Information Dynamics and Applications
https://www.acadlore.com/journals/IDA

Critical Factors Influencing Cloud Security Posture of Enterprises: An Empirical Analysis

Vidura Jayasinghe[1], Emre Erturk[1*], Zhe Li[2]

[1] School of Computing, Eastern Institute of Technology, 4112 Napier, New Zealand
[2] School of Computer and Information Science, Hubei Engineering University, 432000 Xiaogan, China

* Correspondence: Emre Erturk (eerturk@eit.ac.nz)

Received: 11-15-2023 **Revised:** 12-16-2023 **Accepted:** 12-23-2023

Citation: V. Jayasinghe, E. Erturk, and Z. Li, "Critical factors influencing cloud security posture of enterprises: An empirical analysis," *Inf. Dyn. Appl.*, vol. 2, no. 4, pp. 210–222, 2023. https://doi.org/10.56578/ida020405.

Abstract: This study examines the aspects that can impact an organization's cloud security posture and the consequences for their cloud adoption strategies. Based on a thorough examination of existing literature, a conceptual framework is developed that includes several aspects such as organisational, technical, regulatory, operational, and human elements. The cloud security readiness is influenced by these five types of characteristics. A research instrument is utilised to evaluate the hypotheses pertaining to those aspects. The pilot survey showcases the research tool within the framework of a representative sample of organisations. In addition to conducting instrument testing, the initial responses also validate the importance of several elements that impact cloud security. The prominence of technical capabilities as a key factor underscores their vital contribution to bolstering cybersecurity readiness. Regulatory factors have a significant role in emphasising the necessity of compliance in cloud security. Organisational elements, such as managerial support, training, budget allocation, policy adherence, and governance, have a moderate impact. The presence of human elements also appears to contribute to and emphasise the necessity of promoting security awareness and alertness. This study enhances the existing body of knowledge on cloud security by offering insights into the various complex issues involved. The results can provide guidance to professionals seeking to enhance the cloud security of enterprises and scholars studying the changing cloud environment.

Keywords: Cloud security of enterprises; Security vulnerabilities; Cloud security measures; Risk management

1 Introduction

Cloud computing has revolutionised businesses in every industry by providing a wide range of services, software, and infrastructure options, resulting in improved company effectiveness and efficiency. The current advancement in cloud computing allows for uninterrupted internet access to services, files, and applications, providing further advantages such as cost reduction, increased scalability, and enhanced flexibility [1]. However, the adoption of new technologies carries inherent security risks and challenges that companies must address in order to protect sensitive data and maintain a secure working environment [2].

The study examines crucial determinants that impact the security of corporate cloud systems, with the objective of offering valuable insights to enhance current understanding. Additionally, it delves into the obstacles that firms encounter. Organisations may enhance their cloud security plans, reduce risks, and safeguard sensitive data and systems by comprehending these elements. Furthermore, this study examines the interaction between these autonomous variables and their collective influence. Consequently, this paper presents practical suggestions to improve cloud security processes. The objective of the study is to ascertain the primary factors that have a significant impact on cloud security in enterprise environments. Additionally, the study seeks to comprehend the connections and interplay between these factors, assess the efficacy of existing security practices and controls in addressing these factors, and put forth recommendations and guidelines to bolster cloud security strategies and mitigate risks. The research inquiries are as stated below:

(a) What are the primary risks and weaknesses that pose a serious danger to cloud computing?
(b) What are the main aspects that influence the security posture of cloud infrastructures in enterprises?
(c) How do these aspects interact and affect the overall security posture of cloud environments in enterprises?

(d) What methods may enterprises employ to create robust security plans that protect sensitive data and minimise risks?

(e) What security measures may cloud service providers and vendors adopt to enhance their capabilities and guarantee data protection for customers?

(f) What are the most effective techniques for validating security and ensuring compliance in cloud-based systems and applications?

2 Factors Affecting Cloud Security

The advent of cloud computing has generated apprehensions regarding security, encompassing both strategic and tactical aspects. In order to address these concerns, security procedures have been implemented across different cloud service and deployment types [3]. These cloud security measures include governance-related security measures that comprise strategic and policy-related factors within the cloud environment. Conversely, the operational domains focus on resolving tactical security concerns and implementing them inside the architecture [4]. These measures are intended to tackle the interconnected variables that affect cloud security. The choice of cloud service model by an organisation has a substantial impact on the potential security vulnerabilities. Within the context of Infrastructure as a Service (IaaS), the cloud provider assumes responsibility for managing the infrastructure, while the client is accountable for all other aspects, such as the operating system, applications, and data. This architecture offers significant versatility, but it also places a considerable share of the security accountability on the consumer. Platform as a Service (PaaS) involves the supplier taking care of the operating system and middleware, while the customer is responsible for the applications and data. In the context of Software as a Service (SaaS), the supplier assumes responsibility for overseeing all aspects of the software, while the customer primarily functions as a user of the product. The primary role of the user is to effectively handle data management and access control. This helps to minimise the range of potential security concerns, although it may not necessarily mitigate their severity [5].

Furthermore, the selection of the cloud provider plays a crucial role in the process of adopting cloud technology. Cloud providers may employ different security policies and practices. For instance, certain entities may employ powerful encryption methods to protect data during transmission and storage, offer comprehensive identity and access management (IAM) solutions, or provide extensive logging and monitoring features [1]. The provider's transparency regarding its security infrastructure and adherence to security standards and certifications, such as International Organization for Standardization (ISO) 27001 and Payment Card Industry Data Security Standard (PCI DSS), is crucial. Regardless of the level of security in a cloud provider's infrastructure, security in the cloud is governed by a shared responsibility model, where both the provider and the client have distinct security responsibilities [3]. Governance and risk management, encompassing legal matters, compliance and audit management, and information governance, are essential components of cloud security. To achieve secure and efficient utilisation of cloud services, organisations must adequately handle these elements [6].

