How Small Businesses Can Effectively Protect Their Data When Using Public Cloud Services

MSc Research Project

Busayo Joshua Oyebode

Student ID: X22122524

School of Computing

National College of Ireland

Supervisor: Micheal Pantrige

Abstract

This study explores how small businesses can protect their data when using public cloud services. While cloud computing offers benefits like flexibility and cost savings, many small businesses face challenges such as limited resources, lack of expertise, and difficulty meeting regulations like GDPR. Common problems include weak data encryption, poor access control, and incomplete security policies, leaving these businesses vulnerable to cyber threats.

The research combines surveys and case studies to identify these challenges and find solutions. Surveys show trends in how small businesses allocate resources and manage compliance, while case studies highlight specific security gaps and practical needs. Based on these findings, a security framework is developed to help small businesses improve their cloud security. The framework focuses on affordable and practical measures like stronger encryption, role-based access control, and compliance monitoring tools.

This framework offers clear, cost-effective solutions to help small businesses reduce risks and adopt cloud services securely. By addressing their unique needs, the study provides practical strategies that are easy to implement and tailored to the limitations of small businesses.

Table of Contents

Chapter 1 Introduction

1.1 Background on Cloud Computing and Small Businesses

Cloud computing has transformed business operations by providing scalable, flexible, and cost-effective solutions for data storage, processing, and application hosting. For small businesses, in particular, cloud services offer an opportunity to leverage enterprise-grade IT infrastructure and advanced technologies that would otherwise be too expensive to build and maintain in-house. This has led to a rapid increase in cloud adoption among small businesses, driven by benefits such as reduced capital expenditure, enhanced scalability, and improved operational efficiency.

Small businesses encompass diverse industries, including retail, healthcare, professional services, startups, and logistics. Each of these categories faces unique operational challenges and security needs when adopting cloud computing. For instance, healthcare providers must prioritize stringent data privacy measures to comply with regulations like HIPAA, while retail businesses focus on secure payment processing to meet PCI-DSS standards. These variations underline the importance of addressing industry-specific risks as part of any cloud migration strategy.

However, this transition to cloud-based operations is not without challenges. While cloud computing addresses many traditional IT limitations, it also introduces a range of new security issues that businesses must address before migrating to the cloud. Small businesses, often constrained by limited resources and expertise, face unique vulnerabilities such as insufficient security policies, weak access controls, data protection concerns, and network-level threats (Kaplan et al., 2020). These challenges underscore the importance of understanding and mitigating cloud-specific risks to ensure a secure and successful migration.

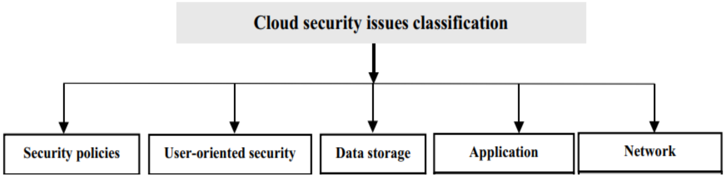

Figure 1: Classification of Cloud Security Challenges

1.2 Importance of Data Protection in Public Cloud Services

Data protection in public cloud services is of paramount importance, especially for small businesses. These organizations often deal with sensitive customer information, financial data, and proprietary business intelligence. A data breach or security incident can have devastating consequences, including financial losses, reputational damage, and legal liabilities (Alsmadi & Prybutok, 2018).

Data protection needs vary significantly across industries. For example, small healthcare practices handle sensitive patient information and face increasing threats of ransomware, whereas startups often prioritize safeguarding intellectual property and ensuring secure collaboration among remote teams. These differences emphasize the need for tailored, category-specific approaches to cloud security.

Moreover, small businesses are increasingly becoming targets for cybercriminals who view them as easier targets compared to larger enterprises with more robust security measures. According to a report by Verizon (2023), 43% of cyber-attacks target small businesses. This highlights the critical need for effective and accessible security solutions tailored to the needs of small businesses operating in public cloud environments.

1.3 Research Objectives

a) Identify the most significant security challenges faced by small businesses in public cloud environments.

b) Assess the effectiveness of existing security measures and their relevance to small business contexts.

c) Develop a practical and cost-effective security framework tailored to the needs and constraints of small businesses.

d) Provide theoretical insights and actionable recommendations for small businesses to enhance their cloud security posture.

1.4 Scope and Limitations of the Study

This research focuses specifically on small businesses, defined as organizations with fewer than 100 employees. The study is limited to public cloud services, as these are the most adopted cloud solutions among small businesses due to their cost-effectiveness and ease of use.

The research encompasses various aspects of cloud security, including data protection, access control, encryption, and compliance. However, it does not delve into the technical implementation details of specific cloud platforms or services. Instead, it aims to provide a generalized framework that can be adapted to different public cloud environments.

Limitations of the study include:

a) Geographic scope: The research primarily focuses on small businesses within the EU(European Union), which may limit the generalizability of findings to other contexts.

b) Rapid technological changes: The fast-paced nature of cloud technology and security threats means that some findings may become outdated quickly.

c) Self-reported data: Much of the data collected relies on self-reporting from small businesses, which may introduce some bias or inaccuracies.

Despite these limitations, this research aims to provide valuable insights and practical guidance for small businesses seeking to enhance their cloud security posture.

Chapter 2 Literature Review

2.1 Cloud Security Challenges for Small Businesses

Cloud computing adoption among small businesses has brought numerous benefits but also introduced significant security challenges. Here's what studies reveal:

a) **Industry-Specific Challenges**:

   i. Retail businesses face risks such as data breaches targeting customer payment details.

   ii. Healthcare providers struggle with insider threats and must ensure compliance with data protection laws like HIPAA.

   iii. Startups often grapple with protecting intellectual property while ensuring secure collaboration among remote teams.

Johnson and Lee (2022) found that 60% of small businesses experience at least one security issue in their first year of using cloud services, primarily due to limited expertise in cloud security. Chen et al. (2023) emphasized that insufficient investment in security measures exacerbates these challenges, with businesses spending at least 5% of their IT budgets on security seeing significantly fewer incidents.

