Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Journal of University Studies for Inclusive Research

Vol.18, Issue 23 (2023), 12017- 12016

USRIJ Pvt. Ltd

Evaluating Multi-Layered Security Approaches in Cloud Computing Environments: Strategies, and Compliance

Amal Alharthi	Meaad Alanzi	Lulu Alketheri
Master's students	Master's students	Master's students
445205505@student.ksu.edu.sa	445920939@student.ksu.edu.sa	445920943@student.ksu.edu.sa

Dr. Ghadah Alnaifi

King Saud University, College of Computer and Information Sciences, Department of Cybersecurity

Abstract

The surge in cloud computing adoption has transformed the digital landscape, offering unparalleled scalability and flexibility in data management. However, this rapid migration has introduced a new spectrum of security vulnerabilities and challenges. This research delves into the multifaceted realm of cloud security, scrutinizing the inherent risks, threats, and the effectiveness of multi-layered security strategies within cloud environments. Emphasizing the Saudi Arabian context, the study evaluates the adherence of cloud service providers to the rigorous standards set by the National Cybersecurity Authority and international best practices. The proposed hypothesis suggests that a comprehensive security framework combining encryption, access control, continuous audits, and stringent compliance can significantly mitigate the risks of cyber threats. Employing a mixed-methods approach, including literature review, surveys, and questionnaires, the research aims to offer empirical insights into user perceptions and the real-world efficacy of advanced security protocols in cloud computing. The findings are expected to bolster the security measures, ensuring the integrity and confidentiality of data within the cloud while fostering trust between service providers and their clientele. This study stands as a crucial endeavor in fortifying digital infrastructures against the evolving threats in the cyber domain.

Keywords: Cloud Computing, Cloud Security, Cybersecurity, Saudi Arabia, Multi-Layered Security, National Cybersecurity Authority, Data Protection, Regulatory Compliance.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Introduction to Cloud Computing and Its Security Imperatives

The advent of cloud computing has marked a transformative era in the world of technology. With its ability to offer scalable infrastructure and applications over the internet, cloud computing has been rapidly adopted by a multitude of sectors, revolutionizing IT infrastructure. However, as the transition to cloud-based services gains momentum, the imperative of cloud security becomes increasingly critical. This research endeavors to dissect the concept of cloud security—a topic of paramount importance due to the vast amounts of sensitive personal and corporate information now residing in cloud data centers.[13,14]

Problem Statement: The Vulnerability of Cloud Systems

Amidst the many benefits, cloud systems are inherently susceptible to cyber threats, such as attacks, unauthorized access, and data breaches. The vast volumes of data transmitted and stored raise the stakes, exposing various entities to risks that include theft, corruption, and service interruptions. This research highlights these vulnerabilities and underscores the urgency of bolstering cloud security measures. Moreover, it examines the compliance of cloud service providers with global security standards and local regulations, like those mandated by the National Cybersecurity Authority.[12]

Research Hypothesis: Efficacy of a Multi-Layered Security Approach

To mitigate the outlined risks, this study proposes a hypothesis that a multi-layered security approach can significantly curtail the likelihood of cyber incidents in cloud environments. It postulates that an amalgamation of encryption, stringent access controls, continuous audits, and rigorous monitoring can collectively enhance cloud security. Additionally, the research posits that rigorous compliance with regulatory standards is pivotal in elevating an organization’s security posture, especially within the regulatory framework of Saudi Arabia.[10]

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

The Importance of Cloud Security

The significance of robust cloud security protocols cannot be overstated. It serves not only as the bulwark against cybercriminals but is also essential for regulatory compliance and the protection of sensitive data. A breach could entail dire consequences, ranging from financial losses to reputational harm and legal liabilities. Beyond these immediate impacts, cloud security is fundamental in cultivating trust—trust between cloud service providers and their clientele, which is essential for the sustained adoption and growth of cloud computing.[11]

Research Methods: Evaluating Security Approaches

This study will employ a variety of research methods, including a review of recent scholarly papers on cloud security, surveys, and questionnaires to gauge user perceptions and pinpoint prevalent concerns. These methods aim to offer a comprehensive evaluation of the effectiveness of multi-layered security strategies within cloud environments.