Cloud computing brings new aspects to the governance and control of organisational risks. Organisations are required to maintain governance accountability, even while using third-party services, due to the shared responsibility paradigm in cloud computing. The choice of service and deployment models, such as SaaS, PaaS, and IaaS, greatly influences governance structures and risk management techniques. Managing public cloud environments can be challenging due to the limited control over assets. Therefore, it is crucial to actively manage relationships with cloud providers, conduct rigorous contract reviews, and implement responsive governance mechanisms [6]. Effective governance and risk management are facilitated by tools and procedures such as supplier assessments, compliance reporting, and risk controls. Conducting regular assessments, audits, and ensuring that risk needs are aligned with assets are essential in reducing possible threats [7]. Organisations should so carefully plan and execute strategies to successfully and safely manage the complexities of cloud computing.

Organisations have many legal considerations when adopting cloud computing, including information protection, disclosure of security breaches, regulatory duties, privacy concerns, and compliance with international laws. These problems emphasise the crucial significance of adhering to the law [6]. Cloud providers and customers face distinct issues due to the differing data protection and privacy legislation in various nations. Hence, organisations must remain updated on the changing rules and regulations that are pertinent to their cloud operations, which can require the assistance of legal advice. Contracts and privacy warnings play a crucial role in safeguarding data, as cloud clients are frequently bound by contractual responsibilities to safeguard personal information and guarantee its security. Although data processing has been outsourced, the responsibility for ensuring data protection lies with the data custodian. Prior to engaging into contracts with cloud providers, organisations should perform comprehensive due diligence, taking into account aspects such as the nature of the service, the provider's reputation, the level of support offered, and the location of the data centre [3]. Managing electronic discovery (e-discovery) is an additional obstacle in cloud computing, requiring meticulous preparation and collaboration between customers and suppliers. To effectively navigate the legal aspects of cloud computing, one must possess a thorough comprehension of pertinent frameworks, precise contract administration, and strong data protection protocols.

Ensuring compliance and effectively handling audits are essential for maintaining the security posture of cloud systems. Transitioning to cloud computing presents organisations with the task of adhering to many regulations in several countries and modifying their operations to suit virtual environments. Given that current legislation frequently overlook virtualized or cloud settings, it is imperative for stakeholders, such as consumers, auditors, and providers, to comprehend the regulatory consequences associated with utilising particular cloud services. Important factors to consider include comprehending the capabilities of service providers in meeting regulatory requirements, the impact of provider audits and certifications on the extent of the customer's own audits, and the management of compliance over an extended period of time. The notion of compliance inheritance, whereby the certified services offered by the supplier relieve the consumer of certain auditing obligations, is crucial. However, customers are still accountable for ensuring that their applications, which are built on top of the provider's services, meet all the necessary requirements. Managing audits include comprehending compliance duties, assessing provider attestations, generating compliance artefacts, and monitoring providers' compliance statuses. Compliance, audit, and assurance should be ongoing procedures, rather than isolated activities. Providers should effectively convey audit findings, certifications, and restrictions to aid customers, while also upholding certifications and promptly informing customers of any changes in status [3]. The transition to cloud-based architectures necessitates new approaches to protecting data, given characteristics such as scalability, shared resource usage, and simplified management.

Cloud computing presents novel obstacles for information governance. The presence of multiple tenants sharing infrastructure in a multitenancy setup gives rise to security and governance concerns. In cloud computing, there is a need for a clear understanding of data ownership and custodianship due to the shared security responsibility. This is particularly important as cloud providers take on the role of additional custodians in the governance paradigm. The involvement of third parties and changes in jurisdiction make compliance, regulations, and privacy policies more intricate.

Cloud computing enables the distribution of data storage across several places, which gives rise to difficulties over adherence to locational and jurisdictional regulations. It is crucial to synchronise information management and security strategies with these duties. The data security lifecycle, which includes the stages of production, storage, usage, sharing, archiving, and destruction, offers a valuable structure for adopting security controls at every stage of the data's existence [8].

Various suggestions arise for tackling these governance obstacles. Prior to migrating to the cloud, organisations should define their governance requirements, taking into account their legal duties, contractual agreements, and corporate policies. Effective management of data in the cloud necessitates the implementation of information governance rules and practices. This entails establishing a strong partnership and cooperation between organisations and cloud service providers. Utilising the data security lifecycle model is advantageous for directing data handling procedures. Lastly, transitioning to the cloud offers a chance to evaluate and enhance information architectures, enabling organisations to tackle any fragmented practices and reorganise existing information management strategies. In summary, it is crucial to have efficient information governance in the cloud to handle potential dangers and safeguard confidential data. This requires the development of innovative approaches to navigate the intricate nature of cloud computing.

Various operational domains in cloud security encompass the management plane, business continuity, infrastructure security, virtualization and containers, incident response and remediation, application security, data security and encryption, identity, entitlement, and access management, security as a service, and related technologies. The overall cloud security posture is directly influenced by internal IT and security practices.

The management plane, serving as the interface that connects and configures the cloud infrastructure, requires robust security measures to restrict access and guarantee the security of the data centre. Centralising the management plane offers advantages such as enhanced visibility and control over resources. However, it also presents notable security and configuration difficulties. To secure the management plane, it is essential to implement strong IAM rules, utilise multi-factor authentication (MFA), and enforce the principle of least privilege access [9].

Ensuring business continuity and disaster recovery (BC/DR) is of utmost importance in the realm of cloud computing. An effective BC/DR strategy must encompass measures to guarantee uninterrupted operations and swift recovery inside the cloud service provider. It should also address the management of provider outages and explore possibilities for seamless migration across other providers or platforms.

