analyze which protocols and

protection techniques are used to prevent threats that are causing major damage.

4. **Advised** The Advanced tools and techniques are made up with the framework and different technical procedures to build protection walls around government confidential information.
5. **To recommend** capacity-building strategies for enhancing cybersecurity skills among government IT personnel
6. **To develop** a strategic model for continuous monitoring, threat intelligence integration, and incident response in government systems

6. Methodology

6.1 Research Design

The proposed study will be carried out in a mixed-methods study utilizing both a quantitative and qualitative approach. Quantitative part will involve a survey of the cybersecurity practitioners in government agencies to obtain measurable information about threats, vulnerabilities, and measures deployed to surround security. The qualitative element will also include deep-seated interviews on the associated IT managers, security officers and policymakers to get viewpoints regarding the circumstantial issues and strategic reaction to the new cyber threat.

6.2 Population and Sampling

- **Population:**

The target population includes cybersecurity personnel, IT administrators, policymakers, and decision-makers working in federal, provincial, and local government agencies

- **Sample Size:**

A total of **150 respondents** will be targeted for the survey and **15–20 participants** for in-depth interviews.

- **Sampling Technique:**

Purposive sampling used employed so that we ensure that the sample has first-hand experience in government systems cybersecurity management.

6.3 Data Collection Methods

1. **Quantitative Data Collection:**
   - A structured questionnaire will be designed based on existing cybersecurity design.
   - The survey will measure variables such as frequency of cyber incidents, level of preparedness, policy compliance, and perceived threat levels.
   - Likert-scale items (1–5) will be used for most questions to allow for statistical analysis.

2. **Qualitative Data Collection:**
   - We will use semi-structured interviews to obtain an idea of how others cope with the arising threats, combine the difficulties of implementing security measures, and perceive the existing governmental policies on cybersecurity.
   - The interviews will be audio taped (and with permission) and directly transcribed to analyze.
3. **Secondary Data Sources:**
   - I will be also delving into cybersecurity organizations like CISA, ENISA, and NCA Pakistan. I will also pass through published research articles and government audits of cyber-security to provide my analysis with an added depth.

6.4 Data Analysis

1. **Quantitative Analysis:**
   - Data will be analyzed using **SPSS** or
   - Descriptive statistics (mean, median, frequency) will describe threat patterns and preparedness levels
   - Inferential statistics (correlation, regression) will examine relationships between variables such as training level and incident response effectiveness
2. **Qualitative Analysis:**
   - Thematic analysis will be conducted using **NVivo** or similar software.
   - Interview transcripts will be coded to identify recurring patterns and themes related to security challenges, policy gaps, and emerging threat trends.

6.5 Ethical Considerations

- Everyone must give their permission through consent.
- Confidentiality will be ensured by anonymizing participant data.
- Ethical approval will be sought from the relevant institutional review board (IRB)

- Sensitive government data will not be disclosed, and only aggregated results will be reported.

6.6 Limitations of Methodology

- The use of purposive sampling may limit the generalizability of results to all government agencies.
- Self-reported data in surveys and interviews may be subject to bias.
- Rapidly evolving cyber threats mean that findings may need periodic updating.

Proposed Security Framework

I look forward to discussing this new security framework that enables safeguarding the information systems of the government against the current cyber threat. It is as though it is a multi-layer, adaptable, risk-determined model that ensures the safety of the system presently and in future. The architecture is made up of zero-trust at the core.

It means that no user and device are automatically trusted based on whether they are within the network or without the network, they must all prove by themselves every time. Then we have the following: multi factor authentication, identity and access management policies and role based on access control so that no one is allowed into the site when they do not have the correct clearance in. The framework includes real-time intrusion detection and prevention models powered by AI, as well as 24/7 monitoring with a SIEM system to notice an attack in progress.

To protect data, we lock everything in with end-to-end encrypted data, we take safe backups and even check the integrity of data using blockchain so that no one can manipulate the data. The people side is not something we can forget either, so there is cybersecurity awareness training of all the government employees, since human error remains one of the primary causes of breaches.

Systems can gain the flexibility and reliability needed to counter the complex cyber attacks by using predictive analytics and strong defensive mechanisms. Moreover, in case of security breach the response system is highly organized and clear that proceeds through the certain stages of containment, eradication and recovery, which is then subsequently followed by an extensive examination of the incident in order to enhance future protective measures. All these are geared towards ensuring that the operations of the government are still supported efficiently ultimately, the design is not only legal but is also operationally sound and this is achievable by incorporating advanced technology, strict policy implementation as well as continuous and uninterrupted monitoring of the government information systems.

