Cloud Computing Security Issues andCountermeasure: A Comprehensive Survey

Shaimaa Salama
Faculty of Computer and Information Technology
King Abdulaziz University

Yasmin Alamoudi
Faculty of Computer and Information Technology
King Abdulaziz University

Ghadeer Alamoudi
Faculty of Computer and Information Technology
King Abdulaziz University

Farah Albeshri
Faculty of Computer and Information Technology
King Abdulaziz University

ABSTRACT
Cloud computing has drawn attention in the current technological world due to its many benefits in contrast to traditional information technology (IT) infrastructure. Nowadays, many companies moved to the cloud instead of hosting computing resources internally in a privately owned cloud data center. As a result, the use of cloud computing has allowed companies to focusmore on their business instead of developing and maintaining their own information technology (IT) equipment. In addition, cloud computing solves the limited resources problem; it intends to minimize the cost of services by sharing valuable resources which can be accessed remotely from anywhere among multiple users. Currently, organizations depend on cloud computingto effectively manage and store their data. However, storing organizational data raises many concerns and vulnerabilities; researchers have experimented with and used a variety of data protection and prevention strategies and techniques to reinforce the security barrier. However, gaps still need to be addressed by improving and strengthening these methods. This paper offersa survey of current relevant work that focuses on security concerns and protective measures in various aspects. These considerations must be taken into account when applying security to cloud computing infrastructure. Moreover, the paper proposesa new classification of the literature review following the CIA common model, which forms the basis for the systems security development.

Keywords
Cloud, Services, Resources, Security Issues, Countermeasure, Data, Storage

1. INTRODUCTION
Cloud computing has become a point of interest and isone of the major driving forces in the current technological world. Cloud computing is a network access model that allowsfor useful, on-demand access to a shared pool of computing resources such as servers, storage, networks, and applications that can be rapidly provisioned and released with little management effort or interaction from the service provider [1].As a result, cloud computing has provided many benefits in contrast to traditional IT. For instance, companies are no longer required to spend money developing and maintaining their own IT infrastructure and can instead focus on theircore business. Furthermore, this platform solves the problem of limited resources and minimizes the cost of services by sharing valuable resources between multiple users remotely from anywhere [2]. The concept of cloud computing arose from the distributed computing model. Architecture for software cloud computing technology is intended to provide internet-based hosted ser- vices. In the field of information technology over the past few years, cloud computing has given rise to various new user groups and markets [3]. The global cloud computing market has witnessed an expansion due to the rapid adoption rate, which is related to the many advantages of moving to the cloud instead of hosting computing resources internally in a privately owned cloud data center [4]. Organizations depend on cloud computing to effectively manage excessive data quantity and handle them. However, storing organizational data outside of premises raises many concerns and vulnerabilities; for instance, a data breach or other significant threat can seriouslyharm the company's reputation and financial standing.

Security and privacy concerns have emerged as significant issues when cloud providers share large amounts of data and critical applications with customers. As a result of these considerations, related topics pose significant challenges in the field of cloud computing [5]. Any cloud-based solution's achievement depends on giving cloud administrators, software developers, and end users the best experience possible. Security is a critical barrier in cloud computing because data and applications may reside at multiple layers depending on the selected cloud service model [6]. Cloud computing introduces several characteristics that require special consideration when it comes to trusting the system. The trustworthiness of the entire system is determined by the data protection and prevention techniques employed. Researchers have tested and introduced different tools and techniques for data protection and prevention to gain and remove the barrier of trust. However, gaps stillneed to be filled by making these techniques much better and more effective. Another issue in cloud computing is resource security, management, and monitoring. There currently needs to be standard regulations and guidelines for cloud applicationdeployment, and there is a lack of control management in the cloud [7].

As cloud computing has quickly evolved, information security issues have surfaced that limit its development andnecessitate a solution as security has grown to be the primary concern. This paper is a survey based on recent related work focusing on security issues and countermeasures that must be considered when applying security to cloud-based infrastructure. In addition, a proposed classification of the papers based on if the security issue is overcome and if CIA property (confidentiality, integrity, and availability) is achieved.

