Surveying Security Challenges in Cloud Computing: Current Landscape and Future Directions

Chandan Kumar Barik[1], Mrs. Barsha Panda[2]

[1,2]Assistant Professor, Driems University

Abstract:
Customers can access a shared computer resource pool on demand or on a pay-per-use basis using a cloud computing paradigm. Cloud computing has advantages for both users and cloud service providers (CSPs). Due to its benefits including cost effectiveness and versatility, it is one of the most alluring technological fields today. Given the lack of a central location, omniscience, and a preexisting trust connection, it allows the virtual organization to pool geographically dispersed resources to accomplish shared objectives. Despite the tremendous investment returns that cloud computing promises, customers are unsure about whether to use its services due to the security risks involved. This article is a survey that focuses more specifically on the various security vulnerabilities that have arisen because of how cloud computing systems deliver services. To deliver data secrecy, data integrity, and data availability, it makes several recommendations that should be implemented in further efforts.

Keywords: Cloud Computing, Virtualization, security vulnerabilities, data integrity.

Introduction:
Cloud computing is a business model that has gained prominence in the delivery of IT infrastructure, components, and applications. It is a means of providing access to computer resources. Cloud computing, according to the National Institute of Standards and Technology (NIST), is a model that allows for easy on-demand network access to a shared pool of reconfigurable computer resources, such as networks, storage, hardware, and applications, that can be quickly allocated, scaled, and released with little involvement from service providers or management. A disruptive transition from IT as a product to IT as a service occurs when cloud computing converts a product-centric approach for IT provisioning into a global, distributed, service-centric. Cloud computing has transformed the processes involved in the creation, development, deployment, scaling, updating, maintenance, and payment of IT services [1].
Internet computing is another name for cloud computing. Cloud computing collections are available on the Internet [2]. Clouds provide users permission to access resources on the internet from wherever. Key resources are not physically affected by accessing the cloud at any time or from any location. The most prominent example of cloud computing is Google Apps, which can provide services across the internet to billions of PCs via web browsers.
The following succinctly describes the primary contributions of this article:

1. It provides the foundations of cloud computing, including the deployment and service models which are covered in Section 2.

2. An overview and description of the efforts undertaken in the literature to address these security concerns is covered in Section 3.
3. We go over current concerns about cloud security and suggest some avenues for further research in Section 4.

Cloud Computing Service Models:

The cloud architecture can be broadly categorized into three cloud service models: platform-as-a-service (PaaS), the middle layer that offers an environment for users to develop and host their applications; infrastructure-as-a-service (IaaS), the lowest layer that provides the basic infrastructure for the other layers; and software-as-a-service (SaaS), the upper layer that offers an application layer that functions as a service on demand [3].

1. Software as a Service (SaaS) SaaS, or software as a service, is the highest tier in the cloud stack [4]. It uses the Internet to offer the service and gives consumers access to cloud-based software and apps. One of SaaS's computational needs benefits is that users don't need to install or maintain any software on their personal PCs. Because the infrastructure and the execution platform are entirely within the service provider's control, the users rely on them for security.
2. Platform as a Service (PaaS) The user can install their own software or apps on the cloud infrastructure by using the resources they have rented from the provider together with the programming languages and tools that the provider supports. The customer may manage the deployment of his applications and the configurations of the application hosting environment under this delivery model, but not the cloud infrastructure. Force.com and Google Application Engine are two instances of PaaS services[5].
3. Infrastructure as a Service (IaaS) The user may install apps, which may include operating systems and other apps, by utilizing a variety of computer resources, including networks, processing, storage, and provisioning. Customers have control over operating systems, storage, applications, and specific networking components based on predetermined needs. However, they lack the capacity to manage and govern cloud infrastructure. Through the Internet, Infrastructure as a Service (IaaS) offers virtualized computing resources like Google Compute Engine (GCE), Microsoft Azure, and Amazon Web Services (AWS), and all services provided by Cloud service providers (CSPs) are integrated across the virtual machines[6].

Cloud Deployment models.

There are four basic deployment types for cloud computing outlined by NIST [7]—public clouds, private clouds, hybrids clouds and community clouds.

Public Clouds

Third-party cloud service providers own and run public clouds, which are openly shared online by a variety of customers for hardware and software resources. Sensitive data should not be stored in such clouds because of security concerns and the fact that a third-party public cloud service provider oversees and maintains this environment [8] [9].