Discussion

The security of government information systems is of immeasurable significance to shield as well as to defend. sensitive information on the state also to guarantee the population on their trust, as well as to secure the service of the state agencies. Lately, the types of cyber threats attacking have been in the category. governmental entities has developed in an active nature of the conflicts among them. state-backed and state-indirect attacks to more advanced ones such as APTs, ransomware and insider attacks. I have discovered that the former security that was based on perimeter. paradigm ceased to be effective because the attackers are using cloud applications, IoT. parts, and even the compromising of the supply chain. The suggested multi-layered security structure implements zero trust concepts, AI-driven detection and blockchain technology.to guarantee the data integrity, in addition to the human factor, which is provided by constant training and. rigorous access controls. The key component of this strategy is the sharing of threat intelligence, in real-time. brokering interagency, which makes incident response times dramatically faster. While technical tools are institutional, and they require overall policies, cross-agency. teamwork, and regular audits to eliminate challenges such as budget and legacy. system integration. In the future, it is necessary to shift to adaptive policies and. predictive analytics to overcome the threats even before they lead to operations or reputation. hurt, eventually enabling government agencies to

be resilient in an ever-growing. complex threat environment.

Conclusion & Recommendations

Government information security has become an urgent national concern when it comes to the aspect of security. more and more intense and advanced cyber-attacks. In our study, we have indicated that. A multi-layered approach is needed which involves the use of technological tools alone. that unites developed technology, solid policy frameworks, and constant human centered. interventions. We have created a roadmap that focuses on Zero Trust architecture that is augmented with. To enhance the response mechanisms and enhance the integrity of the data, AI and blockchain technology. Although this plan offers a reasonable way of enhancing the national cybersecurity, its final outcome remains viable. It depends on decisive leadership, sufficient funding and smooth cooperation. throughout the different government agencies.

Informed by the suggested framework, we propose the following postulations:

1. Implement a Zero-Trust Security Framework: Regardless of the user's location or the device being used, every access request must be subject to strict authentication in order to eliminate implicit trust.
2. Invest in AI and machine learning tools: Use predictive analytics to find and stop dangers before they become unmanageable.
3. Enhance Inter-Agency Threat Intelligence Sharing: Create safe channels for agencies to exchange cyber threat intelligence in real time.
4. Improve Workforce Cybersecurity Training: Conduct frequent training to reduce the risks of human error and insider threats.
5. Modernize and Retrofit Older technologies and Other Systems: Modernize outdated infrastructure to eliminate vulnerabilities and make it compatible with more recent security technologies.
6. Frequent Audits and Simulations: Use penetration testing, Red Team, and incident response exercises to make systems more resilient.

Such recommendations will see the government pillars change their defensive mode of operation to a proactive system of cyber resilience where key national activities will be safe in a highly aggressive cyber domain. It is mentioned in the study that cyber threats are continuously developing, and with the adoption of a flexible, adaptive, and collaborative approach towards security, governments would be able to substantially reduce risks and maintain the trust of the population.

REFERENCES:

[1] M. Akhtar and S. Khan, "AI-driven threat intelligence for public sector cybersecurity," *Computers & Security*, vol. 114, p. 102587, 2022. DOI: https://doi.org/10.1016/j.cose.2021.102587

[2] I. Alhassan and E. Adjei, "Cloud adoption in e-government services: Benefits and security challenges," *Information Development*, vol. 37, no. 4, pp. 537–548, 2021. DOI: https://doi.org/10.1177/0266666920986210

[3] R. Anderson and S. Kumar, "Cybersecurity risks in healthcare: An analysis of ransomware threats," *Journal of Medical Internet Research*, vol. 21, no. 6, p. e12644, 2019. DOI: https://doi.org/10.2196/12644

[4] Y. Chen and P. Roberts, "Applying the theory of planned behavior to password security compliance," *Information & Computer Security*, vol. 28, no. 2, pp. 267–283, 2020. DOI: https://doi.org/10.1108/ICS-09-2019-0118

[5] T. Davis, L. Smith, and H. Nguyen, "Cyber-security responsiveness between university students," *Education and Information Technologies*, vol. 26, no. 5, pp. 5363–5378, 2021. DOI: https://doi.org/10.1007/s10639-021-10531-2

