Data Security in Cloud Computing

Faya Safar[1,*], Raddad Al King[2]

[1]Master of Web Science (MWS) Program, Syrian Virtual University
Syria
[2]Master of Web Science (MWS) Program, Syrian Virtual University
Syria
Emails: faya_243029@svuonline.org; t_ralking@svuonline.org

Abstract

In recent years, cloud computing was and still is one of the most pragmatic and popular topics of research because of its advantages. Cloud storage allows organizations to store information of service providers at remote sites. However, cloud computing has encountered challenges, notably security issues and scheduling problems, primarily stemming from concerns related to data confidentiality and efficient resource allocation among users. These challenges are inherent to cloud computing, where data and computational resources are shared among multiple users and often hosted on remote servers operated by third-party providers. Hence, our objective is to identify and analyze the challenges associated with cloud computing, with a particular focus on data security. In addition to conduct scientific review and compare multiple recent research studies. The focus will be on identify challenges and advantages of cloud computing and data security when going through various data security measures that are currently employed in cloud computing. Eventually we will come up with valid recommendations based on the findings.

Keywords: Cloud computing; Data security; Data leakage; Confidentiality; Privacy; Cryptography; Data integrity

1. Introduction

Cloud computing empowers numerous paths for Web-based service to meet diverse needs. However, data security and privacy have become critical issue that restricts many cloud applications. One of the major concerns in security and privacy is caused by the fact that cloud operators have chances to reach sensitive data. This concern dramatically increases users' anxiety and reduces the adaptability of cloud computing in many fields, such as the financial industry and governmental agencies where security and confidentiality are necessary [1]

This paper focuses on this issue and proposes an intelligent cryptography approach, which provides a higher level of data privacy and security in cloud computing environments. By using strong encryption, data fragmentation, intelligent access control, and homomorphic encryption, it ensures that cloud service operators cannot directly access sensitive data, reducing the risk of unauthorized data exposure and data breaches. This approach enhances user confidence in utilizing cloud services while maintaining control and confidentiality over their data. As per the definition provided by the National Institute for Standards and Technology (NIST) (Badger et al., 2011), "cloud computing is a model for enabling convenient, 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" [2]. Cloud computing is integrating day by day and as it has been implemented in most of the companies the security requirement is increasing. Cloud computing shares characteristics of other computing technologies hence present unique benefits over other technologies but at the same time new security issues arises. Cloud Security means a crucial aspect of cloud computing, encompassing a set of control-based technologies, practices, and policies designed to safeguard data, applications, and infrastructure hosted in cloud environments. Its primary focus is to maintain the confidentiality, integrity, and availability of information stored and processed in the cloud. Which design to maintain the security and protect the information, data security and all the applications associated with it. The security process also

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

includes data backup and business continuity so that the data can be retrieved even if a disaster takes place. Cloud computing process addresses the security controls which provide by the cloud provider to maintain the data and its privacy. We will discuss some of the gaps and challenges related to the data security in cloud computing in this literature review.

This paper is structured as follows: an introduction is given in section 1, background on data security in cloud environment is elaborated in section 2, literature review is presented in section 3, challenges are discussed in section 4, recommendations are provided in section 5, conclusions are offered in section 6.

2. Data Security in Cloud Environment

A cloud environment refers to a virtualized and scalable infrastructure that allows users and organizations to access and utilize computing resources, applications, and services over the internet. Cloud computing has revolutionized the way businesses and individuals' access and manage IT resources, providing on-demand access to a wide range of services without the need for physical hardware or on-premises infrastructure.

Cloud environment Types:

- **Public cloud:** The cloud infrastructure is available to the public on a commercial basis by a cloud service provider. This enables a consumer to develop and deploy a service in the cloud with extraordinarily little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.
- **Private cloud:** The cloud infrastructure has been deployed and is maintained and operated for a specific organization. The operation may be in-house or with a third party on the premises.
- **Community Cloud:** The cloud infrastructure is shared among a number of organizations with similar interests and requirements. This may help limit the capital expenditure costs for its establishment as the costs are shared among the organizations. The operation may be in-house or with a third party on the premises.
- **Hybrid Cloud:** The cloud infrastructure consists of a number of clouds of interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that support the requirement to retain some data [3]

