Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 6, 2026

CLOUD SECURITY RISK MANAGEMENT IN SMES: CHALLENGES, LIMITATIONS, AND STRATEGIC RESPONSES

Shanza Zaman*[1], Muhammad Zubair[2], Muhammad Waqas Riaz [3], Abdul Saboor Khan [4], Sana Parveen[5], Muhammad Yousif[6]

[1]*Department of Informatics and systems, University of Management and Technology, Lahore , Pakistan.*
[2]*Department of Computer Science, Air University Islamabad Multan Campus, Multan 60000, Pakistan.*
[3] *Department of Artificial Intelligence, The Islamia University of Bahawalpur, Bahawalpur 63100, Pakistan.*
[4]*Department of Information Technology , Government College University Hyderabad Pakistan.*
[5]*Department of Artificial Intelligence, The Islamia Univeristy of Bahawalpur, Bahawalpur, Pakistan, sanahaq6677@gmail.com*
[6]*Department of Computer Science, National University of Modern languages Sub-Campus, Lahore, Pakistan,*
shanza.zaman@umt.edu.pk, muhammad.zubair@aumc.edu.pk , mwaqaskp@gmail.com, abdul.saboorkhan2006@gmail.com, sanahaq6677@gmail.com , myousif.cs@gmail.com

DOI: https://doi.org/10.5281/zenodo.20692231

Keywords
cloud security, risk management, SMEs, shared responsibility, strategic responses, risk exposure.

Article History
Received on 20 May 2026
Accepted on 02 June 2026
Published on 14 June 2026

Corresponding Author: * Shanza Zaman*

Abstract
cloud computing provides small and medium-sized enterprises (SMEs) scalability, cost efficiency, and access to advanced features, it also presents security challenges that are not always addressed by these businesses. This research investigates the critical issues and constraints of cloud security risk management in SMEs, quantifies their exposure to selected cloud security risks and assesses the cloud security strategies available to them for the purpose of enhancing their cloud security. In order to reach a comprehensive understanding of the challenges SMEs encounter when dealing with cybersecurity, a mixed-methods design was implemented, which involved a structured survey conducted among 200 SMEs from various sectors and semi-structured interviews with IT managers, owners, and cybersecurity professionals. Each threat was not just ranked by the severity of the threat but evaluated based on a risk exposure score (Likelihood × Impact) and placed in the cloud shared-responsibility model for IaaS, PaaS and SaaS. Results from the analysis suggest that data breaches, resource misconfiguration, and regulatory non-compliance are the top risks, while limited resources, skills gaps, and reliance on third-party providers are considered as constant constraints. The findings also reveal that the security burden is lowest for SMEs on SaaS and highest on IaaS, and that there are still several effective strategic ways to respond, including the use of multi-factor authentication, encryption and

certified providers, which are still under-adopted compared to their perceived effectiveness. Finally, the study suggests a framework for risk management and some practical recommendations for SMEs and policymakers, providing both an analytical perspective to prioritize cloud security risks and actionable advice for resource-limited firms.

INTRODUCTION

Small and medium scale enterprises (SMEs) are the backbone of the world economy accounting for over 90% of the world business and approximately 60% of the employment globally[1]. For survival, more and more of these companies are moving to cloud computing environments which offer increased scalability, reduced capital expenditure and better operational agility. However, cloud adoption can thwart these benefits when security, compliance and risk-management measures are overlooked [2]. The shift to shared, internet-facing infrastructure now puts SMEs at a greater risk of attack, and managing cloud security risk can become an important part of the digital transformation equation and a critical survival factor for SMEs.Increasingly, there is evidence that SMEs are more at risk to cyber threats than larger enterprises. SMEs often fall into the gap for cybersecurity, as they are a vital component of the economy but are not often recognized as a target in cybersecurity programs, and they are under-equipped to face the increased in frequency, sophistication, and destructive nature of cyberattacks today [3]. Cloud environments bring unique exposures with them such as data breaches, misconfiguration, weak identity and access controls, and reliance on third parties. On the other hand, cloud adoption can help with some of the risks, but it also brings new risks and changes the overall threat landscape [4], so SMEs can't simply assume that cloud-based technologies imply a decrease in their security responsibilities.

The problems faced by SMEs are not only technical, but structural as well. The main obstacles to becoming cyber resilient are identified in the literature as limited awareness of cybersecurity risks, restricted cybersecurity literacy and limited financial resources[5]. Likewise, SMEs' limited knowledge, low awareness, and resource constraints limit their ability to implement existing cyber security

frameworks and policies[6]. Regulatory and compliance requirements, such as GDPR, PCI DSS, data sovereignty, and auditing, are particularly pertinent in the cloud environment, adding to the challenges faced by SMEs. Integration challenges between cloud solutions and legacy systems also pose a hurdle to implementing effective IT policies in the cloud context [7]. It can be a significant gap between identifying a risk and having the resources to tackle it, particularly for resource-poor businesses.

In this context strategic countermeasures are required. Scholars recommend a range of anticipatory and customized cybersecurity policies, formal change management, and reskilling of staff, as well as cooperation between SMEs, cloud computing service providers, and policy makers [8]. To truly ensure cloud security risk management, it's important to use proactive technical measures, along with readiness and external relationship building rather than following reactive measures. This study explores the challenges and barriers SMEs encounter when managing cloud security risk and assesses the potential strategic responses they have to them. In the process, it aims to explain to resource-strapped companies how to create resilient, secure, and compliant cloud environments. Cloud computing is an essential technology for organizations looking to be scalable, flexible, and cost-effective. Cloud services are widely adopted by small and midsize businesses (SMBs) in recent years and will likely gain traction even more in the coming years as they realize that cloud-based services eliminate the need for on-premises infrastructure and offer pay-as-you-go service options.

