Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Exploring Threat Vectors and Countermeasures in Cloud Security

Dr. Shrihari M R[1], Ajay N[2], Shwetha B V[3], Mahesh M R[4] , Dr.Vikas Reddy[5]

1Associate Professor, Dept. of CSE, SJCIT, Chickballapur, Visvesvaraya Technological University, Belagavi, Karnataka, India,
2 Assistant Professor,Dept. of CSE, SJCIT, Chickballapur,Visvesvaraya Technological University, Belagavi, Karnataka, India,
Research Scholar, RNSIT, Bangalore, Visvesvaraya Technological University, Belagavi, Karnataka, India,
3 Assistant Professor, Dept. of CSD, SJCIT, Chickballapur, Visvesvaraya Technological University, Belagavi, Karnataka,
4Assistant Professor,Dept. of ECE, NCET, Bangalore,Visvesvaraya Technological University, Belagavi, Karnataka, India,
5 Associate Professor & HoD, Dept. of AI&ML, SJCIT, Chickballapur,Visvesvaraya Technological University, Belagavi, Karnataka,

ARTICLE INFO

Received: 30 Dec 2024

Revised: 05 Feb 2025

Accepted: 25 Feb 2025

ABSTRACT

Introduction: The evolution of Information Technology infrastructure, catalyzed by advancements such as the Internet and mobile devices, has led to the emergence of cloud computing a paradigm shift offering both advantages and challenges. This paper delves into the intricacies of cloud computing security, addressing vulnerabilities and proposing solutions to safeguard critical information assets. Through a meticulous analysis of security threats specific to cloud computing environments, fundamental risk factors are identified and elaborated upon.

Furthermore, practical solutions tailored to enterprises and service providers are provided to enhance information security within cloud deployments. While not introducing groundbreaking innovations, this study serves as a comprehensive guide for those interested in leveraging cloud computing services while ensuring robust security measures. Additionally, this paper explores various facets of cloud security evaluation, presenting a novel Security Threats Measurement Model (STMM) that enables effective assessment of cloud computing environments.

By integrating system, management, and technical security factors, the STMM facilitates the identification of security deficiencies, empowering users to make informed decisions regarding service providers and security enhancements.

Keywords: Cloud computing, Security in cloud environments, Cybersecurity risks, Risk mitigation, Security Threats Measurement Model (STMM).

INTRODUCTION

The emergence of the Internet in 1982, alongside the standardization of TCP/IP, marked a transformative milestone in the realm of Information Technology (IT). Since then, the Internet has revolutionized global communication, introducing various technologies such as electronic mail, instant messaging, and video calls [1]. With the proliferation of smartphones and tablet PCs, the volume of data transmission has surged, necessitating efficient storage and retrieval solutions. In response to these technological advancements, cloud computing has emerged as a pivotal solution, offering a cost-effective model to address computing needs and achieve business objectives[2].

Cloud computing, characterized by convenient on-demand access to shared computing resources, has gained traction across industries. Its unique features, including multi-latency, large-scale infrastructure, and flexible service delivery, present enticing opportunities for organizations seeking to optimize IT operations. However, despite its benefits, cloud computing introduces inherent security risks that must be carefully addressed. Security concerns have become a significant impediment to widespread cloud adoption, necessitating comprehensive risk management strategies.

In this context, this paper endeavours to explore the intricacies of cloud computing security, with a particular focus on identifying and mitigating security threats. By conducting a meticulous analysis of security vulnerabilities specific to cloud environments, this study aims to provide actionable insights and recommendations for enhancing information security within cloud deployments. Additionally, the paper introduces a novel Security Threats

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Measurement Model (STMM) to facilitate effective assessment of cloud computing environments, encompassing system, management, and technical security factors[4].

Through this comprehensive exploration, we aim to shed light on the evolving landscape of cloud computing security, offering valuable insights for organizations navigating the complexities of cloud adoption and security management.

Unique Features of Cloud Computing Security: Cloud computing security continues to advance, utilizing dynamic threat response mechanisms to swiftly adapt to emerging security risks [3]. These systems employ real-time threat detection and response techniques, enabling the prompt identification and mitigation of vulnerabilities. This ensures the resilience of cloud environments against evolving cyber threats. Additionally, their scalable architectures seamlessly accommodate fluctuating workloads and resource demands, ensuring that security measures remain effective regardless of the size or complexity of cloud resources.Moreover, cloud security solutions implement a multi-layered defense strategy, incorporating diverse security measures across infrastructure, applications, and data layers. This comprehensive approach fortifies cloud environments against a wide range of cyber threats, safeguarding sensitive information through robust encryption and stringent access controls. Compliance and regulatory support are also integral, ensuring adherence to industry regulations like GDPR, HIPAA, and PCI DSS, thereby maintaining data security and compliance. Combined with identity and access management capabilities, continuous monitoring, and collaborative security ecosystems, these features bolster the overall security posture of cloud environments, enabling organizations to confidently leverage cloud services while mitigating potential risks [5].