The paper is structured as follows. Section 2 contains the subject background. Next, section 3 presents the literature review. Then, section 4 shows the proposed classification.Next, section 5 discusses the work presented. Finally, section 6 presents the conclusion.

2. BACKGROUND

Cloud computing is a recently developed field of computer technology that enables the cost-effective and flexible expansion of computing environments. It begins with visualization, the concept of utilizing cloud computing resources, which encompasses infrastructure, storage, servers, software products, and services. Amazingly, the amount of money in the cloud market is estimated to reach 623.3 billion worth by 2023 [8] which encourages large companies and even startups to adopt and invest in cloud computing technology. This section will discuss the fundamentals to provide a holistic view of cloud computing.

The National Institute of Standards and Technology (NIST) defined cloud computing as" a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [9]. It also reports that the cloud is driven by four deployment models, three service models, and five critical features; the three most common types of cloud services include the following as-a-Service solutions: Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS). Customers of the cloud are virtually offered resources as a service depending on their membership. Hence, these are the four typical deployment models for launching cloud computing which are a particular kind ofcloud environment that can be identified by its shareholdings, scope, and accessibility [10].

1) Public cloud: In this model, access to the cloud is open to everyone. It has become the most widely used model among many consumers due to its quick configuration and reasonable pricing. The customers can decide onthe required security level and bargain for the level of performance and maintenance within the perquisite agreement. Amazon EC2 is the most well-known and frequently used Web Service.
2) Private cloud: It is completely flexible it can be on-site or off-site and is managed and operated by an entire organization or a third party. It is commonly used only for a particular organization
3) Community cloud: Organizations with similar needs can pool their cloud infrastructure resources to meetsecurity and regulatory specifications. As a matter of fact, the general populace and businesses alike both can benefit from the cloud services provided.
4) Hybrid cloud: It is a mixture of two or multiplepublic, community, and private clouds. With this type of deployment models, organizations looking to use the extensive storage capacity and other cloud infrastructure offered by public clouds but who have cloud incompatibility issues with the external cloud vendors can benefit from this constructed environment

Although cloud technology has various benefits over traditional infrastructure, some difficulties must be overcome. As a result, many studies have examined cloud computing security difficulties in the literature to find effective security mechanisms. The top attacks and shortcomings in cloud computing identified by professionals in the field are listed below.

a) Data breaches: Contain harmful when malicious or illegitimate individuals can make copies, transfer, catch, or alter information that is confidential.
b) Service Traffic Hijacking: Honeypot, forgery, and the subjugation of software flaws can all be used by the attacker to gain access to the user's private data and alter their behavior and exchanges. It may send incorrect data and help to gain unauthorized access to websites.
c) Non-secure integrations and Application programming interfaces (API): API is used by vendors and suppliers to deliver various services to customers. As long asthe regulations for authentication and authorization are poorly controlled, the threat grows, and its prevention becomes more difficult.
d) Shared technology threat: In the cloud infrastructure, the multi-tenant design could be the source of numerous perceived attacks.
e) Hypervisor's threats: A hypervisor oversees running numerous hosted virtual machines (VMs) and applications at once on a single host computer while isolating the hosted VMs. Hypervisors are susceptible to attacks even while they are built to be safe and trustworthy as they are targeted due to the higher level of control, they provided to the entire VMs. The virtual machines and the information obtained through them will be completely in the attacker's possession to exploitif they gain control of the hypervisor [11].
f) Single Point of Failure (SPOF):
Environments work overall and control how virtual machines (VMs) benefit from the physical resources. Thus, the breakdown of the hypervisor may have contributed to the entire system crash.
g) Denial of Service (DoS): The intruder floods the cloud server with a large number of forged queries, which uses up more ram, storage capacity, and processing capacity. This type of attack overwhelms systems, stacks, and restricts the service of legitimate customers.