Cloud computing security is dependent on various essential elements. The Software Defined Perimeter (SDP) concept serves as a fundamental element that enhances infrastructure security by dynamically allocating network access according to device and user authentication. Another crucial factor is incident response and management, which necessitates appropriate procedures for problem identification, communication, and resolution, considering the intricacies brought about by cloud computing. Application security is a crucial aspect that needs careful consideration while creating or transitioning applications to the cloud, taking into account various cloud platforms like SaaS, PaaS, or IaaS. Ensuring the confidentiality and integrity of sensitive information in the cloud requires the use of data security measures, encryption techniques, and robust key management systems. The field of security as a

service investigates the potential advantages and factors to consider when delegating security functions to specialised third-party providers. Finally, it is crucial to thoroughly examine and comprehend the security ramifications of incorporating interconnected technologies like big data, Internet of Things (IoT), and mobile computing into cloud systems.

As stated in the study by Gui et al. [10], the distribution of funds is a crucial determinant of the adoption of security measures in cloud computing. Implementing and sustaining strong security measures in cloud environments sometimes necessitates significant financial commitments. Organisations must take into account costs associated with infrastructure, staff, training, and adherence to regulations. Infrastructure costs encompass expenses related to licencing or subscribing to security solutions, such as firewalls, intrusion detection systems, and encryption tools [1]. The results presented in the study by Gui et al. [10] indicate that organisations should allocate resources towards hiring proficient security experts or partnering with managed security service providers (MSSPs) to develop, execute, and oversee the security architecture. Aside from personnel expenses, budget allocation should also consider provisions for training programmes and certifications to guarantee that security workers are well-informed about the most current cloud security protocols and technology. Compliance and auditing expenses are necessary in order to adhere to regulatory standards and fulfil industry-specific criteria. Hence, organisations must meticulously manage their budget allocation to guarantee efficient cloud security, taking into account their security prerequisites and risk tolerance.

Within the realm of cloud security, the time it takes to bring a product to market is a significant consideration that must be carefully weighed against the demands of ensuring security. As stated in the study by Mozumder et al. [11]. Nevertheless, hasty deployments lacking sufficient security safeguards can subject organisations to substantial risks and vulnerabilities. Hence, it is imperative to integrate security evaluations at the outset of the deployment process. Organisations can detect and resolve potential vulnerabilities by undertaking comprehensive security assessments, which involve architecture reviews, penetration testing, and vulnerability scanning [7]. In order to accelerate the deployment process, it is possible to utilise automation and DevSecOps approaches. By incorporating infrastructure as code (IaC) and continuous integration and deployment (CI/CD) pipelines, security controls can be integrated at the beginning of the development cycle, guaranteeing that security safeguards are not compromised [12]. In addition, organisations have the opportunity to utilise pre-configured security solutions such as cloud-native security services or managed security services. These solutions are specifically designed to expedite implementation and allow organisations to benefit from the knowledge and skills of specialised security providers [13]. Striking a balance between expeditious product release and implementing sufficient security measures is of utmost importance, and organisations ought to develop unambiguous security protocols.

3 Methodology

The study's design was heavily influenced by a well-organized conceptual framework that was developed based on thorough literature reviews on cloud security. This approach methodically classified numerous elements that impact an organization's cloud security posture. Hypotheses were formulated based on this deduction, and a questionnaire was later created to test these assumptions. The found components were further classified into separate clusters to provide organisation and consistency to the study, as demonstrated below in Table 1. These clusters not only enabled a methodical study but also aided in hypothesis formulation.

The mediating factors that can impact the interaction between independent variables and the dependent variable are as follows: the size of the organisation, the sector in which it operates, the type of cloud deployment model used (public, private, hybrid), the geographic location, the size of the Information Technology (IT) staff, the organization's experience with cloud services, the type of data handled, and the cloud service model employed (SaaS, PaaS, IaaS).

After the development of this framework, specific assumptions were formulated. Each independent variable was suggested to have an impact on the dependent variable, presumably through the involvement of the identified mediating variables. The variable being measured in this study is the cloud security posture of an enterprise.

The questionnaire was partitioned into four primary sections, each fulfilling a unique objective:

Part A: Individual profile. This component was designed to gather information about the respondent's history, ensuring that the feedback received was based on their personal experience and knowledge. The participant's level of knowledge and experience in cloud computing, as well as their position within the organisation, would give background information for the following answers.

Part B: Organisational profile. The questions in this area were created to assess the organization's size, industry, cloud service models, and other specific information. Understanding industry-specific or size-related trends and variations in cloud security postures requires key knowledge.

Part C: Evaluation of cloud security posture in enterprises: This section specifically assessed the respondents' perceptions regarding their organization's level of preparedness in terms of cloud security. The Likert scale-based questions were designed to evaluate the participants' confidence levels on their organization's cloud defences.

Table 1. Independent variables

Cluster/Category	Elements and Description
Organisational factors	Internal structure of an organization and its overarching strategies: - Management support for security initiatives - Security awareness and training - Security budget allocation - Security governance
Technical factors	Tangible tech solutions and architectures in place: - Security control implementation - Incident response capability - Secure architecture and design - Encryption and key management - Patch and vulnerability management
Legal & regulatory factors	External legal and regulatory pressures: - Compliance with laws and regulations - Audit and assessment - Data privacy issues - Contractual obligations - Geo-location of data
Operational factors	Day-to-day operational activities and their continuity and resilience: - Identity and access management - Disaster recovery planning - Data backup strategy - Security monitoring and logging - Business continuity management
Human factors	People aspect of security: - Inside threats - Staff competence and expertise - Staff turnover rate - Social engineering threats - Staff adherence to security policies

Part D: Factors. This component of the questionnaire had explicit statements that were directly related to the hypotheses. Participants were once again asked to indicate their level of agreement or disagreement with each statement using a Likert scale. Each question presented here corresponds to a specific hypothesis, and the collected data directly contributes to the validation of these hypotheses.