Private Cloud

A private cloud is one that keeps its software and hardware infrastructure on a private network [10] [11]. Only one organization may use cloud services, and the cloud itself—which can be on- or off-site—is either controlled by the corporation or a third party. It is not given to any other institution. Private cloud computing is expensive, even though it solves the security issues with public cloud computing. This is often used by large enterprises, and small-to-medium-sized businesses should stay away from employing it.

Community Cloud:

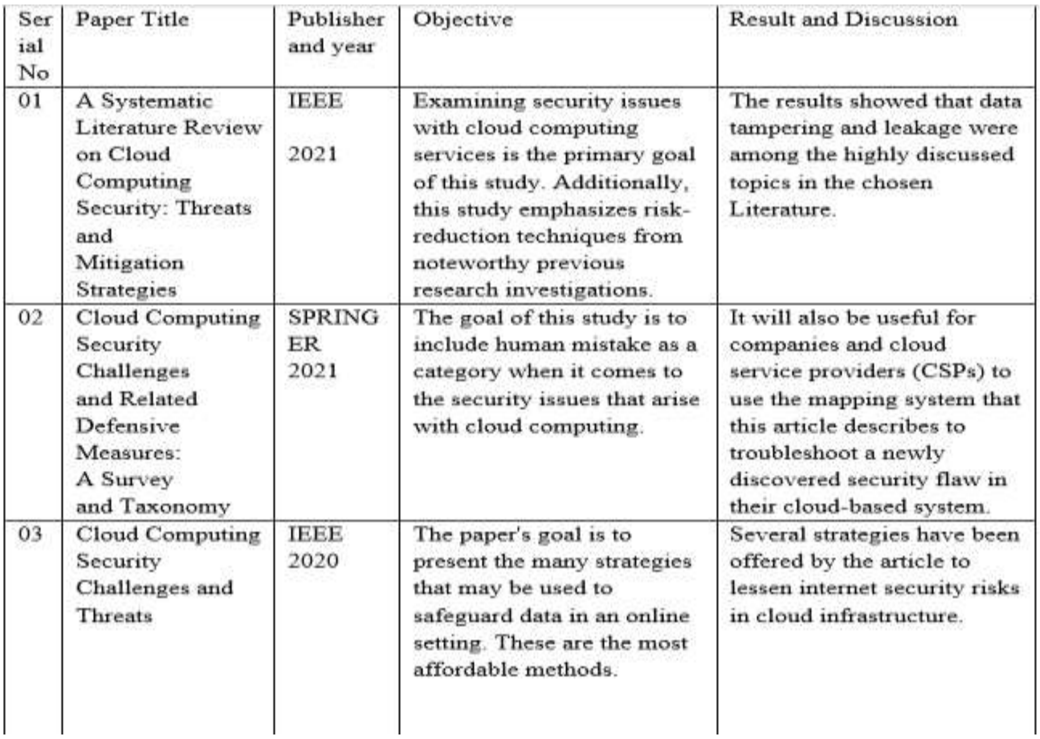
Cloud services are solely offered to a group of enterprises with similar cloud needs. The cloud is hosted either on-site or off-site and is maintained by the organizations or by a third party. The disadvantage of this architecture is that many questions remain unresolved about contractual and security ramifications, as well as service disruptions and difficulties with data being dispersed across various companies and domains [11].

Hybrid Cloud:

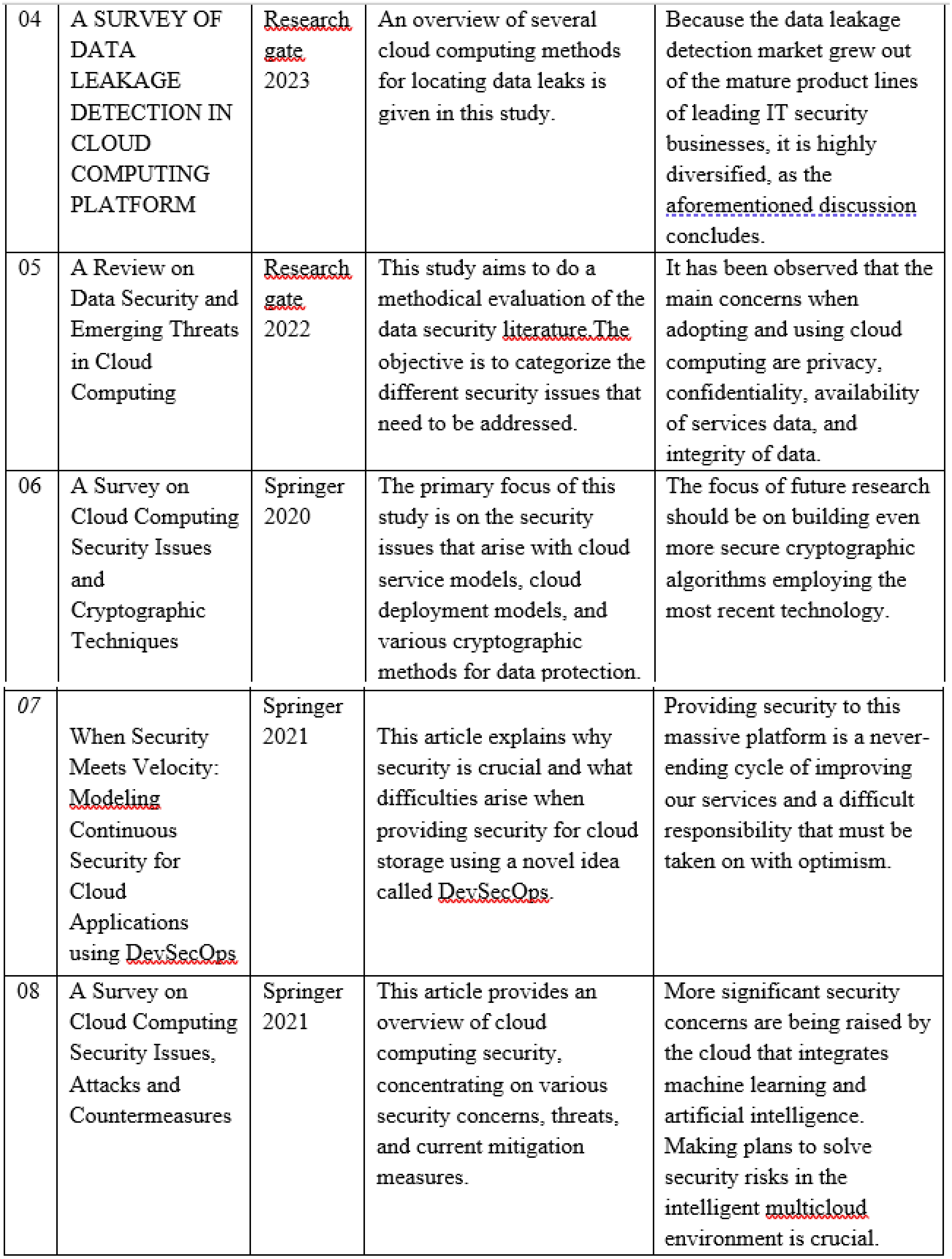
The cloud infrastructure is made up of two or more separate, different cloud infrastructures (public, communal, or private) that continue to exist as separate entities. Using a hybrid method, the clouds exchange resources. Companies can rely on the public cloud as needed while still maintaining control over an internally controlled private cloud by adopting a hybrid strategy [9]. The cost and scalability benefits of public clouds are combined with private cloud management and security in hybrid cloud computing. Concerns over data privacy and integrity, as well as data transfers from public to private environments or vice versa, are among the threats to the hybrid cloud since privacy.

