IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 9, September, 2025, pp. 1901-1907
Journal homepage: http://iieta.org/journals/ijsse

Solution Evaluation to Enhance Cloud Computing Security: Challenges and Solutions

Lubab H. Albak, Arwa Hamid Salih Hamdany, Rabei Raad Ali*

Department of Cloud Computing and IoT Techniques Engineering, College of Technical Engineering for Computer and AI, Northern Technical University, Mosul 41000, Iraq

Corresponding Author Email: rabei@ntu.edu.iq

https://doi.org/10.18280/ijsse.150913

Received: 14 August 2025
Revised: 20 September 2025
Accepted: 25 September 2025
Available online: 30 September 2025

Keywords:
cloud computing, cybersecurity challenges, security architecture, threat mitigation, cloud deployment models, multi-layer protection, data confidentiality

ABSTRACT

Organizations today use cloud computing to achieve cost reduction and performance improvement while handling extensive data systems more effectively. Organizations now use virtual environments to access storage and networking, and applications flexibly because these systems enable them to decrease their need for physical hardware and eliminate the need to handle direct infrastructure management. The fast-growing cloud-based systems have created multiple security issues that threaten to compromise both data confidentiality and system reliability and cyber protection capabilities. The research identifies cloud environment security threats, which include data breaches and system resource unauthorized access and targeted cyberattacks, and API application programming interface vulnerabilities. The research establishes fundamental cloud security principles through authentication systems and system monitoring, and encrypted data exchange and service agreements that define provider and client responsibilities. The research uses structural analysis to study cloud deployment and service models, which shows how they affect security responsibility distribution and technological threat vulnerability. The research establishes a practical framework for organizations to transition to cloud computing through threat identification and strategic mitigation approaches. The research demonstrates that organizations must implement technical controls with organizational policies that promote transparency and fast threat identification, and efficient incident response to achieve cloud security strengthening. Institutions can use cloud technologies with assurance through these measures, which protect their corporate resources and user information.

1. INTRODUCTION

Organizations, together with individual users, depend more and more on software systems and internet networks to operate their applications and platforms and store data remotely. The National Institute of Standards and Technology (NIST) explains that cloud environments create a flexible system that enables users to access information efficiently while processing data quickly and sharing data precisely between distributed networks [1, 2]. Cloud solutions have become popular among institutions because they offer cost-effective hardware savings and simplified maintenance, and better operational performance. The increasing use of cloud environments has led to parallel growth in concerns about protecting data privacy and maintaining system security, and ensuring service continuity. The design of cloud infrastructure through multi-tenant systems and decentralized storage and virtual resource sharing creates security risks because it allows unauthorized access and data breaches [3]. Security as a Service (SECaaS) operates as a major field that provides cloud-based security solutions to defend digital assets from modern cyber threats. Organizations and individual users, and governmental entities need security solutions because they transfer their sensitive data to cloud storage platforms [4]. The research examines cloud computing security threats by studying technological security risks and required protective measures for cloud infrastructure systems. The research combines theoretical knowledge with operational requirements to develop a complete framework for cloud security protection. A cloud security framework requires complete defense of system infrastructure and stored data, and operational applications. The protection system depends on strong authentication systems and advanced access controls, and privacy-enhancing tools that defend cloud resources from unauthorized access [5, 6]. Cloud services have revolutionized business operations through their scalable storage solutions and high-performance computing capabilities, yet they introduce security threats that require continuous assessment and enhancement. Cloud security threats consist of three main categories, which attack cloud data through unauthorized access and service interface vulnerabilities, and data breaches that compromise confidentiality and integrity, and availability. Organizations need complete knowledge of these threats to create effective cloud security defenses that will protect their infrastructure from current and future security risks. Figure 1 shows the percentage of cybersecurity threats in cloud environments.