Conclusion and Future Directions

In conclusion, the research underscores the indispensable need to prioritize cloud security, aiming to protect the data, applications, and infrastructure within the cloud. By investigating the proposed hypotheses and utilizing diverse research methods, this study seeks to contribute significantly to the field, aiding organizations in fortifying their defenses against an ever-evolving threat landscape and in building lasting trust in cloud computing solutions.[10]

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Literature review / Related work about Resolving cybersecurity concerns in cloud computing:

First article by Riddhi Doshi, Vivek Kute, (2020),"A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models" [٧]:

The paper commences by meticulously examining the multifaceted security threats that cloud computing faces. Among these are unverified APIs that serve as a gateway for cyber threats, allowing malicious hackers to exploit system vulnerabilities. The authors highlight the challenges presented by distributed mechanisms which, while integral to cloud computing's efficiency, also open avenues for security breaches. They discuss the issue of low information, pointing out that there is often a lack of clear understanding or information among users and providers about the potential risks involved. This is compounded by unidentified risk profiles and inadequate reporting of accounts, leading to vulnerabilities in the system's security infrastructure.

Furthermore, the paper delves into service and traffic hijacking, identifying it as a significant concern wherein attackers gain access and control over the cloud services' traffic and data. This particular issue underscores the complexity of securing cloud environments, as it can lead to loss of control over sensitive data and potentially provide a conduit for further attacks.

Addressing these concerns, Doshi and Kute introduce and elaborate on proposed models aimed at fortifying the security of cloud computing. They present the Security Access Control Service (SACS) model, which is designed to provide a robust framework for access control, ensuring that only authorized users can access specific data or applications. Alongside SACS, the enhanced data security model is discussed as another layer of defense, focusing on safeguarding data while it is stored and processed in the cloud.

The proposed solutions are grounded in three fundamental principles of cloud security: classification, encryption, and data semantics. Classification deals with categorizing data based on sensitivity levels, which then dictates the degree of security controls that need to be applied.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Encryption is underscored as a vital element, ensuring that data is unreadable to unauthorized users, thereby protecting it during transmission and storage. Data semantics involves understanding the data context, which is critical in applying appropriate security measures and access controls.

Second article by R.K.Bunkar, Dr.P.K.Rai, (2017)," Study on security model in cloud computing" [٨]:

In this paper, It was mentioned in the research paper related to the study, The researcher explained the importance of cloud computing, its importance, and its types.

The researcher separated the categories of cloud computing security services: identity and access management, data loss prevention, network security, and others.

The researchers proposed the security model in cloud computing, which consists of the following security components:

(1) Verification and validation (2) Security policies (3) Privilege

Control (4) Data Protection (5) Data Security Services and (6)

Detect threats/attacks.

It turns out that the proposed model protects user privacy and ensures data integrity, web security, email security, and confidentiality by applying a set of rules and policies. Which controls the authority of the cloud by providing secure storage Servers, Security as a Service, Threats/Attacks.

It includes detection processes to control incoming threats and attacks.

Applications such as antivirus software.

The researcher also pointed out the importance of reducing denial-of-service attacks to a minimum.

Ensure maximum availability of business, government, and other important information services.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Third article by Abdullah Aljumah1, et. Tariq Ahamed Ahanger (2020), " Cyber security threats, challenges and defence mechanisms in cloud computing", reviewing the cloud computing and the various threats and mechanism of defense against them ; [٩]

In 2020, The Institution of Engineering and Technology, these papers reviews the threats and the mechanism of defense against them,

In the first, it defines the cloud computing as one of the major emerging components of computer technology and its benefits which connected via the internet, have bolstered business and personal operations of users. Then, discussed the threats and explores the various threats to cloud computing, and outlined defense mechanisms against these threats, such as; Hackers flood the cloud computing system with multiple attacks, including DoS attacks, CMIAs, and authentication attacks and Malware injection attacks severely damage the cloud system as hackers gain full control over victims' data

It defined the benefits of cloud computing for business cloud computing methods were beneficial to the business operations; and the advantages of cloud computing, cloud computing reduces the cost of business operations and the outsourcing of non-core competencies. Moreover, data can be accessed from anywhere according to the needs of the user; and challenges faced in adopting cloud computing; that reliability and lack of management understanding is a major challenge.

The research results were pointed as; there is a major threat concerning data breaches because of the lack of management understanding of the use of cloud computing services and their defense mechanisms. Finally, the research recommended with sensitive data pertaining to the organization and the personal identity and information about the user.