Cloud virtualization

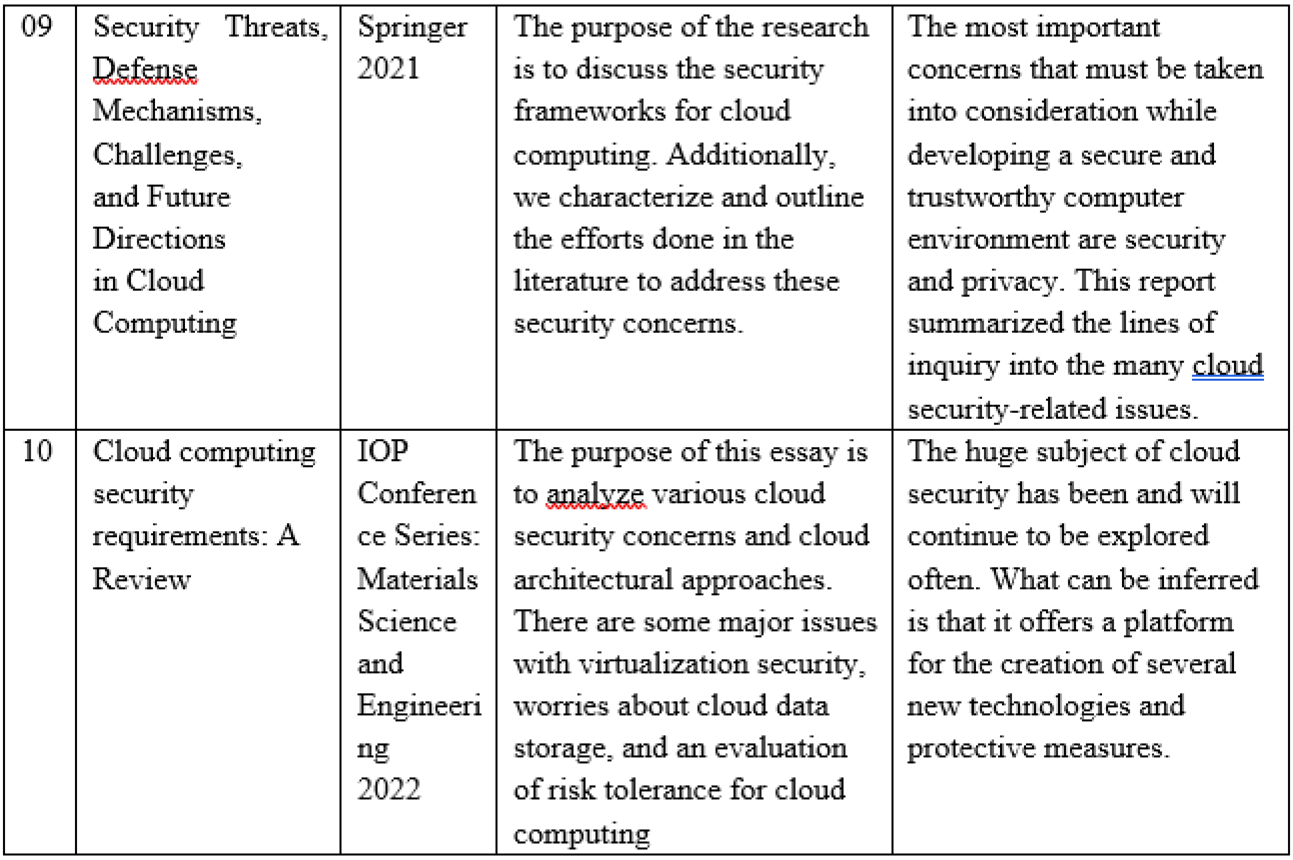
The concept of cloud computing has emerged as a paradigm that offers pay-per-use computer resources that are dynamically configured to meet various workload requirements. This is because virtualization technology allows many virtual machines (VMs) to be created using the same physical resources [14, 15]. Based on virtualization, the virtual machine (VM) can be referred to as an operating system (OS) or software that simulates the behavior of a computing system based on predefined resource characteristics, such as memory capacity and central processor unit.



Serial No	Paper Title	Publisher and year	Objective	Result and Discussion
01	A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies	IEEE 2021	Examining security issues with cloud computing services is the primary goal of this study. Additionally, this study emphasizes risk-reduction techniques from noteworthy previous research investigations.	The results showed that data tampering and leakage were among the highly discussed topics in the chosen Literature.
02	Cloud Computing Security Challenges and Related Defensive Measures: A Survey and Taxonomy	SPRINGER 2021	The goal of this study is to include human mistake as a category when it comes to the security issues that arise with cloud computing.	It will also be useful for companies and cloud service providers (CSPs) to use the mapping system that this article describes to troubleshoot a newly discovered security flaw in their cloud-based system.
03	Cloud Computing Security Challenges and Threats	IEEE 2020	The paper's goal is to present the many strategies that may be used to safeguard data in an online setting. These are the most affordable methods.	Several strategies have been offered by the article to lessen internet security risks in cloud infrastructure.