LITERATURE REVIEW

With the rapid evolution of virtualization-based NFV technology, the SFC resource allocation (SFC-RA) problem has garnered significant attention within the literature, spanning various dimensions such as strategies, stages, and objectives [2]. Researchers have mapped out this landscape in a three-dimensional framework, delineating strategies along the X-axis, including exact methods, heuristics, and meta-heuristics. On the Y-axis, stages of SFC-RA, such as composition, embedding, scheduling, and reconfiguration, are examined, with particular emphasis on embedding. Meanwhile, the Z-axis encompasses attributes like QoS/QoE, security, and reliability. Despite considerable study of SFC embedding in cloud datacenter networks, less focus has been directed towards SSC-DMP, a critical concern for network security in cloud environments. The literature is categorized into QoS/QoE-driven, availability- driven, and security-driven approaches for SFC resource allocation.

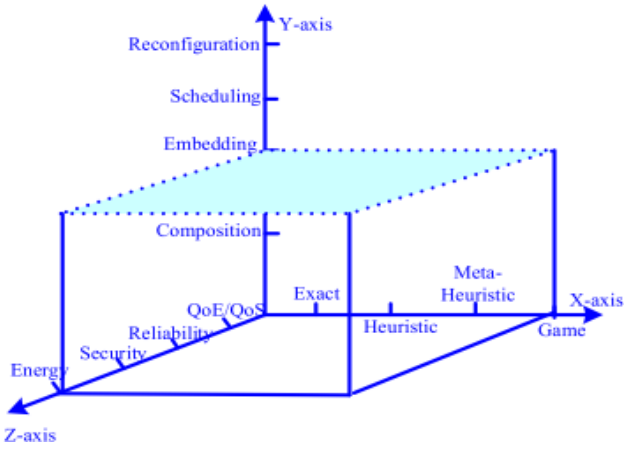

Figure 1: Three-dimensional space regarding the SFC-RA.

In the domain of QoS/QoE-driven methodologies, researchers prioritize meeting service-level agreements, employing a range of techniques from exact algorithms to heuristics and meta-heuristics. Availability-driven strategies aim at ensuring continuous service availability and typically involve considerations of VNF backups and migrations. Security-driven approaches are geared towards enhancing network security, often leveraging SDN/NFV and reinforcement learning techniques. However, prevalent solutions in existing literature predominantly rely on heuristic methods, which may not be optimal for dynamic cloud networks. Hence, there is a growing need for dynamic

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

online methodologies capable of adapting to evolving constraints and objectives. Our proposed approach leverages meta-heuristic algorithms, focusing on security service chain embedding via PSO. Diverging from heuristic-based methodologies, our approach allows for the incorporation of new objectives or constraints without necessitating extensive redesign. We introduce a network security level- based ILP model and propose an efficient SSC dynamic orchestration solution based on PSO, aimed at minimizing resource consumption while satisfying latency constraints. Our work contributes to addressing the challenges of dynamic and online SFC embedding in NFV networks [6].

SECURITY THREATS IN CLOUD COMPUTING

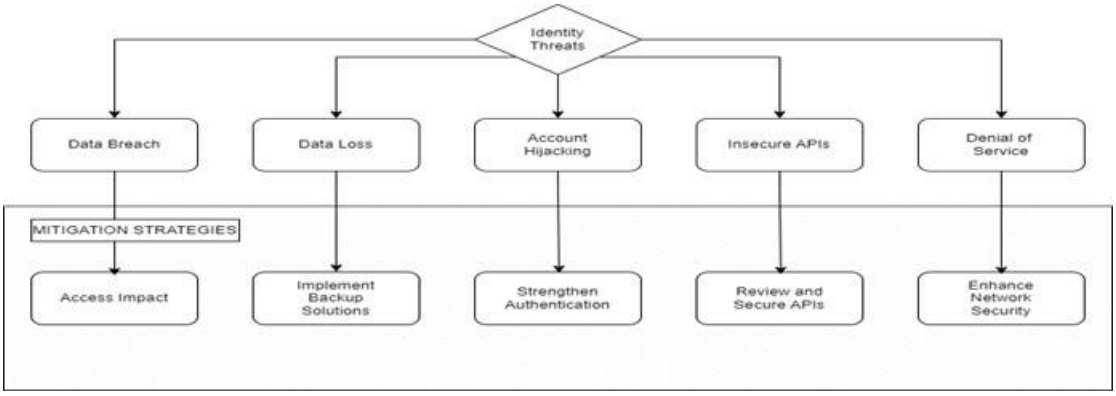

Figure 2: Various threats in cloud computing.

Cloud computing faces a myriad of security threats that can jeopardize the integrity, confidentiality, and availability of data and services [3]. One of the most pressing concerns is data breaches, which can have severe repercussions including financial losses, damage to reputation, and legal ramifications due to regulatory non-compliance. Insufficient access controls represent another significant risk, as weak configurations may allow unauthorized users to gain entry to sensitive cloud resources, potentially resulting in data theft or manipulation. Additionally, insecure APIs present vulnerabilities that attackers can exploit to gain unauthorized access or execute malicious code within cloud environments.