Cloud service can be grouped into four categories [5]:

- **Software as a service (SaaS):** SaaS refers to the software available on the internet. It includes YouTube, Facebook, and google applications.
- **Platform as a service (PaaS):** an operating system, hardware, and network are provided, and the customer installs or develops its own software applications. It includes Amazon DB/S3[5], Google AppEngine.
- **Infrastructure as a service (IaaS):** provides just the hardware and network; the customer installs or develops its own operating systems, software, and applications. Examples of IaaS providers include Amazon EC2, GoGrid, FlexiScale [4].
- **Container as a service (CaaS):** CaaS is based on container virtualization, CaaS has emerged as a cloud model to resolve application development issues in the PaaS environment. The CaaS cloud model aims to free the application by making them independent of PaaS environment specifications. Amazon Elastic Container Service and Google container engine are examples of CaaS model [19]

The cloud environment revolves around three functional units [5]:

- **Cloud service provider**: It is an entity, which manages Cloud Storage Server (CSS), has significant storage space to preserve the clients' data and high computation power.
- **Client/owner:** It is an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation; it can either be individual consumer or organizations.
- **User:** It is a unit, which is registered with the owner and uses the data of owner stored on the cloud. The user can be an owner itself as well.

Let us dive deeper in data security in cloud environment:

1) Integrity of Data

Data integrity may be easily preserved by employing traditional cryptographic methods such as message authentication codes (MAC). It is a fixed size block of data based on file F using any secret key. The data owners maintain small amount of MAC before outsourcing the data and whenever data is needed, MAC is verified with the previously computed MAC to verify the correctness of the received data from cloud. In cloud environments traditional methods are not implemented since the data is dynamic and there is huge cloud storage [6].

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

So, it becomes quite impractical that for checking whether the data is stored securely we retrieve all the data stored on server. Integrity threats include data deletion, and data manipulation. The computation details are not transparent to cloud customers so the CSP behave dishonestly and may alter the data.

2) Data Confidentiality

Data confidentiality is the process of protecting data from illegal access and disclosure from the outsourced server and unauthorized users. This is done by encrypting the data so that only the authorized users can decrypt it [7]

the A user can access the services provided by SaaS model through web browser over the internet. So, to protect the data during transmission HTTPS is implemented. If user uploads data to the CSP, security must be there so that only authorize users access the data, the same requirement with PaaS. While in IaaS, multiple users' data reside on the same location so in IaaS confidentiality arises in a way to include isolation over the different user's data.

3) Data Availability and Management

Data availability is a measure of how often your data is available to be used, whether by your own organization, or by one of your partners. Availability is affected if the server or service organization is penetrated or spoofed. In cloud characteristic broad network access DNS is one of the main attacks on availability [8]. So, for better service offering over the internet user must have reliable DNS. For long term data storage data availability is of much importance due to possibility of data loss.

4) **Data Authenticity**

Authentication is the process of determining the identity of a client. The details of authentication vary depending on how you are accessing Cloud Environment. Cryptographers invent a vast number of primitives for preserving the privacy of users' data.

Among these primitives, anonymous password authentication (APA) has been used for ensuring the private authentication process. Zero knowledge authentications in cloud environment enjoy the benefits of password authentications while offering user privacy preservation.

5) Data Storage & Maintenance

Cloud Storage is a mode of computer data storage in which digital data is stored on servers in off- site locations. The servers are maintained by a third-party provider who is responsible for hosting, managing, and securing data stored on its infrastructure. In cloud environment data is dynamically stored over the cloud servers, so the user is unaware where its data is going to be stored. Due to privacy concerns some EU countries forbid the storage of sensitive data outside the country boundaries. the data locality is considered a critical issue [9]. Another question arises if some investigation occurs, under whose jurisdiction the investigation occurs. The issue can be solved by creating a secure SaaS model which provides reliability of the location the data. The data in cloud may become unavailable or effected due to environmental disaster, and server failure. For this recovery of important documents must be maintained either by user on its local disk or backup services are provided by many cloud vendors like Amazon S3.