04	A SURVEY OF DATA LEAKAGE DETECTION IN CLOUD COMPUTING PLATFORM	Research gate 2023	An overview of several cloud computing methods for locating data leaks is given in this study.	Because the data leakage detection market grew out of the mature product lines of leading IT security businesses, it is highly diversified, as the aforementioned discussion concludes.
05	A Review on Data Security and Emerging Threats in Cloud Computing	Research gate 2022	This study aims to do a methodical evaluation of the data security literature.The objective is to categorize the different security issues that need to be addressed.	It has been observed that the main concerns when adopting and using cloud computing are privacy, confidentiality, availability of services data, and integrity of data.
06	A Survey on Cloud Computing Security Issues and Cryptographic Techniques	Springer 2020	The primary focus of this study is on the security issues that arise with cloud service models, cloud deployment models, and various cryptographic methods for data protection.	The focus of future research should be on building even more secure cryptographic algorithms employing the most recent technology.
07	When Security Meets Velocity: Modeling Continuous Security for Cloud Applications using DevSecOps	Springer 2021	This article explains why security is crucial and what difficulties arise when providing security for cloud storage using a novel idea called DevSecOps.	Providing security to this massive platform is a never-ending cycle of improving our services and a difficult responsibility that must be taken on with optimism.
08	A Survey on Cloud Computing Security Issues, Attacks and Countermeasures	Springer 2021	This article provides an overview of cloud computing security, concentrating on various security concerns, threats, and current mitigation measures.	More significant security concerns are being raised by the cloud that integrates machine learning and artificial intelligence. Making plans to solve security risks in the intelligent multicloud environment is crucial.



09	Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing	Springer 2021	The purpose of the research is to discuss the security frameworks for cloud computing. Additionally, we characterize and outline the efforts done in the literature to address these security concerns.	The most important concerns that must be taken into consideration while developing a secure and trustworthy computer environment are security and privacy. This report summarized the lines of inquiry into the many cloud security-related issues.
10	Cloud computing security requirements: A Review	IOP Conference Series: Materials Science and Engineering 2022	The purpose of this essay is to analyze various cloud security concerns and cloud architectural approaches. There are some major issues with virtualization security, worries about cloud data storage, and an evaluation of risk tolerance for cloud computing	The huge subject of cloud security has been and will continue to be explored often. What can be inferred is that it offers a platform for the creation of several new technologies and protective measures.

Literature Review:

Security concerns with cloud computing services. One collaborating technology that was discussed in this study to ease security concerns was the blockchain. Furthermore, this study highlights risk-reduction strategies from notable earlier studies. Leaks and data manipulation are two of the threats mentioned. The reliability of customers, data outsourcing, and the hazards involved are major issues, Alouffi, Bader, et al, (12).The blockchain-based cloud's security features include network security, access control, privacy, and authentication. This is a thorough work and with the enhanced security may be used for a real-time application. Users' data privacy may now be protected and dependability can be increased thanks to the possibility of tracking changes made by users. When blockchain technology is used effectively, consumers' confidence is maintained even when data is outsourced and an additional security layer is added to cloud data. An authorized user obtains the necessary data.

There is a case to be made for human error to be taken into account when categorizing security risks associated with cloud computing. Both cloud service providers (CSPs) and their clients may fully profit from this computing model's advantages if they are completely aware of the security risks in the cloud. It includes various subcategories like insecure APIs, Vendor Lock-In, Misconfiguration of Computing Assets, Weak Authentication and Authorization (WAA), Weak Control Plane, Limited Cloud Usage Visibility, Maduji-Chuka,et al,(13).The category of human error was added to the list of risks and difficulties associated with cloud computing security throughout the inquiry. Human operators, or employees of a company, are frequently perceived as the weakest link in the chain of information security. Therefore, this study focused on identifying human-related difficulties and threats to cloud security, or more precisely, problems related to human mistake, as well as potential defensive measures to reduce such risks.

Since security is a major worry, most people are worried about storing their data in clouds, especially users who are unaware of the rise in attacks and technological advancements. There are a few strategies and tactics for safeguarding data in an online setting. These are the least expensive tactics and strategies that any user may utilize to easily defend oneself against attacks,Balani, Zina, Varol,et al,(14). Illegal entrance may be stopped and authorized users can access an information system. In order to precisely outline each party's obligations and tasks with regard to the terms of the contract, cloud service providers and users must sign a SLA. Cloud service providers have to guarantee employee openness and tested fixes. In the areas of compatibility, workload analysis, and prototyping, cloud providers need to solve these concerns in order to achieve the flexibility, scalability, and efficiency of available resources.