Cloud platforms are used by SMEs to support business operations, customer management, data storage, collaboration, and digital transformation programs are increasingly being used to support SMEs. But cloud computing comes with many advantages, but also a significant amount of security challenges to address. Cloud Security Risk Management (CSRM) is the process of identifying, evaluating, reducing, and monitoring security risks in a cloud computing environment. Cloud environments come with risks like data breaches, unauthorized access, service interruptions, compliance issues, and insider threats, making effective CSRM a must-have. SMEs are also highly exposed to these risks because they typically lack resources for

cybersecurity, security governance infrastructure, and experience in cybersecurity. This paper aims to critically review the literature on cloud security risk management in SMEs, discuss the key challenges and limitations of organizations, and analyze the different strategic approaches suggested by researchers and practitioners.

Figure 1. Cloud shared Responsibility Model & SME Security Burden

1. Literature Review

Table 1. Summary of Literature Reviews for Cloud Computing and SMEs

Reference	Title	Methodology	Key Observations	Limitations
[9]	Cloud Computing Adoption in SMEs: A TOE Framework	Conceptual framework study	Introduced TOE (Technology–Organization–Environment) framework widely used for technology adoption including cloud computing	Does not include empirical validation for modern cloud

Reference	Title	Methodology	Key Observations	Limitations
	Perspective			security contexts
[10]	Cloud Computing Adoption in SMEs: A Systematic Review	Systematic literature review	Identified cost, flexibility, and scalability as main drivers of SME cloud adoption	Outdated; limited focus on modern cybersecurity risks
[11]	Cloud Security Risks and Challenges in SMEs	Empirical survey study	SMEs face major risks: data breaches, lack of expertise, and weak governance	Limited geographic scope; small sample size
[12]	Cloud Security and Risk Management Framework	Technical literature review	Highlighted major cloud threats including data leakage, account hijacking, and insider threats	Lacks SME-specific focus
[13]	Security Issues in Cloud Computing for SMEs	Analytical study	Identified authentication and data protection as major concerns in cloud systems	Early study; outdated for modern cloud architectures
[14]	Risk Management in Cloud Computing Environment	Conceptual + policy analysis	Proposed risk-based approach for cloud security governance	No empirical validation

Reference	Title	Methodology	Key Observations	Limitations
[15]	Cloud Security Posture in SMEs	Quantitative survey	SMEs with weak cybersecurity policies are more prone to cloud breaches	Limited dataset; regional bias
[16]	ISO/IEC 27001 Implementation in SMEs	Case study analysis	ISO 27001 improves governance but is costly and complex for SMEs	Difficult implementation in resource-limited firms
[17]	Cloud Security Alliance (CSA) Controls Matrix Study	Framework analysis	CSA CCM provides structured cloud security controls for risk mitigation	Requires technical expertise for adoption
[18]	Cybersecurity Risk in Cloud Environments	Qualitative analysis	Identifies regulatory issues and trust as key barriers in cloud adoption	Lacks quantitative validation
[19]	SME Cybersecurity Awareness and Practices	Survey report	SMEs lack awareness of cloud threats and rely heavily on service providers	European-focused; not globally generalizable
[20]	Zero Trust Architecture for Cloud Security	Framework design	Zero Trust improves identity-based security in cloud systems	Implementation complexity in SMEs
[21]	Cloud Security Risk Assessment	Comparative analysis	Hybrid models (TOE + Risk frameworks) improve risk assessment accuracy	Still theoretical, limited real-

Reference	Title	Methodology	Key Observations	Limitations
	Models			world deployment
[22]	AI-Based Cloud Security Monitoring	Machine learning experiments	AI improves anomaly detection in cloud environments	Requires high computation and expertise
[23]	Vendor Risk in Cloud Computing	Qualitative study	Vendor dependency is a major risk factor for SMEs	Limited SME empirical validation

2.1 Cloud Computing and SMEs

Typically, cloud computing is described as the delivery of computing resources (such as storage, applications, processing power, and networking) via the internet as needed. Cloud computing has completely revolutionized enterprise IT, allowing organizations to utilize powerful technology without a significant capital investment. Research shows that SMEs benefit from the cloud the most, as they can compete with larger organizations but do not have to incur the same expenses. Several reasons have been identified to promote cloud adoption among SMEs such as cost savings, scalability, flexibility, collaboration, business continuity, and accessibility. However, in developing nations cloud computing has proved to be especially appealing, as it minimizes technological hurdles and opens up access to sophisticated digital services, which would otherwise be too costly. While these benefits exist, there are still significant concerns in the areas of security, privacy, and regulatory compliance with cloud adoption. One of the biggest challenges for SMEs remains security issues, especially for those sectors that process customer and financial sensitive data. SMEs are often more likely to focus on economic considerations than security, when moving to the cloud, and this creates vulnerabilities that could be exploited by cybercriminals, researchers argue.

2.2 Concept of Cloud Security Risk Management

Cloud Security Risk Management involves identifying potential threats and vulnerabilities

within cloud environments and implementing appropriate controls to minimize their impact. The typical process for risk management frameworks is to identify risks, assess risks, treat risks, monitor risks and continuously improve.