3. LITERATURE REVIEW

A.Behl [12] covered the major issues with cloud computing security along with a detailed explanation of each one. In addition, the paper addressed the shortcomings of the current security approaches being used to safeguard cloud infrastructure and applications. The issues covered are insider threats, outside malicious attacks, multi tenancy issues, and loss of control. The multi-tenant environment that cloud technology creates brings on the majority of problems. Authors suggested that security constraints of cloud computing can be over- come by employing significant approaches such as defense- in-depth and multi-layer security approaches. By employing a defense-in-depth approach, threats are forced to pass through more than one defense layer. Additionally, multi-layer securityapproaches aid in threat containment and provides multiple layers of support if an external/internal layer is broken.

S. Ramgovind *et al.* [13] proposed an overall security perspective, requirements, and concerns, as well as offered strategic guidance for the successful execution of a secure cloud system. The following list contains several security issues highlighted and discussed in the paper that organizations and key decision makers, as a prerequisite, should unpack with cloud computing vendors': privileged access, regulatory compliance, data location, data segregation, recovery, and investigative support, long-term availability, and data availability. Inorder to address efficient management of cloud systems, the paper recommended developing a complete overview of cloud computing guidelines that encompasses

cloud governance, cloud transparency, and the impact of cloud security. As well, it advised adapting and combining data protection and privacypolicies .

V Sureshkumar and B Baranidharan [14] reviewed prevalent challenges to enable more customers to switch to thecloud environment. The paper discussed many essential factors of cloud data protection, like secrecy, authenticity, honesty, availability, and audibility. Additionally, it suggests that a reliable service provider should have the following guarantees for the recovery and gathering of digital evidence of intrusion activities: intrusion detection mechanisms, cryptographic methodology, and electronic forensic software.

Sandesh Achar [15] elaborated the following aspects ofcloud security: identity and access management, data at rest and in transit, egress and ingress traffic control, vulnerability and threat management, and auditing. Meanwhile, it offers best practice recommendations for multi-cloud service providers. Finally, it discusses the challenges of securing a multi-cloud environment and offers solutions by using identity and access management (IAM), data encryption, and access control.

Amara *et al.* [16] summarized the threats and security attacks with their mitigation techniques and categorize themin terms of the cloud services they affect and the network layers where they reside. In addition, it also highlights the issues associated with cloud computing technology that need to be addressed. However, the paper is limited in terms of the implementation of the mitigation techniques presented.

Chou [17] investigated the cloud security issues and threats.In addition, introduced preventative measures for cloud security breaches, including access management by using authentication standards, extensible Access Control Markup Language(XACML)and Security Assertion Markup Language (SAML),and security policy enhancement, and data protection tools (data loss prevention systems, anomalous behavior pattern detection tools, format-preserving, and encryption tools, user behavior profiling), and security techniques implementation such as file allocation table (FAT) system architecture.

Gopala [18] focused on cloud computing security, including cybersecurity attacks, data privacy and integrity, and cloud computing infrastructure stability. However, this paper theoretically indicates that a decentralized cloud is better than a centralized cloud in security techniques. The centralized cloud computing model is more widely used, but it has numerous security risks, concerns regarding privacy and integrity, anda single point of data failure. On the other hand, due to theuse of blockchain networks, the decentralized cloud computingmodel has inherent security, increased data integrity, and privacy through encryption and erasure coding, and no single point of failure due to geo-redundancy.

Kafhali *et al.* [19] summarized related literature and coveredall key concepts of cloud computing while identifying fundamental characteristics, service models, deployment models, and cloud virtualization in data centers. The paper also theoretically discussed major concerns such as cloud computing attacks, privacy challenges, and coping strategies for a securityaudit. In addition, it examined several types of threats and vulnerabilities such as data breaches, data loss, account or servicetraffic hijacking, insecure interfaces and API, denial of service,malicious insiders, insufficient due diligence, shared technology vulnerabilities, loss of governance, availability chain, and insecure or incomplete data deletion. The paper also discussed security issues from a variety of angles, including network security, security for virtual machines and hypervisors, identity and access management, security for data and storage, and governance, legal, and compliance issues. It looked at cloud- based distributed denial-of-service (DDoS) attacks, outlined their defense strategies—from attack detection and preventionto attack mitigation—and explained their benefits and drawbacks. Attack detection methods include count-based filtering, anomaly-based detection, hybrid detection, source and spoof tracing, BotCloud detection, and resource usage. Finally, it summarized researchers' contributions and efforts in the field of cloud computing security taxonomies.