A breach of information's confidentiality is known as data leaking. It refers to unapproved data transmission from a company's internal site to an external place. While data leaking refers to the revelation of private or secret information, data loss refers to the loss of data as a result of deletion, system failure, etc. Both phrases may be used to allude to a data breach, which is one of the main worries that enterprises face these days. The research discusses several modules like data allocation module, fake object module, optimization module, Data Distributor Module and Agent Guilt Module and also discusses The Audit Trail/Transaction, Watermarking Method, Data Allocation Techniques, and VM Migration Process, Ghosh, Anunay, et al(15)

It has been observed that the main concerns while implementing and utilizing cloud computing are privacy, confidentiality, availability of services, and data integrity. This is a result of the security paradigm that services as a service adopted, which allows hackers to get in. Multi-tenancy in the cloud is another huge problem for customers since it increases the likelihood that a hacker would use the same host, Benard, Masese Chuma, et al.(16)

The process of transforming data into undetectable code and then transferring it such that only the intended recipients can access the real information is known as cryptography. Asymmetric key cryptography, symmetric key cryptography, and their encryption algorithms are only a few of the cryptographic processes that may be used in the cloud to safeguard data. Agarwal, Kaushal, Chouhan et al(17).

In order to meet time-to-market goals and maintain competitiveness, the DevOps methodology. The appropriate automation tools are integrated within the CI/CD pipeline to automate has facilitated agility and velocity in the delivery of cloud applications. Unfortunately, most apps are deployed with insufficient security capabilities due to the need to deliver them on time. The inclusion of security tasks along the DevOps practices is institutionalized as DevSecOps . DevSecOps extends the DevOps methodology to embed automated security tasks within the DevOps activities the security tasks and deliver the security enriched cloud applications. This article describes why security is important and what challenges come up when adopting a unique concept called DevSecOps to provide security for cloud storage, Kumar et al[18].

Cloud computing leverages virtualization to provide on-demand IT services. The ideas of programming level virtualization for PaaS and hardware virtualization for IaaS enable the right amount of control, security, isolation, and manageability for on-demand IT service delivery. Virtualization combined with server consolidation enables several applications to share a single physical server's resources at once. An overview of cloud computing security is given in this article, with a focus on different security issues, threats, and available mitigating techniques. The cloud that combines artificial intelligence and machine learning is posing more serious security risks. It is essential to consider how to address security concerns in the intelligent multicloud environment. As machine learning data sets consist of millions of rows of user data, handling sensitive data becomes crucial because the ownership idea breaks down. In order to apply machine learning to the detection of threats in the multicloud environment and to acquire valuable insights while maintaining the privacy of data items, research is necessary, Panda, D et al[19].

Six categories are used to categorize the main security risks and weaknesses associated with cloud computing: network security, virtualization, security of hypervisors, data and storage security, governance, identity and access control, and legal and compliance concerns. Virtualization is one of the main components of cloud computing that plays a vital role in security assessment. It allows the VMs monitoring and performance management of cloud infrastructure Hypervisor represents the abstraction layer that performs the elementary functions needed for resource management to divide the hardware resources between the VMs. Although this technology provides great benefits, it also presents additional security threats such as VM Escape, VM sprawling, Cross VM Side-Channel Attack etc. Numerous active defensive strategies have been implemented to stop and track computer assaults by analysing the attacker's activity and identifying the attacks in their early stages. Cloud service DDoS protections may be set up in four strategic places: the intermediate network, the source end, the access point, and the distributed. The strategies for detecting denial-of-service attacks can be classified as signature-based, anomaly-based, or hybrid depending on whether the traffic is considered normal or abnormal. The intrusion tolerance strategy acknowledges that preventing or thwarting such assaults is impractical. In fact, minimizing the effects of the assault and providing excellent service are its main goals. Fault tolerance and Quality of Service (QoS) are the two main components of intrusion tolerance, Kefhali, S et al[20].

Strong foundations of concepts, structure, and methodology must be built in order to prevent costly and ineffective operations, dysfunctional governance, difficult-to-automate controls or procedures, and inadequate security. Engineering, models, and architectural methods have all affected security architecture. Many new models are based on the System Security Engineering Capability Maturity Model (SSE-CMM), which was developed in the early 2000s and highlights the value of practicing security engineering. These kinds of models may be used as cloud computing, security operations, security architecture, and security engineering reference models, Tsochev, G et al[21].