6) Data Breaches, Leaks and Hacks

Attack - An attack is a purposeful attempt to cause damage or loss through technical or social means. Attacks do not necessarily lead to data breaches. For example, denial of service attacks disrupts normal operations and access but do not expose information.

Breach - A successful attack was able to secure sensitive information from the cloud, also, a breach is an incident where information is stolen or taken from a cloud system without the knowledge or authorization of the system's owner.

Hack - An attack that exploits technical vulnerabilities to secure access that is otherwise unauthorized. A Hack can lead to a breach but may also be used for ransomware, establishing botnets, or misusing computing resources.

Leak - A leak does not require an external actor but is caused by some action or inaction of the party who owns the data [10]

Due to Multi tenancy environment in cloud breaching the data will become a potential threat. Data breach effects two security properties of data confidentiality, integrity & authenticity. Confidentiality refers that only authorized

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

parties or systems can access the data and integrity refers that data is not deleted, manipulated, or fabricated by some third party who is not authenticated to perform such task. Data breach may occur internally by a data manager who has direct access to the data or from outside by malicious hacker. However, confidentiality and integrity issues are addressed by strong cryptographic mechanism like DES and AES with common PKI infrastructure. Data and key management can become an issue for data owner which can be addressed by combining techniques of attribute-based encryption, proxy re-encryption and lazy re-encryption.

7) Data Separation& Filtration

Data separation and other multi-tenant challenges are concerns in the public cloud. Separating cloud compute and storage gives organizations flexibility to accommodate consistent data requirements and meet variable or unforeseen needs.

Multi tenancy is an important characteristic of cloud computing. In multitenant, multiples users and organizations reside at the same location. Therefore, it becomes possible for the malicious users to gain access to the other users' data. So, keeping data separate and maintain isolation among the users is an important issue [11]. These issues can be solved either by creating a robust virtualization platform or by implementing Trusted Platform Module embedded on the motherboard.

3. Literature Review

Avinash Ganne in his paper [12] presents the urge to migrate to the cloud instead of traditional storing, explaining that this has made security of data problematic. This paper offers a solution to this problem by using container clustering technologies (i.e., Kubernetes, Docker Swarm). This research paper presented three main aspects of data security to consider. Data availability, integrity, and secrecy, where data availability was highlighted as one of the most troublesome problems users encounter. In the paper the following problems and challenges were identified: Data Storage, Restoration, Long-Term Validity, Data Separation, and Legal Accessibility for Entitled Users Compliance. The paper details two solutions for securing and containing data, through Docker or Kubernetes, while explaining that Kubernetes outperforms Docker in terms of both capacity and performance Due to Kubernetes' capabilities and more effective distribution and containers characteristics. the study was brief and did not highlight some other methods available, moreover the paper did not go in depth to mention the disadvantages of Docker and Kubernetes:

Kubernetes

More complex migrations: When transitioning to Kubernetes from another platform or setting up a more intricate deployment, the migration process can be challenging and require careful planning. This complexity arises due to the various components and configurations involved in a Kubernetes cluster.

Complex installation and configuration process: Setting up a Kubernetes cluster involves multiple steps and configurations, which can be overwhelming for users who are new to the technology or have limited experience with container orchestration systems.

Incompatible with existing Docker tools: Kubernetes and Docker are not seamlessly compatible, which means that some of the tools and practices used with Docker may not directly translate to Kubernetes. This can lead to confusion and the need to learn new methodologies.

Implementing a manual cluster is complicated: While there are automated tools to help with Kubernetes cluster deployment, setting up a cluster manually can be a daunting task, especially for those without a deep understanding of Kubernetes internals.

Docker

It does not provide a storage option: Docker itself does not offer a comprehensive built-in storage solution for containers. Users need to rely on external storage mechanisms, which can add complexity and overhead to the container deployment process.

Bad follow-up: Docker has faced criticism in the past for issues related to customer support, bug fixes, and timely updates. This lack of responsiveness to user needs can be frustrating for those relying heavily on Docker for their containerization requirements.

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

No automatic reprogramming of inactive nodes: Docker does not have a built-in feature to automatically reprogram or reassign tasks from inactive or failed nodes to active ones. This means that in scenarios where nodes become inactive, manual intervention might be necessary to redistribute the tasks.