The questionnaire was designed to strike a balance between obtaining targeted, hypothesis-driven information and collecting more comprehensive insights regarding cloud security in the contemporary corporate setting. It was imperative to ensure that the questions were unambiguous, impartial, and focused on capturing authentic perceptions of cloud security postures and procedures.

To summarise, the research methodology employed a clearly defined conceptual framework and adhered to a rigorous, literature-supported approach. This approach ensured that the derivation of hypotheses and the development of the questionnaire closely aligned with the research objectives, ultimately aiming for precision and credibility in the study's findings.

An online survey platform was employed to gather data, which included a combination of closed and open-ended questions. This strategy offers significant benefits in terms of both time and cost efficiency when compared to alternative investigation methods.

Data on the proposed security and privacy variables affecting the adoption of cloud computing was collected using a cross-sectional approach. Data collection was conducted at a certain moment, with the goal of minimising errors by implementing suitable procedural techniques. The unit of analysis consists of a diverse variety of enterprises from several business sectors that have either implemented cloud computing or are interested in adopting it.

In order to ascertain the eligibility of the responders, screening questions were implemented with the purpose of evaluating their understanding and enthusiasm towards cloud computing. This was done to exclude those who did not fulfil the requirements for recruitment. The initial inquiry ascertained whether the responder was affiliated with an organisation, while the subsequent question verified their involvement in IT-related decision-making or the acquisition of new IT applications. The third question assessed the respondent's level of acquaintance with cloud computing.

The researcher's discretion was used to determine the suitability and representativeness of the respondents included in the research. A sample is a carefully selected fraction of the population used for a particular study.

This study specifically examines organisations that have implemented cloud computing. The research seeks to analyse the security and privacy concerns that impact the use of cloud computing services by businesses. Hence, the intended participants for this quantitative study were individuals who possess knowledge and experience in deploying or functioning within a cloud environment, and are actively engaged in IT-related decision-making or the acquisition of new IT applications. Hence, the chosen sample method is convenience sampling. Networking for professional purposes LinkedIn was utilised to conduct a targeted search and establish contact with appropriate respondents.

This study employed purposive sampling to specifically select individuals who possess a deep understanding and extensive experience in cloud computing. Subjective judgement was used to include relevant examples in the sample technique, taking into account practical issues. It is crucial to recognise that the presence of self-selection bias can impact the acquired findings, hence constraining their applicability to the overall community. Nevertheless, this research offers vital insights into the intricacies of the acquired sample, instead of striving for generalizability. The main objective of this exploratory research is to investigate the proposed phenomena and its correlation with the provided hypotheses using an appropriate sample size.

The primary objective of this pilot study is to offer preliminary insights into the diverse aspects that impact cloud security. The pilot study also functions as an initial investigation into comprehending the dynamics of cloud security and the array of components that impact company cloud security. The analysis involves verifying the hypotheses that were formulated based on the literature review. The initial regression analysis, which encompasses tables and graphs, investigates each hypothesis by examining the correlations between the variables and the overall level of cloud security. These findings lay the foundation for future, more thorough investigations. Hence, the findings will be analysed within the framework and constraints of a pilot study.

Table 2 below demonstrates that the respondents possess a minimum level of familiarity or proficiency with cloud computing principles. The responders encompass a range of roles, including managerial and technical positions, and possess a combination of decision-making responsibilities. This diversity guarantees a more equitable viewpoint when making decisions on cloud security.

Table 2. Individual profiles of the respondents

Familiarity	IT Decision Making	Role
Proficient	No	IT manager/director
Familiar	Yes	IT business consultant
Expert	Yes	Cloud architect/admin
Proficient	Yes	Engineer
Familiar	No	Software developer
Familiar	No	Software engineer

These discrepancies highlight how diverse professional backgrounds influence the comprehension of cloud security. Participants, ranging from IT managers to cloud architects, have varying perceptions about cloud security that are influenced by their respective roles. For example, a cloud architect may prioritise addressing technical vulnerabilities, whereas an IT manager may place greater emphasis on enforcing organisational policies.

The organisational profile encompasses the internal and external factors that influence an organisation. These components also serve as mediators within the conceptual framework. The pilot sample consisted of individuals from several sectors, with a slight majority coming from the IT/technology and finance sectors. The bulk of organisations were of considerable size, employing over 500 individuals, and a significant proportion have been utilising cloud services for a duration of 4 to 6 years.

This study has compiled comprehensive profiles of the respondent organisations in different nations, which will remain anonymous in scholarly publications. The specific information comprises the size of the organisation, the type of industry it belongs to, the model of cloud deployment, the geographical location, the cloud service models utilised, the size of the internal IT team, the level of experience the organisation has with cloud technology, and the nature of the data kept in the cloud.

The comprehensive organisational profiles reveal diverse cloud adoption patterns that are driven by criteria such as the size of the organisation, industry, and geographical location. Despite the limited size of the pilot sample, a comprehensive correlation analysis was not possible. However, these initial insights provide insight into the many strategies that companies are employing to navigate the cloud landscape, which are influenced by their unique requirements, past experiences, and limitations. Several significant findings from the pilot test, which could only be determined by a large-scale survey, are:

· Cloud service models: The majority of organisations, regardless of their size or industry, have embraced at

least one significant cloud service model. This highlights the growing utilisation of cloud services in contemporary company operations.

· Data type in cloud: Financial data is a prevalent data category stored on the cloud, particularly among finance-focused organisations. This suggests a high level of confidence in cloud services' ability to manage confidential financial information.

