ACADEMIA International Journal for Social Sciences
Volume 4, Issue 4, 2025 ISSN-L (Online): 3006-6638

Cybersecurity Threats in Cloud Computing: A Study On Cloud-Based Security Solutions

Nisar Ahmed Memon
nisar.memon@usindh.edu.pk
Assistant Professor, Department of Telecommunication Engineering, Faculty of Engineering and Technology, University of Sindh Jamshoro

Ziyad Abdullah
za23ahf@herts.ac.uk
Computers and Networks Engineering University of Hertfordshire United Kingdom

Sana Wajid
sanawajid95@yahoo.com
Software Engineer, Interior Ministry of Pakistan
Corresponding Author: * Nisar Ahmed Memon nisar.memon@usindh.edu.pk

Received: 16-08-2025 **Revised:** 22-09-2025 **Accepted:** 17-10-2025 **Published:** 02-11-2025

ABSTRACT

This study explored cloud computing security threats and evaluated cloud security offered solutions in Pakistan. The study was based on a mixed-method study design. The quantitative component was extracted from 200 IT security experts employed in the banking, healthcare, education, and telecommunications industries, while the qualitative component was based on 25 cloud security professionals located in Karachi, Lahore, and Islamabad. Secondary data was information from the literature and cloud security related case studies in Pakistan from the years 2020 through 2024. The study investigated multiple models of cloud services and the common threats such as data breaches, account hijacking, distributed denial of service (DDoS) attacks, and issues of compliance in relation to the regulatory environment in Pakistan. The quantitative data which was analyzed through the use of the SPSS software, showed various threats and security measures to be implemented. The qualitative data provided contextual invaluable insights on security measures that could be employed given the available infrastructures. The results suggest that cloud security within Pakistan was the result of weak security policies, low cloud security awareness, and limited organizational resources. The study suggested the use of internationally accepted security standards, layered security systems, routine security checks, and user training as the best practices. This work highlights the security practices that Pakistan organizations need to consider while adopting cloud computing in order to counter the potential cyber threats.

Keywords: *Cloud computing, security threats, cloud security, IT security, industries, Pakistan.*

INTRODUCTION

Data management in different regions of the world changed with the introduction of cloud computing. As the world moved towards the use of cloud technologies, Pakistan, too, started adopting cloud computing technologies (Sandhu 2021). Over the last decade cloud technologies and computing facilities integration started quickly. Organizations within the telecommunications, banking, healthcare, and educational sectors started focusing their digital transformations and computing facility integrations towards the cloud. Consequently, the desire for operational and cost efficiency within the cloud computing facility integration started the move towards the digital transformation. Unfortunately, the move faced serious digital and data security issues. The cloud computing security model- where both the provider and the client are responsible- poses a unique and proactive facility security model (Gupta, Mazumdar et al. 2023).

Pakistan's unique challenges regarding the implementation of cloud security include a lack of awareness regarding the importance of cybersecurity, a poor legal framework, an absence of security professionals, and resource scarcity of organizations (Khan, Raza et al. 2021). Organizations in Pakistan's cloud environment faced a number of security challenges, including unauthorized system access, data breaches, account takeovers, denial-of-service attacks, malware, and threats from within the organization. Such challenges directly affected several critical organizational functions including operations, trust from customers and clients, and compliance with the law. The sophistication of attacks from cybercriminals and state-sponsored actors required organizations to implement advanced solutions capable of protecting numerous interrelated security gaps. The problematic security situation in the cloud environment is exacerbated by the cloud's flexible, multi-tenancy, and geographically distributed data architecture (Ahmad, Rasool et al. 2021).

The protective measures include encryption, intrusion detection and prevention systems, identity and access management systems, security information and event management systems, and data loss prevention systems. Organizations in Pakistan were unable to select and implement security measures largely due to budget constraints, inadequate cloud security knowledge, and insufficient technical expertise. These gaps were due to over-reliance on cloud service provider's security measures. Without any additional organizational security controls, these measures created gaps for cybercriminals to exploit. The lack of tailored security frameworks for cloud technology further limited the implementation of effective security structures (Mehmood 2025).

