Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 10, 2025

INVESTIGATING THE IMPACT OF INTERNET OF THINGS (IoT) DEVICES ON NETWORK SECURITY

Umair Paracha[*1], Rana Khaleeq Ahmad[2], Amna Ikram[3], Kashif Lodhi[4]

[*1]*Directorate of ICT, Allama Iqbal Open University, Islamabad*
[2]*Lecturer, Department of Computer Science Faculty of Computing, National University of Modern Languages Multan.*
[3]*Government Sadiq College Women University, Bahawalpur.*
[4]*Dipartimento Di Scienza Applicata E Tecnologia-Collegio Di Ingegneria Chimica E Dei Materiali. Politecnico Di Torino Corso Duca Degli Abruzzi, 24 10129 Torino, (ITALY).*

[*1]umair.paracha@aiou.edu.pk, [2]khaleeq.ahmad@numl.edu.pk, [4]k.lodhi@studenti.unibg.it

DOI: https://doi.org/10.5281/zenodo.17347749

Keywords
Growth, Internet of Things (IoT), devices, automation, connectivity, developing economies, Pakistan.

Article History
Received: 18 July 2025
Accepted: 28 September 2025
Published: 10 October 2025

Corresponding Author: *
Umair Paracha

Abstract
The rapid growth of Internet of Things (IoT) devices has transformed automation and connectivity in various industries, especially in developing economies, such as Pakistan. This growth has also brought various network infrastructure security risks. This research analyzes the impact of IoT devices on the network security of organizations in Pakistan, which focuses on technical risks, challenges during implementation, and the preparedness of the organization. This research fills this gap by utilizing mixed methods, receiving both qualitative and quantitative data from 150 organizations within the telecommunications, banking, healthcare, and manufacturing industries. The research reveals active security gaps; a lack of incorporated countermeasures; and the magnitude of IoT driven cyber incidences. The research demonstrates a lack of organizational security posture on the threats exposed by the IoT. This research serves as a foundation for inform policy formulation, assist organizations in developing security plans, and raising the level of understanding in best security practices on IoT for the digital infrastructure of Pakistan as it seeks to improve automation, and interconnectedness.

INTRODUCTION

The Internet of Things is a new and innovative technology (Duguma and Bai 2024). The Internet of Things Pakistan is driven by operational efficiencies, service delivery improvements, and the growing need for cost-effective solutions. The telecommunications, energy, healthcare, and manufacturing sectors automate and remotely monitor systems, collect real-time data, and deploy IoT devices. Unfortunately, this advancement is taking place without a properly conceived and implemented security plan, putting the organization and the data at risk (Ahmed, Alam et al. 2023).

The potential security risks associated with an organization's adoption of IoT systems are no longer limited to individual devices but include entire networks and an organization's infrastructure as a whole (Khan and Abid , Saleem, Usman et al. 2024). IoT devices are poorly configured and customized security infrastructures, are rarely secured with routine updates, and are poorly authenticated. This makes them particularly vulnerable to attacks, whether they are perpetrated by individual criminals, state actors, or both (Aslam, Aslam et al. 2025). In Pakistan, where the cybersecurity ecosystem is less

developed than in advanced economies, the problem is even worse. The country has been targeted in cyber-attacks that at a minimum include the exploitation of IoT weaknesses in critical infrastructure, the financial sector, and government systems. Furthermore, the systemic nature of IoT infrastructures and ecosystems suggest that a single hacked device can provide unauthorized access to a network in its entirety, exposing sensitive information, and offering the opportunity to disrupt services or inflict severe financial harm (Shah, Hussain Madni et al. 2024).

Pakistani organizations are vulnerable to poorly secured IoT ecosystems. Lack of adequate understanding of IoT threats and poorly developed local technical skills, coupled with underfunded organizational cybersecurity and poorly developed and absent national IoT security standards, leave security gaps (Petrillo, Rehman et al. 2024). The failure of many organizations to complete security assessments and implement IoT system countermeasures to clearance and system deployment is concerning (Aslam, Aslam et al. 2025). The focus placed on reactive rather than proactive security measures create even greater risks with heterogeneous IoT ecosystems made up of devices from multiple manufacturers that have varying levels of security. The lack of precision and predictability that come from absent legal and regulatory measures concerning IoT security result in organizations consistently under-protecting their IoT systems (Mariam, Fiza et al. 2024).