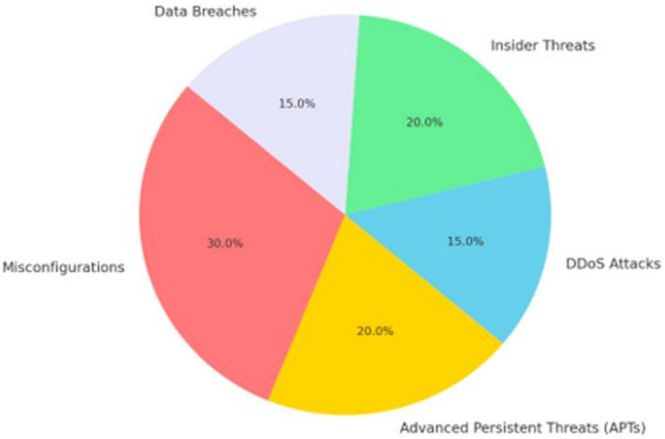

Figure 1. Distribution of cybersecurity threats in cloud environments

2. RELATED WORKS

The academic literature contains multiple viewpoints about cloud computing, which explain its fundamental structure and operational framework, and security aspects that affect its complete operation. Cloud computing functions as a technological system that delivers computing resources through distant platforms that let users access infrastructure services without needing to manage local systems. According to Khan et al. [1], the service model allows organizations to delegate core operations to external vendors, resulting in improved operational efficiency by removing the dependence on local hardware infrastructure.

Cloud technology development has enabled researchers to analyze its operational behavior by using complex adaptive systems, which show adaptable and responsive properties. The research by Taylor et al. [3] shows that cloud environments let organizations manage their resources automatically, which enables them to adjust their workloads effectively while reducing their expenses for physical infrastructure growth. The research by An et al. [4] demonstrates that cloud platforms achieve better data storage efficiency through their replacement of traditional hardware-based systems which reduces the need for extensive local storage infrastructure. Their internet-based storage model provides scalable and cost-efficient data management through cloud-driven solutions. The research confirms the previous study by Arogundade and Palla [7], which demonstrates that flexible cloud systems enable better management of changing workload demands thus minimizing the need for major initial capital expenditures on physical equipment. The research by Goutas et al. [8] extends the current understanding of the subject. Cloud computing technology provides essential benefits to startups and research institutions because it enables them to use adaptable operational systems which scale up or down based on their requirements. The research by Basu et al. [5] further demonstrates that cloud platforms improve system performance by allocating resources precisely when required. The system allows for immediate provisioning which enables organizations to perform their operations at high speed and minimizes the requirement for scheduled maintenance of typical IT infrastructure [5, 6]. Syed et al. [9] explain that cloud computing operates as a strategic method which helps organizations reduce their IT costs while maintaining their ability to adjust their computing resources. Cloud computing provides businesses with instant operational scaling through its built-in scalability feature which suits organizations that need fast responses. The fast development of cloud-based systems has created new security risks which modern businesses need to handle. The protection of cloud-based data storage requires organizations to maintain permanent surveillance according to Alouffi et al. [10] and Patel and Alabisi [11]. Organizations need to create multiple security layers that perform continuous risk assessments and active threat monitoring to defend their critical business data from modern cyber threats. The research demonstrates how cloud computing technology can revolutionize operations, but organizations must develop robust security systems to protect against its developing security risks.

3. CLOUD SERVICE, AND CLOUD DEPLOYMENT MODELS

The structural framework of this study appears in Figure 2, which shows cloud service and deployment models. The models establish the fundamental structure of cloud computing because they determine how businesses access virtualized resources. The following sections explain the fundamental operations of these models together with their associated security aspects.