The need to understand Pakistan-organizations specific cybersecurity threats and assess how effectively cloud-based security systems accommodate these threats is how the significance of the research emerged. Earlier, established cloud security research focused only on more developed countries with advanced cybersecurity infrastructures and developed regulations. Before this research, the analysis of cloud security challenges in Pakistan and developing countries was limited. Organizations in these developing countries faced different challenges and worked in different regulations (Qasim, Ahmad et al. 2025). This research filled the gap with first-hand evidence on the cybersecurity threats Pakistani organizations face and the security measures used to address these threats. The results added to the understanding of cloud security within the context of developing countries and advanced practical implications for organizations in Pakistan looking to strengthen their cloud security systems (Saleem, Ahmed et al. 2024).

The various cloud service models adopted by organizations in Pakistan, particularly Infrastructure as a Service, Platform as a Service, and Software as a Service, were studied. Each service model had customization security difficulties that required bespoke security measures. Infrastructure as a Service had the most control, but organizations had to defend multiple security levels. Platform as a Service lessened the management of the infrastructure but increased reliance on the provider's security controls, which poses security risks (Iqbal and us Shan 2024). Software as a Service shifted most security responsibilities away from the user and to the provider, but the user's control over security and customization was greatly diminished. Organizations were able to adopt and secure cloud services in a manner that matched their needs and risk profile following the assessment of the various cloud service models and their associated security risks (Kausar, Leghari et al. 2023).

Research Objectives

1. To explore and detail the key cybersecurity risks in cloud computing faced by organizations in Pakistan from various industries, such as banking, healthcare, education, and telecom.
2. To assess the protective capacity of the cloud security controls that Pakistani organizations implemented in response to the identified cyber security risks to sensitive organizational data.

3. To propose practical improvements to cloud security in Pakistani organizations based on the adoption of suitable security frameworks, technologies, and policies.

Research Questions

1. What types of cybersecurity threats are the most common amongst Pakistani cloud users across diverse industries?
2. How successful are the cloud security measures used by Pakistani organizations in avoiding and addressing cybersecurity threats?
3. Which security models, technologies, and practices should Pakistani organizations implement to bolster their cloud security and defend against advanced cyber threats?

Significance of the Study

This study, the first of its kind on empirical research on cloud security in Pakistan, lay the groundwork for understanding the security challenges of the cloud within Pakistan's unique context. For organizations in Pakistan moving to the cloud, the research offered insights on the threats they are likely to face and the well-matched security solutions, considering the available infrastructure and resource challenges. For stakeholders such as organizational leaders, professionals in IT security, and cloud service providers, the research outlined the measures essential in safeguarding sensitive data and avoiding the cloud security compliance penalties. The research also addressed the gap in IT cloud security in developing countries by documenting the distinctive Pakistani organizational challenges. The unique challenges outlined helped in developing recommendations that formed the tailored security policies and frameworks which Pakistani organizations can implement in their operations to comply with global security practices and standards.

LITERATURE REVIEW

In the context of computer technology Cloud computing is delivering a new model for constructing IT infrastructure globally. Organizations of all types and sizes have been drawn to the advantages Cloud computing supports documented in the literature, including lowered costs, increased collaboration, and improved adaptability. Yet, the most important factor for Cloud computing widespread adoption remains the lack of perceived security in the Cloud and worries of data confidentiality and compliance. This is where shared responsibility models and the lack of clarification on security responsibilities create gaps in Cloud protections and business. For organizations misunderstanding the model, particularly those lacking expertise in Cloud technology, the gaps can be substantial and present dangerous entry points for cybercriminals (Alam 2021). Cloud technology research points in the direction of security misconfiguration and the considerable amount of data breaches as a highly relevant issue in the organization’s responsibility to secure their infrastructure (Matthew, Kazaure et al. 2021).

The escalation of cybersecurity threats within the domain of cloud computing persisted alongside the adoption of new attack methodologies to leverage cloud infrastructure weaknesses. One of the most significant threats was the data breach. Attackers infiltrated the systems of organizations and acquired, removed, or revealed sensitive data, including customer information, financial data, and proprietary information. Weak authentication processes, poorly defined access controls, unaddressed system vulnerabilities, and threats posed by insiders facilitated such breaches. Account hijacking became another significant threat as attackers gained unauthorized access to cloud systems by acquiring user credentials through phishing, credential stuffing, and password guessing. Once attackers acquired these accounts, they could cut out and erase critical data, cripple access to services, and undermine other accounts. Distributed denial of service attacks targeted cloud infrastructure to cause an outage by bombarding the system with an avalanche of requests coming from several locations (Wu and Plakhtii 2021).