Makkaoui *et al.* [20] introduced the cloud security and privacy model (CSPM) which is a five layer-based model for cloud privacy and security to assist cloud service providersin identifying and categorizing various privacy and security issues, as well as taking the necessary actions to provide secure services and increase customer trust in cloud-based infrastructure services. The layers of the model are physical and environmental security Layer (PESL), cloud Infrastructure

Security Layer (CISL), network security Layer (NSL), data Layer (DL), and Access Control and Privilege Management (ACPML). Using an intrusion detection system or/an intrusion prevention system for each CSPM layer will guaranteethe security and reliability of cloud services. Especially in comparison to other environments, the cloud environment is more vulnerable to threats and attacks which can be Insider attacks, Cloud Malware Injection attacks, cryptographic attacks, account and service hijacking attacks. The paper proposed recommendations for defenses against attacks on cloud security using cryptographic techniques, including symmetric-key, asymmetric-key, or using homomorphic encryption techniques. Finally, the paper suggests using control and management techniques, such as attribute-based encryption (ABE), key policy attribute-based encryption, and cipher text policy attribute-based encryption.

Vinoth S Dr *et al.* [21] addressed diverse cloud uses and investigated the most significant network security and data security risks on cloud systems, using a literature analysis as a guide. In addition, it examines several cloud computing applications in e-commerce and banking, as well as the related security challenges.

Sanjeev Kumar *et al.* [22] proposed a hybrid approach model of symmetric and asymmetric key cryptography algorithms. Implementing the Data Encryption Standard (DES) andRSA, in this case, increases cloud storage security by offering several levels of encryption and decryption at the sender and receiver sides, respectively. The cloud simulator tools and Java were used to implement the suggested model. Compared tothe current system, this model speeds up text file uploading and downloading while increasing data security to the highest possible level.

P. Chinnasamy *et al.* [23] introduced a new hybrid cryptography technique to overcome symmetric and asymmetric limitations and to achieve high data security and confidential- ity. A hybrid algorithm is implemented by combining the best techniques of a symmetric key (Blowfish) and asymmetric key(ECC). The proposed model is designed and implemented in Java. As a result, it offers high security and confidentialityof patient data when the performance of the hybrid system is compared to the current hybrid method.

Mohanaprakash *et al.* [24] examined recent cloud security threats in data security, network security,

environment, and virtualization. This paper also examined and evaluated the roles of various algorithms used in cloud computing for security.In addition, it is a theory paper that uses theoretical proof. It suggested using a hashing algorithm such as message digest 5(MD5) and secure hashing algorithm (SHA) by making a comparison between them in some factors, including (messageblock size, output size, collisions, speed, execution time, and throughput). Although this paper considered a precursor to more in-depth research and analysis of cloud security services, it has no improvement or enhancement.

Abroshan [25] proposed an efficient cryptography solution to improve cloud computing security while having a minimal impact on performance. This solution combines an improved Blowfish algorithm with an elliptic curve-based algorithm.The data will be encrypted using Blowfish, and the key willbe encrypted using the elliptic curve algorithm, which leadsto increased security and performance. As a result, it showsan improvement in cloud computing performance parameters such as throughput, execution time, and memory consumption.

B. Seth *et al.* [26] provided a novel two-tier cloud computing architecture (HBDaSeC) that is effectively resistant to security attacks. The simulation experiments were implemented on the Ubuntu 16.04 platform, a Fog environment, and an Or- acle virtual machine running in Virtual Box while taking into account cloud computing security principles and requirements like confidentiality, integrity, availability, authorization, and nonrepudiation. The framework includes data fragmentation and dual encryption techniques that aim to distribute data securely in a multi-cloud environment. Finally, it is determined that HBDaSec is effective and capable of realizing securecloud computing based on comprehensive security analyses and performance simulations.