Cloud security resources suggest that risk management effectiveness hinges on knowledge of the shared responsibility model between cloud service providers and cloud consumers. In this approach, cloud service providers manage the underlying infrastructure, and the customers manage data security, identity management, security settings and compliance requirements. Failure to understand these responsibilities can lead to major security issues [24].

The ISO/IEC 27001, ISO/IEC 27017, the NIST Cybersecurity Framework and the Cloud Security Alliance (CSA) Cloud Controls Matrix are a few of the proposed frameworks for cloud security risk management. These frameworks offer a method for identifying vulnerabilities and implementing security controls. But the study showed that some SMEs face challenges in putting these into practice because they are often complex, lack of resources and specialist knowledge [25].

2.3 Security Risks Associated with Cloud Computing

There are many security problems identified in the literature for cloud computing environments.

2.3.1 Data Breaches

One of the biggest issues with cloud security is data breaches. The potential consequences of sensitive data breaches include financial damages, reputational damage, and regulatory fines. Large amounts of valuable information typically make cloud-based data repositories a tempting target for cybercriminals. Data breaches are consistently cited as a huge risk for businesses switching to cloud services.

2.3.2 Misconfiguration Risks

One of the top contributors to security incidents is cloud misconfigurations. Security issues can arise if storage buckets, databases, access control and virtual machines are misconfigured or improperly set up, which could expose sensitive information to unauthorized users.

2.3.3 Identity and Access Management Threats

Throughout the cloud environment, vulnerabilities have grown to be more noticeable when it comes to identity.

Insufficient authentication, weak passwords and poor password management, excess privileges, and stolen credentials allow attackers to get past the front door. Researchers stress that identity and access management mistakes are among the top reasons for cloud security incidents.

2.3.4 Insider Threats

Insider threats come from any employee, contractor or other authorized person who abuses their access. Unlike external threats, insider threats are harder to detect because malicious activities can seem legit. SMEs can be particularly vulnerable as they often do not have advanced monitoring and auditing systems.

2.3.5 Distributed Denial-of-Service Attacks

Distributed Denial-of-Service (DDoS) attacks aim to make clouds unavailable by flooding them with too much traffic. These attacks can cause downtime, loss of customer confidence and financial losses. With more reliance on cloud services, DDoS attacks have grown in threat to SMEs.

2.3.6 Compliance and Privacy Risks

Often times, data is stored in multiple jurisdictions with cloud computing, which can result in legal and regulatory issues. There are several regulations that organizations are subject to that cover data protection and privacy. The penalties and reputational impact for not comply can be significant. Many SMEs have a poor grasp of and are unable to meet the regulatory requirements.

2.4 Challenges of Cloud Security Risk Management in SMEs

2.4.1 Limited Financial Resources

Financial limitations have been cited as one of the main challenges to make good cybersecurity implementation in SMEs in the literature consistently. Bigger companies may also need more advanced security solutions, threat detection systems and compliance programs, which can be more expensive than smaller companies can afford. This means that SMEs often implement very low levels of security, further exposing them to cyber threats.

2.4.2 Lack of Cybersecurity Expertise

Most SMEs do not have cybersecurity employees and rely on the general IT employees to manage cybersecurity. This lack of knowledge puts the organization at risk of not identifying vulnerabilities, responding to incidents and taking effective risk management measures. According to research, Cybersecurity

literacy is among the most important factors influencing SMEs' security resilience.

2.4.3 Complexity of Cloud Environments

Cloud environments are modern, in terms of virtualization, multi-cloud, hybrid, and dynamic resource allocation. These features make security management more complex, and pose problems for organizations with less technical expertise.

2.4.4 Rapidly Evolving Threat Landscape

With the advent of AI-powered attack methods and ever-more sophisticated threat actors, cyber threats are constantly changing and growing. It is often difficult for security teams to keep track of all attack surfaces, especially when they are growing, and to manage the complexity of cloud-based infrastructures. The attack surface of the cloud has been evolving in recent times and research indicates that the attacks are increasingly automated and fast, posing more challenges to constrained SME resources.

2.5 Strategic Responses to Cloud Security Risks

Various strategic response options have been suggested in the literature for enhancing the cloud security risk management in SMEs.

2.5.1 Adoption of Security Frameworks

ISOs (ISO/IEC 27001), NIST, and CSA controls are recommended by researchers to be adopted internationally. These frameworks offer a systematic method for detection, analysis and reduction of security threats in cloud computing. Easy-to-implement solutions adapted to SMEs could enhance uptake.

2.5.2 Multi-Factor Authentication

Multi-factor authentication (MFA) decreases the risk of credentials being compromised and the chances of unauthorized access. Many studies name MFA as one of the most cost-effective security measures that can be implemented by SMEs.

2.5.3 Employee Security Awareness Programs

People can be a significant factor in cyber incidents. Security awareness training programs can help employees identify phishing, social engineering, and unsafe cloud usage. There are numerous continuous education programs that can help organizations significantly limit their risk exposure.

2.5.4 Continuous Monitoring and Automation

By monitoring activities continuously, the organizations can be able to detect the suspicious activities and respond to the incidents in time. Automated security

solutions such as AI-powered threat detection and cloud-based security offerings present a chance to enhance security efficiency and cut costs.

2.5.5 Zero Trust Security Architecture

Zero Trust Architecture has become a well-known security architecture that takes the stance of not trusting any user, device or application by default. Zero Trust approaches offer a way to greatly mitigate the risks of unauthorized access and insider threats.