In summary, Kubernetes can present challenges with complex migrations, installation, and configuration, while also requiring additional effort to integrate existing Docker tools. On the other hand, Docker lacks a native storage option and has been criticized for its customer support and the absence of automatic reprogramming for inactive nodes.

Rishabh Gupta et al [13] envisages a discussion of cloud environment, its utilities, challenges, and emerging research trends confined to secure processing and sharing of data. The paper identifies cloud security issues such as man-in-the-middle attacks, data leaks, etc. in addition, to obstacles while uploading data on the cloud, like high bandwidth requirement, high latency, and a large volume of data. These are the biggest obstacles limiting cloud development. This paper offers encryption schemes (Privacy-Preserving Based on Cryptography Mechanism, and Privacy-Preserving Based on Perturbation Mechanism) to solve the identified challenges providing pros and cons of each approach. The paper presented research gaps such as less protection, and privacy of the outsourced data, the efficiency of methods to protect privacy must be increased, multiple user-based protection techniques are required, computational and communication costs during the data transfer must be reduce, minimization of the threats of data leakage during transmission. In addition, the paper contained suggestions to enhance cloud facilities such as: more quality of service (QoS), better resource utilization, improves confidence in cryptography services, low the cost of computation of the process, less service level agreement (SLA) violation, better use of the cloud for securely sharing of data among the organizations, better efficiency, saving the cost, access the file universally, increase the security. The paper may have a limited scope, focusing only on certain aspects of data security and privacy in cloud computing while overlooking other relevant factors. This could leave the reader with an incomplete understanding of the broader landscape of the subject. Nevertheless, the paper delves into the fundamental concepts of data security and privacy in the context of cloud computing. It discusses encryption techniques, access controls, authentication mechanisms, and other security measures that are crucial for safeguarding data in the cloud environment. Furthermore, the suggestions were efficient to address some of the issues identified.

Sajid Habib Gill et al [14] this paper presents a detailed analysis of privacy and security challenges in the cloud. Demonstrating the importance of security challenges in a case study in the context of smart campus security, which will encourage researchers to examine security issues in cloud computing in the future. This paper identifies security and privacy concerns facing the cloud and explores their nature and possible solutions, such as standardization of APIs, public key infrastructure, and data distribution, to reduce the risks. Access control, authentication, and authorization for the storage of data are essential to enhance security levels in cloud computing. The article proposed Blockchain technology to protect data, according to the study it can enhance security and ensure anonymity in a cloud computing environment, Blockchain overcomes the key challenge of cost in cloud computing, enabling its decentralization to eliminate the risk of data violations. Moreover, the paper presented Challenges and Privacy Aspects of Cloud Computing and Possible Solutions. it was emphasized to deploy the efficient security and privacy measures to ensure data integrity, privacy, and reliability. However, cloud service providers are not providing enough security to satisfy users.
Additionally, blockchain improves security problems in cloud computing by improving cloud security through decentralization, immutable data, enhanced data privacy, and better authentication and access control.

It mitigates DDoS attacks, ensures transparent transactions, enables secure automation with smart contracts, and maintains data integrity and provenance. Considerations for scalability and regulatory aspects are essential for successful implementation. The article highlighted cloud security concerns/challenges and their behavior/nature with suggested solutions that will benefit other researchers. This paper was incredibly detailed and professional as it had survey results, and case study. The research demonstrated the need for heightened security measures and the potential of emerging technologies like blockchain to bolster cloud security. The proposed solutions serve as a steppingstone for future investigations, guiding the development of more secure and reliable cloud computing environments. Nevertheless, Nevertheless, Blockchain shortcomings includes scalability and energy consumption issues, data storage challenges, governance complexities, immutability limitations, security risks, and regulatory uncertainty. Interoperability between different blockchain networks is also a concern.