Failures of internet of things (IoT) security breaches not only affect individual businesses but the entire digital economy and the national security framework (Aslam, Kalinaki et al. 2025). Compromised IoT technology poses the threat of stolen data and lost service and accounts for the loss of reputation (Aslam, Aslam et al. 2025). In critical areas such as healthcare and energy, the IoT breaches pose threats to life. Public confidence in digital services may be lost (Farooq 2024). Risks to the national security of most countries are substantial. Pakistan, to a large extent, due to a lack comprehensive research, and most of the literature concentrating on developed countries, has been the beneficiary of such ignorance. The Advanced economies focus on security, technology, and regulation. Pakistan is no-where close to these standards. The current research intends to fill the gap and focus on IoT security breaches and the implications in Pakistan, the weaknesses in context, the preparedness of the organization in the context of IoT security, and the recommended approach to developing the IoT security and systems in the Pakistan context (Jabeen and Ishaq 2024).

Research objectives

1. To determine and understand the system weaknesses and the potential security concerns in relation to IoT devices used and the sectors of telecom, banking, healthcare, and manufacturing in Pakistan.
2. To establish the state when IoT has been protected and state of protective measures, determine and assess the position of the organization in the context of IoT, and the steps for managing potential risks.
3. To formulate tailored recommendations focused on developing IoT security frameworks. Policies and practices should be pastoral considering the organizational contexts, technological environments and the regulations within Pakistan.

Research Questions

1. What are the main technical vulnerabilities and security threats IoT devices pose to the network infrastructure of organizations in Pakistan?
2. What are the existing practices in IoT security and how well do organizations respond to the IoT security risks?
3. What policy and organizational measures are best suited to improve the IoT security in organizations in Pakistan?

Significance of the Study

This research represents the first step towards understanding the implications of IoT security in Pakistan from a holistic organizational and national perspective. The potential risks to organizations and national infrastructure are immense due to digital transformation and increasing IoT adoption in Pakistan, where security research and frameworks are lacking. This study articulates the specific IoT security vulnerabilities within the Pakistani context, looks at the organizational level gaps concerning the

enforcement of security, and the incidence of IoT security breaches and their nature. The insights will shape the policies at the public and organizational levels, prioritize investments in cybersecurity, and raise the level of discourse around IoT security within organizations. The research will be the first to offer baseline evidence on the maturity of IoT security in organizations in Pakistan and key areas where intervention is necessary. With the level of organizational capabilities and the legal frameworks, this will enhance the strategic development of security and the resource allocation in Pakistan.

LITERATURE REVIEW

The Internet of Things (IoT) comprises a growing network of connected devices, sensors, and systems that autonomously gather, analyze, and share data over a network. IoT devices can be as simple as a sensor that tracks environmental data, or as complex as a smart device that controls various elements of an industrial process. There have been remarkable advances in organizational innovation, efficiency, and service improvements in various industries, including healthcare, manufacturing, agriculture, energy, and transportation, due to the proliferation of IoT enabled devices. Nevertheless, the rapid increase in IoT use seems to have left the development of comprehensive and appropriate security provisions lagging. This has led to a situation where large-scale, unregulated, and poorly managed IoT systems pose serious security risks and threats that are poorly managed (Haldorai 2023).

Most IoT devices work with restricted computational resources, limited memory, and minimal processing capabilities, making it impractical to adopt traditional security mechanisms designed for computers and servers, which are typically much larger. These limitations mean that lightweight security protocols must be developed specifically for resource-limited IoT environments (Islam, Bhuiyan et al. 2024). IoT devices often deploy customized proprietary software and hardware, which limits configurational interoperability, making it even harder to adopt generalized security protocols. The heterogeneous nature of IoT ecosystems in and of themselves represent a multitude of challenges, as devices from various manufacturers are designed with differing and conflicting security capacities and standardized implementations. Additionally, for prolonged periods many IoT devices are designed and deployed to be exploit-free and remain un-patched, making the devices susceptible to unaddressed known exploits for long periods of time (Magara and Zhou 2024).