The multi-tenancy framework in cloud computing created new security issues due to several customers using the same physical infrastructure. This setup can expose weaknesses that allow malicious actors to enter and obtain sensitive information belonging to other tenants. Side-channel attacks utilized shared resources to gain access to and extract confidential data from adjacent virtual machines using timing and resource consumption metrics. Threats to cloud systems arose when corporations neglected to secure their APIs by employing inadequate client authentication, access control, and data encryption. In cloud environments, infections by malware and ransomware can paralyze virtual machines and containers, encrypt data, and force payment for decryption keys. Service provider failure, natural disaster, malicious, and accidental deletion causes data loss. This emphasizes the importance of employing suitable backup, recovery, and disaster recovery frameworks (Hashim and Hussein 2024).

Cloud-focused security methodologies have adapted to protect the dynamic and distributed contexts within the respective Cloud environments. Building on previous work in encryption technology, confidentiality and access control policies in Identity and Access Management Systems and Multi-Factor Authentication frameworks ensured that even authorized pupils could not access sensitive information. Unauthorized interception of transmitted data remained a concern, thus data shredders erased sensitive information prior to the termination of a user session. Role-based access control, single sign-on, and selective fusion of data streams revealed information to only the deserving parties. Automated compliance frameworks also used encryption to control the movement of data in and out of the systems, thus applying data loss prevention policies. USB interface shredders have also become the norm to control the locomotive movement of data. Intrusion detection and prevention systems, enabled compromised user session identification and active machine association. They examined the session, cross-analyzed the tokens used, and lifted the policy to scan for passive session tokens. Ensuring control of compromised tokens needed shredders and other data loss prevention policies to ensure encryption and control automated compliance (Chippagiri 2025). Automated compliance frameworks also used encryption to control the movement of data in and out of the systems, thus applying data loss prevention policies. USB interface shredders have also become the norm to control the locomotive movement of data. Intrusion detection and prevention systems, enabled compromised user session identification and active machine association. They examined the session, cross-analyzed the tokens used, and lifted the policy to scan for passive session tokens. Ensuring control of compromised tokens needed shredders and other data loss prevention policies to ensure encryption and control automated compliance. Automated compliance frameworks also used encryption to control the movement of data in and out of the systems, thus applying data loss prevention policies. USB interface shredders have also become the norm to control the locomotive movement of data. Intrusion detection and prevention systems, enabled compromised user session identification and active machine association. They examined the session, cross-analyzed the tokens used, and lifted the policy to scan for passive session tokens. Ensuring control of compromised tokens needed shredders and other data loss prevention policies to ensure encryption and control automated compliance (Waghmare, Khandve et al. 2021).

In developing countries, studies focused on cloud security highlighted problems that are different from those in developed countries. In developing countries, business leaders may have little awareness of cybersecurity risks and therefore overlook the need for adequate funding and prioritization of security activities. The difficulty of implementing and maintaining advanced security measures due to the lack of qualified personnel in the field of security exacerbates the situation. Weak security practices are in part perpetuated by inadequate regulatory frameworks and the lack of enforcement that could drive organizations to adopt better security practices (Aderibigbe, Ohenhen et al. 2023). When there are limitations in infrastructure, such as weak and unreliable internet and power, the capabilities for security monitoring and incident response are adversely impacted. In cultures where short-term operational goals are prioritized, security investments are postponed, and this may explain some organizational practices

seen in developing countries. As regulatory compliance burdens increase and the risk of cyberattacks escalates, there are definable and growing security risk practices that cloud security in developing countries complies with. These organizations require default security practices that are responsive to the local context to effectively secure their cloud assets, while still adhering to the international standards and best practices that the literature outlines (Saleem, Ahmed et al. 2024).