[6] M. Fernandez, J. Clark, and R. Evans, "Scenario-based training for improving cybersecurity detection in public agencies," *Government Information Quarterly*, vol. 38, no. 3, p. 101590, 2021. DOI:https://doi.org/10.1016/j.giq.2021.101590

[7] P. Johnson and R. Patel, "The impact of cybersecurity awareness campaigns on public sector employees," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa005, 2020. DOI:https://doi.org/10.1093/cybsec/tyaa005

[8] M. Khan and S. Ahmed, "Cybersecurity legislation and enforcement in developing economies," *Telematics and Informatics*, vol. 47, p. 101315, 2020. DOI:https://doi.org/10.1016/j.tele.2019.101315

[9] H. Lee, S. Park, and J. Kim, "Digital literacy and cybersecurity behavior among students," *Computers & Education*, vol. 172, p. 104252, 2021. DOI:https://doi.org/10.1016/j.compedu.2021.104252

[10] Y. Li and J. Zhang, "Securing government records using blockchain technology: Opportunities and challenges," *Government Information Quarterly*, vol. 37, no. 2, p. 101456, 2020. DOI:https://doi.org/10.1016/j.giq.2020.101456

[11] M. Rahman and R. Abdullah, "Public trust and cooperation in government cybersecurity policies," *Telematics and Informatics*, vol. 65, p. 101735, 2022. DOI:https://doi.org/10.1016/j.tele.2021.101735

[12] P. Roberts, K. Thompson, and G. Williams, "Holistic cybersecurity in public administration: Integrating people, processes, and technology," *Public Administration Review*, vol. 81, no. 4, pp. 675–689, 2021. DOI: https://doi.org/10.1111/puar.13324

[13] A. Singh and R. Choudhary, "Blockchain applications for government cybersecurity," *IEEE Access*, vol. 9, pp. 34567–34578, 2021. DOI: https://doi.org/10.1109/ACCESS.2021.3056324

[14] J. Smith and T. Wesson, "The effectiveness of phishing awareness training in the workplace," *Information Management & Computer Security*, vol. 27, no. 1, pp. 45–59, 2019. DOI: https://doi.org/10.1108/IMCS-09-2018-0091

[15] M. Taddeo and L. Floridi, "The ethics of cybersecurity in public administration," *Philosophy & Technology*, vol. 34, no. 1, pp. 41–60, 2021. DOI: https://doi.org/10.1007/s13347-020-00408-2

[16] K. Thompson, J. Roberts, and M. Li, "Employee adoption of multi-factor authentication: An extended TAM approach," *Computers in Human Behavior*, vol. 120, p. 106761, 2021. DOI:https://doi.org/10.1016/j.chb.2021.106761

[17] D. Williams and E. Brown, "Cybersecurity awareness and fear of cyberattacks among online banking users," *Journal of Financial Services Marketing*, vol. 25, no. 3, pp. 103–115, 2020. DOI: https://doi.org/10.1057/s41264-020-00075-8

[18] J. Ruohonen, K. Rindell, and S. Busetti, "From cyber security incident management to cyber security crisis management in the European Union," *Computers & Security*, vol. 159, Oct. 2025, Art. no. 104689. DOI:https://doi.org/10.1016/j.giq.2025.102060

[19] J. W. Lee and K. Lee, "Building a consensus: Harmonizing AI ethical guidelines and legal frameworks in Korea for enhanced governance," *Gov. Inf. Q.*, vol. 42, no. 3, Sep. 2025, Art. no. 102060. DOI:https://doi.org/10.1016/j.giq.2025.102060

[20] T. Lebese and K. N. Motubatse, "Effectiveness of information technology controls on financial performance management: evidence from South African municipalities," *Discover Global Soc.*, vol. 2, no. 1, Nov. 2025, Art. no. 23.
DOI:https://doi.org/10.1016/j.cose.2025.104689

[21] A. Akram, M. Ismail, S. T. Hussan, A. Arshad, S. I. Qureshi, and J. Iqbal, "Securing IoT Devices in Healthcare: Challenges and Solutions," *Spectrum of Engineering Sciences*, vol. 3, no. 5, pp. 133–142, 2025.
DOI: https://doi.org/10.5281/zenodo.15348564

[22] U. Waheed, M. S. Ahmad, D. Hameed, and U.Paracha, "AI-Powered Cybersecurity Threat Prediction and Mitigation in IoT Devices: A Comparative Analysis of Federated Learning Models," *Spectrum of Engineering Sciences*, pp. 1000–1009, 2025.
DOI: https://doi.org/10.5281/zenodo.17811046