Inadequate methods of authentication and access control pose considerable risks in the realm of IoT (Aslam, Aslam et al. 2025). A considerable number of IoT devices utilize vulnerable, and at times, downright weak, methods of authentication, such as default, and often impossible to change, credentials, hard-coded passwords, and minimal user access settings. Due to the scale at which IoT is deployed, organizations are offered poorly designed credentials focusing on authentication and access control (Khan, Ahmad et al. 2022). The lack of adequate control opens the door to unauthorized access, allowing attackers to take control of devices and to compromise the rest of the network. The other major reason for concern is the lack of security at the network level. IoT devices are connected to and communicate over networks using protocols that lack sufficient encryption, and often basic authentication, when communicating over networks. Sensitive data that is unencrypted is at risk, as are communication protocols that provide opportunities for man-in-the-middle attacks and data manipulation (Singh and Singh 2023).

Within the Internet of Things (IoT) ecosystems, the issues of security and privacy of data remain of paramount importance. As IoT devices capture data related to operations of organizations, user activities, and situational context of the environment, data of a sensitive and personally identifiable nature is included. There is often insufficient comprehensive data protection within organizations, leading to inadequate securing of data during transit, at rest, and during processing. This inadequacy results to leaks of sensitive data, unauthorized access, privacy violation, and breaches of state information. The collection of data by IoT devices also raises issues of surveillance. In Pakistan and in other regions, the inadequacy of state protection of privacy regulations is compounded by the absence, incompleteness, and inadequacy of laws pertaining to data protection and data privacy (Kamarudin, Suhaimi et al. 2024).

The supply chain security risks in IoT ecosystems remain unaddressed. Potential security weaknesses may be intentionally or unintentionally designed into

IoT devices developed by third-party vendors during the fabrication or coding processes. Devices may also encompass counterfeit or inferior security components. In addition, the absence of security oversight from IoT device manufacturers and suppliers renders organizations unable to gauge the security level of devices that have been acquired. When the fabrication, component sourcing, and software engineering of devices takes place in numerous countries and different organizations, the risks of planning supply chain attacks may be heightened. Complexity also results from the need to manage security across multiple jurisdictions (Joshua, Bhattacharyya et al. 2022).

In Pakistan, the complexities surrounding the security issues related to the Internet of Things Technology are magnified by several factors, including the nascent stage of the country's cybersecurity framework, limited technological know-how, restricted existing infrastructure, and the relatively weak comprehensive IoT security policies and supervisory mechanisms. The absence of a comprehensive IoT security policies and supervisory mechanisms (Ullah, Khan et al. 2024). While installing IoT systems, Pakistan's enterprises, spanning all sectors, tend to focus on the security of their operational objectives by sacrificing the security of the IoT systems which leads to the configuration of their systems. With regards to the pace of the IoT systems implementation, the lack of comprehensive policies and the weak supervisory mechanisms in the other systems lead to a habitat with high levels of exposed IoT system vulnerabilities (Khan, Mazhar et al. 2025).

Research Methodology

The researchers adopted the mixed method research design to assess the scope of the impact of IoT security in Pakistan. The quantitative aspect consisted of a structured questionnaire distributed to 150 organizations within the telecom, banking, healthcare, and manufacturing industries. Specifically, the questionnaire assessed the magnitude of IoT security vulnerability and the frequency of security incidents. The quantitative data were categorized per organization and sector, taking into account small (51-250 employees), medium (251-1000 employees), and large (>1000 employees) organization variations for cross comparison. The qualitative aspect included semi-structured interviews with 30 security professionals, IT managers, and decision-makers within the organizations regarding IoT security impediments, organizational competencies, policies that restrict security within the device and context, and factors that affect the enforcement of security. Descriptive statistics were used to analyze the quantitative data, chi-square tests for the associative analysis of the categorical data, and thematic analysis for the qualitative data, focusing on patterns, themes, and contextual factors related to IoT security in Pakistan.