Bayan A. Alenizi et al [15] presented a framework to address the security and privacy concerns in cloud computing. Proposed framework uses hybrid authentication mechanism for the security of cloud computing. The study provides a deeper insight to the researchers and practitioners about cloud computing and underlying security and privacy concerns along with countermeasures and a novel solution. The paper provided an overview of cloud

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

security and privacy attacks, with briefly elaborate on some key attacks (malware attack, accounts hijack, Man in the middle attacks, etc.) and challenges faced in cloud computing for better understand ability of the area under study. Discussion shows that cryptographic solutions.
provide a common way to secure cloud computing environment. Cloud cryptography uses encryption methods to protect data that is used or stored in the cloud. It helps users to access shared cloud resources easily and safely, as all hosted by cloud providers is secured by encryption. In addition, to provide existing cryptographic solutions and then based on these solutions the paper provided a framework that will address the security and privacy concerns of cloud computing such as: 1) symmetric-key encryption, which is an easy and fast method of encrypting data in cloud computing. 2) Asymmetric-key encryption is more secure and effective encryption technique, but it is slow and normally requires huge ciphers with complexed algorithms. 3) Secure Hash Algorithms SHA is widely used technique for securing and authenticating data. In this method, values are created using hash functions. 4) Advanced Cryptographic Solutions: Some of the common encryption solutions are Homomorphic encryption, multi-party secure computation, and verifiable computation. The paper was detailed and well established, the recommendations were logical, detailed, and addressed the identified challenges but, the proposed framework demonstrates a high level of security as it effectively counters dictionary attacks, brute-force attacks, keyloggers, and replay attacks by incorporating CAPTCHA and two-factor authentication (TFA) mechanisms. The paper was detailed and well established, the recommendations were logical, detailed, and addressed the identified challenges but in the paper, the proposed framework demonstrates a high level of security as it effectively counters dictionary attacks, brute-force attacks, keyloggers, and replay attacks by incorporating CAPTCHA and two-factor authentication (TFA) mechanisms. Utilizing two servers addresses concerns related to security and server speed, resulting in improved overall server performance, but it may introduce complexity and usability challenges for users. Utilizing two servers improves performance but increases the risk of single points of failure, requiring careful monitoring and user education.

Table 1: Summery of findings

This table presents the key results and conclusions derived from the reviewed papers. It outlines the papers' findings on data security issues, proposed solutions, the composition of the paper structure, and whether the authors included statistics, charts, and examples:

Study	Comparison of studies
CLOUD DATA SECURITY METHODS: KUBERNETES VS DOCKER SWARM	the paper identified the protection of data as a problem (Data Storage, Restoration, Long-Term Validity, Data Separation, and Legal Accessibility for Entitled Users Compliance), as well as cyber-attacks. The paper proposed two tarnishes to solve this issue to safeguard the private data. Data stored in the cloud is protected using container technology (Kubernetes and Docker). Well Structured paper. No statistics. Examples were provided.
DATASECURITY & PRIVACY IN CLOUD COMPUTING: CONCEPTS AND EMERGING TRENDS	Massive usage and sharing of data among users open door to security loopholes was identified as a problem in this paper. Proposed solutions were reducing data leakage by using advanced encryption techniques. Well Structured paper. Statistics and expletory pictures were provided. Examples were provided.
SECURTY AND PRIVACY ASPECTS OF COULD COMPUTING: A SMART CAMPUS CASE STUDY	In this paper, the authors have identified the issue of data violations, specifically concerning the lack of secure and reliable services provided by cloud service providers to end-users. The paper introduces a groundbreaking technology that offers persuasive data integrity properties, which effectively address security concerns. Blockchain overcomes the key challenge of cost in cloud computing, enabling its decentralization to eliminate the risk of data violations. Well Structured paper. Statistics and surveys were indicated.

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

	Figures and charts were provided. Examples were provided.
SECURITY AND PRIVACY ISSUES IN CLOUD COMPUTING	A critical concern is security and privacy, extensively researched but persistently problematic. Assuring security is crucial for promoting cloud adoption and deployment. To offer a comprehensive perspective, the authors presented a detailed survey of prevalent cloud security and privacy issues, accompanied by mitigation strategies. Additionally, providing a framework for addressing security and privacy concerns in this context. Well Structured paper. Statistics and surveys were indicated. Figures and charts were provided.

4. Challenges

There are various difficulties related to security of data in cloud computing. When a user uses the internet-cloud platform, data protection and privacy need to be strongly.