2. Proposed Methodology

The research approach used in this study is the combination of quantitative and qualitative methods. Quantitative method is used to investigate the difficulties experienced by Small and Medium Enterprises (SMEs) in implementing Cloud Computing. Qualitative method is used to support the quantitative method, by using the tools of focus group, in-depth interviews and case studies. Case studies and interviews with various SMEs, IT professionals, and industry experts were conducted to collect the qualitative data related to experiences and perspectives of SMEs in implementing cloud computing. Qualitative data was also gathered through surveys of selected SMEs, covering which barriers they are experiencing or how they perceive them to be significant, in the context of Cloud technology.

3.1 Stage 1: Problem Identification. This is where you define the actual problem the research tackles. You identify that as SMEs are increasingly adopting cloud services, security challenges are causing them problems – and you're able to identify the reason: budgetary constraints, a lack of in-house security expertise, reliance on third parties and compliance with data-protection regulations. The goal is to prove that there is a definite problem that can be investigated, not merely a concern. The result is a lucid declaration of the unique cloud-security issues and restrictions that face SMEs.

3.2 Stage 2: Research Objectives. After the problem has been defined, you frame it as specific, measurable, attainable, realistic, time-bound and answerable objectives. In this, you agree to two things: How vulnerable are SMEs really to various cloud-security threats, and how can strategic measures (controls, practices, policies) increase their security. Good objectives are specific enough to help direct the entire study and are to be tested later to prevent the study from going "off-track". Result:

a set of clear goals that link risk exposure to strategic action.

3.3 Stage 3: Research Design. This is the plan for conducting the study. You select a mixed-methods (numbers and narrative) approach using a familiar lens (e.g., technology-organization-environment (TOE) model), and you determine what sectors, firm sizes and numbers of SMEs to study in order to fairly represent the population. These decisions are made in advance, ensuring the validity and repeatability of the study. Result: A validated methodology that includes a sampling plan and the survey and interview instruments.

3.4 Stage 4: Data Collection. Structured surveys are sent to IT managers and owners, asking them to score each risk based on how likely it is to occur and the impact that it will have, if it does. Learning from semi-structured interviews are getting the nuances of actual practices, barriers, and context that a survey simply cannot get. Both provide breadth (statistics across many companies) and depth (the "why" of the statistics) and both sources check each other. The result is a quantitative and qualitative risk and response data set.

3.5 Stage 5: Data Analysis. This is where you analyze the information you've gathered and derive conclusions. On the quantitative aspect, you calculate the risk exposure to each threat (Likelihood x Impact), rank them, and perform statistical tests to determine whether there are relationships and to evaluate the effectiveness of various responses. Thematic analysis reveals recurring themes from the interviews on the qualitative side. This is where you get the answer to your goals. The result is a ranked Risk Profile with evidence of the best strategic responses.

3.6 Stage 6: Conclusions and Recommendations. Lastly, you interpret the results and translate the results to something usable. You distill the implications of the findings, develop a strategy for a cloud-security response plan that SMEs can implement, and provide business owners and policy makers with some tips. By incorporating the problem, you came up with in Stage 1, this ties the whole loop together. The resulting output is a set of recommendations for action and a cloud-security risk-management framework.


METHODOLOGY STAGE
EXPECTED OUTPUT
01
PROBLEM IDENTIFICATION
• Identify the cloud security challenges SMEs face.
• Examine barriers: limited resources, skills gaps, vendor lock-in.
OUTPUT
A clear set of cloud security challenges and limitations specific to SMEs.
02
RESEARCH OBJECTIVES
• Assess SMEs' exposure to cloud security risks.
• Identify strategic responses that strengthen posture.
OUTPUT
Well-defined objectives linking risk exposure to strategic responses.
03
RESEARCH DESIGN
• Adopt a mixed-methods, risk-based (TOE) approach.
• Sample SMEs across multiple sectors and sizes.
OUTPUT
A validated methodology, sampling plan and survey / interview instruments.
04
DATA COLLECTION
• Survey IT managers / owners on risk likelihood & impact.
• Interview participants on practices and barriers.
OUTPUT
A combined quantitative + qualitative dataset on risks and responses.
05
DATA ANALYSIS
• Compute risk exposure (Likelihood × Impact); rank threats.
• Evaluate response effectiveness (statistical + thematic).
OUTPUT
A ranked risk profile and evidence on strategic-response effectiveness.
06
CONCLUSIONS & RECOMMENDATIONS
• Derive a strategic cloud-security response framework.
• Offer practical guidance for SMEs and policymakers.
OUTPUT
Actionable recommendations and a cloud-security risk-management framework.

Figure 2. Proposed Research Methodology

3. Results and Simulation

Table 2. Sample Characteristics – Interview Participants (Qualitative Phase)

Participant Category	No.	Female	Male	<5 yrs exp.	5–10 yrs	>10 yrs
SME Owners / Managers	18	6	12	5	8	5
IT / Cloud Staff	12	4	8	3	6	3
Cybersecurity Experts / MSSPs	8	2	6	1	4	3
Regulators / Policy Experts	4	2	2	0	1	3
Total	**42**	**14**	**28**	**9**	**19**	**14**

Table 1 presents a profile of the 42 participants in the qualitative interview stage in terms of their role, gender, and experience in years with relevant experience. The sample was specifically selected from 4 complementary groups in order to view cloud security risk management from multiple perspectives: 18 business owners/managers of SMEs (who have business and resource knowledge), 12 IT and cloud staff (who are directly involved in the day-to-day running of the business), 8 cybersecurity experts or managed security service providers (who have specialist threat and control knowledge), and 4 regulators/policy experts (who have knowledge of compliance and the wider environment). Of the 32 people, 14 were female and 28 were male, with 14 having less than five years' experience, 19 having five-10 years, and 14 having more than 10 years' experience with cloud adoption and security. The table shows that the study has included a wide range and quality of voices, thus enhancing the credibility and depth to the qualitative findings.