RESEARCH METHODOLOGY

The researchers adopted the mixed-methods approach to explore the scope of cyber-attacks on cloud computing technology and evaluate the cloud security technology case study in Pakistan at both qualitative and quantitative levels. It involved the distribution of quantitative surveys to 200 IT security professionals in the banking and healthcare sectors, and the education and telecommunications industries, and semi-structured qualitative interviews with 25 cloud security experts based in Karachi, Lahore, and Islamabad. Primary data was also complemented by a review of the literature, which consisted of scholarly articles, business insights, and technically oriented analyses of client reports and case studies of cloud security breach reports within Pakistan from 2020 to 2024. Likewise, the researcher explored the various models of cloud services (IaaS, PaaS, SaaS) used by the targeted Pakistani businesses and examined the threats posed by data breaches, hijacking, DDoS attacks, and compliance within the Pakistani legal framework. To assess the quantitative data, correlation and pattern analyses on the various cyber-attack types and the security levels in the Pakistani establishments was carried out using the SPSS software, while for the qualitative data from the interviews, thematic coding was conducted to ascertain expert views on practical security options that could work for the local infrastructure and resources. The study also included a comparative analysis of the cloud security paradigms used by Pakistani institutions with the encryption technologies, multi-factor authentication, and intrusion detection systems. Confidentiality of the participants as well as the organizations was observed throughout the research, and the necessary permissions of the relevant institutions were secured.

RESULTS AND DATA ANALYSIS

Quantitative Analysis

The quantitative analysis examined survey responses from 200 IT security professionals working in Pakistani organizations to identify cybersecurity threats and evaluate security solution effectiveness. The data collected through structured questionnaires was analyzed using SPSS software to generate descriptive statistics, frequency distributions, and correlation analyses that revealed important patterns regarding cloud security practices in Pakistani organizations.

Table 1: Distribution of Respondents by Sector

Sector	Frequency	Percentage
Banking	65	32.5%
Healthcare	48	24.0%
Education	42	21.0%
Telecommunications	45	22.5%
Total	200	100%

The sectoral distribution of respondents indicated that banking sector represented the largest proportion at 32.5 percent followed by healthcare at 24 percent, telecommunications at 22.5 percent, and education at 21 percent. This distribution reflected the varying levels of cloud adoption across different sectors in

Pakistan where banking institutions led digital transformation initiatives due to competitive pressures and customer expectations. Healthcare organizations increasingly adopted cloud solutions for electronic health records and telemedicine applications. Educational institutions utilized cloud platforms for learning management systems and administrative functions. Telecommunications companies leveraged cloud infrastructure to deliver services efficiently. The relatively balanced distribution across sectors enabled comprehensive analysis of cloud security practices across diverse organizational contexts.

Table 2: Prevalence of Cybersecurity Threats

Threat Type	Very High	High	Moderate	Low	Mean Score
Data Breaches	78 (39%)	85 (42.5%)	30 (15%)	7 (3.5%)	4.17
Account Hijacking	65 (32.5%)	82 (41%)	43 (21.5%)	10 (5%)	4.01
DDoS Attacks	52 (26%)	71 (35.5%)	58 (29%)	19 (9.5%)	3.78
Malware Infections	48 (24%)	68 (34%)	63 (31.5%)	21 (10.5%)	3.71
Insider Threats	42 (21%)	61 (30.5%)	72 (36%)	25 (12.5%)	3.60
API Vulnerabilities	38 (19%)	58 (29%)	78 (39%)	26 (13%)	3.54

The threat prevalence analysis revealed that data breaches represented the most critical concern with a mean score of 4.17 where 81.5 percent of respondents rated it as high or very high threat. Account hijacking emerged as the second most prevalent threat with a mean score of 4.01 and 73.5 percent rating it as high or very high. Distributed denial of service attacks, malware infections, insider threats, and application programming interface vulnerabilities followed in descending order of prevalence. These findings indicated that Pakistani organizations faced multiple sophisticated threats requiring comprehensive security approaches. The high prevalence of data breaches and account hijacking emphasized the critical need for robust access controls, encryption, and authentication mechanisms to protect sensitive organizational data and prevent unauthorized access.

Table 3: Implementation Status of Security Solutions

Security Solution	Fully Implemented	Partially Implemented	Planning	Not Implemented
Encryption	112 (56%)	58 (29%)	22 (11%)	8 (4%)
Multi-Factor Authentication	95 (47.5%)	68 (34%)	28 (14%)	9 (4.5%)
Intrusion Detection Systems	78 (39%)	72 (36%)	38 (19%)	12 (6%)
SIEM Platforms	62 (31%)	71 (35.5%)	48 (24%)	19 (9.5%)
Data Loss Prevention	58 (29%)	68 (34%)	52 (26%)	22 (11%)
Security Audits	52 (26%)	81 (40.5%)	47 (23.5%)	20 (10%)