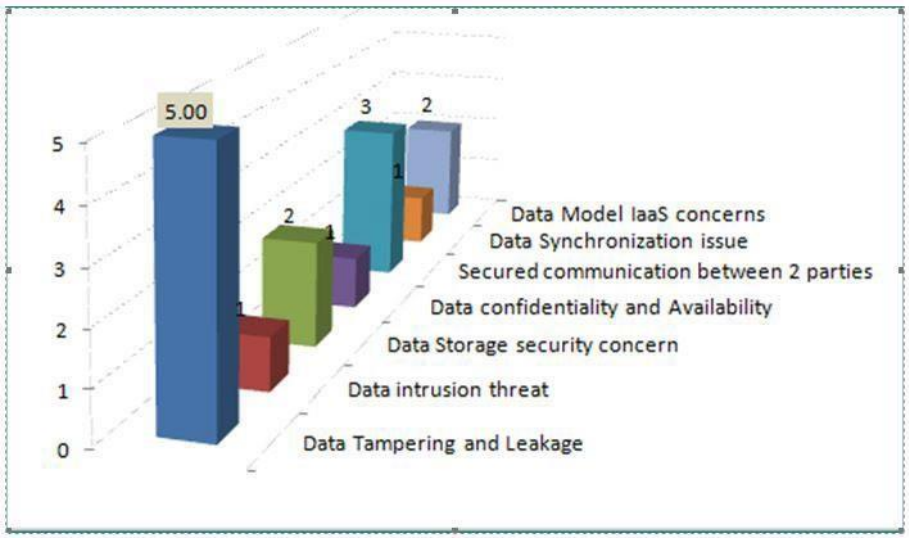

Figure 1: Identified cloud computing security threats [16]

Emphasized. Information loss or data exposure can seriously affect a company's reputation and confidence. Prevention of data tampering and leakage is regarded to be the most critical problem with 88% of major challenges. Likewise, data remoteness and privacy impact security problems by 92%. Cloud computing most critical security concerns are data protection, reliability, honesty, availability, authentication and confidentiality, lack of resources and skills etc. data lie cycle has six phases build inventory, Use, Transfer, Archive and Kill [17]

The table comprehensively examines various challenges related to data security in cloud computing, including vendor lock-in, availability, data security, and integrity. Each challenge is thoroughly described, providing a comprehensive understanding of their implications. Additionally, proposed models to tackle these challenges are presented, offering potential solutions to enhance data security in cloud computing environments.

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

Table 2: Challenges of cloud computing

Challenge	Model	Description	Significance	Limitation / F. W
Data availability	service provider agreement framework	SLA parameters and flexible negotiation methods	Manage the appropriate emergency response and plan. and unplanned	Needed complex computation. Should provide high protection mechanisms.
Data Storage	Data storage framework PaaS	Combine and extend multiple databases and.	user centric trust model to help users to manage. the storage	Need less time.
Integrity	MAC algorithms	The owner of data must Import the outsourced data. and then measure	Unplanned and expected changes will be noted	Run on only client side. Should need to technique to detect attackers.
Security	Hidden Markov Model (HMM)	detect any type of security breach	identify security in cloud computing network	Sometimes employee cannot Use it. It Should provide flexible modal.
Resource scheduling	skewness matrix	the capacities of servers are well utilized	Equally shared serviced between cloud users and provider of infrastructure	Just consider user's priorities. Should need best measurement level.
To protect the data	cryptographic	Security of data stored in database	Backup data needed, tenacity storage unit	Transmission of very large documents are prohibitive.
authentication	two factor and multifactor authentication	migrating your system to the cloud	technologies come with vulnerabilities like Public Key Infrastructure solution	Security proofing technique is on process.
Privacy and Security	The community understanding of privacy and protection	Massage data at the edge of the network	Personal data may be extracted before processing	limited number of people. Opportunity for human error should be reduced.

5. Recommendations

We can summarize the security requirements that should be considered when delegating or exporting data to the cloud as follows:

1) Confidentiality: Data must be encrypted before it is outsourced, to protect it from malicious internal or external attacks.