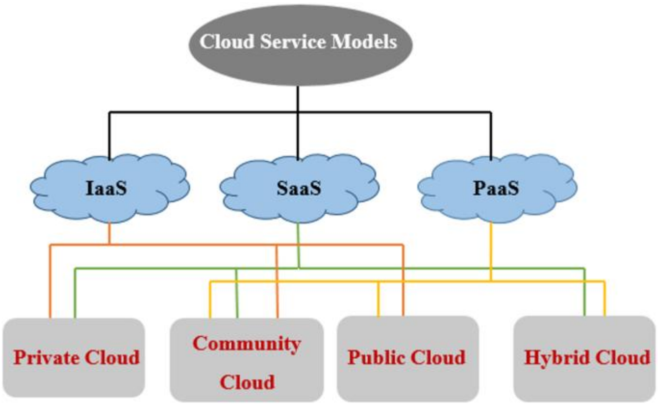

Figure 2. Cloud service and cloud deployment model

3.1 Cloud service models

The NIST has established three main cloud service models, which include Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), and Software as a Service (SaaS). The three cloud service models provide organizations with different operational capabilities to support their security requirements and operational needs. The IaaS model provides users with virtualized hardware resources, which include storage and networking, and computing power. Organizations can eliminate physical infrastructure maintenance through IaaS while maintaining complete control over their operating systems and software configurations. The operational-cost-based consumption model of IaaS provides companies with flexible resource management according to Patel and Alabisi [11], who recommend this solution for organizations that need scalable resource management. The security risks of IaaS environments stem from the need to govern virtual machines (VMs) and hypervisors, and resource allocation processes. The development process under PaaS becomes more efficient because developers can concentrate on coding and application design without needing to handle hardware or system management tasks. The simplified development environment enables fast project completion and lower expenses, yet it restricts user flexibility because of vendor control. The use of proprietary platforms restricts future adaptability, so organizations need to implement robust authentication systems and perform thorough application verification to protect their operations and security [12]. Figure 3 shows the comparative analysis of cloud deployment models (public, private, hybrid).

SaaS delivers complete applications that users can access through web interfaces as their primary interface. The model simplifies internal IT operations while enabling organizations to implement software solutions at high speed. SaaS environments need sophisticated encryption systems and robust browser security measures, according to Fraihat [12], to protect data transmission and control access to protected resources. The different service models demonstrate that users need to handle security duties at distinct levels. Users need to handle security responsibilities for data protection and application security, and access permission control in IaaS and PaaS environments, although SaaS providers handle most security tasks. These security responsibilities across service models are summarized in Table 1.

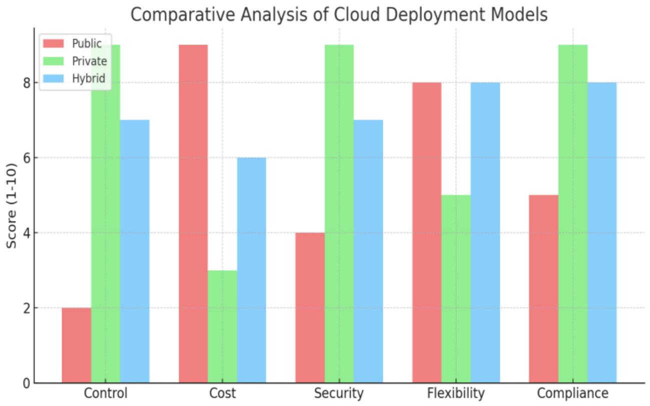

Figure 3. Comparative analysis of cloud deployment models (public, private, hybrid)

Table 1. Comparison of cloud service models in terms of security responsibility

Aspect	IaaS	PaaS	SaaS
Provider Responsibility	Virtualization, Storage	Runtime, Middleware	Application, Data
Consumer Responsibility	OS, Applications, Data	Applications, Data	Minimal (Mainly Access)
Common Security Concern	Misconfigured VMs	Insecure APIs	Weak Authentication

3.2 Cloud deployment models

Cloud deployment strategies exist in three main deployment models which include public cloud deployments and private cloud deployments and hybrid cloud deployments. The different models provide organizations with different levels of administrative control and customization options and security features. Public cloud infrastructures operate through open networks which users can access to purchase services at a pay-per-use pricing model. Public cloud solutions attract organizations from all industries because they provide elastic scalability together with cost-efficient operations. The use of common infrastructure in public cloud systems creates major security risks because it threatens both data confidentiality and service-level agreement (SLA) compliance, according to Latha [13]. Organizations that select public cloud services must create particular security responsibilities that they need to execute through partnerships with their service providers for defining service level agreements. Organizations that need to follow strict governance rules and maintain complete control over their internal security policies and operational protocols and fulfill regulatory requirements should use private cloud deployments.

Private clouds operate from organization-owned data centers, which enable businesses to create customized security frameworks that match their particular industry needs. The model provides security benefits for sensitive and essential data processing according to Dooley [14], although it comes with increased operational expenses. Organizations use hybrid cloud systems to combine public and private cloud elements, which enable them to place workloads according to security requirements and performance standards, and budget constraints. Verma et al. [15] explained that hybrid systems provide organizations with better flexibility because they enable strategic outsourcing and enhance disaster recovery functions, and enable optimal resource allocation. The figure below presents a detailed evaluation of these deployment approaches.