Table 2: Respondent Characteristics – Survey (Quantitative Phase, N = 200)

Firm Size	No.	Sector	No.	Cloud Adoption Stage	No.	Prior Security Incident	No.
Micro (1–9)	46	Retail / E-commerce	52	Not adopted (planning)	38	Yes	71
Small (10–49)	98	Manufacturing	41	Early adopter (<2 yrs)	74	No	102
Medium (50–250)	56	Financial / Fintech	33	Established (2–5 yrs)	59	Not sure	27
		Healthcare	29	Mature (>5 yrs)	29		
		IT / Software services	26				
		Other	19				
Total	**200**	**Total**	**200**	**Total**	**200**	**Total**	**200**

Table 2 details the 200 SMEs that completed the quantitative survey, giving a profile of the sample across the four dimensions, demonstrating that the sample is wide and representative. The sample is weighted towards genuine micro firms (1-9 employees) and small firms (10-49 employees) and medium firms (50-250 employees). Its sector range is diverse, with the highest number of members in retail/e-commerce (52), manufacturing (41), financial and fintech (33), healthcare (29), IT/software services (26), and other sectors (19): These different sectors have very different exposure to the risks of security breaches and regulatory pressures. The cloud adoption stage column represents the current state of each firm: 38 firms have not adopted cloud yet but are planning to do so, 74 firms are early adopters (less than 2 years) and 59 are established users (2-5 years) and 29 are mature users (more than 5 years) so it is possible to compare the risk perception by experience level. Last, the prior security incident dimension reveals that 71 firms had an incident while 102 firms did not have an incident and 27 firms were not certain,

allowing for an analysis of the impact of an incident on SMEs' cloud security perceptions and management. All of these qualities indicate a diverse sample and thus establish the baseline for the subsequent cross-sectional comparisons throughout the study.

Table 3: Cloud Security Risk Assessment – Likelihood × Impact (N = 200)

Cloud Security Risk	Mean Likelihood (1–5)	Mean Impact (1–5)	Risk Exposure Score (L × I)	Rank
Data breach / unauthorized access	4.1	4.5	**18.45**	1
Misconfiguration of cloud resources	4.0	4.2	**16.80**	2
Regulatory / data-protection non-compliance	3.8	4.3	**16.34**	3
Account / credential compromise	3.9	4.0	**15.60**	4
Vendor lock-in & loss of data control	3.5	3.8	**13.30**	5
Insider threat / human error	3.7	3.5	**12.95**	6
Service outage / availability loss	3.4	3.6	**12.24**	7
Insecure third-party integrations (APIs)	3.3	3.5	**11.55**	8

Table 3 lists the eight cloud security threats along with probability and severity of each threat, or a combination of both. Each risk was rated on two scales ranging from 1 (lowest) to 5 (highest) for likelihood (L) and impact (I), with the highest possible score being 25. The scores were then ranked by multiplying the two ratings and the most critical risk is the one with the highest score. Data breaches and unauthorized access come in first place (18.45) in the "critical" band, followed by non-compliance with regulations or data-protection policies (16.34) and insecure third-party API integrations (16.80); account or credential compromise (15.60) and insecure third-party API integrations (13.30) are in the "high" band, and insider threat/human error (12.95), service outages (12.24), and insecure third-party API integrations (11.55) are in the "medium" band. The benefit of this is that it

isn't just about the significance of how challenging a challenge feels: They are able to separate the likelihood from the impact, which then gives them a ranked list of challenges which is also decision-useful and can be mapped to a risk matrix, and which can direct SMEs to prioritise where they invest the limited security resources. The concentration of the top scores around data, configuration and compliance further emphasizes that the risks that are the most critical are a primary responsibility of the SME, further conveying the shared-responsibility message throughout the study.

The study examined the adoption of cloud-based Management Information Systems (MIS) in Small and Medium Enterprises (SMEs) and how this affects a number of performance indicators. The four main variables analyzed were Operational Efficiency, Cost Management, Competitive Advantage and User Satisfaction, as well as Security Concerns. The findings presented in the following sections are detailed and supported with four detailed tables.