Furthermore, denial of service (DoS) attacks pose a threat by disrupting the availability of cloud services, leading to downtime and accessibility issues for legitimate users. Data loss incidents, whether due to hardware failures or human error, can have detrimental effects if proper backup and recovery mechanisms are not in place. Weaknesses in cloud management interfaces and consoles also pose risks, enabling attackers to manipulate configurations or extract sensitive information [8].

Moreover, malware injection remains a persistent threat, with attackers leveraging various vectors to infiltrate cloud environments and compromise data integrity. Shared technology vulnerabilities are another concern, as exploits in underlying components can lead to unauthorized access or service disruption across multiple tenants. Inadequate security architecture further exacerbates these risks, leaving cloud environments susceptible to exploitation due to deficiencies in network segmentation, encryption, and monitoring capabilities [2].Additionally, compliance and legal risks loom large, with non-compliance potentially resulting in hefty penalties and loss of trust among stakeholders. Addressing these threats necessitates a holistic approach involving technical controls, employee training, and proactive threat intelligence. Regular risk assessments and security audits are vital for identifying and mitigating vulnerabilities before they can be exploited by malicious actors [9].

SOLUTIONS TO SAFEGURAD CRITICAL INFORMATION ASSETS IN CLOUD COMPUTING

To ensure the security of sensitive data stored in the cloud, organizations should adopt a comprehensive set of security measures. Data encryption stands as a fundamental practice, ensuring that even if unauthorized access occurs, the data remains unreadable and unusable to attackers. Robust access control mechanisms, such as multi-factor authentication and role-based access control, help limit access to critical information assets based on user roles and privileges. Regular security audits and assessments play a crucial role in identifying vulnerabilities and compliance gaps within cloud environments, allowing organizations to proactively remediate security issues [4].

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Additionally, deploying data loss prevention solutions aids in monitoring and preventing unauthorized transmission or sharing of sensitive information [6].

Leveraging secure cloud storage solutions with built-in encryption and access controls is essential for protecting critical data from unauthorized access and breaches. Identity and access management solutions facilitate centralized management of user identities and access permissions, reducing the risk of unauthorized access. Network segmentation and firewalls help isolate critical assets from potential threats within cloud environments. Establishing robust backup and disaster recovery plans ensures the availability and integrity of data in case of data loss or cyberattacks. Furthermore, employee training and awareness programs promote a culture of security and ensure compliance with security policies and procedures [7].

Continuous monitoring and threat detection solutions are vital for identifying and responding to security incidents in real-time. Utilizing security information and event management systems and behavior analytics platforms helps detect and mitigate security threats across cloud infrastructures proactively. By integrating these solutions into a comprehensive cloud security strategy, organizations can effectively safeguard critical information assets and mitigate the risks associated with cloud computing [5].

METHODOLOGY

To delve into the intricacies of the proposed scheme, we focus on the data owner, typically an organization deploying a standalone workstation within its network. This workstation consists of six key components. The Security Level Policy (SLP) governs the data access and control policy, while the Key Establishment Unit (KEU) serves as the central component. The KEU manages secret key splitting, computing operations, shares generation, and approval, along with key derivation mechanisms based on inputs from LDAP queries and the SLP. The Credential Generator (CG) creates secret keys using components from the KEU and sends them to either the Data Processor (DP) or the Cloud Management Client (CMC). These entities encrypt data before transmission to the public cloud and decrypt it upon retrieval. Furthermore, the Network Control Policy (NCP) validates requests received inside or outside the network, while the Integrity Controller (IC) ensures data integrity within the public cloud [1].