Key challenges include:

a) **Data Breaches**: Difficulties in protecting sensitive data make small businesses vulnerable.

b) **Insider Threats**: Limited resources and improper access controls increase risks.

c) **Regulatory Compliance**: A lack of understanding and resources to meet data protection laws.

d) **Misconfigurations**: Incorrect setups of cloud services lead to security vulnerabilities.

e) **Insufficient Encryption**: Weak or absent encryption methods leave data exposed.

2.2 Cost-effective Security Measures for Public Clouds

Given resource constraints, small businesses require affordable security solutions:

a) Wang and Smith (2021) proposed a framework focusing on access control and encryption, reducing security incidents by 30% for businesses with fewer than 50 employees.

b) Patel et al. (2023) identified valuable features offered by public cloud providers, including:

i. Multi-factor authentication (MFA)

ii. Encryption for data at rest and in transit

iii. Virtual private networks (VPNs)

iv. Regular security audits and compliance checks

While these solutions are effective, the lack of practical implementation guidelines limits their adoption.

2.3 Regulatory Compliance in Cloud Environments

Compliance with data protection regulations remains a significant challenge. Brown and Taylor (2022) found that 70% of small businesses using cloud services were non-compliant with GDPR due to a lack of understanding. This underscores the need for clear, actionable guidance tailored to small business contexts.

2.4 Emerging Technologies in Small Business Cloud Security

Emerging technologies offer promising solutions:

a) Martinez (2023) demonstrated that AI-powered threat detection tools improve early threat detection by 25%, though these tools may be too complex for very small businesses.

b) Nguyen and Park (2022) argued for simpler, rule-based security systems as more cost-effective for businesses with fewer than 20 employees.

2.5 Identified Research Gaps

This literature review has identified several key gaps in the existing research including:

a) Lack of a comprehensive, practical security guide tailored to small businesses.

b) Insufficient guidance on balancing security needs with budget constraints.

c) Limited focus on frameworks addressing small business-specific challenges.

d) Inadequate strategies for regulatory compliance tailored to small businesses.

The present study aims to address these gaps by developing an affordable, practical security framework for small businesses using public cloud services, with a focus on real-world applicability and scalability.

Chapter 3: Research Methodology

3.1 Introduction

This chapter presents the research approach utilised in the study of how small businesses can secure their data when adopting public cloud services. A quantitative and qualitative research design has been applied to achieve a holistic analysis of the research goals and objectives. The structured questionnaire was used to gather quantitative data on the level of security practised in small business organisations, while the case study approach and interviews were used to collect qualitative data from IT decision-makers. These methods help to obtain a complete understanding of the problem area and thereby create constructive and affordable action-oriented security framework required by small businesses.

3.2 Research Design

This research also uses both quantitative and qualitative research approaches based on a mixed-methods research design to establish how SMEs can adequately safeguard their data when employing public cloud services. The use of a mixed methods research approach allows for gathering various forms of data to tap into both quantitative alignment of low-level patterns and richer qualitative context. The quantitative part involves questionnaires that were administered to 200 small business organisations with a view of collecting numerical information on security measures implemented, resources committed, and usual security issues experienced within cloud systems (Ngcobo et al., 2024). The research enables the establishment of a relationship between two variables or a number of variables and reveals trends, associations and other features in the large picture of things. This qualitative part is made up of case studies and semi-structured interviews with IT decision-makers from the chosen small businesses. This method allows for the analysis of certain security risks, decisions or practices and their applicability. Consequently, the research provides finer details on various cases that specific quantitative analysis may need to reveal due to their complexity. The use of combined methods is a result of understanding the strengths that each has to offer. Consequently, quantitative encompasses the large picture and tendencies as opposed to qualitative data, which gives a detailed understanding of the day-to-day realities faced by small business owners. Combined, these methods increase the validity and reliability of the research and provide a theoretical foundation for evidence-based security solutions that are relevant to small businesses.

3.3 Data Collection Methods

Survey Design

The survey aspect of this quantitative research concerned the small businesses that use public cloud services. The target population comprised organisations with up to 100 employees, and these organisations were drawn from various sectors, including retail, healthcare and professional services (Ajimoko, 2018). To achieve this, purposive sampling was used, which created sub-groups of the sample population based on business size, industry type and the period of cloud service usage. This allowed the gathering of a rich, diverse sample and variability in terms of views within the small business grouping. The survey consisted of structured questions designed to capture key information regarding:

- Current Security Practices: Use encryption mechanisms, access controls, and security policies.
- Resource Allocation: Specific dollars allocated and headcount focused specifically on cloud security.
- Compliance Challenges: Other requirements that need to be addressed include but are not limited to GDPR.
- Technical Capabilities: Knowledge about your advanced security appliances and settings.

The survey was delivered electronically to ensure the sample size and variability, and data collection was carried out over three months.

Case Studies

In addition to the survey results, qualitative data was obtained through case studies of a number of small businesses. The selection criteria for these businesses included:

- Industry Representation: One of the best aspects of the field is the numerous industries to consider when encountering different types of security issues.
- Business Size: Seasoned small businesses in various categories across the small business spectrum.
- Cloud Adoption Level: Companies' dependence on public cloud services ranges from high to medium and low.

Like most case studies, this research primarily used interviews and documentary analysis with IT decision-makers. The interviews focused on disclosing actual security practices, decisions, and perceptions of threats and difficulties so that systematic patterns and similarities across different cases could be revealed (Spanoudaki et al., 2019). Azure risk assessment involved getting working documents to assess current practices and determine gaps, which included reviewing security policies, analysing incident reports, and evaluating vendor agreements.

Analysis of Cloud Service Providers

This work also assessed the security solutions provided by the leading public cloud platforms, including AWS, Azure, and GCP (Saraswat and Tripathi, 2020). The evaluation included:

- Security Features: Anti-virus protection, secure IDs, password controls, encryption and protected access to data and programs.
- Cost Analysis: The cost of implementing security in a small business enterprise and how this could be done on a small scale.
- Compatibility: Relevance of the proposed features with the amount of technical knowledge and the degree of innovation that small businesses can employ.