Methodology for Cloud Computing Security Research:

1. Research Design

- Literature Review: Conducted a comprehensive review of existing literature on cloud computing security, including seminal papers, recent studies, and industry reports.
- Identification of Research Gaps: Identified gaps in the literature concerning specific security challenges, emerging threats, and mitigation strategies in cloud computing.

2. Data Collection

- Primary Data: Gathered primary data through surveys, interviews, or case studies with industry experts, cloud service providers (CSPs), and IT professionals to understand real-world challenges and practices.
- Secondary Data: Utilized secondary data sources such as academic journals, conference proceedings, white papers, and official reports to supplement primary findings and validate research outcomes.

3. Research Framework

- Conceptual Framework: Developed a conceptual framework based on NIST’s cloud computing models (SaaS, PaaS, IaaS) and deployment types (public, private, hybrid, community) to categorize and analyze security concerns.

- Theoretical Approach: Applied theoretical perspectives from cybersecurity, risk management, and cloud computing architectures to analyze security issues and propose solutions.

4. **Data Analysis**

- Qualitative Analysis: Employed qualitative methods to analyze interview transcripts, case studies, and qualitative survey responses for thematic patterns related to security challenges and mitigation strategies.
- Quantitative Analysis: Utilized statistical analysis techniques (if applicable) to analyze survey data, identifying trends, correlations, and statistical significance in security incidents or practices.

5. **Research Findings**

- Identification of Security Challenges: Summarized and categorized identified security challenges in cloud computing based on findings from literature review and primary data analysis.
- Proposed Mitigation Strategies: Developed and proposed effective mitigation strategies, including technological solutions, policy recommendations, and best practices derived from empirical findings and theoretical insights.

6. **Limitations**

- Scope Limitations: Acknowledged limitations related to scope of research, such as geographical focus, industry-specific considerations, and depth of data analysis.
- Data Limitations: Addressed any constraints related to data availability, reliability, or access during the research process.

7. **Conclusion and Implications**

- Conclusion: Summarized key findings and contributions of the study in addressing current gaps in cloud computing security literature.
- Implications: Discussed implications of the findings for cloud service providers, IT professionals, policymakers, and researchers in enhancing cloud security practices and resilience.

8. **Recommendations for Further Research**

- Future Research Directions: Proposed avenues for future research, including exploring emerging technologies (e.g., blockchain, AI) for enhancing cloud security, addressing evolving threats, and evaluating long-term impacts of security measures.

Result and Discussion:

1. **Data Security and Privacy:**

Data Integrity: Ensuring that data is accurate and reliable throughout its lifecycle.

Data Privacy and Confidentiality: Protecting sensitive information from unauthorized access or disclosure.

Location of Data: Knowing where data resides physically and ensuring compliance with data sovereignty laws.

Availability of Data: Ensuring data is accessible to authorized users whenever needed.

Data Storage, Backup, and Recovery: Safeguarding data against loss and ensuring timely recovery in case of failures.

Data Authentication: Verifying the identity of users and systems accessing data.

2. Sensitive Data Access:

Controlling and monitoring access to sensitive data to prevent unauthorized access and data breaches.

3. Data Segregation:
Implementing mechanisms to ensure that data from different clients or users is logically separated and protected from unauthorized access.

4. Privacy Concerns:
Addressing privacy issues associated with sensitive information stored in the cloud, ensuring compliance with privacy regulations.

5. Bug Exploitation:
Mitigating vulnerabilities in cloud systems that could be exploited by attackers to gain unauthorized access or disrupt services.

6. Recovery and Accountability:
Ensuring robust mechanisms for data recovery in case of incidents and establishing clear accountability for security breaches.

7. Malicious Insiders:
Preventing threats posed by insiders who have authorized access to systems and data but may misuse their privileges.

8. Management Console Security:
Securing administrative interfaces and management tools to prevent unauthorized access and potential manipulation of cloud resources.

9. Account Control:
Implementing strong authentication and access control measures to protect user accounts and prevent unauthorized use.

10. Multi-tenancy Issues:
Addressing security challenges arising from the shared use of cloud resources among multiple tenants, ensuring isolation and protection.

These points highlight the diverse range of security challenges that organizations face when adopting cloud computing. Effective security strategies involve a combination of technological solutions (e.g., encryption, access controls), adherence to best practices (e.g., data segregation, regular audits), and compliance with regulatory requirements to mitigate these risks and build trust among cloud service users.