RESULTS AND DATA ANALYSIS

Quantitative Analysis

Table 1: IoT Deployment and Security Infrastructure Across Organizational Sectors in Pakistan

Organizational Sector	Total Organizations	IoT Deployment Rate (%)	Average IoT Devices per Organization	Organizations with Dedicated IoT Security	Security Incidents Reported in Past Year
Telecommunications	38	84.2%	847	8 (21.1%)	18
Banking and Finance	32	65.6%	234	11 (34.4%)	9
Healthcare	35	71.4%	156	7 (20.0%)	14
Manufacturing	45	77.8%	512	9 (20.0%)	24
Total	**150**	**74.7%**	**437**	**35 (23.3%)**	**65**

This table presents IoT deployment characteristics across Pakistani organizations by sector. Telecommunications demonstrate the highest IoT adoption at 84.2%, maintaining average device deployments of 847 devices per organization, reflecting substantial IoT integration within network infrastructure and service delivery operations. Banking and finance, despite lower deployment rates at 65.6%, maintains moderate device quantities averaging 234 devices, indicating selective but strategic IoT implementation focused on transaction security and operational monitoring. Healthcare organizations deploy 156 devices on average, supporting patient monitoring and facility management, while manufacturing sectors deploy 512 devices supporting production monitoring and industrial automation. Notably, only 23.3% of organizations employ dedicated personnel or teams for IoT security, indicating severe organizational capacity limitations. The telecommunications sector particularly demonstrates vulnerability with only 21.1% maintaining dedicated IoT security functions despite highest device deployment rates. Security incident reporting reveals concerning prevalence, with manufacturing reporting highest frequency (24 incidents), followed by telecommunications (18 incidents), suggesting that higher deployment density correlates with increased security event occurrence.

Table 2: Organizational Size and IoT Security Maturity Indicators

Organization Size Category	Number of Organizations	Percentage with IoT Deployment	Average Response Time to Security Incidents (hours)	Organizations with Security Training Programs	Percentage with Vulnerability Assessment Programs
Small (51-250 employees)	42	61.9%	8.5	6 (14.3%)	9.5%
Medium (251-1000 employees)	58	77.6%	5.2	18 (31.0%)	24.8%
Large (>1000 employees)	50	86.0%	2.8	22 (44.0%)	48.0%

Organizational scale significantly influences IoT adoption rates and security maturity. Small organizations demonstrate lowest IoT deployment at 61.9%, with notably prolonged incident response times averaging 8.5 hours, substantially exceeding international benchmarks. This extended response period reflects limited technical resources and emergency response capabilities within smaller organizations. Conversely, large organizations achieve 86.0% IoT deployment rates with incident response times of 2.8 hours, indicating superior technical capabilities and established security operations. Security training programs demonstrate strong correlation with organizational size, with only 14.3% of small organizations implementing such programs compared to 44.0% within large organizations. Vulnerability assessment programs similarly show scale-related variation, with large organizations conducting regular assessments in 48.0% of cases compared to merely 9.5% within small organizations. These findings demonstrate that smaller organizations, despite operating with more limited resources and technical capacity, frequently deploy IoT solutions without corresponding security investments, creating disproportionate risk profiles.

Table 3: Primary IoT Security Challenges Faced by Pakistani Organizations

Security Challenge Category	Percentage of Organizations Identifying Challenge	Priority Ranking (1=Highest Priority)
Lack of Security Expertise	78.7%	1

Inadequate Budget Allocation	71.3%	2
Absent IoT Security Standards	68.9%	3
Device Management Complexity	64.2%	4
Limited Vendor Support	52.1%	5
Regulatory Uncertainty	49.3%	6