Organizations select their deployment model based on their security requirements and their need to comply with regulations and their operational targets. Figure 4 demonstrates how deployment models connect to service delivery frameworks.

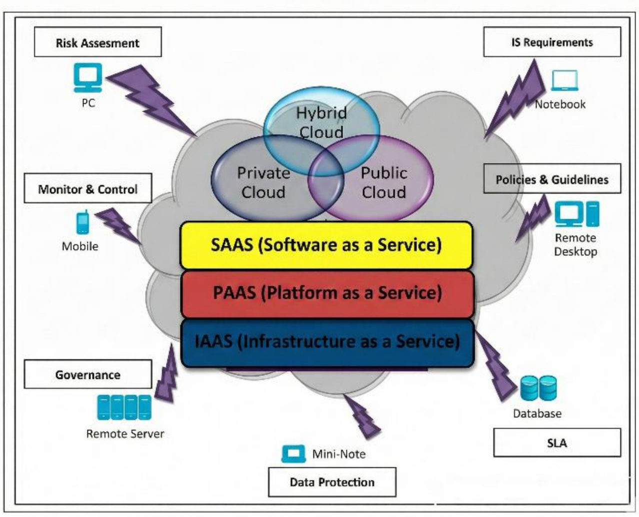

Figure 4. A holistic cloud illustration

4. CLOUD COMPUTING CHARACTERISTICS

Cloud computing operates through essential characteristics that have transformed digital resource management and IT service delivery for organizations. The characteristics provide organizations with flexible and scalable solutions, yet organizations need to handle security and governance challenges that come with these benefits. Cloud computing enables users to access computing resources through on-demand self-service, which eliminates the need for human intervention with service providers. Users can perform operational and administrative tasks through any endpoint device, including smartphones and tablets, and laptops, to access network resources at any time. Cloud platforms have revolutionized corporate operations through their ability to deploy new solutions and expand existing ones at a faster pace. The quick system response enables business expansion and creative development because organizations use cloud infrastructure to handle data organization and asset management, and service delivery to multiple user segments. The high degree of flexibility demands improved security protocols and ongoing surveillance to defend users, according to Khan et al. [1], who identified these measures as vital for achieving maximum resource efficiency. Organizations can expand their computing power at speed through elastic resource allocation, which enables systems to automatically adjust performance based on changing operational requirements in real-time.

The system provides two essential advantages through its adaptive function because it delivers resources only when needed which results in better operational performance and decreased total operational expenses. Cloud platforms allow organizations to track their resource usage through sophisticated monitoring systems which help with billing operations and produce precise financial statements.

The system enables better financial control because it helps organizations analyze their spending behavior and investment return effectiveness with enhanced precision.

Cloud computing has become popular among public and private sector institutions because it delivers flexible resources and efficient workload management, and decreased hardware needs. The fast response capability of cloud computing makes it the top technology choice for various contemporary businesses.

5. CLOUD SECURITY

Cloud-environment data security requires equal protection of confidentiality and integrity, and availability, because these elements form the fundamental CIA triad framework. The three core principles of the CIA triad maintain their integrity through encryption protocols and digital signatures, and structured access-control systems, which protect information from unauthorized access during all system operations. The framework enables users to establish protected communication paths with service providers, which defends systems against breaches and unauthorized access to support cloud operations through enhanced transparency and system resilience.

5.1 Cloud computing concerns

Organizations now depend more on third-party service providers, including Gartner, because they evaluate cloud solutions and establish security protocols for protecting essential data [11].

Multiple industries now use cloud-based systems which require strong regulatory systems to protect both service providers and their end users. Business data confidentiality protection during all operational stages depends on stakeholders upholding trust through legal and contractual systems which outline their rights and responsibilities. The location of data centers together with their geographical area determines which cloud security standards need to be applied. User confidence depends on the regulatory environment of data centers operating in different jurisdictions. The combination of strong encryption systems with properly designed service contracts provides complete data protection and ensures service availability and transparency, and accountability from start to finish.

5.2 Settings affecting cloud security

Cloud security depends on the fundamental design structure of cloud systems. The security posture of the system depends on virtual tenant access (see Figure 5) [14].