Security Concerns in Cloud Computing:

- Data Security: Focuses on confidentiality, integrity, availability, and privacy of data.
- Access Control: Ensuring only authorized users have access to data and resources.
- Compliance and Legal Issues: Addressing regulatory requirements and data sovereignty concerns.
- Virtualization Security: Managing risks associated with virtual machine (VM) environments and hypervisors.
- Service Models Security: Specific challenges and vulnerabilities associated with SaaS, PaaS, and IaaS.

Conclusion and Recommendations:

- Summarizes identified security challenges and proposes mitigation strategies such as encryption, access control, and compliance frameworks.
- Discusses implications for cloud service providers, IT professionals, policymakers, and researchers.

- Suggests future research directions, emphasizing the need for enhanced security measures and integration of emerging technologies.

REFERENCES

1. A. Sunyaev, Internet Computing," Principles of Distributed Systems and Emerging Internet-Based Technologies"
2. Saurabh Singh1 , Young-Sik Jeong2 , Jong Hyuk Park1*,"A Survey on Cloud Computing Security: Issues, Threats, and Solutions"
3. L. Alhenaki, A. Alwatban, B. Alamri, N. Alarifi, A survey on the security of cloud computing, in 2019 2nd International Conference on Computer Applications and Information Security (ICCAIS) (Riyadh, Saudi Arabia, 2019), pp. 1–7. https://doi.org/10.1109/CAIS.2019.8769497
4. Software as a Service (SaaS). Cloud Taxonomy. Open crowd
5. Gourisaria MK, Samanta A, Saha A, Patra SS, Khilar PM (2020) An extensive review on cloud computing. In: Data engineering and communication technology. Springer, Singapore, pp 53–78
6. Attaran M, Woods J (2019) Cloud computing technology: improving small business performance using the Internet. J Small Bus Entrep 31(6):495–519 9.
7. P.M. Mell, T. Grance, The NIST definition of cloud computing, in Computer Security Publications from the National Institute of Standards and Technology (NIST) SP 800145 (National Institute of Standards & Technology, Gaithersburg, 2011)
8. T.S. Chou, Security threats on cloud computing vulnerabilities. Int. J. Comput. Sci. Inf. Technol. 5(3), 79 (2013)
9. W.C.N. Nimit Kaura, C.A.L. Lal, Survey paper on cloud computing security, in International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)
10. There's No Such Thing As A Private Cloud. Information Week. 30 June 2010
11. S. Goyal, Public versus private versus hybrid versus community—cloud computing: a critical review. Int. J. Comput. Netw. Inf. Secur. 6, 20–29 (2014). https://doi.org/10.5815/ijcnis.ii2014. 03.03
12. 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.
13. Chuka-Maduji, Nnamdi, and Vaibhav Anu. "Cloud computing security challenges and related defensive measures: A survey and taxonomy." *SN Computer Science* 2.4 (2021): 331.
14. Balani, Z., & Varol, H. (2020, June). Cloud computing security challenges and threats. In *2020 8th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-4). IEEE.
15. Ghosh, A., Dhar, P., Banerjee, A., & Sanyal, M. (2023). A Survey of Data Leakage Detection in Cloud Computing Platform.
16. . Benard, M. C., Hussein, M., Victor, T., & Charo, J. S. (2022). A Review on Data Security and Emerging Threats in Cloud Computing. *International Journal of Research and Scientific Innovation*, *9*(VI).
17. Agarwal, V., Kaushal, A. K., & Chouhan, L. (2020). A survey on cloud computing security issues and cryptographic techniques. In *Social Networking and Computational Intelligence: Proceedings of SCI-2018* (pp. 119-134). Springer Singapore.

18. Kumar, R., & Goyal, R. (2021). When security meets velocity: Modeling continuous security for cloud applications using DevSecOps. In *Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020* (pp. 415-432). Springer Singapore.
19. Panda, D. R., Behera, S. K., & Jena, D. (2021). A survey on cloud computing security issues, attacks and countermeasures. In *Advances in Machine Learning and Computational Intelligence: Proceedings of ICMLCI 2019* (pp. 513-524). Springer Singapore.
20. El Kafhali, S., El Mir, I., & Hanini, M. (2022). Security threats, defense mechanisms, challenges, and future directions in cloud computing. *Archives of Computational Methods in Engineering*, *29*(1), 223-246.
21. Tsochev, G. R., & Trifonov, R. I. (2022). Cloud computing security requirements: A Review. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1216, No. 1, p. 012001). IOP Publishing.