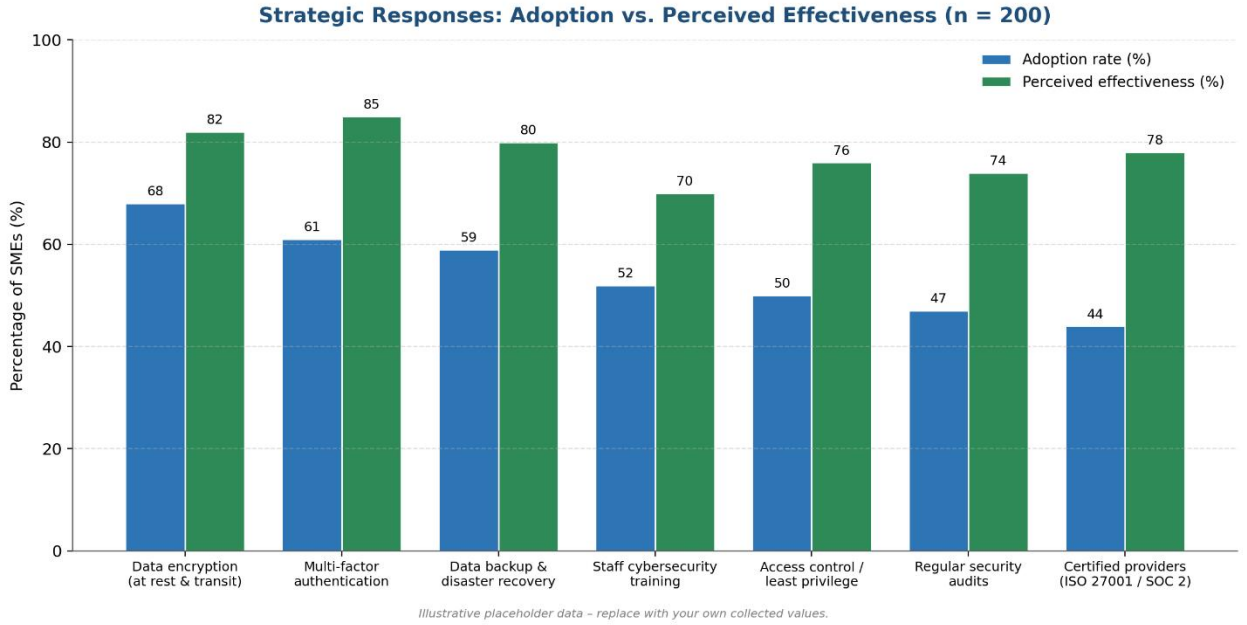

Figure 3. Strategic Responses: Adoption vs. Perceived Effectiveness

The figure below (Figure 3) shows the correlation between adoption rate and effectiveness of the different cybersecurity strategies for 200 SMEs. The findings indicate that the organizations have a good understanding of the effectiveness of these

measures, however, their implementation in the organizations is at a medium level. Over half of respondents (68%) reported using data encryption and multi-factor authentication is thought to be the most effective approach (85%). Likewise, data backup and disaster recovery and access control, regular security audits, staff cybersecurity training, and utilization of certified providers are all significantly underutilized, given that they have a high effectiveness rating. The significant disparity between the level of adoption and perceived effectiveness indicates that while SMEs appreciate the benefit of these cyber security practices, some funding, technical, and resource limitations lie in the way of implementing them. The overall results show significant potential for SMEs to step up their cybersecurity game through promoting the use of these proven security measures.

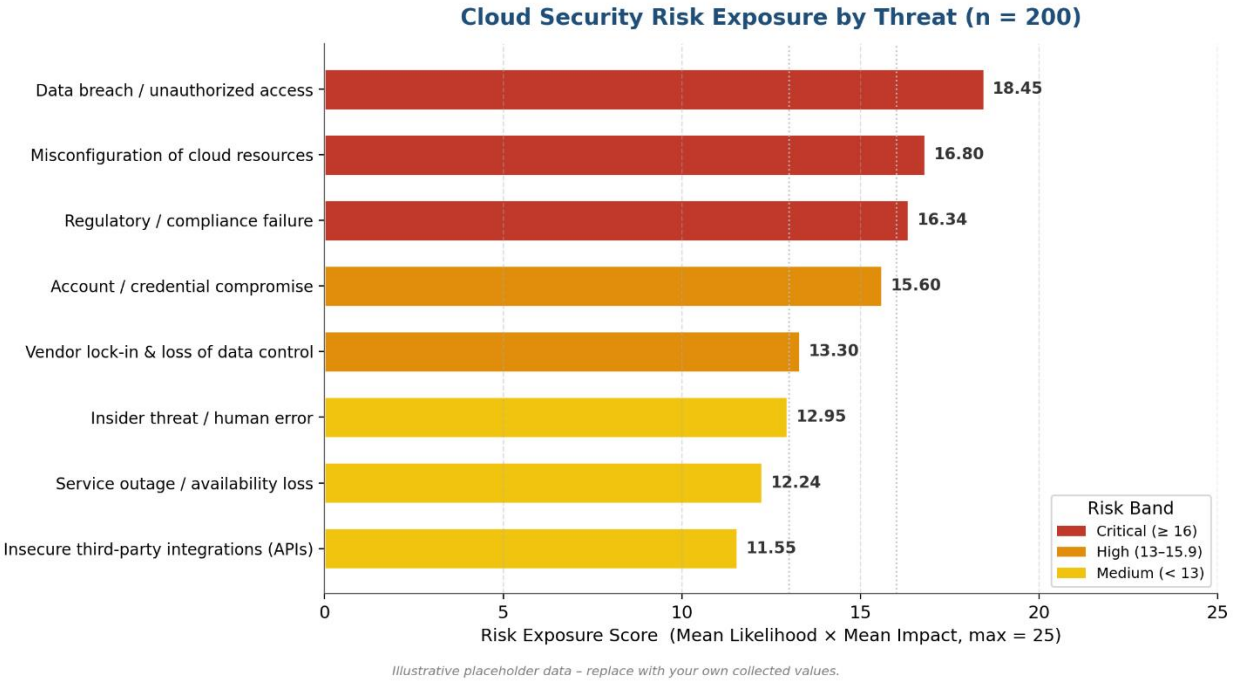

Figure 4. Cloud Security Risk Exposure by Threat

The risk exposure scores for each of the cloud security risks listed in this report are shown in Figure 4, based on the mean likelihood and impact of the threat (maximum risk exposure score = 25). According to the results, data breaches and unauthorized access are the highest risk (18.45), followed by misconfiguration of cloud resources (16.80) and regulatory/compliance failures (16.34) with these items falling into the critical risk