Organizations overwhelmingly identify security expertise deficiency as the primary challenge, with 78.7% reporting insufficient internal capacity to implement and maintain effective IoT security measures. This expertise gap reflects broader cybersecurity skills shortages within Pakistan's technology sector and the nascent status of specialized IoT security knowledge within the nation. Inadequate budget allocation represents the second priority concern, cited by 71.3% of organizations, indicating that financial constraints substantially limit organizations' ability to invest in IoT security infrastructure, training, and personnel. The absence of national IoT security standards, identified by 68.9% of organizations, creates ambiguity regarding security requirements and best practices, leaving organizations without clear guidance for developing effective security frameworks. Device management complexity, affecting 64.2% of organizations, reflects challenges inherent to managing heterogeneous IoT ecosystems comprising devices from multiple manufacturers with varying security capabilities. Limited vendor support and regulatory uncertainty round out the primary challenges, acknowledged by 52.1% and 49.3% of organizations respectively, indicating inadequate support mechanisms for organizations attempting to establish effective IoT security programs.

Qualitative Analysis

Theme 1: Organizational Culture and Security Awareness

Interviews show that within Pakistan's enterprises, cultures focus on operational aspects, increasingly considering budget efficiencies and ignoring security, especially when it comes to IoT security. Security professionals repeatedly told us that the higher management considers security to be an operational cost rather than a protective investment, thus leading to restricted budgets, prolonged initiation of enforcement, and a passive approach to the implementation of security measures. IoT devices are often put into circulation and are not taken through security assessments simply because there's a race to deploy the new IoT technology. As prioritizing tech deployment predicts the market, a manager at a telecoms company said, "We are always pressured to roll out new services. Security is an afterthought, and there are gaps in security by the time multiple devices are in use." However, an increasing number of respondents suggested that recent, highly publicized cyber incidents affecting local organizations have begun to change organizational mindsets, resulting in an increasing number of organizations beginning to foundationally align their assessments and budgets around security, especially IoT security. It is noteworthy that the difference in security awareness between larger organizations and smaller organizations poses the greater risk as smaller organizations, particularly those with limited technical resources, are the ones engaging IoT security with the least awareness of the underlying threats and vulnerabilities.

Theme 2: Technical and Resource Limitations

Pakistani organizations report significant technical impediments to the effective implementation of IoT security. Some organizations still maintain legacy systems that cannot be updated to modern security systems; hence the integration of IoT devices into existing security systems becomes increasingly difficult. Respondents also described the diffuse and distributed nature of the ecosystems as a major challenge to securing IoT devices that operate without centralized control and span across multiple geographies. One IT director in the banking sector described the challenge as follows: "We simply do not have the technical infrastructure and the skillset to

monitor thousands of devices that are spread across various branches. Conventional security methods used in the traditional systems do not work, and we are trying to figure this out in in a very painful trial and error process." The problem of inadequate IoT security knowledge in the IT labor force has its roots in the lack of local training and educational resources and the IoT security knowledge gap in Pakistan. Organizations trying to fill the skill gap with outside consultants, often face high costs, and also provide little in the way of long-term, sustainable, and meaningful capacity building. IoT devices and their associated security challenges also pose a problem in the Pakistan context, as local vulnerabilities and organizational characteristics are often neglected in the threat assessments and security solutions that are developed and implemented in the West.

Theme 3: Regulatory and Policy Environment

Pakistani organizations function in an inadequately developed regulatory environment with negligible compulsory IoT security stipulations. According to interview respondents, the lack of definitive IoT security regulations fuels uncertainty around organizational security obligations and the proper levels of security to be implemented. Some organizations opportunistically fill this regulatory void, putting in place the barest security measures possible as legally defensible positions while putting up an elaborate security façade in public. However, respondents more often than not see value in the goals of such regulations as they would provide guiding clarity and perhaps level competitive playing fields. "Clear regulatory requirements would help us justify security investments to senior management. Currently, we must make security decisions largely autonomously without regulatory guidance," said a compliance officer in the banking sector. Several respondents call for the IoT security mandate to be legislated as a government responsibility aligned with Pakistan's technological and organizational capabilities. The lack of national mechanisms for reporting cybersecurity incidents constrains organizations' ability to undertake a more holistic assessment of operational and strategic IoT security threats and learn from IoT security breaches of peers. While the creation of voluntary security standards is weak and underdeveloped in Pakistan, there is potential for this to be done through industry associations.