4. CLASSIFICATION UNDER CIA MODEL

The CIA triad is a widely accepted model in information security which includes three core components (Confidentiality, Integrity, and Availability). The model provides a comprehensive high-level checklist to help organizations evaluate their incident response plan in case of a cyber breach and assess thesecurity procedures and tools. In addition, it helps to address vulnerabilities and identify areas of strength [27]. This paper has classified the related work based on the achievement ofthe CIA model, illustrated in (Table 1).

Table 1: Paper Achievement of CIA Model

Paper	CIA Triad		
	Confidentiality	*Integrity*	*Availability*
A. Behl [12]		X	X
S. Ramgovind *et al.* [13]	X	X	X
V Sureshkumar *et al.* [14]	X		X
Sandesh Achar [15]	X		
Amara *et al.* [16]	X	X	
Chou [17]	X	X	X
Gopala [18]		X	
Kafhali *et al.* [19]	X	X	X
Makkaoui *et al.* [20]	X	X	X
Vinoth S Dr *et al.* [21]	X		X
Sanjeev Kumar *et al.* [22]	X	X	X
P. Chinnasamy *et al.* [23]	X	X	X
Mohanaprakash *et al.* [24]	X	X	
Abroshan [25]	X	X	
B. Seth *et al.* [26]	X	X	X

5. DISCUSSION

Cloud-based infrastructure has become an essential model for computing power due to its advantages. However, there are major security concerns in the cloud computing environment need to be addressed. Security and privacy consider major drawbacks, limiting the adoption of computational offloading technology by several institutions and organizations. As previously stated, cloud computing faces various security andprivacy threats, the most notable of which are DoS/DDoS attacks. For example, cloud customers may suffer if attackers breach cloud services and resources for a brief period. In addition, cloud systems face extreme latency and high costs in communication and data storage. These issues exist due to the Cloud's centralized nature and geographical distance from end devices that generate data. Many researchers studied security concerns and protective measures to reinforce the security barrier, summarized in (Table 2).

A. Behl [12] and S. Ramgovind *et al.* [13] have covered the major cloud computing security issues and provided a detailed description of each. In addition, the studies also discussed the flaws in the security strategies currently employed to protect cloud infrastructure. However, the papers didn't highlight the challenges from the customer point of view and discuss cloud computing issues in a theoretical way without using tables or measure factors. V Sureshkumar and B Baranidharan

[14] discussed the most essential challenge to enable more customers to switch to the cloud environment. In addition, Sandesh Achar [15] offered the best practice recommendations for multi-cloud service providers. Amara *et al.* [16], provided a comparison including security attack, security levels, and mitigation techniques, and not provide numerical analysis, Kafhali *et al.* [19] presented a include detection mechanism with Strong points and limitations. Chou [17], Gopala [18], and Makkaoui *et al.* [20] summarized threats and securityissues affecting cloud infrastructure. However, did not provideany numeric analysis. Virtual environments have received much industry attention as the answer to current security issues. However, virtualization adds more software to the net- work system, which, if improperly designed and implemented,could have a negative impact on security. Vinoth S Dr *et al.*

[21] investigated the security affect the virtualization added layer only in theoretical manner. Sanjeev Kumar *et al.* [22],

P. Chinnasamy *et al.* [23], Mohanaprakash *et al.* [24] and Abroshan [25] proposed a using an algorithm to improve cloud computing security. However, [23] and [24] focused on measure algorithm performance. Another way of improving security defense was conducting by B. Seth *et al.* [26] in simulation environment, to improve the blowfish algorithm.

It is concluded from the discussions presented in this work that the security and privacy issues raised by the heterogeneityof this cloud computing model pose a significant challenge. Data transfer from and to computing systems exposes many security and privacy flaws, though some are easily detectable and resolved. In addition, the multi-tenant environment that cloud technology creates brings on most problems.