category. The two threats listed are categorized as high-risk threats and are significant concerns about identity security and reliance on cloud vendors – account or credential compromise (15.60) and vendor lock-in and loss of data control (13.30). Meanwhile, insider threats and human error (12.95), service outages and loss of availability (12.24), and insecure third-party integrations/APIs (11.55) are still major problems, but not quite as concerning as those on the high-risk list. Overall, the figure indicates that security breaches, cloud misconfigurations and compliance issues are the most significant cloud security threats to SMEs, and that these are the threats that need to be prioritized for mitigation to lower the risks to the organization and increase its cloud security resilience.

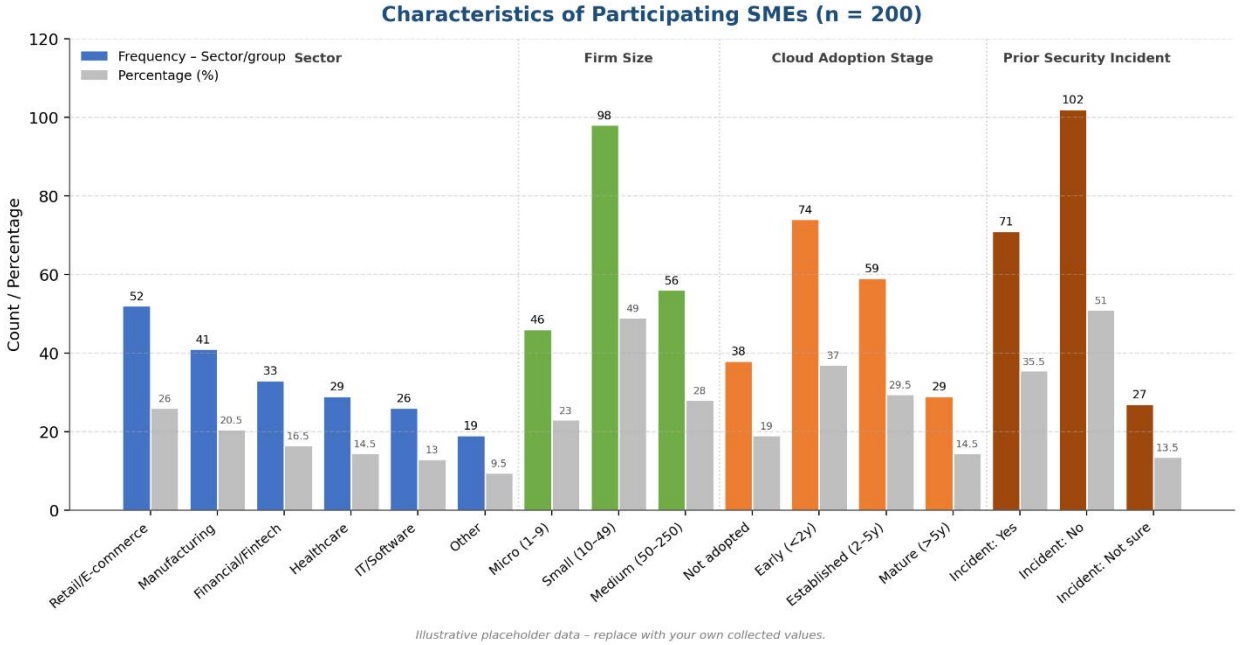

Figure 5. Characteristics of Participating SMEs

As shown in Figure 5, the demographics of the 200 SMEs in this study, by sector, firm size, cloud adoption stage, and experience with previous security incidents. The biggest portion of respondents was from the Retail/E-commerce sector (26%), followed by Manufacturing (20.5%), Financial/FinTech (16.5%), Healthcare (14.5%), IT/Software (13%), and other sectors (9.5%). By size, the small ones (10-49 employees) represented almost half of the sample (49%), the medium sized ones (50-250 employees) represented 28% and the micro-ones (1-9 employees) represented 23%. In terms of cloud adoption,

37% of SMEs were in the early stage of cloud adoption (<2 years), 29.5% had established cloud environments (2-5 years) and 19% have not adopted cloud services, and 14.5% had mature cloud adoption (> 5 years). As far as security experience goes, 35.5% of SMEs said they had suffered a security breach in the past, 51% said they hadn't had a security incident, and 13.5% didn't know. The overall picture shows that the sample is quite eclectic, with the majority being small companies, early-stage cloud customers and retailers and manufacturers.

4. Conclusion

This study examined the security concerns that SMBs face when adopting the cloud and attempted to do more than just identify the issues; it also sought to get a little deeper than that and determine what risks were most significant and what security solutions were most effective. It identified three distinct risks for SMEs: data breach, misconfigured cloud settings, and not adhering to regulations, all exacerbated by limited budgets, lack of in-house security skills, and overreliance on external security providers, according to the findings of a survey of 200 SMEs and interviews with owners, IT staff, security professionals and policy experts. Security that a business must manage is at its lowest in the least secure cloud service (IaaS), and at its highest in the most secure cloud service (SaaS), and wherein risk is highest, data is typically a business's responsibility, not the cloud service provider. The study also observed an intriguing disconnect: while certain practices, such as using multi-factor authentication, encryption and selecting certified providers, are reported to be effective, they're not being used as widely as they should be by SMEs. The key message is that a few high value protections, employee training, careful choices of providers, and enhanced support from regulators and providers can help SMEs go to the cloud more safely and with greater confidence, and by prioritizing risks based on their likelihood and impact, SMEs can focus their limited time and money on the protections that truly are worth their while.