Additionally, it is possible to evaluate the influence of mediating variables on Hypothesis 6, namely the impact of organisational context and features (such as size and industry) and demographics, in moderating the correlations outlined in Hypotheses 1-5. This will demonstrate the significant influence of the larger organisational environment on its cloud security dynamics.

4 Descriptive Analysis of Responses

4.1 Cloud Security Posture

The analysis of the cloud security posture reveals a widespread tendency to agree or strongly agree with the significance of cloud security, with an average rating of 4.30. The respondents' strong affirmative reaction, as seen in Table 3, indicates that they generally hold a confident perspective regarding their organization's cloud security procedures. This suggests a broad adoption of cloud technologies and their built-in security measures. This further implies that the security of cloud computing continues to be a primary concern for the majority of companies.

Table 3. Responses to cloud security posture

	Mean	Median	Mode	Deviation	Avg. Response
Overall Cloud Security	**4.30**				**Agree to Strongly Agree**
Perception on Overall Cloud Security	4.17	4.00	4.00	0.37	Agree to Strongly Agree
Security against data breaches	4.50	4.00	4.00	0.50	Agree to Strongly Agree
Cyber threat cloud protection	4.33	4.50	4.00	0.47	Agree to Strongly Agree
Cyber threat cloud resistance	4.33	4.00	4.00	0.47	Agree to Strongly Agree
Incident detection & response	4.67	4.00	5.00	0.47	Agree to Strongly Agree
Future-proof cloud security	4.00	5.00	4.00	0.58	Agree to Strongly Agree
Cloud service availability	4.17	4.00	4.00	0.37	Agree to Strongly Agree
Security regulations & compliance	4.17	4.00	5.00	1.07	Agree to Strongly Agree
Effectiveness of security controls	4.33	4.50	4.00	0.47	Agree to Strongly Agree

The majority of businesses assessed their cloud security posture as "secure," suggesting a prevailing sense of vulnerability since most respondents did not choose the option of being "highly secure." This issue is further emphasised when the participants acknowledged previous instances of security breaches and potential risks to their data kept in the cloud. Nevertheless, the data also indicates that these businesses are highly proactive in addressing issues. The cloud's ability to protect against cyber threats, detect and respond to incidents, and the efficiency of its security policies are all rated as "secure to strongly agree." This underscores the importance that businesses have placed on having strong and reliable cloud security measures.

4.2 Organisational Factors

Table 4. Descriptive analysis of the organisational factors

	Mean	Median	Model Single	Standard Deviation	Average Cluster/Factor Attitude
Organizational Factors	**3.80**				**Neutralto Agree**
Management support for security initiatives	3.67	4.00	4.00	0.47	Neutralto Agree
Security awareness and training	3.67	4.00	4.00	0.94	Neutralto Agree
Security budget allocation	3.67	4.00	4.00	0.94	Neutralto Agree
Security policy	3.67	4.00	4.00	0.94	Neutralto Agree
Security governance	4.33	4.00	4.00	0.47	Agree to Strongly Agree

An average score of 3.80 in Table 4 above suggests that companies acknowledge these elements, but they may not consistently apply them uniformly.

4.3 Technical Factors

The Technical Factors, with an average of 4.33 as shown in Table 5, highlight the acknowledged importance of technical measures in ensuring cloud security. The continuously high results in key categories indicate not only recognition but also successful execution across multiple organisations.

Table 5. Descriptive analysis of the technical factors

	Mean	Median	Model Single	Standard Deviation	Average Cluster/Factor Attitude
Technical Factors	**4.33**				**Agree to Strongly Agree**
Security controls implementation	4.50	4.50	4.00	0.50	Neutralto Agree
Incident response capability	4.17	4.00	4.00	0.37	Neutralto Agree
Secure architecture and design	4.33	4.50	5.00	0.75	Neutralto Agree
Encryption and key management	4.33	4.50	5.00	0.75	Neutralto Agree
Patch and vulnerability management	4.33	4.00	4.00	0.47	Agree to Strongly Agree

4.4 Legal and Regulatory Factors

The notable mean score of 4.23 for this factor underscores a significant focus on tackling legal and regulatory factors, however somewhat diminished by the lower score in "compliance with laws and regulations", suggesting the difficulties that certain businesses have, particularly across diverse industries. The topics of data privacy, contractual duties, and geo-location of data were rated highly, indicating their considerable significance. While there was considerable variation in adhering to laws and regulations, the audit and assessment processes were consistently acknowledged.

4.5 Operational Factors

The average operational factors score of 4.27 for this factor highlights the significance placed on the day-to-day procedures of cloud security. The constant emphasis on security monitoring and logging underscores its significance, albeit with potential variations in its interpretation.

4.6 Human Factors

The Human Factors domain, with an average score of 4.13 for this factor, emphasises the crucial understanding that, in addition to technology, human factors play a vital role in ensuring cloud security. Industry concerns about insider threats and social engineering threats align with worries about the potential vulnerabilities that can be introduced by the human element.

5 Hypothesis Testing

Inferential analysis is employed to assess and establish the connections between variables for the purpose of testing the hypothesis derived from the literature study. Hypothesis testing is a method used to determine if an observed effect in the data can be applied to a larger population or if it is simply due to random chance. The results of this study provide initial observations, given it was simply a pilot done with a restricted sample size.

5.1 Organisational Factors

Hypothesis 1: Organisational factors, such as management support, training, budget allocation, policy, and governance, have a favourable impact on the cloud security posture of enterprises.

Although the sample has limitations, the regression results provide valuable insights into the extent to which organisational characteristics affect the cloud security posture of organisations. Based on the regression research, organisational factors account for just 17.11% of the variation in cloud security posture (R^2 = 0.1711). The model exhibits a suboptimal alignment with the data, as indicated by the negative corrected R-square value of -0.036. A more extensive dataset is required to accurately distinguish the genuine impacts.