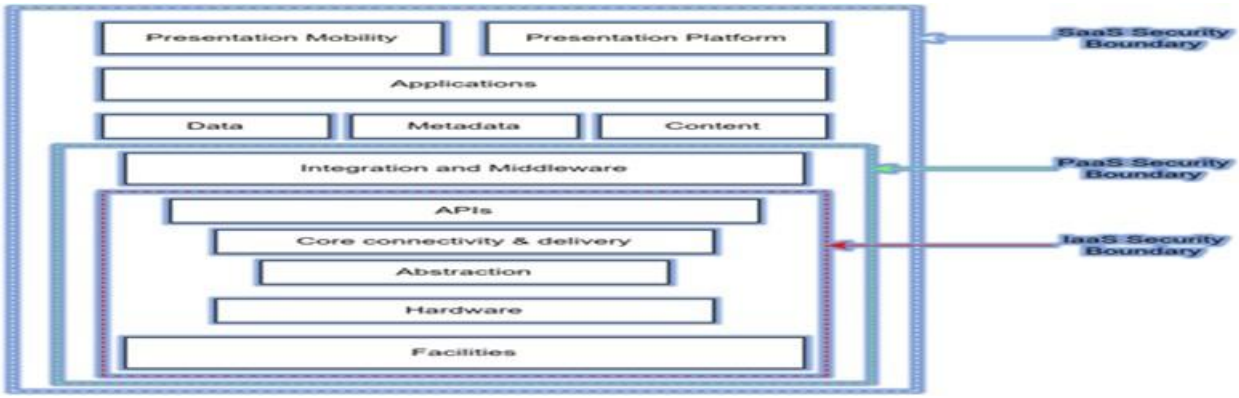

Figure 3: CSA Stack Model

In addition, the data owner installs a CMC application for each external user, facilitating secure communication with the standalone workstation and managing data encryption before upload and decryption post-download. Essentially, the CMC serves a role similar to the DP. In this scheme, the data owner relies on a Key Distribution Center (KDC) responsible for generating a secret key for each organizational unit within the Computing Component. With this approach, the KDC does not need to store these keys, thereby reducing risks associated with data breaches and key disclosure.To explain the scheme's components and workflow, we divide it into four steps: the system preparation process, the KEU operations phase, uploading data to the public cloud, and downloading data from the public cloud. Particularly, the core of the proposed scheme during the KEU operation phase is intricately linked to secret key derivation, essential for secure data handling [9].

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Cloud Security Alliance (CSA) has developed the Cloud Controls Matrix (CCM) as a framework to provide organizations with a structured approach to cloud security. The CCM is structured into 14 domains, covering various aspects of cloud security [13]. These domains include areas such as compliance and audit, data security, identity and access management, incident response, and more.At the core of the CSA Stack Model Architecture lies the CCM, which serves as a comprehensive set of controls and guidelines for securing cloud environments. Each domain within the CCM addresses specific security concerns and provides recommendations for implementing security measures effectively [11].

Additionally, the CSA Stack Model Architecture encompasses other CSA frameworks and initiatives, such as the Security Guidance for Critical Areas of Focus in Cloud Computing (CCSK) and the Cloud Security Alliance Cloud Controls Matrix (CCM). These resources offer further guidance and best practices for securing cloud environments.Overall, the CSA Stack Model Architecture provides organizations with a structured framework for understanding, implementing, and managing cloud security. By leveraging the guidance and controls outlined in the CCM and other CSA resources, organizations can enhance their cloud security posture and mitigate risks effectively [12].

The architecture for exploring threat vectors and countermeasures in cloud security encompasses several layers and components aimed at comprehensively securing cloud environments [13]. At the data collection layer, information is gathered from diverse sources including cloud platforms, network traffic, and system logs, alongside integrating external threat intelligence feeds. Subsequently, the data undergoes processing and analysis to discern potential threats, utilizing techniques such as machine learning algorithms and anomaly detection systems. Threat detection and identification follow suit, employing signature-based and anomaly detection methods to pinpoint potential risks within the cloud infrastructure. The risk assessment and prioritization component then evaluate the severity and potential impact of identified threats, facilitating prioritization based on risk levels. Leveraging this assessment, the countermeasure recommendation engine suggests appropriate mitigation strategies such as configuration changes or network segmentation. In the event of confirmed security incidents, the incident response and remediation component orchestrate response actions, aided by incident response playbooks and collaboration tools. Moreover, reporting and visualization functionalities offer stakeholders insights into the security posture and mitigation efforts, ensuring transparency and accountability. Compliance monitoring and governance ensure adherence to regulatory requirements and internal policies, while continuous improvement mechanisms facilitate adaptation to evolving threat landscapes. Through these integrated layers and components, the architecture fosters proactive threat mitigation, rapid incident response, and ongoing enhancement of cloud security measures [14].

RSA ALGORITHM

In the context of RSA encryption, the evaluation of computational time for generating multiple sets of public and private keys holds significant importance. This evaluation becomes even more critical when considering the trade-off between computational efficiency and security in comparison to the standard RSA algorithm. By implementing an optimized or enhanced variant of RSA, which involves the utilization of four prime numbers to generate two pairs of public and private keys, a higher level of security can be attained [7]. This enhanced RSA approach operates by employing two distinct public keys for encryption and two private keys for decryption, thereby fortifying the encryption process against potential attacks. The workflow or architecture of this enhanced RSA algorithm underscores its defensive capabilities. It involves three primary stages: Key Generation, Encryption, and Decryption. This methodology significantly enhances security by augmenting encryption complexity while preserving efficient decryption functionality [8].

After generating the public and private keys, the data to be transmitted is encrypted using the public key, while decryption is performed using the private key. The encryption and decryption processes follow these steps:

-The ciphertext C is obtained using the formula C' = M^e mod n', where M represents the original message.

The original message M can be retrieved from the ciphertext C using the formula M' = C^d mod n'.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Algorithm 1 The structure of RSA algorithm as follows.