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

2) Integrity: Protect the data from the unauthorized insert, update, or delete. The data owner and authorized users should be able to recognize if the data is corrupted or incomplete and receive the most recent updated version of the data, which guarantees accuracy and consistency of data.
3) Availability: The data in the cloud servers should be accessible to its users. Major threats to availability are denial of service (DOS) attacks, natural disasters, and equipment failures at the service provider's end.
4) Access control: The data should be accessed only by authorized users.
5) Firewall: The CSP must be safeguarded against false accusations that may be claimed by dishonest owners or users.

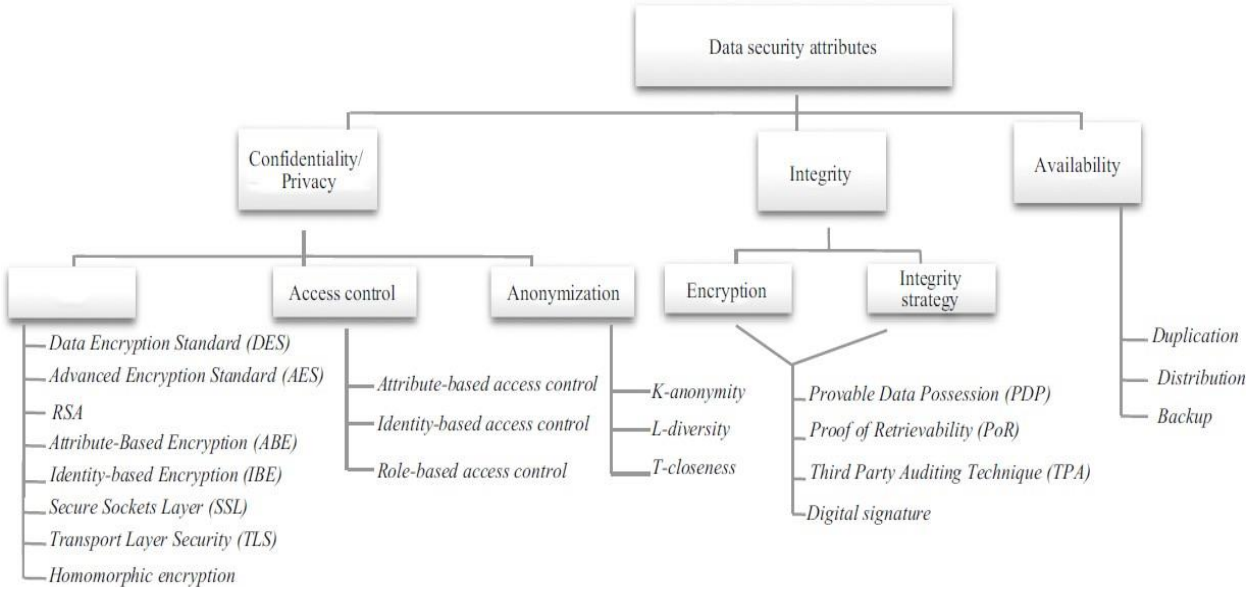

Figure 2: Common data security techniques associated to data security attributes [18]

As a safer way to protected records, encryption is proposed. It is easier to store data in the cloud server until for encrypting files. Data Owner should grant permission to specific member of the community so that details can be readily accessible via them. To include data access control, heterogeneous data- centric authentication should be used. A blueprint for data protection it must be designed for authentication, data encryption and data integrity, data recovery, user protection, and improve the protection of data in the cloud. Data encryption should be used as a service to ensure privacy and data confidentiality. Apply encryption to data that makes data unusable and unusable to block access to data from other users. Accessibility can be complicated by standard encryption.
Users are advised to review before uploading data to the cloud if the data is stored on backup drives and the keywords remain unchanged in the files. Compute the hash of the file would ensure that the data is not changed until transferring it to cloud servers. It is possible to use this hash calculation for integrity of records, but it is very difficult to preserve it.
Testing the integrity of RSA-based data can be done by merging identity based and RSA Signature cryptography. SaaS guarantees that all constraints must be transparent at the stage of the to segregate data from various participants, physical level, and device level. Architecture for distributed access management may It is used in cloud computing for access control.
Usage of passwords or attribution to recognize unauthorized users' policies that are centered are stronger. Permission as a service can be used to warn the customer that it is possible to access that part of the data. The fine-grained access management scheme helps the owner to assign most computer-intensive functions to the cloud without revealing the data material, servers.
For stable data collection, a data-driven architecture can be designed to and sharing with users of clouds. To track attacks in real-time, a network-based intrusion prevention framework is used.
Computing huge files of varying sizes and addressing the RSA-based storage security approach of remote data security can be used [17] In addition, cloud computing Requires a constant Internet connection, does not work well with low-speed connections, can be slow, features might be limited, stored data might not be secure, and stored data can be Lost [19]