The security solution implementation analysis demonstrated varying adoption levels across different technologies. Encryption showed the highest full implementation rate at 56 percent followed by multi-factor authentication at 47.5 percent, reflecting recognition of their fundamental importance for data protection and access control. Intrusion detection systems, security information and event management platforms, data loss prevention tools, and regular security audits showed lower full implementation rates ranging from 26 to 39 percent. A significant proportion of organizations partially implemented these solutions, indicating resource constraints, technical challenges, or gradual deployment approaches. The findings revealed implementation gaps particularly for advanced security solutions requiring specialized

expertise and significant investments, highlighting the need for capacity building and resource allocation to strengthen organizational security postures comprehensively.

Table 4: Challenges in Cloud Security Implementation

Challenge	Very Significant	Significant	Moderate	Minor
Limited Budget	89 (44.5%)	76 (38%)	28 (14%)	7 (3.5%)
Shortage of Skilled Personnel	82 (41%)	81 (40.5%)	30 (15%)	7 (3.5%)
Lack of Awareness	76 (38%)	78 (39%)	36 (18%)	10 (5%)
Insufficient Security Policies	71 (35.5%)	82 (41%)	38 (19%)	9 (4.5%)
Compliance Requirements	65 (32.5%)	75 (37.5%)	48 (24%)	12 (6%)
Vendor Lock-in Concerns	48 (24%)	68 (34%)	62 (31%)	22 (11%)

The challenges analysis identified limited budget as the most significant barrier with 82.5 percent of respondents rating it as significant or very significant, reflecting resource constraints faced by many Pakistani organizations. Shortage of skilled security personnel emerged as another critical challenge with 81.5 percent rating it as significant or very significant, indicating the cybersecurity talent gap in Pakistan. Lack of awareness among organizational leadership and staff, insufficient security policies, and compliance requirements represented additional significant challenges. Vendor lock-in concerns showed relatively lower significance levels. These findings highlighted systemic issues requiring multi-stakeholder interventions including government support for cybersecurity education, industry investment in training programs, and organizational commitment to security initiatives. Addressing these challenges required coordinated efforts to build cybersecurity capacity and foster security-conscious organizational cultures.

Table 5: Effectiveness of Implemented Security Solutions

Security Solution	Very Effective	Effective	Moderately Effective	Ineffective
Encryption	92 (54.1%)	64 (37.6%)	12 (7.1%)	2 (1.2%)
Multi-Factor Authentication	85 (52.1%)	58 (35.6%)	17 (10.4%)	3 (1.8%)
Intrusion Detection Systems	68 (45.3%)	62 (41.3%)	17 (11.3%)	3 (2%)
SIEM Platforms	58 (43.6%)	54 (40.6%)	18 (13.5%)	3 (2.3%)
Data Loss Prevention	52 (41.3%)	56 (44.4%)	15 (11.9%)	3 (2.4%)

The effectiveness evaluation examined perceptions of organizations that implemented various security solutions. Encryption demonstrated the highest effectiveness rating with 91.7 percent of implementing organizations rating it as effective or very effective, confirming its fundamental role in data protection. Multi-factor authentication showed similar effectiveness levels at 87.7 percent, validating its importance for preventing unauthorized access. Intrusion detection systems, security information and event management platforms, and data loss prevention tools showed effectiveness ratings ranging from 84 to 86.6 percent among implementing organizations. The generally high effectiveness ratings indicated that properly implemented security solutions significantly enhanced organizational security postures. However, the moderate effectiveness ratings by some respondents suggested implementation quality variations,

emphasizing the importance of proper configuration, continuous monitoring, and regular updates to maximize security solution effectiveness.

Qualitative Analysis

Qualitative analysis focused on understanding threats and countermeasures in the cybersecurity landscape of organizations in Pakistan and involved interviews with 25 experts in the field. The interviews were analyzed thematically and 6 broad themes were identified. These were the themes within the experts discoursing on the issues around cloud security and the possible ways to address them.