Therefore, adopting a multimethod approach to data collection was effective in capturing cross-sectional quantitative data and qualitative information with contextual analysis, which helped develop a sound, feasible, and considerate security framework for small businesses.

3.4 Data Analysis Techniques

Quantitative Data Analysis

Descriptive statistics, correlation analysis, and cost-benefit analysis were used to obtain the quantitative data from the survey.

- Descriptive Statistics: Quantitative data regarding security practices, budget spending and compliance with or without regulatory requirements were analysed using percentage, average and frequency distribution. This gave a clear picture of the different trends and practices which were identifiable in the current cloud security aspect among small businesses.

- Correlation Analysis: Causal correlations between major measures, including the level of security spending employed and the number of security events experienced, were analysed for crucial determinants of cloud security outcomes (Alkhater et al., 2018). For example, in terms of businesses, the degree of relatedness was examined to show whether those companies funding security initiatives with greater budgets were faced with fewer incidents.
- Cost-Benefit Analysis: The performance of different variants of security measures, including second factor, encryption, etc., was examined based on costs, which helped examine what solutions could be optimal for a small business in terms of costs (Qasem et al., 2024).

Qualitative Data Analysis

Case studies and interviews were analysed employing thematic content analysis and cross-case analysis.

- Thematic Analysis: The main themes concerning security issues and solutions, pros and cons, and successful factors hindering the implementation of secure systems have been defined. These themes were developed after content analysis of interviews and documents for small businesses to gain first-hand insights into these enterprises' experiences (Schmitter & Bühler, 2022).
- Cross-Case Analysis: Thus, the lessons derived from the case analysis included the similarities and differences between the companies and explicit or hidden issues of the industry.

Integration of Findings

A framework for security was inferred from the quantitative and qualitative findings. This integration ensured that the logical framework captured general patterns in trends as identified by the quantitative findings together with specific, feasible, and contextualised strategies as identified by the qualitative work. This approach increases the reliability and usability of the solutions proposed in the work.

3.5 Ethical Considerations

Ethical considerations were at the heart of this research to warrant research credibility while respecting the rights of the participants. The identity of all of the participants involved in the study was also not revealed. In survey responses and interviews conducted with the participants, the information that could match an individual to his or her identity was deleted. Companies had their specific identification number so that confidentiality was achieved during the processing of the information collected. All collected data was saved in accordance with the data protection laws, including the General Data Protection Regulation (GDPR). Data collection also observes data protection; the data collected was only accessed by the research team and stored in encrypted formats in a bid to avoid exposing the data to the wrong hands (Vlahou et al., 2021). Participants' consent was sought, and all participants were assured that they could withdraw at any time. They were also briefly informed of the purpose, nature, and procedures of the research and their rights regarding withdrawal from the study. This research received a certificate from a suitable IRB, which implied compliance with the ethical practices that were laid down.

Chapter 4: Results and Analysis

4.1 Introduction

This chapter offers the findings of the research based on survey data as well as case study observation and interviews. The study identifies the security issues of utilising public cloud services among small businesses, presents practices of security, and assesses the reliability of the existing countermeasures (Tabrizchi et al., 2020). Based on these outcomes, the chapter reveals openings and challenges for improving data protection approaches for SMBs. The results offer a straight answer to the research questions that underpin the proposed security framework and guide specific recommendations for small businesses while considering their peculiarities and limitations.

4.2 Quantitative Findings

The survey results align the research survey with the most pressing security issues that affect small businesses when utilising public cloud services. Through the patterns and correlations this data presents, it becomes clear why precise and efficient security solutions are so important and hard to come by.

Security Practices of Small Businesses

The survey found that as few as 32% of small businesses have written security policies, while 45% have written but informal security policies. A quarter of the respondents have no security policies in place and are extremely susceptible to threats. This problem exposes a chasm in knowledge and utilisation of basic security protocols and practices. Companies with documented information security policies incur less loss due to security violations; thus, there is a need to adopt standard security strategies (Nel and Drevin, 2019).

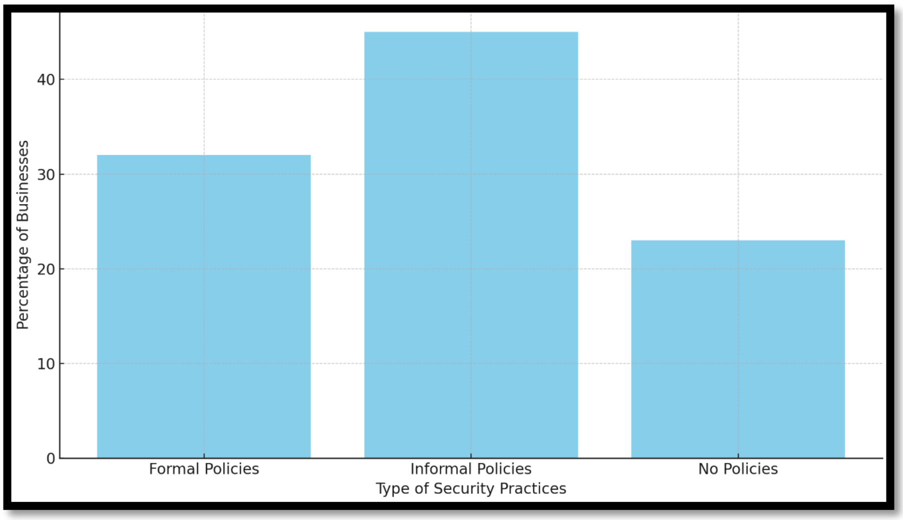

Figure 2: Security Practices in Small Businesses

Resource Allocation

IT professionals suggest that as much as 45% of businesses dedicate less than 3% of their IT budget to security, 35% between 3-5%, and 20% more than 5%. This limited budget is quite reasonable given the fact that the majority of small businesses, Inc., struggle financially, where meeting daily running costs is of paramount importance, as compared to investing in security (Tam et al., 2021). Nevertheless, organisations and companies investing an amount of more than 5% in their total proportion of IT budget have revealed better shields and a low rate of incidents that underline the correlation between IT resources spending and security results.