References

[1] Rahman, S., & Hossain, M. Z. (2024). Cloud-based management information systems opportunities and challenges for small and medium enterprises (SMEs). Pacific Journal of Business Innovation and Strategy, 1(1), 28-37.

[2] Adelusi, B. S., Ojika, F. U., & Uzoka, A. C. (2022). Advances in Cybersecurity Strategy and Cloud Infrastructure Protection for SMEs in Emerging Markets. Journal of Frontiers in Multidisciplinary Research, 3(1), 467-482.

[3] James, H., & Bello, S. Balancing Innovation and Risk: Cybersecurity Challenges in SME Cloud Adoption.

[4] Arogundade, O. R. (2023). Strategic security risk management in cloud computing: a comprehensive examination and application of the risk management framework.

[5] Awan, M., & Alam, A. (2025). Cybersecurity Threats and Defensive Strategies for Small and Medium Firms: A Systematic Mapping Study. Administrative Sciences, 15(12), 481.

[6] Benjamin, L. B., Adegbola, A. E., Amajuoyi, P., Adegbola, M. D., & Adeusi, K. B. (2024). Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies. Global Journal of Engineering and Technology Advances, 19(2), 134-153.

[7] Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. IEEe Access, 10, 85701-85719.

[8] Kezron, I. E. (2025). Cloud adoption and digital transformation cybersecurity consideration for SMEs. Iconic Research And Engineering Journals, 8(7), 453-458.

[9] Baalbaki, C., Shamieh, S., & Bodolica, V. (2025). Cloud computing adoption in disruptive contexts: a TOE framework approach. VINE Journal of Information and Knowledge Management Systems, 55(6), 1696-1721.

[10] Mkhize, A., Mokhothu, K. D., Tshikhotho, M., & Thango, B. A. (2025). Evaluating the impact of cloud computing on SME performance: A systematic review. Businesses, 5(2), 23.

[11] Haddara, M., Gøthesen, S., & Langseth, M. (2022). Challenges of cloud-ERP adoptions in SMEs. Procedia computer science, 196, 973-981.

[12] Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. Network, 3(3), 422-450.

[13] Al-Mutawa, B., & Saeed Al Mubarak, M. M. (2024). Impact of cloud computing as a digital technology on SMEs

sustainability. Competitiveness Review: An International Business Journal, 34(1), 72-91.

[14] Maheswari, J. U., Vijayalakshmi, S., N, R. G., Alzubaidi, L. H., Anvar, K., & Elangovan, R. (2023, January). Data privacy and security in cloud computing environments. In E3S Web of Conferences (Vol. 399, p. 04040). EDP Sciences.

[15] Rönn, P. (2025). Assessing and improving the security posture of a cloud-based saas application for smes.

[16] Ramadhan, N., & Rose, U. (2022). Adapting ISO/IEC 27001 information security management standard to SMEs. Master Degree Project. Lulea University of Technology.

[17] Hegde, T., Gangl, J., Babenko, S., & Coffman, J. (2023, December). Cloud security frameworks: A comparison to evaluate cloud control standards. In Proceedings of the IEEE/ACM 16th International Conference on Utility and Cloud Computing (pp. 1-6).

[18] Hassan, O. F., Fatai, F. O., Aderibigbe, O., Akinde, A. O., Onasanya, T., Sanusi, M. A., & Odukoya, O. (2024). Enhancing cybersecurity through cloud computing solutions in the United States. Intelligent Information Management, 16(4), 176-193.

[19] Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023, February). Cybersecurity Awareness and Capacities of SMEs. In ICISSP (pp. 296-304).

[20] Rajendran, R. K., Priya, T. M., Goundar, S., Madhavi, K. R., Avanija, J., & Avula, B. R. (2025). Zero trust architecture in cloud security. In Convergence of Cybersecurity and Cloud Computing (pp. 515-530). IGI Global Scientific Publishing.

[21] Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2026). Information security risk assessment methods in cloud computing: Comprehensive review. Journal of Computer Information Systems, 66(1), 123-150.

[22] Patel, A., Gudur, V., Matam, P., Upadhyay, C., Achanta, A., Dave, S., & Sudarsan, S. (2026, March). AI-Driven Cloud Security: AIOps for Threat Detection and Compliance. In Journal of The Colloquium for Information Systems Security Education (Vol. 13, No. 1, pp. 13-13).

[23] Faruq, M. O. (2024). Vendor risk management in cloud-centric architectures: A systematic review of soc 2, Fedramp, and ISO 27001 practices. International Journal of Business and Economics Insights, 4(1), 01-32.

[24] Yousif, M., Abbas, A., Hasan, Z., Ali, D., & Sarfraz, M. (2021). Smart Village Health System IoT to Envisage Chronical Disease Using Artificial Neural Network. Internet Things Cloud Comput., 9(4), 27.

[25] Chauhan, M., & Shiaeles, S. (2023). An analysis of cloud security frameworks, problems and proposed solutions. Network, 3(3), 422-450.