Theme 1: Inadequate Security Awareness and Training

The experts pointed out and explained that the absence of security awareness training and the overall awareness of organizational leadership and employees in the entire organizational vertical and the lack of security resources in volunteer organizations amounted to the ineffective and poorly defined organizational security resources. Decision makers in management and security volunteers poorly defined and explained organizational security resources and training to staff. Employees exhibited security negligence and participated in security risky behaviors which included collaboration in unauthorized access of organizational resources, illicit credential sharing, phishing and the use of weak and easily guessed passwords. Organizations and staff teaching security awareness neglect to provide and teach staff security awareness systems on a regular basis, leaving them security awareness training to focus on a couple of mass simulated phishing exercises. These deficiencies and gaps in organizational and staff security training and awareness neglected organizational hierarchy from commandeering to the lowest levels.

Theme 2: Reactive Rather Than Proactive Security Approaches

Pakistani enterprises largely apply reactive security approaches, wherein security is deployed purely in response to incidents, or only within the confines of the legal minimum requirements. Business executives in Pakistan tend to approach security as a necessary expense, rather than as a strategic component of a business. Because of this approach, security expenditures tend to be reactive and event-driven, i.e., a business incident will be security gated, and to address short-term business security, a security solution that only addresses the business incident and does not consider long-term security integration is deployed. This absence of an integrated risk management approach enables and emboldens attackers to exploit the security incident and exposes the organization to an increased risk of liability. Security experts in the region stress the need and value to mitigate the risk of an incident by proactively designing threat-driven risk management controls and security systems. Advanced and integrated security systems, as described above, would allow organizations to pinpoint problem areas before attackers do. This advanced integrated approach dramatically increases the effectiveness of an organization's security and decreases the probability of, and the impact of, a security breach incident.

Theme 3: Insufficient Integration of Security in Development Processes

Experts have stressed the need to address the lack of coordinated security within software development and systems deployment processes in the Pakistani context. Several organizations viewed security as a peripheral consideration during the later stages of deployment instead of a primary aspect in each phase of the development lifecycle. Developers, in many cases, did not receive adequate training in security and thus applied weak coding practices, thereby creating vulnerabilities like SQL injection, cross-site scripting, and insecure authentication. Most organizations also did not identify security gaps prior to deployment through code reviews, static or dynamic testing. The rapid deployment of DevOps practices without embedding security provisions contributed further to the problem as organizations focused on

speed rather than security. Experts called for the adoption of DevOps practices in which security is embedded in all phases of development pipelines through automated testing, continuous monitoring, and the articulation of security requirements during the design phase of development. This approach of 'shift-left' security facilitates the discovery and resolution of security vulnerabilities early in the development phase, thus alleviating a significant part of the cost and risk associated with securing a product post-deployment. Most importantly, it facilitates the rapid pace of development.

Theme 4: Dependency on Provider Security Without Adequate Organizational Controls

Organizations have shown a lack of organizational-level controls sufficient to protect their assets and organizational specific security needs yet described CSP security controls as overly protective. Experts find that gaps related to breaches of an organization's data classification, access controls, application security, and employee training may derive from organizations misunderstanding the implications of the shared responsibility model and the assumption that CSP security controls are sufficient. Organizations appear to lack an understanding of the security feature configurations of the CSP, as organizations leave features on default settings that may not coincide with organizational security policies. A lack of visibility of security practices of CSP, and the controls thereof, leads to an inability to determine the actual security posture of the organization, as well as compliance with regulatory requirements. Experts have suggested that organizations perform necessary due diligence on potential cloud providers, understand the boundaries of responsibility, implement organizational security controls that work with the protective measures of providers, and ensure security configurations are subject to continuous surveillance and compliance enforcement.

Theme 5: Resource Constraints Impacting Security Implementation

Particularly among small to mid-sized enterprises, the absence of financial and personnel resources resulted in the over-constrained implementation of cloud security across organizations in Pakistan. Even organizations that recognized the importance of security provisions offered in the cloud, and the need to make arrangements for the allocation of budgetary resources, security provisions offered in the cloud remained unimplemented. With the ever-growing demand for cybersecurity practitioners leaving many organizations in Pakistan without the required personnel for understaffed security positions, security functions became even more expensive to acquire. Competitively assigned security responsibilities to in-house IT personnel without the requisite skills resulted in dysfunctional security implementations and prolonged response times to security events. Resource constraints resulted in organizations having to choose between operational requirements and security enhancements which, in the majority of cases, resulted in detrimental operational impacts. Resource constraints prompted the need for even greater organizational security to adopt economically viable security strategies utilizing open-source security utilities, cloud-native security provisions, and automation. Security-related regional collaboration and inter-organizational synergies could help alleviate the lack of resources.