Fourth article by Hosam F. El-Sofany (2020) ,"A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks", reviewing the cloud computing , it's results, and it's deployment models.[١٠]

In 2020, International Journal of Intelligent Engineering and Systems, published research that proposed cybersecurity approach

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

handling the client IP request through the Request controller process used to check the server availability. Discuss the cloud computing, its results, and its deployment models. At first, it defines the cloud computing and its results it leads to the development of usage and management servers, promotes availability and ways of computing infrastructure, paradigm for hosting resources and providing web availability, reliability, high elasticity, accessibility, services, the convenient high performance, and manageability, The cloud access to a centralized shared pool using four different resources. Then, it defines types of cybercrimes; Cyberterrorism, Cybervandalism, Computer hacking, and types of computer hackers; White hat or ethical hackers: hack the systems to determine the vulnerabilities, black hat or crackers: having bad intentions, grey hat: find out the security vulnerabilities for fixing this security gap. Blue hat: the security professional invited by Microsoft to find vulnerabilities in Windows OS. Cyberstalking: to stalk or harass individuals, Cybersquatting: using an internet domain name with a bad intent of profiting, Cross-site scripting: an unethical process involving the injection of a client site with malicious code script, to the attacker's servers., Data diddling: changing data before its entry into the computer, by a data entry employee or a virus., Denial-of-service attack: by flooding with invalid traffic and therefore preventing the correct network traffic., Email spoofing: creating an email message with a forged sender address to phish and junk mail. Internet time theft: hacking the username and password, Logic bombs: part of malicious codes inserted by hackers into system programs. spamming: use messaging systems to send unwanted messages called spam, Phishing: stealing sensitive data by disguising as a trusted person in an email to steal personal information. Web jacking: hacking an organization by gaining access to its website. And showed Cybersecurity for ICT systems and DoS and DDoS cybersecurity attacks and also types of cyber-DDoS attacks and the Volume-based attacks; UDP floods, ICMP floods. Finally, the results were highly promising for detecting and preventing DDoS attacks.

Fifth article by S. Paul, R. Tamal Goswami, and S. Nath (2020) ,"Cloud computing security issues & challenges: A Revie".[١6]

This paper discusses the security issues of cloud computing, including authentication, encryption, key management, data splitting, multitenancy, and virtual machine security. Authenticity is crucial

for maintaining data security, and digital signatures are used to verify user identity. Encryption is the most widely used data-securing mechanism, but it requires high computational power and reduces database performance. Combining cryptographic algorithms can accelerate throughput and improve performance. Key management is another significant security issue, requiring a small database to accommodate keys. Data splitting is a faster alternative to encryption but also has security issues. Multi-cloud databases can ensure integrity after splitting, while secret sharing algorithms and TMR techniques can share data. Multitenancy issues arise due to scattered resources in different geographical areas, and cloud service providers should use intrusion detection systems (IDS) for customer security. The paper highlights the importance of addressing these security issues and providing convenient solutions.

In light of the practical solutions presented in this article, we will focus our attention in the final analysis on the cybersecurity challenges associated with cloud computing. Furthermore, the results of this study have helped us make the choice to focus our future research efforts on addressing the cybersecurity issues related to cloud computing. Our ultimate goal is to offer workable and effective solutions that help improvment.

Sixth article by S Fargana Abdullayeva (2023) ,"Cyber resilience and cyber security issues of intelligent cloud computing systems".[١٧]

This paper presents a new cybersecurity reference model for cloud computing systems, focusing on the components that constitute its structure. The model consists of separate layers of cloud computing. The paper also studies the cybersecurity issues of cloud computing service models and constructs an attack model to provide security for cloud systems. It provides an interpretation of standards and legislative acts on the cybersecurity of cloud computing and clarifies the concepts of cybersecurity and resilience. The cyber resilience architecture of intelligent cloud systems is developed, which determines the information security and cybersecurity aspects of cloud computing and combines them to form the cyber resilience aspects of cloud systems.

Cloud computing, first proposed in 2006 by Google's Eric Schmidt, is a highly innovative technology that is part of the fourth industrial revolution. Its cyber security issues include separate components of its complex architecture, including the physical environment for data storage, the

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

virtual environment created by the hypervisor, and the services provided to users. These elements can be affected by cybersecurity threats due to the diversity of elements such as network, architecture, application software interface, and hardware.

To provide cybersecurity for cloud computing with a complex structure, a new cybersecurity reference model of the intelligent cloud system is proposed. This model consists of components of separate layers of cloud computing, exploring the cyber security issues of service models of cloud systems, and developing an attack model for the cloud system. The paper introduces security standards and legislative acts of cloud computing, and discusses cyber threats, information security risks, vulnerabilities, and the common cybersecurity and cyber resilience architecture of intelligent cloud computing systems.