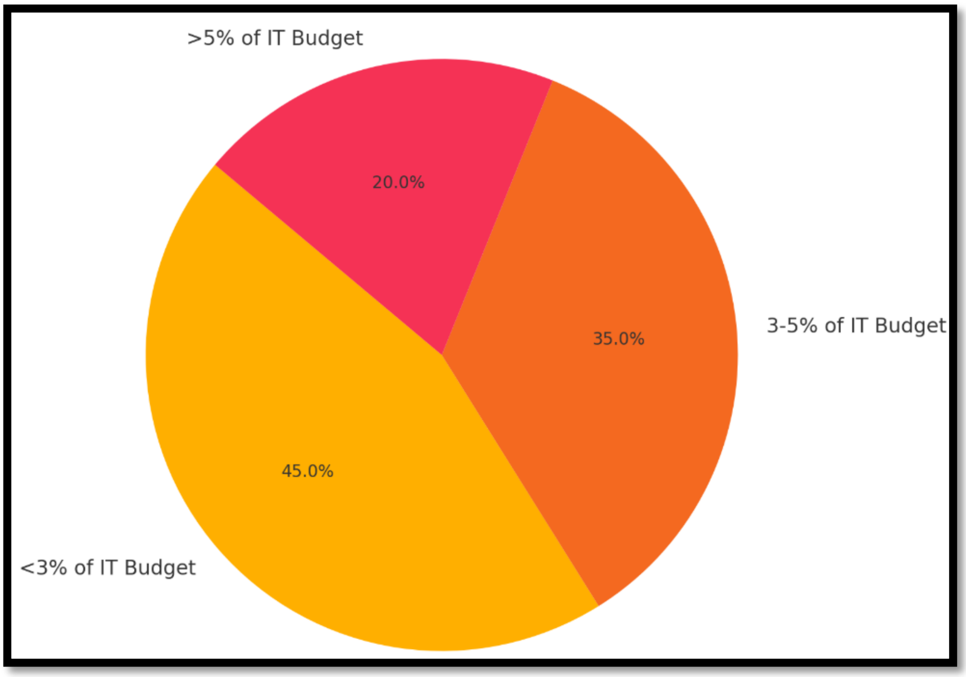

Figure 3: Resource Allocation for Cloud Security

Compliance Challenges

Challenges like compliance with regulations such as GDPR still persist. The current year shows that 40% of businesses have needed help with compliance requirements (Sirur et al., 2018). A further 35% stated that this view, as also insufficient security know-how, is the reason why they are inadequate in the effective security measures implemented; 25% stated that they lack suitable tools for addressing security and compliance matters. These challenges point to a need to provide affordable and workable compliance assistance to small businesses (Hashmi et al., 2018).

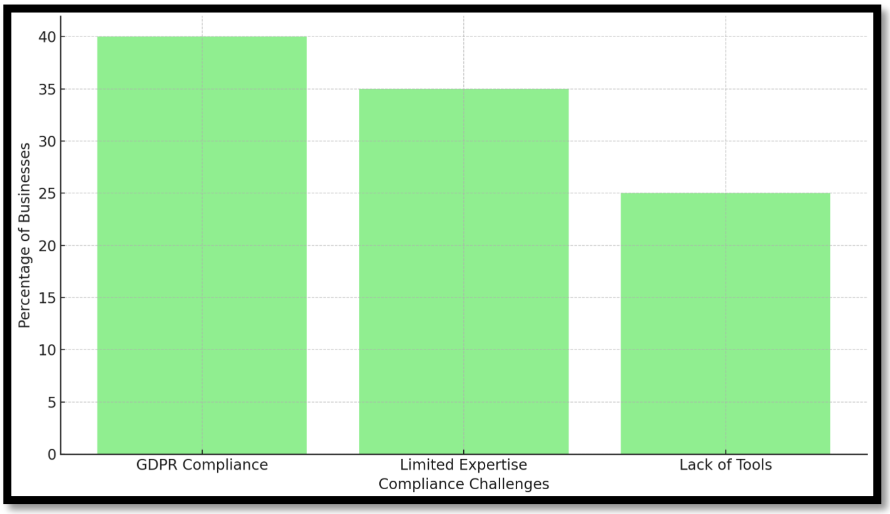

Figure 4: Compliance Challenges Faced by Small Businesses

Patterns and Correlations in Security Incidents

The survey further confirmed the negative relationship between a lack of adequate policies and a higher incidence of security attacks. Companies without such policies encountered ill(stage 2) at double the rate of companies that have created policies (Maynard et al., 2018). Likewise, organisations with a more secure budget reported the fewest breaches, pointing to the fact that proper financial commitment is key to risk minimisation.

Table 1: Quantitative findings

Category	Details	Percentage
Security Practices	Formal Policies	32%
	Informal Policies	45%
	No Policies	23%
Resource Allocation	<3% of IT Budget	45%
	3-5% of IT Budget	35%
	>5% of IT Budget	20%
Compliance Challenges	GDPR Compliance	40%
	Limited Expertise	35%
	Lack of Tools	25%

These quantitative results form a basis for knowing the risks and limitations faced by small businesses in protecting their data stored on open cloud solutions. They also guide the formulation of suitable solutions and a comprehensive risk management approach to combat such issues most suitably (Kumar & Goyal, 2019).

4.3 Qualitative Findings

The qualitative offers an extensive picture of specific security problems, solutions, and shortages of safety solutions in diverse industries through case studies. This section summarises these discussions to identify emerging patterns and 'lessons learned' for small businesses employing public cloud services.