Theme 6: Inadequate Incident Response Capabilities

Pakistani organizations seemed to exhibit egregious failures in the ability to respond to incidents whereby they are expected to identify, isolate, and, eventually, recover from breaches in security protocols. Professionals in the field claimed to be seeing organizations without even rudimentary incident response documents outlining each personnel assigned tasks and communications expectancy protocols. Furthermore, organizations did not appear to be engaging in incident response practice drills of any sort. The attempt to capture security incidents in real time was further hampered by the absence of security monitoring and logging. This failure in security logging and monitoring allowed criminals prolonged entry into the compromised system, to gain further resources and to illegally transfer even more data.

Organizations did not seem to capture, also, the essential elements of the incident, missing tools for containment, forensic analysis, and evidence collection. The absence of, for example, adequate disaster recovery plans simply prolonged the time and effort needed to recover critical services. The construction of comprehensive incident response plans was, thus, deemed critical: the acquisition of security operations centers, or the subscription to managed detection and response services, the completion of logging and monitoring, routine incident response drills, and the recovery provision. This, in effect, would be expected to minimize the impact of incidents and restore normal business operations.

DISCUSSION

Limited awareness, inadequate resources, and a reactive approach toward securing cloud environments were the most important obstacles that organizations in Pakistan faced while trying to adopt protective measures for cloud-based environments. Organizations struggling with data breaches and account hijacking lacked sufficient data access controls and sufficient data protective measures. Most organizations went only as far as implementing the basics in protective measures, such as encryption and multi-factor authentication, while advanced security measures that demand high-level expertise remained unimplemented. The challenges analysis made it clear that budget constraints and the unavailability of qualified personnel for developing comprehensive protective measures are prevalent even in the developing world. Qualitative evidence underscored that culture, commitment of leadership, and a proactive approach to security, as opposed to just technology deployment, are equally important for efficient cloud security management.

Appraisal of the security solutions already put in place showed that well-configured systems substantially improved organizations' security postures relative to threats. The implemented solutions' still partial status suggested, however, that organizations were unable to complete deployment owing to technical issues and the lack of properly allocated resources. The lack of appropriate organization controls and the excessive reliance on provider security underscored dangerous misunderstandings regarding the shared responsibility model and the creation of security gaps. Organizations' lack of appropriate incident response solutions suggested the focus on preventative measures was at the expense of the critical detecting and responding layers that help mitigate the impact of an incident when preventative measures fail.

The need to address people, processes, and technology aspects of security in an integrated manner was highlighted. Technical security measures will always be inadequate if organizations do not also devote resources to training people, developing policies, and establishing processes that promote a security culture within the organization. Cost-effective strategies such as the use of security features incorporated in the cloud and cloud automation and managed security services will help Pakistani organizations overcome security resource gaps while improving security postures. The need to work and fill systemic challenges such as the lack of cyber security talent, low awareness, and weak regulatory frameworks to improve organizations' cloud security was underscored. The need for this work, to be sustainable, was emphasized to come from the government, the affected industries, and the academic sector.

CONCLUSION

Through the use of a mixed-method research approach of quantitative surveys and qualitative expert interviews, the study analyzed cloud-security practices offered to Pakistani organizations and identified the key cybersecurity challenges threats faced. It also analyzed the cloud-security practices offered to Pakistani organizations. Results show Pakistani organizations faced operational challenges stemming from sophisticated threats such as data breaches, account hijacking, DDoS attacks, and various forms of malware, all of which could severely erode trust with stakeholders. Although organizations prioritized

security and implemented a variety of security measures, critical weaknesses remained, especially in the provision of coverage for security technologies reviews and the availability of tools and technologies. The identified issues of budget constraints, a lack of skilled personnel, a lack of organizational awareness, and an inconsistent security posture were of a systemic nature and, as such, will require collaborative efforts of multiple stakeholders, as opposed to single organizational action.