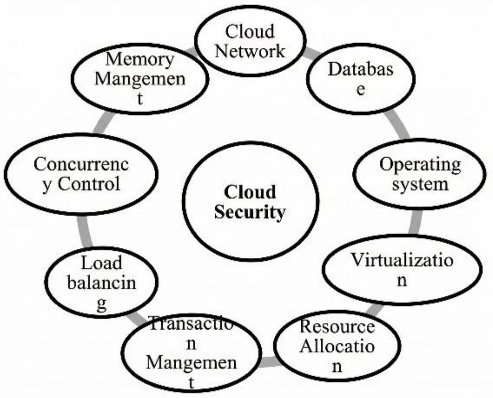

Figure 5. Key parameters influencing cloud security

Figure 5 shows the main factors that affect cloudization technologies and concurrency control and memory-management frameworks, which determine their ability to protect data from unauthorized cross-security. The system requires correct VM mapping and isolation with secure hypervisor settings to stop attacks that target internal system interference and privilege elevation. The system protects confidential data through effective encryption, which defends information during both transmission and storage periods. The system becomes more resistant to external attacks and internal weaknesses through improved resource management algorithms and secure data storage systems.

5.3 Information security requirements

Cloud environments need to follow internationally recognized standards which include ISO standards as described by Alouffi et al. [10]. The first security measure needs identification and authentication systems which check user identities before granting access to cloud resources. Organizations can create defined access-control systems through authentication which enables them to control system interactions. The system allows users to authenticate before it performs permission assessment to protect resources from unauthorized access. Public cloud services need virtual machine separation from physical infrastructure because multiple customers must use the same physical equipment. Organizations need to implement strong encryption methods alongside tailored security protocols which prevent unauthorized data access to safeguard sensitive information in these environments. The system protects data integrity through its authorized modification tracking system which monitors all changes and blocks unauthorized users from accessing stored information. The system uses digital signatures together with timestamping for integrity assurance because these features enable non-repudiation through their ability to track system activities to their origin and prevent users from denying their system interactions. Cloud services require continuous operation because users need their systems to stay accessible during system failures and security incidents to preserve trust and business operations. Table 2 shows how information security requirements distribute between public and private cloud systems and hybrid cloud environments which define essential security measures for IaaS and PaaS and SaaS service layers.

Table 2. Mapping of information security requirements across cloud delivery models

Information Security Requirement	Public Cloud (IaaS / SaaS / PaaS)	Private Cloud (IaaS / SaaS / PaaS)	Hybrid Cloud (IaaS / SaaS / PaaS)
Identification and Authentication	* / * / #	* / * / *	# / * / *
Authorization	* / * / *	* / * / *	* / * / *
Confidentiality	# / * / *	* / * / *	* / * / *
Integrity	* / * / *	* / * / *	* / * / *
Non-Repudiation	# / # / #	# / # / #	# / # / #
Availability	* / * / *	* / * / *	* / * / *

Note: “#” indicates optional criteria; “*” indicates required requirements.

5.4 Threats issues

The Cloud Security Alliance (CSA) identified the most dangerous cloud security threats through its "Notorious Nine" report from 2013 which still affects modern cloud infrastructure [16]. Data breaches stand as the most dangerous threat because they enable unauthorized access to sensitive data which leads to major financial losses and operational disruptions and permanent harm to organizational reputation [17]. Organizations need reliable backup systems and effective disaster recovery plans because data loss events occur frequently due to human errors and system failures and natural disasters [18].

Attackers who hijack accounts can use stolen credentials to access systems without permission, which creates a major operational threat to system security [19]. Unprotected APIs create new security risks because their weak security measures allow attackers to access communication pathways. Table 3 shows the main cloud security threats and recommended mitigation measures.

The network becomes unavailable because Denial of Service (DoS) attacks consume all available resources (Figure 6).