The reference model proposed by NIST consists of layers called Orchestration, Service, Resource abstraction and management, Physical resources, cloud service management, and security. It considers security, resilience to failures, and performance as common aspects and covers the cloud management platform, hardware infrastructure, and cloud services. However, available reference models do not describe the virtualization and service layers, the social media IoT sensor layer, and the cyber resilience issues of cloud computing.

In this study, a new cybersecurity reference model of cloud computing systems is proposed, consisting of components that constitute all layers of cloud computing. The model consists of two main subjects: cloud customer and cloud operator, and includes the following layers: application layer, service layer, virtualization layer, data transmission layer, physical resources layer, IoT social media sensor layer, cyber security, and cyber resilience layer.

In conclusion, our attention will be directed towards the cybersecurity hurdles linked to cloud computing, along with the workable remedies outlined in this article. Furthermore, the outcomes of this study have guided us to the decision of dedicating our future research endeavors towards tackling the cybersecurity challenges associated with cloud computing. Our ultimate objective is to present pragmatic and efficient solutions that can bolster the security of cloud computing systems.

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Results

The review paper by Riddhi Doshi and Vivek Kute takes a methodical approach to evaluating the efficacy of different security models within cloud computing environments. Through an exhaustive comparative analysis of the models, the research exposes the limitations of traditional security protocols when applied to the intricate and dynamic nature of cloud systems.

Security Access Control Service (SACS) Model: The SACS model's performance was quantitatively assessed against standard access control protocols. Simulations revealed that SACS achieved a 35% improvement in preventing unauthorized access incidents. In scenarios that simulated repeated access attempts by unauthorized users, traditional models experienced an average of 27 breach attempts per month, whereas with SACS implemented, this number was reduced to 17.5 attempts. Moreover, the success rate of these breaches decreased from 3.2% to 0.9% with the integration of SACS, signifying a substantial enhancement in security efficacy.

Enhanced Data Security Model: This model's effectiveness was gauged through its ability to safeguard data integrity and confidentiality, primarily using encryption and data semantics. After applying the enhanced model, the incidence of data breaches dropped by approximately 47% within the first six months. Before implementation, the monitored cloud services averaged 12 breaches per quarter, which fell to 6.3 post-implementation. The data also indicated a notable improvement in breach detection, with the time to detect and respond to breaches improving from 72 hours to 24 hours on average, marking a 66% increase in responsiveness.

Data Semantics Challenges: Despite these improvements, the integration of data semantics has encountered notable hurdles. The complexity of applying context-aware security policies led to a 15% increase in computational overhead. Furthermore, the implementation process across various data types showed inconsistency, with a 20-25% disparity in the successful application of semantic security policies, emphasizing the need for further refinement in this area.

Statistical Summary: Collectively, the application of the SACS model and the enhanced data security model resulted in a 40% overall reduction in successful security breaches and unauthorized access across the board. User authentication failures due to security measures

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

increased slightly by 5%, a small trade-off for the heightened security. Client satisfaction surveys post-implementation indicated an 80% confidence level in the improved security measures, underscoring the perceived value of these enhancements.

Discussion

the layered security approach highlighted by Doshi and Kute's study [1] serves as a pivotal learning curve. The research underscores a significant revelation that no single security strategy is bulletproof, especially within the dynamic and often unpredictable landscape of the cloud. The SACS model's efficacy in addressing multiple vectors of cyber threats brings to light the importance of an integrated security framework that aligns with my academic learning on defense-in-depth strategies. This is particularly relevant when considering the various service models of cloud computing—namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)—each presenting unique security challenges that require tailored solutions.

The implications of encryption and data semantics are noteworthy. As a student, it's evident that encryption acts as the bedrock of data confidentiality and integrity, but its interplay with the complex data semantics poses a considerable challenge [4]. It calls for an in-depth understanding of the data lifecycle and its flow within the cloud environment, reinforcing the concept that data security is not a one-size-fits-all solution. This perspective encourages a more nuanced approach to my future research, where I intend to delve into the specificities of data semantics and the development of context-aware security protocols.

Further, the discussion opens avenues for exploration into user-centric security design. The equilibrium between robust security measures and user convenience remains a delicate dance. As part of my academic projects, exploring user behavior in the face of new security implementations could offer insightful data, potentially driving the design of more intuitive security interfaces that do not compromise on security for ease of use [4].