1: **Input Values:** p and q
2: **Compute:**
3: n = p x q
4: (n) = (p-1) (q-1)
5: **Select Integer values:** e [(gcd (), e) - 1; 1 < e < ϕ (n)]
6: **Compute:** d de *mod* ϕ (n) = 1
7: C = Cg 1 *mod* (z)
8: **Encryption:** M < n C = M (*mod* n)
9: **Decryption:** CM = C(*mod* n)

Data encrypted with the public key is decrypted with the corresponding private key. Enhancing security involves selecting two prime numbers simultaneously. However, this requires implementing efficient algorithms like Exponentiation by Squaring and Square and Multiply for effective encryption and decryption. For simplicity, the program is designed with relatively small prime numbers [9].

Table 1: Difference between Symmetric and Asymmetric Encryption

Symmetric Encryption	**Asymmetric Encryption**
It is a type of encryption that uses a single key to both encrypt (encode) and decrypt (decode) data or information.	It is a type of encryption that uses two keys, a private and a public key, to encrypt and decrypt data.
The same private key is used for both encoding and decoding information.	The public key is only used to encrypt the data and the private key is used to decrypt the data.
This type of encryption is mostly used in modern computer systems to protect user privacy and enhance security.	This type of encryption is widely used for sharing of information or data between organizations and to secure online transactions.
AES is a standard symmetricencryption algorithm.	RSA is a standard asymmetric algorithm. encryption
The widely used symmetric encryption algorithms are AES-128, AES-192, and AES-256.	The widely used asymmetric encryption algorithms are Diffie- Hellman, ECC, ElGamal, DSA, Elliptic curve cryptography (ECC), etc.

FUTURE ADVANCEMENTS IN THE FIELD OF CLOUD COMPUTING

Over the next five years, the IT industry is poised for a significant shift towards automation, with Artificial Intelligence (AI) and Machine Learning (ML) playing pivotal roles in driving this transformation. This shift is expected to have profound implications, potentially leading to a decrease in traditional programming jobs within the industry. As automation gains momentum, it introduces new challenges, particularly in terms of security and intrusion detection [15].

Consider an illustrative example: as machines increasingly take on the task of logic building, the risk of intrusion escalates. Unlike traditional programmers, who may require substantial time to exploit computer resources, automated processes enabled by AI and ML can execute tasks in mere seconds. Consequently, conventional Intrusion Detection Systems (IDS) may no longer suffice in the face of automation-driven threats. Hence, there is an urgent imperative to bolster traditional security mechanisms, notably Firewalls and IDS, to effectively mitigate emerging risks [16].

According to the report "Cyber Security: Threats, Reports, and Challenges" , in 2016, merely one percent of the world's devices utilized internet and cloud-based services. However, projections suggest that by 2023, this figure will surge to 85 percent, highlighting the escalating reliance on internet and cloud services across industries. With the proliferation of vulnerabilities. Addressing these challenges demands advancements in security measures and rigorous research to enhance cloud security protocols. It is imperative to explore avenues for fortifying security

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

systems and devising proactive strategies to thwart potential attacks, even amidst the evolving landscape of automation technologies [15].

Table 2: Comparsion of some cloud computing platform

Property	Different Platforms				
	Amazon Elastic Compute Cloud (EC2)	Microsoft Azure	Google App Engine	Sun Network.com (Sun Grid)	GRIDS Lab Aneka
Focus	Infrastructure	Platform	Platform	Infrastructure	Enterprise clouds
Service Type	Compute, Storage (Amazon S3)	Web and non-web application	Web Application	Computing	Computing
User Access Interface	Amazon EC2 command-line tools	Microsoft windows azure portal	Web-based administration	scripts, Sun Grid web portal	Work- bench, web- based portal
Value-added service providers	Yes	Yes	No	Yes	No
Virtualization	OS level running on a Xen hypervisor	OS level through fabric controller	Application container	Job management system (Sun Grid Engine)	Resource and manager scheduler
Web APIs	Yes	Yes	Yes	Yes	Yes
Dynamic negotiation of QoS	None	None	None	None	SLA-base resources reservation
Programming Frame-work	Amazon Machine Images (AMI)	Microsoft. NET	Python	Solaris OS. Java, C, C++, FORTRAN	APIs supporting models in c#.Net

Cloud computing adoption witnessed significant momentum in 2020, spanning various industries as numerous businesses made the transition to cloud-based operations [5]. However, as we look ahead to 2025, the trajectory indicates a near- universal embrace of cloud infrastructure and services across the board. This encompasses not only enterprises but also small businesses and government agencies, marking a substantial shift in IT paradigms.

In 2020, the emergence of hybrid cloud strategies signalled a growing trend, as organizations sought to leverage a mix of on-premises, public cloud, and private cloud resources. Fast forward to 2025, and hybrid and multi-cloud strategies have become the de facto standard. Organizations are now intricately optimizing their cloud environments, capitalizing on the distinctive offerings of various cloud providers while safeguarding control over sensitive data and applications [11].