Table 3. Summary of major cloud security threats and recommended mitigation measures

Threat	Description	Impact Severity	Recommended Countermeasures
Data Breach	Unauthorized retrieval or exposure of sensitive information	High	Implement strong encryption protocols and robust access control policies
Insecure Interfaces	Exploitable vulnerabilities in APIs and communication channels	Medium	Utilize secure API gateways and enforce strict authentication mechanisms
Account Hijacking	Unauthorized use of legitimate credentials to gain control over accounts	High	Deploy multi-factor authentication (MFA) and continuous account monitoring
Denial of Service (DoS)	Overwhelming of network resources leading to service outages	High	Apply advanced traffic filtering, redundancy strategies, and network segmentation

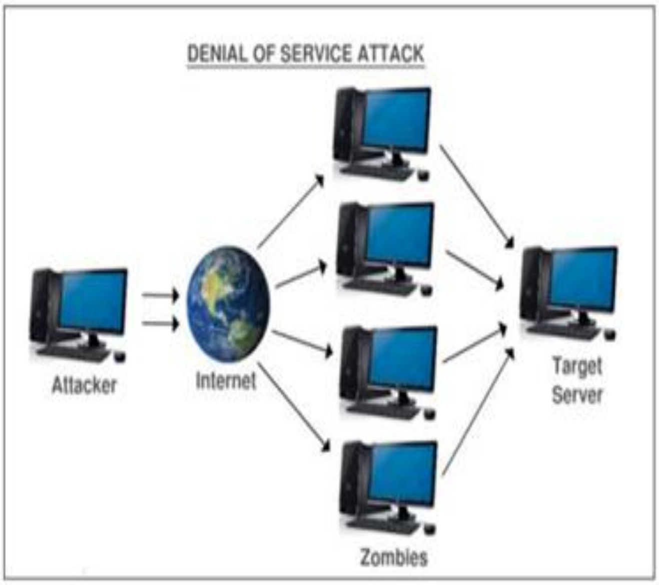

Figure 6. Works of a DoS attack

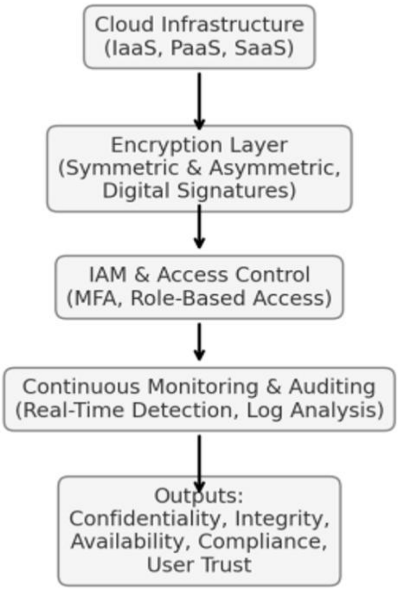
Cloud Infrastructure (IaaS, PaaS, SaaS)
Encryption Layer (Symmetric & Asymmetric, Digital Signatures)
IAM & Access Control (MFA, Role-Based Access)
Continuous Monitoring & Auditing (Real-Time Detection, Log Analysis)
Outputs: Confidentiality, Integrity, Availability, Compliance, User Trust

Figure 7. Conceptual framework

5.5 Mechanisms of cloud security

Cloud environments protect data confidentiality through symmetric and asymmetric encryption methods, which transform readable information into protected, non-interpretable formats [20, 21]. The system uses symmetric encryption for speed but asymmetric encryption for secure key distribution and digital signature functionality. Digital signatures confirm data origin and protect against unauthorized changes while ensuring non-repudiation capabilities. Hashing algorithms enhance security through their ability to create fixed-length data representations that enable tamper detection without needing reversible encryption [22, 23]. The security framework in Figure 7 demonstrates how encryption systems and identity management tools, and continuous monitoring functions protect cloud systems from attacks while fulfilling regulatory requirements.

5.6 Cloud security issues solution and practices

Cloud security depends on technical protection measures and established organizational policies, which create the fundamental security framework for protected cloud environments [24, 25]. The system needs immediate patching of vulnerabilities through regular vulnerability assessments to prevent potential exploits from occurring.

Organizations need to choose dependable cloud service providers who establish solid data governance frameworks, according to Meenakshi and Neha [26], who show that organizations with effective governance systems face reduced security risk exposure [27, 28]. Organizations need to define security responsibilities through contracts and establish incident response systems and auditing protocols to prevent confusion and achieve operational preparedness [26]. The protection of essential operational assets against cyber threats requires organizations to establish security systems which perform user verification and data protection through encryption and maintain confidentiality of important data [29, 30].