6. CONCLUSION

Subsequent to its many advantages, such as on-demand infrastructure, increased profitability, communicating and configuring network infrastructure, and enhanced service agility. Cloud computing is growingly seen as a perfect solution and a broadly used future technology for distributed cloud applications. However, the principle of security and privacy has grown to be a significant obstacle to adapting cloud services since the development of this technology. As a result, the diversity of the new industries using cloud computingwill increase the cloud paradigm's threats and security risks. This paper provides an overview of recent, pertinent research focusing on numerous perspectives of security challenges and safety precautions from various angles. When implementing security on cloud computing infrastructure, these factors need to be considered. Additionally, the paper suggests labeling the literature review in accordance with the CIA comprehensive model, which serves as the foundation for improving security protection. Future work will concentrate on running tests on virtual machines in cloud environments using various defense algorithms, studying the practicability of current techniques, and trying to enhance and accommodate them in the cloud environment.

7. REFERENCES

[1] Rabi Prasad Padhy, Manas Ranjan Patra, and Suresh Chandra Satapathy.Cloud computing: security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, 1(2):136–146, 2011.

[2] Hayes Brian, Thomas Brunschwiler, Heinz Dill, Hanspeter Christ, Babak Falsafi, Markus Fischer, Stella Gatziu Grivas, Claudio Giovanoli,Roger Eric Gisi, Reto Gutmann, et al. Cloud computing. *Communica- tions of the ACM*, 51(7):9–11, 2008.

[3] Bader Alouffi, Muhammad Hasnain, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz. A systematic literature review on cloud computing security: Threats and mitigation strategies. *IEEE Access*, 9:57792–57807, 2021.

[4] Derrick Sampson and MD Minhaz Chowdhury. The growing security concerns of cloud computing. pages 050–055, 2021. doi:10.1109/EIT51626.2021.9491902.

[5] Aleksandr Ometov, Oliver Liombe Molua, Mikhail Komarov, and Jari Nurmi. A survey of security in cloud, edge, and fog computing. *Sensors*,22(3):927, 2022.

[6] Waqas Ahmad, Aamir Rasool, Abdul Rehman Javed, Thar Baker, and Zunera Jalil. Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, 11(1):16, 2021.

[7] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu. Data security and privacy in cloud computing. *International Journal of Distributed Sensor Networks*, 10(7):190903, 2014.

[8] Yu-Hsin Hung. Investigating how the cloud computing transforms the development of industries. *IEEE Access*, 7:181505–181517, 2019.

[9] Peter Mell, Tim Grance, et al. The nist definition of cloud computing. 2011.

[10] Mohsen Attaran and Jeremy Woods. Cloud computing technology: improving small business performance using the internet. *Journal of Small Business & Entrepreneurship*, 31(6):495–519, 2019.

[11] Su Su Win and Mie Mie Su Thwin. Handling the hypervisor hijacking attacks on virtual cloud environment. In *Advances in Biometrics*, pages 25–50. Springer, 2019.

[12] Akhil Behl. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. pages 217– 222, 2011.

[13] Sumant Ramgovind, Mariki M Eloff, and Elme Smith. The managementof security in cloud computing. pages 1–7, 2010.

[14] V Sureshkumar and B Baranidharan. A study of the cloud se- curity attacks and threats. *Journal of Physics: Conference Series*, 1964(4):042061, jul 2021.

[15] Sandesh Achar. Cloud computing security for multi-cloud service providers: Controls and techniques in our modern threat landscape. 09 2022. doi:10.5281/zenodo.7084251.

[16] Amara Naseer, Huang Zhiqui, and Awais Ali. Cloud computing security threats and attacks with their mitigation techniques. pages 244–251, 10 2017. doi:10.1109/CyberC.2017.37.

[17] Te-Shun Chou. Security threats on cloud computing vulnerabilities. *International Journal of Computer Science & Information Technology*, 5(3):79, 2013.

[18] GS Sriram. Resolving security and data concerns in cloud computing by utilizing a decentralized cloud computing option. *International Research Journal of Modernization in Engineering Technology and Science*, 4(1):1269–1273, 2022.