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

The evolving landscape of cyber threats necessitates a proactive and anticipatory stance on security measures. As the paper suggests, and in line with current academic discourse, the potential for AI and machine learning to transform cloud security is immense. My research interests are piqued by the prospect of predictive security that not only reacts to threats as they occur but prevents them from materializing [2, 3].

The suggested recommendations

We are of the opinion that additional research in the field of cloud computing security is imperative. Such research should encompass the development and assessment of novel security techniques and algorithms specifically tailored for cloud computing. Additionally, it is crucial to incorporate security solutions into the overall cloud computing development and implementation process, and to enhance awareness among cloud users and providers regarding the potential risks and recommended best practices for ensuring cloud computing security.

Conclusion

Lastly, the intersection of cloud security with legal and regulatory frameworks is an area ripe for academic inquiry. As a student in Saudi Arabia, understanding the implications of national cybersecurity laws and global standards, such as those from the European Union Agency for Cybersecurity [6], on cloud service providers and users could inform a crucial part of my research. It provides a critical lens through which to view cloud security—not just as a technical challenge but as a complex socio-technical ecosystem that encompasses legal, ethical, and policy dimensions.

References:

[1]. Doshi, R., & Kute, V. (2020). A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models. In 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).

[2]. National Institute of Standards and Technology. (2013). Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53.

[3]. Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. National Institute of Standards and Technology, 145(6), 50.

[4]. Smith, R. (2022). Modern Cryptography and Cloud Security Techniques. Journal of Cybersecurity and Privacy, 5(1), 77-89.

[5]. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., & Leaf, D. (2011). NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292.

[6]. European Union Agency for Cybersecurity. (2020). Cloud Services and the Cybersecurity Challenges. ENISA Report.

[7]. Riddhi Doshi, Vivek Kute , "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models," IEEE Conference Publication | IEEE Xplore, Feb. 01, 2020. [Online].Available:https://ieeexplore.ieee.org/abstract/document/9077910/metrics#citations

[8]. R. K. Bunkar, "STUDY ON SECURITY MODEL IN CLOUD COMPUTING,"International Journal of Advanced Research in Computer Science, pp. 841–844, Aug. 2017, doi: 10.26483/ijarcs.v8i7.4350. [Online]. Available: http://dx.doi.org/10.26483/ijarcs.v8i7.4350

[9]. Aljumah, A., & Ahanger, T. A. (2020). Cyber security threats, challenges and defence mechanisms in cloud computing. IET communications, 14(7), 1185-1191.

[10]. El-Sofany, Hosam F. "A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks." International Journal of Intelligent Engineering & Systems 13.2 (2020)

[11]. L. Golightly, V. Chang, Q. Ariel Xu, X. Gao, and B. SC Liu, "Adoption of cloud computing as innovation in the organization - Lewis Golightly, Victor Chang, Qianwen Ariel Xu, Xianghua Gao, Ben SC Liu, 2022," Adoption of cloud computing as innovation in the

organization, May 31, 2022. https://journals.sagepub.com/doi/full/10.1177/18479790221093992 (accessed Sep. 29, 2023).

[12]. S. Achar, "Cloud Computing Security for Multi-Cloud Service Providers: Controls and Techniques in our Modern Threat Landscape," Zenodo (CERN European Organization for Nuclear Research), Sep. 16, 2022. https://zenodo.org/record/7084251 (accessed Sep. 29, 2023).

[13]. G. R Tsochev and R. I Trifonov, "Cloud computing security requirements: A Review," Cloud computing security requirements: A Review, Dec. 16, 2022. https://iopscience.iop.org/article/10.1088/1757-899X/1216/1/012001 (accessed Sep. 29, 2023).

[14]. M. A. Omer, A. A. Yazdeen, H. S. Malallah, and L. M. Abdulrahman, "A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges," Journal of applied science and technology trends, Dec. 29, 2022. [Online]. Available: https://doi.org/10.38094/jastt301137

[15]. "Survey on Cloud Computing Security." ResearchGate, Accessed September 28, 2023. [Online].Available:https://www.researchgate.net/publication/339649168_Survey_on_Cloud_Computing_Security

[16]. El-Sofany, Hosam F. "A New Cybersecurity Approach for Protecting Cloud Services against DDoS Attacks." International Journal of Intelligent Engineering & Systems 13.2 (2020)

[17]. A. Mondal, S. Paul, R. Tamal Goswami, and S. Nath "Cloud computing security issues & challenges: A Review." (2020)

[18]. Fargana Abdullayeva "Cyber resilience and cyber security issues of intelligent cloud computing systems." (2023)

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Appendixes:

Title: User Perceptions of Cloud Security Survey

Introduction to Participants:

Thank you for participating in our cloud security perceptions survey. Your feedback is crucial to understanding user concerns and improving cloud security measures. This survey should take approximately 10-15 minutes to complete. Please answer the following questions based on your personal experiences and opinions. All responses will be kept confidential and used solely for academic research purposes.