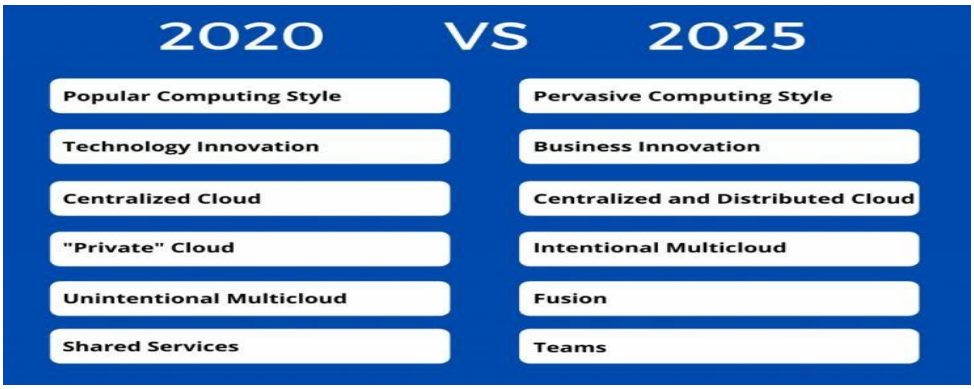

Figure 5: Cloud computing compared to 2020 vs 2025

Edge computing, which began gaining traction in 2020, has now evolved into an indispensable component of cloud architecture by 2025. The widespread deployment of edge nodes and devices caters to the burgeoning demand for real-time data processing and analysis, especially critical for applications like IoT, autonomous vehicles, and augmented reality.

Similarly, the integration of AI and machine learning into cloud services, which was already underway in 2020, has now reached unprecedented levels by 2025. Advanced AI models and algorithms power a diverse array of applications

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and services, with cloud providers rolling out specialized AI tools to facilitate seamless development and deployment of AI-powered solutions. Security and compliance, perennial concerns in cloud adoption, saw significant strides in 2020 with the development of robust security measures and compliance frameworks. In 2025, this trend continues, Internet of Things (IoT) devices, the burden on cloud infrastructure intensifies, exacerbating security [5] with a heightened focus on encryption, identity management, and threat detection. Cloud providers are at the forefront, offering enhanced security features and compliance certifications to meet evolving customer needs [8].

Moreover, the concept of green cloud computing, which gained traction in 2020, has become paramount by 2025. Cloud providers are heavily investing in renewable energy sources, energy-efficient infrastructure, and carbon offset initiatives to minimize the environmental impact of data centers, signaling a concerted effort towards sustainability. Overall, cloud computing in 2025 is poised to be more advanced, integrated, and pervasive compared toits2020 counterpart. Organizations across the spectrum are increasingly reliant on the cloud for driving innovation, fostering agility, and gaining a competitive edge in the ever- evolving digital landscape [9].

RESULTS AND DISCUSSION

The analysis conducted in this paper delves deep into the realm of cloud computing security, shedding light on the various concerns and vulnerabilities inherent in cloud environments. By meticulously identifying fundamental risk factors and elucidating on specific security threats, the study underscores the critical importance of implementing robust security measures to safeguard valuable information assets within cloud deployments.Proposed solutions tailored to enterprises and service providers offer practical avenues for enhancing information security within cloud environments. These solutions encompass a range of measures such as data encryption, access control mechanisms, security audits, and continuous monitoring. By adopting these proactive measures, organizations can effectively mitigate security risks and enhance the overall security posture of their cloud deployments.

SECURITY PROBLEMS WITH GROUPED CATEGORIES

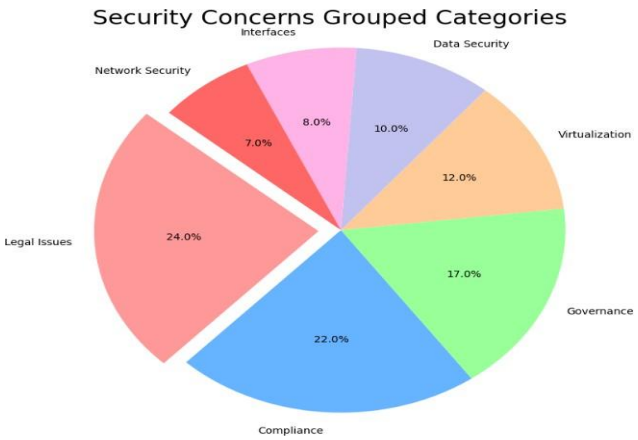

Figure 6: Security concerns with grouped categories.

The pie chart provides an overview of security concerns across seven grouped categories, offering insights into the primary areas of focus for organizations in managing cybersecurity risks [8]. Here's a detailed breakdown of each category: Legal Issues: This category encompasses concerns associated with adhering to legal regulations and compliance requirements, as well as addressing potential legal ramifications arising from security breaches.

Compliance: Compliance concerns center around ensuring adherence to industry standards, regulatory mandates, and internal policies aimed at safeguarding data privacy and security.