6. CONCLUSIONS

Cloud computing has transformed data management through its adaptable infrastructure which operates independently from hardware to enable organizations lower their expenses while delivering enhanced system performance. Cloud adoption effectiveness depends on the implementation of sophisticated security systems which defend essential data from advanced cyber-attacks. Cloud security needs multiple defensive systems to achieve robustness because it requires encryption technologies and secure data storage and controlled access mechanisms to protect data confidentiality and integrity and maintain user trust. Organizations can create protected cloud systems for their digital transformation journey through the implementation of digital signature technologies and multi-layer encryption methods and continuous monitoring systems.

REFERENCES

[1] Khan, M.W., Khan, S.Y., Altaf, S., Ali, M.W. (2021). A review of the security issues in cloud computing and its remedial action. Information Technology in Industry, 9(1): 444-455. https://doi.org/10.17762/itii.v9i1.150

[2] Sucipto, A., Zyen, A.K., Wahono, B.B., Tamrin, T., Mulyo, H., Ali, R.R. (2021). Linear discriminant analysis for apples fruit variety based on color feature extraction. In 2021 International Seminar on Application for Technology of Information and Communication (iSemantic), Semarangin, Indonesia, pp. 184-189. https://doi.org/10.1109/iSemantic52711.2021.9573200

[3] Taylor, S., Gilje Jaatun, M., Bernsmed, K., Androutsos, C., et al. (2024). A way forward for the MDCG 2019-16 medical device security guidance. In Proceedings of the 17th International Conference on PErvasive Technologies Related to Assistive Environments, Crete, Greece, pp. 593-599. https://doi.org/10.1145/3652037.3663894

[4] An, Y.Z., Zaaba, Z.F., Samsudin, N.F. (2016). Reviews on security issues and challenges in cloud computing. IOP Conference Series: Materials Science and Engineering, 160: 012106. https://doi.org/10.1088/1757-899X/160/1/012106

[5] Basu, S., Bardhan, A., Gupta, K., Saha, P., et al. (2018). Cloud computing security challenges & solutions-A survey. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 347-356. https://doi.org/10.1109/CCWC.2018.8301700

[6] Defense Information Systems Agency. (2017). Department of Defense Cloud Computing Security Requirements Guide. https://rmf.org/wp-content/uploads/2018/05/Cloud_Computing_SRG_v1r3 .pdf.

[7] Arogundade, O.R., Palla, K. (2023). Virtualization revolution: Transforming cloud computing with scalability and agility. International Advanced Research Journal in Science, Engineering and Technology, 10(6): 619-632. https://doi.org/10.17148/IARJSET.2023.106104

[8] Goutas, L., Sutanto, J., Aldarbesti, H. (2015). The building blocks of a cloud strategy: Evidence from three SaaS providers. Communications of the ACM, 59(1): 90-97. https://doi.org/10.1145/2756545

[9] Syed, H.J., Gani, A., Ahmad, R.W., Khan, M.K., Ahmed, A.I.A. (2017). Cloud monitoring: A review, taxonomy, and open research issues. Journal of Network and Computer Applications, 98: 11-26. https://doi.org/10.1016/j.jnca.2017.08.021

[10] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., Ayaz, M. (2021). A systematic literature review on cloud computing security: Threats and mitigation strategies. IEEE Access, 9: 57792-57807. https://doi.org/10.1109/ACCESS.2021.3073203

[11] Patel, K., Alabisi, A. (2019). Cloud computing security risks: Identification and assessment. The Journal of New Business Ideas & Trends, 17(2): 11-19. https://www.proquest.com/openview/a4067650c81bcf3fbb589d7e01473710/1.

[12] Fraihat, A. (2021). Computer networking layers based on the OSI model. Test Engineering and Management, 83: 6485-6495.

[13] Latha, K. (2023). A review on cloud computing security issues. AIP Conference Proceedings, 2523(1): 020138. https://doi.org/10.1063/5.0111138

[14] Dooley, B. (2010). Architectural requirements of the

hybrid cloud. Cutter Consortium, Executive Update. https://www.cutter.com/article/architectural-requirements-hybrid-cloud-391271.