5.2 Technical Factors

Hypothesis 2: Enhanced technical capabilities result in an improved cloud security posture of enterprises.

The most influential element in cloud security posture is technical variables, which explain for 88.89% of the variance ($R^2 = 0.8889$). An organization's cloud security is directly impacted by its technical skills, which encompass the use of sophisticated tools, state-of-the-art infrastructure, cloud security architecture, and effective design and management practices.

5.3 Legal and Regulatory Factors

Hypothesis 3: Compliance with legal and regulatory norms enhances the cloud security posture of enterprises.

The R^2 value of 0.7199 indicates a strong association between legal and regulatory factors and cloud security, explaining approximately 71.99% of the variance. There is a significant correlation between following legal and regulatory norms and maintaining a secure cloud security posture. With a statistically significant P-value of 0.0327, this element has a crucial impact on improving cloud security. Hence, it can be inferred that strict compliance with international laws, local regulations, and industry standards significantly influences the cloud security position of a business. Nevertheless, a comprehensive survey must be conducted to verify the validity of this idea.

5.4 Operational Factors

Hypothesis 4: Effective operational strategies correlate positively with improved cloud security posture of enterprises.

The R^2 value of 0.0673 indicates a somewhat poor association, suggesting that operational factors may not be robust indicators for cloud security posture. The P-value is similarly not statistically significant, corroborating the earlier findings. This implies that although day-to-day operations are important for the general functioning of a business, they may not be the primary factors that determine the security level of cloud systems. This could also imply that numerous organisations have already implemented standardised operations, resulting in minimal heterogeneity in the impact of this aspect on security. This highlights the necessity for conducting more comprehensive investigations into these factors in studies of a bigger magnitude.

5.5 Human Factors

Hypothesis 5: A strong correlation exists between positive human factors and a higher cloud security posture of enterprises.

The relationship between human factors and the given variable is moderately strong, as indicated by a R^2 value of 0.5919. Due to the fact that cyber-attacks frequently take advantage of human mistakes, it is essential to prioritise staff knowledge, training, and vigilance in order to maintain a strong cloud security position. Given the P-value of 0.0737, which is close to the threshold of statistical significance, it is advisable to conduct further inquiry in this area. The p-value, which is close to being statistically significant, indicates that doing a larger study could provide even more compelling evidence regarding the significance of human-centered tactics in cybersecurity.

5.6 Comparative Analysis

The coefficient of determination, R^2, provides a quantifiable assessment of the extent to which each element contributes to explaining the variation in the security posture of enterprise cloud systems. As seen in Figure 1, technological factors had the highest value of 0.8889 among the determinants. This indicates that about 88.89% of the variability in the cloud security posture may be attributed to technological factors. The subsequent section focuses on Legal and Regulatory Factors, which has an R^2 value of 0.7199. This value suggests that these factors contribute to approximately 71.99% of the observed variability. The Human Factors exhibit a significant impact, as evidenced by an R^2 value of 0.5919, explaining approximately 59.19% of the variability. On the other hand, organisational factors account for only 17.11% of the variation, while operational factors have the lowest impact in this comparison analysis, representing 0.0673 or 6.73%. The bar chart visually depicts the disparities, emphasising the prominent impact of technical factors and the comparatively weaker effect of operational factors on shaping the enterprise cloud security posture.

The technical, legal, and regulatory factors have the most impact on cloud security posture. These findings are consistent with industry trends that highlight the importance of technical capabilities and compliance in improving security. While the pilot study acknowledges the significance of organisational and human elements, it is crucial to note that there may be additional underlying elements that were not included in this study.

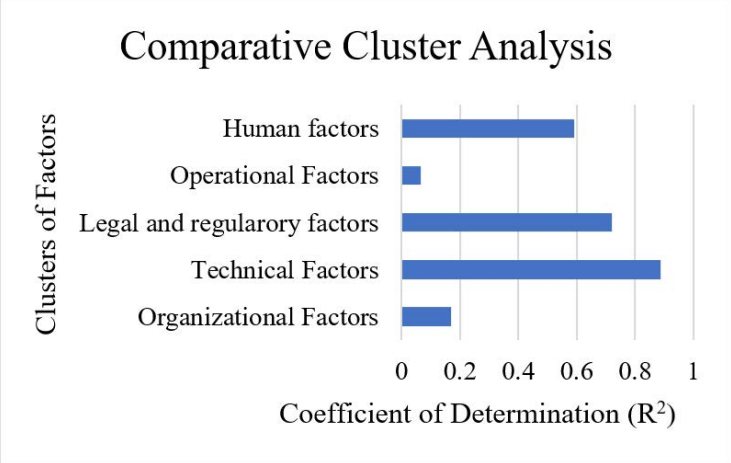

Figure 1. Regression analysis comparison of clusters

6 Summary

Based on the regression analysis, it was observed that technological variables and legal and regulatory considerations exerted the most substantial impact. While some insights were obtained initially, the specific impacts of other factors remained uncertain given the constraints of this small-scale pilot dataset. However, it is crucial to recognise that these supplementary characteristics, despite being less noticeable in the pilot study, should not be disregarded. These provide valuable opportunities for in-depth investigation in future studies.

6.1 Cloud Security Posture

The cloud security posture of an organisation reflects its preparedness to counter both external and internal threats. This stance exemplifies the all-encompassing defence strategy that the company has adopted to address difficulties related to cloud computing (Hussain, Fatima, Saeed, Raza, & Shahzad, 2017). Although the majority of organisations in the survey exhibited a significant level of attentiveness to cloud security, the extent and scope of their readiness differed depending on the specific characteristics that each organisation had emphasised. From the literature review, two clear tactics were identified: protection, which involves preventing threats, and resistance, which involves addressing active threats. The empirical study found that sectors such as IT and Finance, which were prominent in the pilot sample, demonstrated robust protective and resistance capabilities. However, there were slightly concerning findings regarding the future-proofing of cloud security posture, indicating a potential vulnerability. This underscores the significance of continuously upgrading cloud security strategies and measures to ensure ongoing security and preparedness for the future.