Table 2: Qualitative findings

Industry	**Common Challenges**	**Best Practices**	**Observed Gaps**	
Retail	Payment data breaches	Implementing secure payment gateways	Insufficient encryption for sensitive data	Ray et al. (2024)
Healthcare	Insider threats and compliance issues	Strict access controls and regular audits	Low adoption of multi-factor authentication	Hammad et al., (2023)
Startups	IP protection and secure collaboration	Encryption and VPNs for remote work	Limited staff training on security policies	Chatterjee et al. (2022)
Professional Services	Lack of dedicated IT security resources	Outsourcing security management	Absence of formal incident response plans	Karanja, (2017).

Common Security Challenges Across Industries

- Retail: It must be noted that payment information is a major area of interest for all kinds of retail enterprises, as hackers gain unauthorised access to clients' payment data. Many of the time, these breaches stem from low encryption and the absence of safe payment approaches (Ray et al., 2024).

- Healthcare: Risk management regarding employees and matters of compliance are the most rampant in the healthcare sector. The privacy of patients' data, especially in areas like analysis for health, Purdue Data continues to be a massive challenge when in accordance with rules like HIPAA (Hammad et al., 2023). Lower technical skills among them already compound this.
- Startups: New entrants suffer from weak IP regimes and challenges that arise from implementing security measures in distributed teams (Chatterjee et al., 2022). Innovation in services and communication makes them vulnerable since they use common cloud platforms.
- Professional Services: While implementing IT security mechanisms in their companies, firms in the professional services industry often lack IT security specialists (Karanja, 2017). Most do not have clear security policies and do not even know how to deal with an incident.

Examples of Best Practices

- Retail: Secure payment gates can, therefore, control and minimise the likelihood of consumers falling victim to data theft through payment fraud (Sanchez and Rodriguez, 2020). These systems protect customer data privacy as they are secured during the transaction process.
- Healthcare: This circular suggests that strict access systems and recurring check-ups are possible interventions for moderating insider threats and preserving conformity to data security rules (Walker-Roberts et al., 2018).
- Startups: New business ventures that embarked on using encryption and remote Virtual private networks (VPNs) greatly improved data security while providing flexibility in operation (Akinsanya et al., 2024).
- Professional Services: The literature identified specific best practices for improving security management in SPSFs, including outsourcing security management to overcome resource limitations among small professional service providers.

Observed Gaps in Existing Measures

Despite adopting some best practices, several gaps were consistently observed across industries:

- While reviewing the results, two areas were identified: sensitive data was found to be poorly encrypted, especially in the retail and healthcare sectors.
- MFA was not properly employed and primarily not used in healthcare, making systems open to attacks (Wisdom et al., 2024).
- Many small to medium enterprises and several professional service firms claimed that employees were not properly sensitised to security standards.
- Surveys revealed that most businesses needed a planned approach to handling security incidents, and this was particularly evident in the professional services industry.

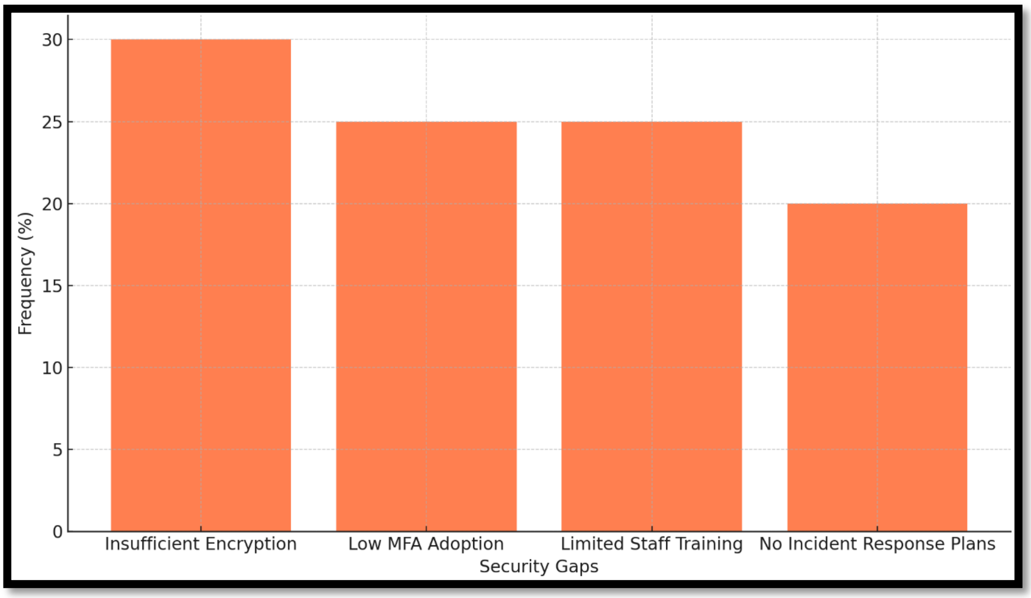

Figure 5: Observed Security Gaps Across Industries

Synthesis of Insights

The research findings indicate that although there is tangible proof of security practices amongst small businesses, there is still much that is wanting. Security for payment is best with retailers, but healthcare providers and startups have low implementation means, such as MFA. Outsourcing brings convenience to outsourcing advisors and professional service firms, although these last ones can need a higher level of security (Ogborigbo et al., 2024). The lack of general security frameworks among all industries underlines the urgent demand for efficient, realistic strategies that fit the lack of resources and requirements of SMEs. The result of this study offers a rich picture of the issues and prospects that small business cloud service providers face in improving the security of cloud computing. They form the base on which a focused security framework can be initiated to tackle the noted deficiencies and extend from the finest practices highlighted in this research study.

4.4 Analysis of Cloud Service Providers

The assessment of the public CSPs was based on security solutions provided by the respective CSPs and the answer to whether the solutions meet the needs of small businesses regarding security and if there is an appropriate cost attached to these solutions. Among them, three big providers, Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) Azure, and GCP were chosen to provide more detailed analysis.