Theme 4: Financial and Economic Constraints

Within Pakistani organizations, financial limitations act as substantial barriers to the implementation of effective IoT security practices. The first of these barriers is the consistently poor allocation of organizational resources to overall cyber security. Even amongst the various cyber security components, IoT security is the least prioritized. This misallocation of resources is justified by the prevailing belief amongst stakeholders that security investments should be proportional to the costs of losses over time and security incident costs. Respondents pointed out that many IoT security incidents are unreported and unchecked, so the costs that organizations assume and the costs that would be incurred by incidents that are undetected are vastly underestimated. As one operations manager in the manufacturing sector stated: "Current loss data makes it impossible to justify increased security spending. If we had accurate incident reporting across the sector, management would understand the true costs of inadequate IoT security." Many organizations are unable to allocate the financial resources needed to perform adequate device updates, maintain over comprehensive monitoring systems, or employ dedicated IoT security staff. Respondents highlighted the potential positive impact of government support, tax incentives, and subsidized security services on small and mid-size enterprises striving to improve security IoT capabilities.

Theme 5: Vendor Relationships and Supply Chain Security

Not everyone understands the security policies of IoT device manufacturers and suppliers. Some organizations do not consider security as a significant criterion when selecting a vendor, especially smaller organizations that lack procurement experience and focus on cost and functionality. Respondents highlighted the lack of security documentation, the absence of devices' vulnerability explanations, and the late delivery or lack of security updates. A healthcare procurement officer explained, "Vendors rarely provide complete technical documentation or security specifications. We're making security decisions based

on incomplete information." There are reported vendor lock-in scenarios where organizations receive no responsive support on security updates or vulnerability mitigation. Such problematic dynamics foster the desire of organizations to build symbiotic security relationships, and, unfortunately, such relationships are exceedingly rare in the Pakistani context. Collaborative procurement mechanisms would allow organizations to negotiate on upper hand with security provisions. Respondents propose that, due to the lack of proprietary assessments, organizations would benefit from independent security assessments of IoT devices and these vendors funded by commercial organizations.

DISCUSSION

Findings on the level of IoT adoption in the Telecommunication sector of Pakistan as of the year 2023 exhibit trends that show entities leveraging IoT across all 4 major business sectors of Pakistan (Infrastructure/Banking, Telecommunication, Health care, and Manufacturing) and failing to account for the proportional development of IoT safeguards across the multiple business sectors. This oversight results in a significant level of risk presence. 74.7% of the surveyed organizations having access to IoT services shows that IoT is a major part of the digital services offered in Pakistan. However, the finding that less than a quarter (23.3%) of the organizations having personnel dedicated to maintaining IoT security is a glaring sign of the disparity. This imbalance has created organizational ecosystems conducive to the manifestation of security vulnerabilities and the occurrence of multiple 65 reported security cases amongst the 150 organizations surveyed in the instance of Pakistan. Worrisome trends in telecommunication and manufacture sectors which had the most security cases, most cases of the most rapid IoT growth, and most rapid IoT security growth suggest that shifting risk in IoT adoption is directly proportional to the level of security investments to be made. There is a direct risk in IoT levels of comfort offered. These trends as seen in smaller organizations, which statistically has the larger part of the risk profile in Pakistan. Identifying a shortage of expertise in security as a primary concern for organizations is consistent with general cybersecurity workforce challenges in Pakistan and reflects the still-developing status of specialized security knowledge for the IoT sphere. The lack of specialist knowledge within the region is largely a result of the limited IoT security educational and training materials available in the local market. The lack of local IoT security qualified personnel also corresponds to the lack of locally available educational materials. The lack of national standards in IoT security further perpetuates this shortage. Organizations require guidance on defensible and maintainable security control measures and need collaboration. The view of security expenses as operational costs, rather than as an investment to mitigate risks, does explain the organizational financial limitations that result in budget constraints identified as the second most important challenge. However, the findings of this research that show strong connections between the size of organizations and the maturity of their security practices suggests that investments in IoT security will improve incident response and overall security posture of organizations. The concern of regulatory uncertainty reflects the underdeveloped IoT security laws in Pakistan. However, the designed regulations should be appropriate and flexible enough to align with the local technological environment and avoid stifling innovation.