Furthermore, it may be inferred that while certain organisations fully include cloud security best practices, others merely adhere to fundamental legal obligations, suggesting varying degrees of dedication to security. This preliminary investigation reveals a wide range of cloud security methods, highlighting the necessity for a more comprehensive research investigation.

6.2 Organisational Factors

An analysis of organisational characteristics in connection to cloud security posture revealed subtle and detailed findings. The obtained R^2 value of 0.171126761 indicates a modest level of influence. Although certain academic perspectives highlight the pivotal significance of organisational factors such as leadership support and governance [10], empirical data suggest a more moderate influence. The precise magnitude of influence varies, maybe as a result of the interaction of components in real-world environments. Although internal policies hold significance, the research suggests that they are but one element within a wider framework of cloud security procedures.

6.3 Technical Factors

The examination of technical factors resulted in a discovery that substantially aligns with known perspectives. The technological factors were shown to be the strongest factor in determining the cloud security posture, with a R^2 value of 0.888933602. This discovery aligns with existing research and stands out as crucial factors that determine the security position of cloud systems. The study determined that the harmonious integration of hardware, software, and network settings is essential for ensuring cloud security. Any weaknesses at any point in this technical range can result in the entire system being compromised, making these criteria crucial in determining cloud security issues.

6.4 Legal and Regulatory Factors

Significant insights were obtained through the examination of legal and regulatory factors in the context of cloud security. The achieved R^2 value of 0.719930201 highlights the significant influence of compliance frameworks on security preparedness. This empirical correlation confirms that this is a crucial element of a strong cloud security position. Industries such as Finance and Healthcare may be required to demonstrate a strong dedication to following legal regulations, as they acknowledge the advantages of compliance, which include reducing risks and building confidence.

6.5 Operational Factors

The investigation of operational parameters and their correlation with cloud security posture reveals a substantial relationship. The calculated R^2 coefficient of 0.067301536 suggests that operational techniques have a discernible but rather modest impact on security readiness. Although some may consider this influence to be insignificant compared to other aspects, the study supports the known idea that streamlined workflows, specified processes, and efficient operational standards contribute to an organization's overall security position (Cloud Security Alliance, 2017). This discovery emphasises the significance of not just having sophisticated technology measures but also upholding clearly established operating norms. An organization's defence against threats and vulnerabilities is strengthened by a well-balanced approach that effectively combines technology and operational processes.

6.6 Human Factors

The inquiry into human variables and their influence on cloud security posture provided enlightening insights. The obtained R^2 value of 0.591869398 indicates a moderate association between positive human characteristics and security readiness. Although technological advancements are progressing, the results emphasise the ongoing importance of staff conduct, knowledge, and compliance with security protocols. The empirical findings corroborate the literature that emphasises the significance of acknowledging that cultivating a security-conscious workforce is a strategic investment in order to limit risks stemming from human errors and neglect.

6.7 Contribution and Limitations

The research findings provide substantial value to both practitioners and researchers in the topic of cloud security, with practical implications for organisations.

· Comprehensive framework: This study offers a thorough and all-encompassing framework for comprehending the security status of enterprise cloud systems. It considers a wide range of factors and prioritises them, providing guidance to enterprises on their cloud security strategies and appropriate investments.

· Empirical evidence: The empirical evidence provided in this research strengthens and expands upon current theories and conceptions. The findings validate the significance of organisational, technical, legal, operational, and human variables in impacting cloud security posture.

· Instructions for organisations: The findings provide valuable information for businesses seeking to enhance their cloud security. The highlighted elements provide a clear plan for businesses to strategically spend resources and develop security solutions.

It is crucial to recognise the limitations that exist within the scope of the pilot test. Given that this is an initial investigation, it is not advisable to make generalisations based on the findings. However, the pilot study acts as a preliminary step, shedding light on prospective areas of emphasis for a larger survey. By carefully crafting questions to elicit insightful replies and focusing on certain sectors, the study can enhance the depth and quality of its findings.

The sample included several sectors, however it mostly consisted of the IT and finance domains. Additional investigation could explore the extent to which the findings can be applied to other industries, such as healthcare or manufacturing. An extensive examination of "human factors" holds the potential to provide practical insights that enhance the comprehension of cloud security deployment.

7 Prospects for Further Research and Application

The field of enterprise cloud security is undergoing significant changes due to continuous technology breakthroughs and the constantly changing environment of threats. Hence, there exists the possibility for additional investigation and study to align with these modifications. Some research areas to explore include:

· Sector/industry-specific research: The pilot study primarily focuses on the representation of the IT and finance sectors. Industries such as healthcare, industry, and education each have distinct difficulties that require specific research.

· Comprehensive study of human factors: The significant association discovered between human factors and security readiness suggests a wide scope for further investigation. Further investigation into the intricacies of human behaviour concerning cloud security might assist organisations in developing focused interventions and training initiatives.

· Technological threat evolution: The advancement of technology leads to the emergence of new and changing threats. Subsequent research should predict and analyse these dangers by employing threat modelling and sophisticated computational methods, guaranteeing the security of cloud infrastructure in a constantly evolving environment.

· Integration of artificial intelligence and machine learning: The use of both techniques into cloud security presents significant opportunities. Subsequent investigations should explore their function in proactive identification and reaction to potential dangers, potentially transforming enterprise cloud security.