[15] Verma, A., Malla, D., Choudhary, A.K., Arora, V. (2019). A detailed study of azure platform & its cognitive services. In 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, pp. 129-134. https://doi.org/10.1109/COMITCon.2019.8862178

[16] Seetharamarao, R.Y. (2023). A unified approach towards security audit and compliance in cloud computing environment. In 2023 16th International Conference on Developments in eSystems Engineering (DeSE), Istanbul, Turkiye, pp. 623-629. https://doi.org/10.1109/DeSE60595.2023.10469536

[17] Naikwade, N., Pathan, S. (2024). Strategies for data security and privacy protection in cloud infrastructure. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, pp. 1-6. https://doi.org/10.1109/ICBDS61829.2024.10837059

[18] Rainer, A., Wohlin, C. (2022). Recruiting credible participants for field studies in software engineering research. Information and Software Technology, 151: 107002. https://doi.org/10.1016/j.infsof.2022.107002

[19] Goel, P.K., Singhal, A. (2023). Security issues and threats in cloud computing: Problems and solutions. In 2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), Ghaziabad, India, pp. 1019-1023. https://doi.org/10.1109/AECE59614.2023.10428390

[20] Hashizume, K., Rosado, D.G., Fernández-Medina, E., Fernandez, E.B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1): 5. https://doi.org/10.1186/1869-0238-4-5

[21] Jiang, W., Gu, C., Wu, J. (2017). A quality-of-service evaluation method based on the cloud model for routing protocols in wireless sensor network. International Journal of Distributed Sensor Networks, 13(9): 1550147717731247. https://doi.org/10.1177/1550147717731247

[22] Oliveira, D., Squicciarini, A., Lin, D. (2020). Cloud security baselines. In Cloud Computing Security, pp. 31-44. https://www.taylorfrancis.com/chapters/edit/10.1201/9780429055126-4/cloud-security-baselines-daniela-oliveira-anna-squicciarini-dan-lin.

[23] Al-Nima, R.R.O., Albak, L.H., Al-Hamdany, A.H. (2024). Translating Sumerian symbols into French letters. NTU Journal of Engineering and Technology, 3(1): 12-17. https://doi.org/10.56286/ntujet.v3i1.660

[24] Miftakhov, E., Ivanov, D. (2024). Utilizing cloud technologies in the investigation of physicochemical processes. In 2024 International Russian Smart Industry Conference (SmartIndustryCon), Sochi, Russian Federation, pp. 819-823. https://doi.org/10.1109/SmartIndustryCon61328.2024.10515726

[25] Alrasheed, S.H., Adubaykhi, S.A., El Khediri, S. (2022). Cloud computing security and challenges: Issues, threats, and solutions. In 2022 5th Conference on Cloud and Internet of Things (CIoT), Marrakech, Morocco, pp. 166-172. https://doi.org/10.1109/CIoT53061.2022.9766571

[26] Meenakshi, S., Neha, B. (2023). Cloud system performance and security improvements with multi-tenancy integration. Journal of Multimedia Technology & Recent Advancements, 10(2): 10-16. https://research-reels.com/wp-content/uploads/2023/12/jomtra.pdf.

[27] Lejaka, T. (2021). A framework for cyber security awareness in small, medium and micro enterprises (SMMEs) in South Africa. Master's thesis, University of South Africa (South Africa). https://www.proquest.com/openview/009ca195a5f93c13645407624d7aff49/1.

[28] Ojugo, A.A., Eboka, A.O. (2021). Empirical Bayesian network to improve service delivery and performance dependability on a campus network. IAES International Journal of Artificial Intelligence, 10(3): 623-635. https://doi.org/10.11591/ijai.v10.i3.pp623-635

[29] Ali, R.R., Mohamad, K.M.B., Mostafa, S.A., Zebari, D.A., Jubair, M.A., Alouane, M.T.H. (2023). A meta-heuristic method for reassemble bifragmented intertwined JPEG image files in digital forensic investigation. IEEE Access, 11: 111789-111800. https://doi.org/10.1109/ACCESS.2023.3321680

[30] Bashir, A., Hilal, S. (2023). Cloud of things: A survey on critical research issues. In Image Processing and Intelligent Computing Systems, pp. 245-266. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003267782-18/cloud-things-adil-bashir-saba-hilal.