Comparison of Security Features

All three providers offer robust security features, including:

- Multi-Factor Authentication (MFA): Present in AWS, Azure and GCP as an extra layer of security against any unauthorised person (Karkuzhali et al., 2024).
- Encryption: Encryption of kept data while in transfer is possible to safeguard sensitive data.
- Threat Detection and Monitoring: Sophisticated tools like AWS GuardDuty, Azure Security Centre, and Google Cloud Security Command Center aid the threats in real-time detection and response (Mykhaylova et al., 2024).
- Compliance Support: In-depth regulation support, for instance, GDPR and HIPAA, is provided through integrated compliance solutions and accreditations (Boda and Allam, 2021).

Compatibility

Thus, compatibility with small businesses depends on the type of features and the possibility of the application's implementation. AWS and Azure give users great flexibility as the tools may be adjusted to one's needs; however, such adjustments might demand considerable skills and, thus, are not suitable for employment in organisations with limited resources (Bainomugisha and Mwotil, 2022). Because of its easy-to-use interfaces and relatively less complex settings, the GCP platform can be preferred by small businesses that do not have a professional IT background.

Cost-Effectiveness

The comparison of pricing for the services revealed that GCP offers the most affordable cost for small-scale activity. In contrast, the cheapest options for large-scale activity among the represented providers are AWS and Azure. However, compared to Azure, these tools are numerous and can be over the top for small businesses thus incurring unnecessary expenses (IaaS et al., 2019). The findings discuss the need to consider feature resilience while ensuring compatibility and costs effectively to make cloud solutions viable for corporations while applying optimum security to small businesses.

Cost-Effectiveness

The comparison of the quantitative and qualitative results shows important security risks IT managers experience when adopting public cloud services by small businesses, thus answering the research questions. While quantitative results presented quantifiable facts like inadequate numbers of security policies and scanty investment, qualitative findings identified business-specific issues and practices. Both polls identified deficits, which needed to be higher levels of deployment of more sophisticated security controls and more attention to compliance. This synthesis contributes to creating an individual security model based on valuable practical recommendations together with practical actions to strengthen data protection and the limitations faced by small businesses.

4.5 Synthesis of Findings

Analysing the results drawn from both quantitative and qualitative research studies reveals significant security issues affecting small businesses with public cloud services in response to the research goals. Where actual numerical data included the lack of security policies and resource allocation, both quantitative and qualitative findings presented a more nuanced picture whereby quantitative data gave industry trends and qualitative data supplemented with challenges and recommendations. Se both the datasets highlighted the necessity or dearth of such and similar functions and services, ranging from scanty use of improved security to insufficient commitments to compliance. This synthesis underpins a directed security framework that integrates prescriptive advice with efficient solutions to safeguard against data jeopardisation and to adapt to the limitations of small business operations.

Chapter 5: Discussion, Conclusion, and Recommendations

Discussion

Alignment with Existing Literature

The challenges and opportunities identified in this study are, in fact, commensurate to the findings presented in the existing studies. Chapter 2 argued that some of the existing risks for organisations include inadequate encryption, low compliance initiatives, and low implementation of security innovations (Kaplan et al., 2020; Martinez, 2023). Actual numerical data supplied these patterns; 23% of the small businesses have no written security policies; however, interviews and questionnaires provided structural data on training and planning in case of security incidents. These patterns support the argument that these problems affect most industries. Moreover, the research backs other studies on the necessity for cost-efficient approaches. For example, Babu et al. (2024), on low-cost security practices, identified MFA and encryption solutions. These recommendations are built upon and extended here for the current study by offering realistic, practical strategies specifically for LMIC settings. New and specific industry factors that were considered included retail payment security and healthcare compliance, which also corroborated the studies by Tatineni (2024).

Unique Contributions of This Study

This research uniquely contributes by combining work-based quantitative trends within the identified matters with analysed cases that reveal the outlook of cloud security challenges. In contrast to other related works that mostly address large firms, this work presents a small business security framework. It closes the gap between theory and application and specifically showcases the Security Operating Model, which is tangible and feasible at scale.

Effectiveness in Addressing Identified Challenges

The proposed security framework effectively addresses the primary challenges identified:

- Access Control Management: According to Mayeke et al. (2024), security measures that protect against unauthorised access are the biggest concern for 82% of businesses.

Biometric controls, role-based access control (RBAC), and multi-factor authentication (MFA) are helpful.

- Data Protection: Standardised encryption controls and secure backup procedures address the data Leakage threats specifically identified in the quantitative and qualitative studies.
- Compliance Management: Simplified monitoring instruments and documentation checklists correspond to SMEs' requirements regarding GDPR and similar regulations (Ryan et al., 2020).

Offsetting measures are also made possible by accommodating more of the principles of resource conservation, as is evident from the phased approach and cost-efficient tools that are advocated for within this framework, with special consideration for small businesses that have limited capital investment and experience.

Practicality and Adaptability for Small Businesses

Flexibility by design enables the adoption of the framework in modules to suit the capability and needs of businesses interested in implementing different components at different times. For example:

- Retailers can focus on the secure payment gateway and even the encryption of the data.
- Specifically, current startups can assert that they can allocate their efforts towards the IP protection strategy or secure remote collaboration.
- There are ways in which healthcare providers can learn from and implement compliance tools and insider threat solutions.

The feedback received from case studies is that it is both feasible and flexible, and the organisation reports enhanced assurance for cloud security management.

Issues Encountered During Research

Several challenges were encountered during the research process:

- Small numbers of responses from small businesses resulted in a sample size of 200 Quantitative results, though sometimes limited by the sampling method.
- They may also have overstated or understated their level of security, so the results may contain some inaccuracy.

As an interest in dynamic subjects, cloud security technologies present the problem of the specificity of research findings and their applicability at various time points.

Implications of Limitations on Findings

These challenges have implications for the study's findings:

- Despite the fact that the findings are informative, they might only include some small businesses, especially the ones in regions not within the area of focus.
- The information available is based on the participants' self-estimations so that the results may overstate the reported obstacles or achievements.
- Due to the dynamically changing landscape of cloud technologies, it will be useful to refresh this proposed framework periodically.