[19] Said El Kafhali, Iman El Mir, and Mohamed Hanini. Security threats, defense mechanisms, challenges, and future directions in cloud comput- ing. *Archives of Computational Methods in Engineering*, 29(1):223–246, 2022.

[20] Khalid El Makkaoui, Abdellah Ezzati, Abderrahim Beni-Hssane, and Cina Motamed. Cloud security and privacy model for providing secure cloud services. pages 81–86, 2016.

[21] Vinoth Dr, Hari Vemula, Dr Haralayya, Pradeep Mamgain, Mo- hammed Faez Hasan, and Mohd Naved. Application of cloud computing in banking and e-commerce and related security threats. *Materials Today: Proceedings*, 51, 12 2021. doi:10.1016/j.matpr.2021.11.121.

[22] Sanjeev Kumar, Garima Karnani, Madhu Gaur, and Anju Mishra. Cloud security using hybrid cryptography algorithms. pages 599–604, 04 2021. doi:10.1109/ICIEM51511.2021.9445377.

[23] Chinnasamy Ponnusamy, S Padmavathi, and R Swathy. *Efficient Data Security Using Hybrid Cryptography on Cloud Computing*, pages 537– 547. 09 2020.

[24] TA Mohanaprakash and DV Nirmalrani. Exploration of various view- points in cloud computing security threats. *Journal of Theoretical and Applied Information Technology*, 99(5):1172–1183, 2021.

[25] Hossein Abroshan. A hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography al- gorithms. *International Journal of Advanced Computer Science and Applications*, 12(6), 2021.

[26] Bijeta Seth, Surjeet Dalal, Vivek Jaglan, Dac-Nhuong Le, Senthilkumar Mohan, and Gautam Srivastava. Integrating encryption techniques for secure data storage in the cloud. *Transactions on Emerging Telecom- munications Technologies*, 33(4):e4108, 2022.

[27] fortinet.com. Cia triad. 2010.

Table 2: Summary of Existing Papers

Reference	Year	Target	Security Issues	Countermeasures
Cloud computing security for multi-cloud services providers: Controls and techniques in our modern threat	2022	Cloud security include (identity and access management, data at rest and in transit, egress and ingress traffic control)	- Data loss or theft. - impact on protect data at rest	- using identity and access management (IAM). -Data encryption (protect data at rest) - Access control
Resolve Security and Data Concerns in cloud computing-ing by utilizing a decentralized cloud computing option	2022	Cloud computing security include cybersecurity attacks, data privacy and integrity, and cloud computing infrastructure stability vulnerable target (e.g. schools, hospitals, hospices)	-Phishing -Ransomware -Trojan -Botnet -Distributed Denial of Service -Adware -Crypto mining	- Data encryption methods known as Ried Solomon erasure coding - Geo-redundancy for data integrity
Cloud Security using Hybrid Cryptography Algorithms	2021	Increases cloud storage security using hybrid algorithms	-Data Integrity -Data Availability -Data Confidentiality -Denial Of Service -Data Location -Data Breach -Data Loss	-Digital Signatures -Data Encryption -Intrusion Detection System (IDS)
Efficient data Security using hybrid cryptography on cloud computing	2021	Increases security and confidentiality of patient data in cloud storage	Data confidentiality	A hybrid cryptosystem
Security threats, defense mechanisms, challenges, and Future directions in cloud computing	2021	- Provide a full cloud computing fundamentals review -Discuss the major security issues and defence techniques. -Summarizing and compare the literature	Data breaches, data loss, account or service traffic hijacking, insecure interfaces and API, denial of service, malicious insiders, insufficient due diligence, shared technology vulnerabilities, loss of governance, availability chain, and insecure or incomplete data deletion.	For DDoS attack: - Defence deployment: Source-End Deployment, access Point deployment, Intermediate-network deployment, and distributed defense. -Defence detection: source and spoof trace, or based on signature/patten, hybrid, anomaly mechanisms, count based filtering, resource usage, and BotCloud.
Application of cloud computing in banking and e-commerce and related security threats	2021	Examines several cloud computing applications in e-commerce and banking as well as the related security challenges	-Multi tenancy - Semantic gap - Trust - Loss of control	Proper planning and understanding of emerging risks, threats, vulnerabilities and potential solutions are necessary