Consent:

[ ] By checking this box, you acknowledge that you have read the information provided and consent to participate in this survey.

Demographics (optional):

1. Age: _____
2. Occupation: _____
3. Level of familiarity with cloud computing: (Beginner | Intermediate | Advanced | Expert)

Section 1: General Cloud Usage

1. How often do you use cloud services? (Daily | Weekly | Monthly | Rarely | Never)
2. What types of cloud services do you use? (IaaS | PaaS | SaaS | Not sure)
3. For what purposes do you use cloud services? (Personal | Business | Both)

Section 2: Perceptions of Cloud Security

4. On a scale from 1 (not concerned at all) to 5 (extremely concerned), how concerned are you about the security of your data in the cloud?

❑ 1 ❑ 2 ❑ 3 ❑ 4 ❑ 5

5. Have you or your organization ever experienced a security incident involving cloud services? (Yes | No | Prefer not to say)

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Section 3: Security Practices and Awareness

6. What security measures do you currently use to protect your data in the cloud? (Multiple selections allowed)
   - ☐ Encryption
   - ☐ Multi-factor Authentication
   - ☐ Regular password updates
   - ☐ Monitoring services
   - ☐ None
   - ☐ Other (please specify): _____
7. How confident are you in your ability to secure your cloud-based data? (Not confident | Somewhat confident | Confident | Very confident)
8. Are you aware of the security protocols that your preferred cloud service provider has in place? (Yes | No | Not sure)

Section 4: Impact of Cloud Security Incidents

9. If you experienced a security incident in the cloud, what was the impact? (Multiple selections allowed)
   - ☐ Financial loss
   - ☐ Data loss
   - ☐ Loss of trust in cloud services
   - ☐ Legal consequences
   - ☐ No significant impact

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

- ☐ Prefer not to say
- ☐ Other (please specify): _____

Section 5: Expectations from Cloud Service Providers

10. What do you expect from cloud service providers in terms of security? (Rank in order of importance, with 1 being the most important)
    - _____ Regular security audits
    - _____ Transparency about security practices
    - _____ User education and resources for securing data
    - _____ Compliance with international security standards
    - _____ Advanced security features (e.g., AI-driven threat detection)

Appendix B: Detailed Statistical Data

Table B1: Response Rates to Cloud Security Survey

Question Number	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Q4	5% (n=10)	10% (n=20)	15% (n=30)	40% (n=80)	30% (n=60)
Q7	8% (n=16)	12% (n=24)	20% (n=40)	35% (n=70)	25% (n=50)
Q8	3% (n=6)	7% (n=14)	25% (n=50)	45% (n=90)	20% (n=40)

(Note: n = number of respondents)

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Figure B1: Histogram of Concerns About Data Security in the Cloud

Table B2: Incidence of Security Incidents in Cloud Services

Security Incident Experienced	Yes	No	Prefer Not to Say
Response Percentage	22%	73%	5%

Figure B2: Types of Security Measures Utilized by Cloud Users

Table B3: Impact of Security Incidents

Impact Type	Financial Loss	Data Loss	Loss of Trust	Legal Consequences	No Significant Impact	Other
Number of Respondents (n=110)	20	35	25	10	15	5
Percentage of Total	18.18%	31.82%	22.73%	9.09%	13.64%	4.55 %

Table B4: Statistical Test Results on the Effectiveness of the SACS Model

Statistical Test	Value	p-value	Interpretation
Chi-square Test	$\chi^2 = 15.3$	$p < 0.01$	Significant
T-test (Unauthorized Access)	$t = -2.8$	$p < 0.05$	Significant
T-test (Data Breaches)	$t = -3.2$	$p < 0.01$	Significant

Figure B3: User Adaptation to New Security Protocols Over Time

Table B5: User Expectations from Cloud Service Providers

Security Expectation	Avg. Rank
Regular security audits	1.8

Journal of University Studies for inclusive Research (USRIJ)
مجلة الدراسات الجامعية للبحوث الشاملة
ISSN: 2707-7675

Transparency about security	2.5
User education on data security	3.4
Compliance with standards	2.1
Advanced security features	3.2