Qualitative insights provide additional context to the quantitative measures on the scales of policies, organizational cultures, and technical constraints around the implementation of security measures for the Internet of Things (IoT). The security of information systems is often subordinated to organizational goals of operational efficiency and the aggressive pursuit of efficiency gains; this is consistent with findings on the business context of Pakistan, where operational technologies are deployed at high speed to maximize competitiveness. Unfortunately, this operational focus permits security exploits with damaging consequences. The observed skill gaps and technical constraints suggest many organizations do not possess the requisite foundational technical security infrastructure and expertise and that meaningful security advancements will require capacity-building investments in security infrastructure. The difficulties in vendor relations, exacerbated by concerns regarding the security of supply chains, point to the necessity of collaboration

between private organizations and the State to institutionalize controls around the IoT devices that are security-sourced at critical supply chain points, as attempts to secure a device after it is deployed in the operational environment are often ineffective or disproportionately costly.

CONCLUSION

This research scopes the extent of IoT security issues within Pakistani organizations in terms of defenses, deployment, security gaps, organizational issues, and security maturity across key economic sectors. The research demonstrates the extent to which Pakistani organizations have implemented IoT technologies for operational efficiencies and competitive advantages, but the absence of security frameworks at the same pace leads to environments with increased security risks and vulnerabilities. The shortage of in-house security expertise and financial investment, in conjunction with the lack of formal national IoT security frameworks, identifies the pivotal organizational issues to implant security effective within IoT. Those organizations with low technical maturity and security-conscious resources are more at risk, especially smaller organizations that activate IoT technologies and retain very basic security resources. The nexus between the size of an organization and the security maturity presents an opportunity to Positively Impact the IoT security environment across the region by working with smaller organizations.

The research findings illustrate the importance of sophisticated policy solutions to address IoT security issues for both the state and the organization. By offering the leadership necessary to set nationally relevant IoT security standards, the state sets the scope of authority, outlines security requirements, and helps the organizations make the case for security savings to stakeholders. There is an urgent need for training institutions and training providers to build faculty and program offerings focused on IoT security to address the training gap. In their roles as industry associations and collaborative frameworks for joint procurement, sharing of threat intelligence, and creation of operational models. Best practices in organizations are still in their infancy and need to strengthen their IoT security governance in the areas of budgeting for security resources, procurement integration of security obligations, security breach detection and response, and remediation of security breach. Rapid technology adoption, security infrastructure, and regulatory frameworks present serious security challenges to organizations and national cyber security. Inaction on the issues outlined will diminish the organizational benefits of IoT technology, and reduce both organizational and national security. Interventions will enhance the organizational and national security posture of Pakistan.

RECOMMENDATIONS

Pakistani entities and public institutions should undertake the formulation and implementation of a full-scale national IoT security policy which includes the setting of standards, guidelines, and regulatory frameworks that are congruent with Pakistan's technology level and organizations' capacities. Government should create specific channels of funding and other financial tools that would allow organizations, particularly the SMEs, to improve IoT security without excessive investments. Stakeholders must close the capacity gap by developing IoT security curricula and training and certification programs. Professional bodies, training institutions and the IoT security community would also help to build the local capacity. Industry bodies should create cooperative frameworks that allow organizations to develop security standards, define requirements for supplier security, and exchange IoT security incident information and emergent vulnerability threat intelligence. Organizations should install governance systems with board accountability for IoT security, allocate resources to implement IoT security, and develop plans for rapid threat detection and remediation. There is insufficient attention to supply chain security which is a responsibility of the organization and the government. Governments should provide mechanisms to enforce standards of security in IoT devices during the consolidation and transport of devices. Organizations should implement a policy of security assessments of their vendors.

REFERENCES

Ahmed, S. F., et al. (2023). "Industrial Internet of Things enabled technologies, challenges, and future directions." Computers and Electrical Engineering 110: 108847.