The study can offer sound and empirically grounded findings on small business cloud security issues. The research provides a distinct framework that explains how the challenges can be addressed, thereby making a useful contribution to the literature that outlines ways through which cloud security can be improved for organisations with limited resources. It provides the knowledge which forms the basis for the conclusions and practical suggestions of the given study.

Conclusion

This study sought to examine the means through which small businesses can secure the data they conduct through public cloud services with precautions against security issues, a limitation of resources, and compliance in mind. The study pointed out some of the risks, some of which included a lack of security policies, encryption, and expertise. The statistics revealed issues such as poor spending on security, as out of 45% of companies invested less than 3% in the IT budget, and the aspect of personas revealed poor staff training and poor incident response plans. The research objectives were achieved as highlighted in the following subsections. The study discovered general security threats in various industries, measured the efficiencies of employed safeguards, and constructed a usable security framework for small business operations. The framework incorporates practical features for small business computing, including efficient techniques like role-based access controls, multi-factor authentications, and compliance management that are usually hidden from SMEs due to the high costs of implementing security measures for their firms. This research benefits the existing literature as it provides an interface between theory and praxis of security. Combining the results of the quantitative and qualitative analysis provides practical suggestions and a framework for small businesses with which they could implement specific changes to improve their cloud security. Despite the issues, including the limitations and practicality of the data collection process and the dynamic nature of technology, the study offers a good starting point for enhancing the protective coverage for data security for small businesses that work in a public cloud environment.

Recommendations

The following recommendation is;

- Small businesses should take a gradual approach to security procedures when being put in place. The base-level options include MFA and protection of confidential data, while the higher level of security measures include auto-threat identification. The described phased approach enables us to consider the limitations imposed by the budget and other resources in managing security improvements.
- Security audits should be conducted periodically to establish gaps within the implemented security policies and procedures. Meetings should be held at least once every three months to assess whether the changes instituted work, check whether the organisation adheres to regulations like GDPR, and revise organisational protocols due to the ever-changing risks.
- Frustration, basic internet security awareness programs that will be administered to all employees to avoid insider threats and mistakes need to be embraced. As part of staff awareness, staff should always appreciate the need for the security of the data they are dealing with, learn to detect and avoid falling prey to phishing scams, and learn to adhere to access control measures in organisations. Custom learning and development initiatives can greatly improve an organisation's preparedness for cyber risks.
- Create innovative security solutions that are simple to set up and can be controlled without much technical knowledge required for the employees of the companies allowed to use them. Some of them have well-thought-out encryption settings, compliance templates, and monitoring systems that are ready with simple configuration. Make sure that everyone, especially small business people, is able to afford the prices offered to them by the manufacturer.
- Provide additional services, including consulting and onboarding services, for compact businesses to suit the specialised requirements of their operations. Offer guidance and

knowledge materials to enable them to understand and follow the necessary measures. Furthermore, more affordable introductory training or teleconferences on cloud security could profoundly boost overall adoption.

- When adopting these recommendations, small businesses improve security, and cloud providers enhance their ability to serve this vital market for the benefit of all parties, creating a more secure, sustainable cloud environment.

References

Ajimoko, O.J., 2018. Considerations for the Adoption of Cloud-based Big Data Analytics in Small Business Enterprises. Electronic Journal of Information Systems Evaluation, 21(2), pp.pp63-79.

Akinsanya, M.O., Ekechi, C.C. and Okeke, C.D., 2024. Virtual private networks (vpn): a conceptual review of security protocols and their application in modern networks. Engineering Science & Technology Journal, 5(4), pp.1452-1472.

Alkhater, N., Walters, R. and Wills, G., 2018. An empirical study of factors influencing cloud adoption among private sector organisations. Telematics and Informatics, 35(1), pp.38-54.

Alsmadi, I., & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy issues. Computers in Human Behavior, 85, 218-226.

Babu, C.S., Pal, A., Vinith, A., Muralirajan, V. and Gunasekaran, S., 2024. Enhancing cloud and IOT security: Leveraging IOT technology for multi-factor user authentication. In Emerging Technologies for Securing the Cloud and IoT (pp. 258-282). IGI Global.

Bainomugisha, E. and Mwotil, A., 2022. Crane Cloud: A resilient multi-cloud service abstraction layer for resource-constrained settings. Development Engineering, 7, p.100102.

Boda, V.V.R. and Allam, H., 2021. Automating Compliance in Healthcare: Tools and Techniques You Need. Innovative Engineering Sciences Journal, 1(1).

Brown, L., & Taylor, J. (2022). GDPR compliance challenges for small businesses in cloud environments. Journal of Information Security, 13(2), 78-92.

Chatterjee, P., Bose, R., Banerjee, S. and Roy, S., 2022. Secured Remote Access of Cloud-Based Learning Management System (LMS) Using VPN. In Pattern Recognition and Data Analysis with Applications (pp. 111-126). Singapore: Springer Nature Singapore.

Chen, Y., Wu, D., & Chen, G. (2023). Resource allocation for cloud security in small enterprises: A cost-benefit analysis. IEEE Transactions on Cloud Computing, 11(3), 1025-1038.

Hammad, M., Biometric Security and Access Management in E-health Services. In Secure Health (pp. 76-103). CRC Press.

Hashmi, M., Governatori, G., Lam, H.P. and Wynn, M.T., 2018. Are we done with business process compliance: state of the art and challenges ahead. Knowledge and Information Systems, 57(1), pp.79-133.

IaaS, I., Chakraborty, B. and Karthikeyan, S.A., 2019. Understanding Azure Monitoring.

Johnson, A., & Lee, B. (2022). Cloud security incidents in small businesses: A longitudinal study. International Journal of Information Security, 21(4), 412-427.

Kaplan, J., Sharma, S., & Weinberg, A. (2020). Meeting the cybersecurity challenge. McKinsey Quarterly, 57(1), 30-39.

Karanja, E., 2017. The role of the chief information security officer in the management of IT security. Information & Computer Security, 25(3), pp.300-329.