Governance: Governance pertains to the establishment of policies, protocols, and controls necessary for effectively managing and mitigating security risks within an organization's operations.

Virtualization: Virtualization concerns focus on securing virtualized environments, such as virtual machines and containers, to prevent unauthorized access and maintain the integrity of data stored within these environments.

Journal of Information Systems Engineering and Management
2025, 10(56s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Data Security: Data security involves implementing measures to protect sensitive information from unauthorized access, disclosure, manipulation, or destruction, thereby safeguarding the confidentiality and integrity of data assets.

Interfaces: Interface security is crucial for securing communication channels, APIs, and interfaces between different systems or components, aiming to prevent data breaches and unauthorized access attempts.

Network Security: Network security encompasses strategies and technologies designed to safeguard network infrastructure, devices, and communication protocols against cyber threats, unauthorized intrusions, and malicious activities.

Through this comprehensive analysis of security concerns, organizations can gain valuable insights into the diverse aspects of cybersecurity risk management and prioritize their efforts and resources effectively to address critical areas of vulnerability and mitigate potential risks.

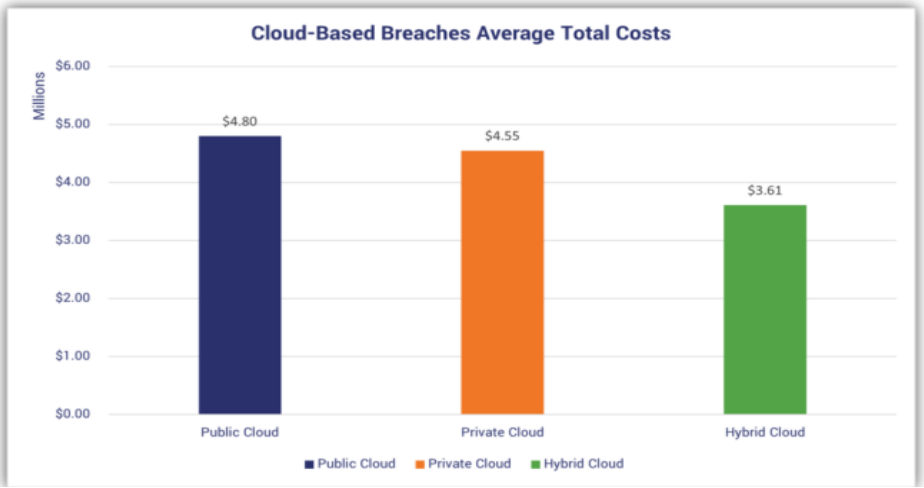

Figure 5: Cloud-Based Breaches Cost.

According to the 2021 Cost of a Data Breach report, jointly conducted by IBM and the Ponemon Institute, organizations utilizing a hybrid cloud infrastructure experienced an average data breach cost of $3.61 million. This figure is notably lower than the costs associated with data breaches in other cloud deployment models, such as on-premises, private, and public clouds [9]. On a global scale, businesses encountered an average total cost of $4.24 million per data breach incident. These findings underscore the significant financial impacts of cybersecurity breaches across diverse industries and deployment scenarios.

The introduction of the Security Threats Measurement Model (STMM) presents a novel approach to assessing security threats in cloud computing environments. By integrating system, management, and technical security factors, the STMM provides a comprehensive framework for identifying security deficiencies and making informed decisions regarding service providers and security enhancements. This model empowers organizations to conduct thorough security assessments and implement targeted mitigation strategies.Looking towards future advancements, the study highlights the increasing reliance on automation, artificial intelligence (AI), and machine learning (ML) technologies in cloud computing. It emphasizes the need for enhanced security measures to address emerging risks posed by automation- driven threats. Additionally, the paper underscores the importance of fortifying security systems and devising proactive strategies to tackle evolving security challenges in cloud environments.A comparison of cloud computing trends between 2020 and 2025 reveals significant shifts in adoption rates, hybrid and multi-cloud strategies, edge computing integration, AI and machine learning integration, security, compliance, and green cloud computing initiatives. These trends underscore the evolving landscape of cloud computing and underscore the growing importance of cloud services in driving innovation and competitiveness across industries.In conclusion, the insights presented in this paper offer valuable guidance for organizations navigating the complexities of cloud adoption and security management. By addressing security concerns, implementing practical solutions, and staying

informed about emerging trends, organizations can effectively harness the benefits of cloud computing while ensuring robust security measures are in place