· Cost-benefit Analysis: Ultimately, it is important to conduct a thorough and systematic evaluation of the costs and benefits associated with different security methods. Gaining insight into the return on investment (ROI) of security efforts can assist organisations in efficiently prioritising their security operations.

After doing extensive study on the elements that affect cloud security posture, a number of practical recommendations have been identified for organisations looking to improve their cloud security strategies:

(a) Holistic security integration

· Acknowledge the multidimensional nature of cloud security.

· Integrate managerial backing, technical proficiency, regulatory compliance, operational efficiency, and human consciousness to establish a well-rounded defence against diverse dangers.

(b) Adapt strategies to the specific circumstances

· Recognise that the effectiveness of cloud security is influenced by factors such as the size and industry of the organization's internal and external surroundings.

· Tailor solutions to address the unique issues and requirements of your industry, recognising that a one-size-fits-all approach to cloud security is not effective.

(c) Ongoing technological advancement

· Continuously maintain and upgrade IT infrastructure and tools.

· Continuously be informed about emerging technologies in order to effectively protect against increasing risks.

(d) Enhance human factors

· Emphasise the importance of human factors in ensuring cloud security.

· Implement ongoing employee training programmes to mitigate the risk of insider threats.

· Foster a widespread culture that prioritises security awareness and mindfulness.

These recommendations are designed to assist enterprises in effectively managing cloud security, guaranteeing the safeguarding of critical assets and maintaining uninterrupted digital operations.

8 Conclusion

This study has emphasised the intricacy of cloud security and the necessity for a holistic approach that combines technical expertise, adherence to legal regulations, effective governance, and resilient and dependable human behaviours. As organisations transition to the cloud, it is important for them to recognise that security is not a universal problem that can be solved in the same way for everyone. Instead, it requires a continuous collaboration between service providers and end users to enhance the digital infrastructure that underpins modern enterprises.

The investigation reveals that although organisations express confidence in their cloud security, there are underlying weaknesses present. Although technology has made significant progress, human issues, particularly the vulnerability to social engineering, continue to be a source of worry. The varying opinions on how to allocate security budget and implement data backup procedures highlight the necessity for standardised protocols. Given the dynamic nature of cloud services, businesses must allocate resources towards both technological advancements and continuous staff training, particularly in light of the growing risks associated with social engineering. As organisations increasingly use cloud technology, the findings of this study might provide a basis for making well-informed decisions and implementing proactive security measures. To establish a strong cloud security position, one must consider a wide range of influential elements.

Ultimately, this study enhances the comprehension of enterprise cloud security posture by analysing the intricate interconnections among different aspects. The findings highlight the complex and diverse nature of cloud security, where several factors such as organisational, technical, legal, operational, and human elements intersect to influence the overall security position. This research enhances the greater discussion on cloud security by recognising the significance of these elements and offering specific advise. It assists companies in navigating the intricate terrain with increased assurance.

Data Availability

The data used to support the research findings are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] A. Rashid and A. Chaturvedi, "Cloud computing characteristics and services: A brief review," *Int. J. Comput. Sci. Eng.*, vol. 7, no. 2, pp. 421–426, 2019. https://doi.org/10.26438/ijcse/v7i2.421426

[2] KPMG International, "Cybersecurity considerations 2023: The golden thread," 2023. https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2023/cybersecurity-considerations.pdf

[3] Cloud Security Alliance, "Security guidance for critical areas of cloud computing v4.0," 2017. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf

[4] K. Spanaki, Z. Gürgüç, C. Mulligan, and E. Lupu, "Organizational cloud security and control: A proactive approach," *Inf. Technol. People*, pp. 516–537, 2019.

[5] R. Aljamal, A. El-Mousa, and F. Jubair, "A user perspective overview of the top infrastructure as a service and high performance computing cloud service providers," in *IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology*, Amman, Jordan, 2019, pp. 244–249.

[6] R. Kemp, "Legal aspects of cloud security," *Comput. Law Secur. Issues*, vol. 34, pp. 928–932, 2018. https://doi.org/10.1016/j.clsr.2018.06.001

[7] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Comput. Sci. Rev.*, vol. 33, pp. 1–48, 2019. https://doi.org/10.1016/j.cosrev.2019.05.002

[8] K. B. Reddy, "A study of security threats and attacks in cloud computing," *Soc. Sci. J.*, vol. 12, no. 6, pp. 550–568, 2022.

[9] Cloud Security Alliance, "Top threats to cloud computing: Pandemic eleven," 2022. https://assets.extrahop.com/pdfs/analyst-reports/top-threats-to-cloud-computing-pandemic-eleven.pdf

[10] A. Gui, Y. Fernando, M. S. Shaharudin, M. Mokhtar, G. M. Karmawan, and Suryanto, "Cloud computing adoption using toe framework for indonesia's micro small medium enterprises," *Int. J. Inform. Vis.*, pp. 237–242, 2020.

[11] D. P. Mozumder, M. J. Mahi, and M. Whaiduzzaman, "Cloud computing security breaches and threats analysis," *Int. J. Sci. Eng. Res.*, vol. 8, no. 1, pp. 1287–1297, 2017. https://www.researchgate.net/publication/320124329

[12] K. Fonseka, A. A. Jaharadak, M. Raman, and I. R. Dharmaratne, "Literature review of technology adoption models at firm level; special reference to e-commerce adoption," *Glob. J. Manag. Bus. Res.: B Econ. Commer.*, vol. 20, no. 6, 2020.

[13] A. Gutierrez, E. Boukrami, and R. Lumsden, "Technological, organisational and environmental factors influencing managers' decision to adopt cloud," *J. Enterp. Inf. Manag.*, vol. 28, no. 6, 2015. http://doi.org/10.1108/JEIM-01-2015-0001