Aslam, M. M., et al. (2025). "Social Engineering Attacks in Industrial Internet of Things and Smart Industry: Detection and Prevention." Emerging Threats and Countermeasures in Cybersecurity: 389-412.

Aslam, M. W., et al. (2025). "ADVANCEMENTS IN MEDICAL IMAGING FROM TRADITIONAL TECHNIQUES TO AI-DRIVEN INNOVATIONS."

Aslam, M. W., et al. (2025). "A COMPREHENSIVE REVIEW OF WEARABLE HEALTH DEVICES: ADVANCES, CHALLENGES, AND FUTURE DIRECTIONS."

Aslam, M. W., et al. (2025). "FINANCIAL FEASIBILITY OF IMPLEMENTING SMART SAFETY TECHNOLOGIES IN ELECTRICAL ENGINEERING PROJECTS: A REVIEW OF CURRENT STATUS AND FUTURE PROSPECTS." Spectrum of Engineering Sciences 3(3): 557-567.

Aslam, M. W., et al. (2025). "THE ROLE OF ARTIFICIAL INTELLIGENCE IN ELECTRICAL ENGINEERING APPLICATIONS IN SMART GRIDS, POWER SYSTEMS, AND AUTOMATION." Spectrum of Engineering Sciences 3(3): 540-556.

Duguma, A. L. and X. Bai (2024). "How the internet of things technology improves agricultural efficiency." Artificial Intelligence Review 58(2): 63.

Farooq, A. (2024). "EXPLORING THE ROLE OF IOT IN SMART CITIES: INNOVATIONS IN URBAN INFRASTRUCTURE AND CONNECTIVITY." Scientific Insights and Perspectives 1(02): 147-158.

Haldorai, A. (2023). "A review on artificial intelligence in internet of things and cyber physical systems." Journal of Computing and Natural Science 3(1): 012-023.

Islam, Z., et al. (2024). "Gravitating towards internet of things: Prospective applications, challenges, and solutions of using IoT." International Journal of Religion 5(2): 436-451.

Jabeen, M. and K. Ishaq (2024). "Adoption of Internet of Things in Telecommunications: An Emerging Market Case." International Journal of Innovation and Technology Management 21(03): 2450020.

Joshua, E. S. N., et al. (2022). Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: a complete systematic approach. Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems, Elsevier: 291-310.

Kamarudin, N. H., et al. (2024). "Exploring authentication paradigms in the internet of things: A comprehensive scoping review." Symmetry 16(2): 171.

Khan, A., et al. (2022). "Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends." Complex & Intelligent Systems 8(5): 3919-3941.

Khan, M. H. A. and F. Abid "Future Landscape, Challenges, and The Role of the Internet of Things (IoT) in Empowering Sustainable Development Goals (SDGs) in Pakistan."

Khan, S., et al. (2025). "Integrating IoT and WSN: Enhancing quality of service through energy efficiency, scalability, and secure communication in smart systems." Peer-to-Peer Networking and Applications 18(5): 249.

Magara, T. and Y. Zhou (2024). "Internet of things (IoT) of smart homes: privacy and security." Journal of Electrical and Computer Engineering 2024(1): 7716956.

Mariam, H., et al. (2024). "Exploiting Internet of Things to address climate change: Case study and analysis on the perception of stakeholders in Pakistan." Journal of Climate and Community Development 3(2): 264-285.

Petrillo, A., et al. (2024). "Digital and sustainable transition in textile industry through Internet of Things technologies: A Pakistani case study." Applied Sciences 14(13): 5380.

Saleem, M. U., et al. (2024). "Smarter grid in the 5G era: Integrating the internet of things with a

cyber-physical system." IEEE Access 12: 34002-34018.

Shah, S., et al. (2024). "Factors influencing the adoption of industrial internet of things for the manufacturing and production small and medium enterprises in developing countries." IET Collaborative Intelligent Manufacturing 6(1): e12093.

Singh, I. and B. Singh (2023). "Access management of IoT devices using access control mechanism and decentralized authentication: A review." Measurement: Sensors 25: 100591.

Ullah, I., et al. (2024). Future communication systems using artificial intelligence, internet of things and data science, CRC Press.