CONCLUSION

Cloud computing is an emerging technology that embodies the concept of distributed computing. While it has yet to reach its full potential, the future of the software industry hinges significantly on this paradigm shift. This paper delves into an exploration of cloud computing, elucidating its core principles and the diverse array of services it offers. Furthermore, it examines the pivotal role of cloud computing in key industries, addressing pertinent issues such as security challenges and research imperatives. A critical aspect discussed in this paper revolves around the security challenges inherent in cloud computing, particularly concerning network security and virtualization. By shedding light on these challenges, the paper aims to propose strategies for mitigating risks and fortifying cloud security. It underscores the need for the development of innovative security technologies tailored to the unique architecture of cloud computing, alongside the adaptation of existing security measures to align with evolving industry standards. Moreover, the paper explores the utilization of cloud services across five key industries, offering insights into the increasing adoption of cloud technology from 2015 to 2017. This analysis underscores the growing significance of cloud computingacross diverse sectors, highlighting its transformative impact on industry operations and efficiency. Finally, the paper touches upon the burgeoning realm of automation in cloud computing, presenting an overview of its potential implications and associated security challenges. While automation in cloud computing remains an evolving concept requiring further research and clarity, this paper aims to contribute to the discourse by delineating key design challenges and paving the way for future research endeavors in this dynamic field.

REFERENCES

[1] Junyi Deng, (Member, Ieee), Jikai Deng, Peihao Liu, Huan Wang, (Member, Ieee), Junjie Yan, Deru Pan, And Jiahua Liu, “A Survey on Vehicular Cloud Network Security,” IEEE Access, 2023
[2] Waleed Almuseelem,“Energy-Efficient and Security-Aware Task Offloading for Multi-Tier Edge-CC Systems,” IEEE Access, 2023
[3] S. V. Aswin Kumer, N. Prabakaran, E. Mohan, Balaji Natarajan, G. Sambasivam, (Member, Ieee), And Vaibhav Bhushan Tyagi, “Enhancing Cloud Task Scheduling With a Robust Security Approach and Optimized Hybrid POA,” IEEE Access, 2023
[4] Ishu Gupta, (Member, Ieee), Ashutosh Kumar Singh, (Senior Member, Ieee), Chung-Nan Lee, (Member, Ieee), And Rajkumar Buyya, (Fellow, Ieee), “Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions,” IEEE Access, 2022
[5] Seongmo An, Asher Leung, Jin B. Hong, (Member, Ieee), Taehoon Eom, And Jong Sou Park, “Toward Automated Security Analysis and Enforcement for Cloud Computing Using Graphical Models for Security,” IEEE Access, 2022
[6] Baris Celiktas, Ibrahim Celikbilek, And Enver Ozdemir, “A Higher-Level Security Scheme for Key Access on Cloud Computing,” IEEE Access, 2021
[7] Wenxin Qiao , Yicen Liu , Leiping Xi, Xi Li, Zhiwei Li , Donghao Zhao, And Yu Lu, “A Novel Method for Resource Efficient Security Service Chain Embedding Oriented to Cloud Datacenter Networks,” IEEE Access, 2021
[8] Ijaz Ahmad, Jarno Pinola, (Member, Ieee), Ilkka Harjula, Jani Suomalainen, Erkki Harjula, (Member, Ieee), Jyrki Huusko, And Tanesh Kumar, (Member, Ieee), “An Overview of the Security Landscape of Virtual Mobile Networks,” IEEE Access, 2021.
[9] Belal Ali, (Member, Ieee), Mark A. Gregory, (Senior Member, Ieee), And Shuo Li, (Member, Ieee), “Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review,” IEEE Access, 2021.
[10] Ruba Awadallah And Azman Samsudin, “Using Blockchain in Cloud Computing to Enhance Relational Database Security,” IEEE Access, 2021
[11] M. R. Shrihari, T. N. Manjunath, R. A. Archana, and R. S. Hegadi, “Development of security performance and comparative analyses process for big data in cloud,” in Lecture notes in electrical engineering, 2021, pp. 147–160. doi: 10.1007/978-981-16-1338-8_13.
[12] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, “Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach,” IEEE Internet Things J., vol. 8, no. 4, pp. 2226–2237, Feb. 2021.

[13] Q. Su, R. Zhang, R. Xue, and P. Li, "Revocable attribute-based signature for blockchain-based healthcare system," IEEE Access, vol. 8, pp. 127884–127896, 2020.
[14] Shrihari, G. Singh, K. Reddy, and N. Ajay, "Organ Donation and Transplantation Framework using Blockchain," IEEE, pp. 1–6, Apr. 2024, doi: 10.1109/ickecs61492.2024.10616806.
[15] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen, and Z. Weizhe, "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," IEEE Internet Things J., vol. 7, no. 5, pp. 4000–4015, May 2020.
[16] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for secure EHRs sharing of mobile cloud based E-Health systems," IEEE Access, vol. 7, pp. 66792–66806, 2019.
[17] M. T. N, S. M. R, and P. S. K, "A Survey on Machine Learning Techniques Using Quantum Computing," IEEE, Dec. 2022, doi: 10.1109/icerect56837.2022.10059764.
[18] .N. Ajay, H. S. Mohan, B. V. Shwetha, M. R. Shrihari, and T. N. Anitha, "Access Control Framework in the Cloud based on Multi-Blockchain with Light Privacy Protection," 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), pp. 1–5, Apr. 2022, doi: 10.1109/icdcece53908.2022.9792816.