Explosion of various viewpoint in cloud computing security threats	2021	Data security, Network security, Environmental and Virtualization issues	-Malicious attacks Data -Data Breach -Data loss -Impact on data integrity - Data Seizure -Storage compatibility issue Network -Denial of service -Man in the middle attack -Packet sniffing Environment -Inside user (hacker) - Misusedof cloud assists Virtualization -Impact on(VM cache, migration , andcloning)	Use hashing algorithms: - Message digest 5(MD5) - Secure hashing algorithm (SHA) - Use cryptographic methodology
A Hybrid encryption solution to improve cloud computing security using symmetric and asymmetric cryptography algorithms	2021	Improve Cloud computing security with minimal impacton performance	-Impact on data integrity	Improved Blowfish algorithm with an elliptic curve-based algorithm
A Study of the cloud security attacks and threats	2020	Cloud-related protection challenges and risks	Secrecy, authenticity, honesty, availability, and auditability	Intrusion detection mechanisms, cryptographic methodology electronic forensic software
Integrating encryption techniques for secure data storage in the cloud	2020	Increases security by providing a novel two-tier cloud computing architecture (HB-DaSeC) that indicates security storage, verification, and auditing.	-Information leaks - Confidentiality and privacy issues	- HBDaSeC: applied Data fragmentation, dual encryption techniques
Cloud computing security threats and attacks with their mitigation techniques	2017	Categorize security attacks in terms of the cloud services they affect and the network layers where they reside	- CIaaS, PaaS, SaaS -Data breach -Data loss -Account or service hijacking -Insecure interfaces and APIs -Malicious insiders -Insufficient due diligence -Unknown risk profile Identity theft -Changes to business odel -Lock-IN - IaaS, PaaS,abusive use of cloud services - IaaS Shared technology issues	Backup -Encryption - Protect data in transit - Strong key generation, storage and management -Strong API - Understanding of security polices - Strong Authentications - Using strong authorization and authentication. - Properly auditing network traffic. - credit card fraud monitoring - Using better authentication and access control mechanisms. • -Inspect vulnerabilities and configuration. - Monitor environment for unauthorized changes/activities - Use of SLA for patch-

				ing and vulnerability remediation.
Cloud security and privacy model for providing secure cloud services	2016	Provide cloud security and privacy model (CSPM) to in- crease security and customer trust also help orgnization to identify the security issues	-Insider attacks -Cloud malware injection attacks -Cryptographic attacks -Account and service hijacking attacks.	Deploy intrusion detection system or/an intrusion prevention system for each CSPM layer. -Cryptographic techniques, including symmetric-key, asymmetric-key - Homomorphic encryption techniques - Control and manage- ment techniques, such as attribute-based en- cryption (ABE), key policy attribute based encryption, and cipher text policy attribute- based encryption
Security threats on cloud computing vulnerabilities	2013	Cloud security risks and threats based on the natureof the cloud service models	- Distributed denial of service (DDoS) attacks - Data loss - Malicious programs (virus and Trojan, and brute force attack) - Malicious insider -Online cyber theft - Malware injection attack -Wrapping attack	- Security policy enhancement - Access management by using authentication standards security (SAML) and (XACML)
Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation	2011	Discuss major cloud comput- ing security issues and defense mechanisms	Insider threats Outside malicious attacks Multitenancy issues Loss of control.	Defense-in-depth approach Multi-layer security approach
The Management Of Security In Cloud Computing	2010	Deliver strategic direction for the implementation of a se- cure cloud system. - Discuss security perspectives require- ment, and issues	-privileged access -Regulatory compliance -Data location -Data segregation -Data recovery, -Investigative support -Long-term availability -Data availability	-Modifying and combining data security and pri- vacy regulations -Constructing a holistic view of cloud computing rules