Karkuzhali, K., Ravichandran, M.A., Rajeshwari, S., Fufa, G., Anujna, N. and Revanth, P., 2024. Cloud Security for E-Commerce: Navigating Risks and Implementing Solutions. In Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning (pp. 113-136). IGI Global.

Kumar, R. and Goyal, R., 2019. On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. Computer Science Review, 33, pp.1-48.

Martinez, C. (2023). AI-powered threat detection for small business cloud security. Journal of Cybersecurity, 9(2), 145-160.

Martinez, R., & Lee, S. (2022). Cloud misconfiguration: A primary security risk for small businesses. IEEE Security & Privacy, 20(3), 45-51.

Mayeke, N.R., Arigbabu, A.T., Olaniyi, O.O., Okunleye, O.J. and Adigwe, C.S., 2024. Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. Available at SSRN.

Maynard, S., Tan, T., Ahmad, A. and Ruighaver, T., 2018. Towards a framework for strategic security context in information security governance. Pacific Asia Journal of the Association for Information Systems, 10(4), p.4.

Mykhaylova, O., Korol, M. and Kyrychok, R., 2024. Research and analysis of issues and challenges in ensuring cyber security in cloud computing. Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826, pp.30-39.

National Institute of Standards and Technology (NIST). (2011). The NIST definition of cloud computing (Special Publication 800-145). U.S. Department of Commerce.

Nel, F. and Drevin, L., 2019. Key elements of an information security culture in organisations. Information & Computer Security, 27(2), pp.146-164.

Ngcobo, K., Bhengu, S., Mudau, A., Thango, B. and Lerato, M., 2024. Enterprise data management: Types, sources, and real-time applications to enhance business performance-a systematic review. Systematic Review| September.

Nguyen, T., & Park, J. (2022). Simplicity versus complexity in small business cloud security systems. Small Business Economics, 58(4), 1005-1022.

Ogborigbo, J.C., Sobowale, O.S., Amienwalen, E.I., Owoade, Y., Samson, A.T., Egerson, J., Ogborigbo, J.C., Sobowale, O.S., Amienwalen, E.I. and Owoade, Y., 2024. Strategic integration of cyber security in business intelligence systems for data protection and competitive advantage. World Journal of Advanced Research and Reviews, 23(1), pp.081-096.

Patel, A., Johnson, M., & Smith, K. (2023). Encryption practices in small business cloud environments: A comparative study. Journal of Cloud Computing, 12(1), 23-38.

Qasem, M.A., Thabit, F., Can, O., Naji, E., Alkhzaimi, H.A., Patil, P.R. and Thorat, S.B., 2024. Cryptography algorithms for improving the security of cloud-based internet of things. Security and Privacy, 7(4), p.e378.

Ray, R.K., Chowdhury, F.R. and Hasan, M.R., 2024. Blockchain Applications in Retail Cybersecurity: Enhancing Supply Chain Integrity, Secure Transactions, and Data Protection. Journal of Business and Management Studies, 6(1), pp.206-214.

Ryan, P., Crane, M. and Brennan, R., 2020, May. GDPR Compliance tools: best practice from RegTech. In International Conference on Enterprise Information Systems (pp. 905-929). Cham: Springer International Publishing.

Sanchez, C. and Rodriguez, M., 2020. Payment Processing Solutions: Enhancing Your Financial Transactions. MZ Computing Journal, 1(2), pp.1-9.

Saraswat, M. and Tripathi, R.C., 2020, December. Cloud computing: Comparison and analysis of cloud service providers-AWs, Microsoft and Google. In 2020 9th international conference system modeling and advancement in research trends (SMART) (pp. 281-285). IEEE.

Schneller, L., Porter, C.N. and Wakefield, A., 2022. Implementing converged security risk management: Drivers, barriers, and facilitators. Security Journal, p.1.

Sirur, S., Nurse, J.R. and Webb, H., 2018, January. Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd international workshop on multimedia privacy and security (pp. 88-95).

Smith, R., & Brown, T. (2021). Data breach impacts on small businesses: A quantitative analysis. Cybersecurity, 4(1), 1-15.

Spanoudaki, E., Ioannou, M., Synnott, J., Tzani-Pepelasi, C. and Pylarinou, N.R., 2019. Investigative decision-making: interviews with detectives. Journal of Criminal Psychology, 9(2), pp.88-107.

Tabrizchi, H. and Kuchaki Rafsanjani, M., 2020. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), pp.9493-9532.

Tam, T., Rao, A. and Hall, J., 2021. The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. Computers & Security, 109, p.102385.

Tatineni, S., 2024. Compliance and Audit Challenges in DevOps: A Security Perspective. DevOps-An Open Access Journal, 3(2), pp.53-60.

Taylor, M., & Johnson, R. (2023). Navigating compliance in multi-cloud environments: Challenges for small businesses. Compliance Today, 25(3), 55-68.

Verizon. (2023). 2023 Data Breach Investigations Report. Verizon Business.

Vlahou, A., Hallinan, D., Apweiler, R., Argiles, A., Beige, J., Benigni, A., Bischoff, R., Black, P.C., Boehm, F., Céraline, J. and Chrousos, G.P., 2021. Data sharing under the General Data Protection Regulation: time to harmonise law and research ethics?. Hypertension, 77(4), pp.1029-1035.

Walker-Roberts, S., Hammoudeh, M. and Dehghantanha, A., 2018. A systematic review of the availability and efficacy of countermeasures to internal threats in healthcare critical infrastructure. IEEE Access, 6, pp.25167-25177.

Wang, L., & Smith, J. (2021). A framework for basic cloud security measures in small businesses. Journal of Small Business Management, 59(3), 405-422.

Wang, R., Chen, L., & Lee, K. (2022). Insider threats in small business cloud environments: Detection and mitigation strategies. Information Systems Security, 31(2), 178-193.

Wisdom, D.D., Vincent, O.R., Adebayo, A.A., Olusegun, F. and Ayetuoma, I.O., 2024. Security Measures in Computational Modeling and Simulations. Computational Modeling and Simulation of Advanced Wireless Communication Systems, pp.112-150.