The study showed that deploying technological solutions alone is not sufficient for securing the cloud. Comprehensive solutions must address the technical, organizational, and social components at the same time. There will always be a gap that is uncompensated between the provider and the organizational security, hence, an organizational and cultural shift must be made from a reactive mindset that merely contains incidents, toward proactive security, risk assessment, and integration within all business processes. The organization must define and document all security gaps, and establish the endpoints of their security responsibilities within the shared responsibility model. Moreover, 'building organizational culture of security through upper management support, employee security policy training and administration of training, is critical for positive and sustainable security culture' is something that all organizations must enforce. The study provided empirical evidence to be used for securing the cloud within the resources of Pakistani organizations eclipse your offered empirical evidence here within the provided sentence.

RECOMMENDATIONS

Organizations in Pakistan should implement holistic security strategies that meet internationally recognized practices like ISO 27001 and NIST Cybersecurity Framework, with contextual flexibility regarding local conditions and available resources. Such organizations should train staff regularly and defensively on security awareness to tackle the human-factor vulnerabilities, focusing on recognizing phishing, maintaining passwords, social engineering, and secure cloud usage practices. The prioritized implementation of multi-layered security frameworks that incorporate varying degrees of encryption, multifactor authentication, intrusion detection, and integration of security information and event management systems is essential for organizations seeking to mitigate multiple threat vectors. Organizations should mitigate the impacts of incidents and allow quick recovery by establishing formal incident response plans, conducting regular security exercises, and maintaining validated backup and disaster recovery strategies. Engaging managed security service providers allows organizations to address continuous monitoring and threat detection, compensating for unfulfilled security human resource positions. The government should strengthen support for systemic talent and awareness gap intervention strategies, such as cybersecurity education programs, industry certifications, and public-private partnership initiatives. Organizations should conduct routine security audits, vulnerability assessments, and penetration testing to anticipate and mitigate security weaknesses before adversaries exploit them.

REFERENCES

Aderibigbe, A. O., et al. (2023). "Artificial intelligence in developing countries: Bridging the gap between potential and implementation." Computer Science & IT Research Journal **4**(3): 185-199.

Ahmad, W., et al. (2021). "Cyber security in iot-based cloud computing: A comprehensive survey." Electronics **11**(1): 16.

Alam, A. (2021). Cloud-based e-learning: development of conceptual model for adaptive e-learning ecosystem based on cloud computing infrastructure. International Conference on Artificial Intelligence and Data Science, Springer.

Chippagiri, S. (2025). "A Study of Cloud Security Frameworks for Safeguarding Multi-Tenant Cloud Architectures." International Journal of Computer Applications **975**: 8887.

Gupta, A., et al. (2023). "Role of cloud computing in management and education." Materials Today: Proceedings **80**: 3726-3729.

Hashim, W. and N. A.-H. K. Hussein (2024). "Securing cloud computing environments: An analysis of multi-tenancy vulnerabilities and countermeasures." SHIFRA **2024**: 8-16.

Iqbal, Z. and R. us Shan (2024). "Pakistan's Cybersecurity Landscape." CISS Insight Journal **12**(2): P105-131.

Kausar, S., et al. (2023). "Analysis of the cyber security challenges and solutions." Journal of Positive School Psychology **7**(1).

Khan, M. F., et al. (2021). "Cyber security and challenges faced by Pakistan." Pakistan Journal of International Affairs **4**(4): 865-881.

Matthew, U. O., et al. (2021). "Contemporary development in E-Learning education, cloud computing technology & internet of things." EAI Endorsed Trans. Cloud Syst. **7**(20): e3.

Mehmood, M. (2025). "The Role of Cyber Security in Promoting Digital Inclusion: A Case Study of Pakistan." Annals of Human and Social Sciences **6**(1): 35-44.

Qasim, M. S., et al. (2025). "ASSESSING CYBERSECURITY CHALLENGES AND RESPONSE READINESS IN PAKISTAN: A COMPREHENSIVE ANALYSIS." Kashf Journal of Multidisciplinary Research **2**(01): 115-125.

Saleem, B., et al. (2024). "A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap." International Cybersecurity Law Review **5**(4): 533-561.

Sandhu, A. K. (2021). "Big data with cloud computing: Discussions and challenges." Big Data Mining and Analytics **5**(1): 32-40.

Waghmare, V., et al. (2021). "Privacy in Multi-Tenancy Cloud." International Journal of Innovative Research in Computer and Communication Engineering **9**(11): 14498-14503.

Wu, W. and A. Plakhtii (2021). "E-learning based on cloud computing." International Journal of Emerging Technologies in Learning (iJET) **16**(10): 4-17.