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

6. Conclusion

Cloud computing services have significant advantages for organizations, vendors and users but need to bridge security gaps for cloud users to prevent any harm. Overall, this scientific literature review claimed that security was the most critical issue for users and CSPs. It is well-known that cloud computing has many potential advantages, there are still many actual problems that need to be solved and data are migrating to public or hybrid cloud. According to the analysis for data security, it is expected to have an integrated and comprehensive security solution to meet the needs of defense in depth. For data security issues, the primary challenges are separation of sensitive data and access control. In future objective is to design a set of unified identity management and data security-based framework across applications or cloud computing services. Future research should focus on the rapidly growing Computing domain by studying deeply and critically the security threats and issues that users encounter in order to prescribe appropriate measures and solutions [20]

The literature review provides substantial evidence supporting this assertion, indicating the need to propose well-suited measures for cloud computing security policies and standards. In section 5, it has outlined pertinent recommendations that can be adopted and executed effectively. These recommendations offer practical and actionable steps towards bolstering cloud security and ensuring adherence to established standards.

7. Acronyms and Abbreviations

Acronyms	Abbreviations
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
CaaS	Container as a Service
CSS	Cloud Storage Services
CDC	Cloud Data Storage
IT	Information Technology
MAC	Message Authentication Codes
CSP	Cloud Service Provider
HTTPS	Hypertext Transfer Protocol Secure
DOS	Denial of Service
DNS	Domain Name System
APA	Anonymous Password Authentication
EU	End User
DES	Data Encryption Standard
AES	Advanced Encryption Standard
PKI	Public key infrastructure
RSA	Rivest-Shamir-Adleman Algorithm
SLA	Service Level Agreement
HMM	Hidden Markov Model
DPHE	Double-Permitted Homomorphic Encryption
MK-FHE	Multi-Key Fully Homomorphic Encryption
POCC	Privacy-Preserving Outsourced Classification in Cloud Computing
QoS	Quality of Service
SLA	Service Level Agreement
API	Application Programming Interface

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Li Yibin, Keke Gai, Longfei Qiu, Meikang Qiu, Zhao Hui, "(Intelligent cryptography approach for secure distributed big data storage in cloud computing) 3 September 2016. Published by Science Direct journal. https://www.sciencedirect.com/science/article/abs/pii/S0020025516307319

[2] Jaydip Sen "Security and Privacy Issues in Cloud Computing" Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.

[3] Rajeev Kumar "DATA SECURITY IN CLOUD COMPUTING AND COST ANALYSIS: REVIEW" International Journal of Technical Research and Applications e-ISSN: 2320-8163, www.ijtra.com Volume 1, Issue 3 (July-August 2013), PP. 40-46.

[4] S. Sakr, A. Liu, D. M. Batista, and M. Alomari, "A Survey of Large-Scale Data Management Approaches in Cloud Environments," Communications Surveys & Tutorials, IEEE, vol. 13, pp. 311-336.

[5] Dr. C. Krishna Priya, Dr. JVN Ramesh, Dr V Srinivas, Dr. S. Kalaimagal "Data Security Analysis in Cloud Environment: A Review" National Conference on Advances in Computer Science, Engineering and Technology (NACET)-2017.

[6] W. Cong, R. Kui, L. Wenjing, and L. Jin, "Toward publicly auditable secure cloud data storage services" Network, IEEE, vol. 24, pp. 19-24

[7] Mai Rady ⇑, Tamer Abdelkader, Rasha Ismail "Integrity and Confidentiality in Cloud Outsourced Data" Ain Shams Engineering Journal 10 (2019) 275–285.

[8] T. Hsin-Yi, M. Siebenhaar, A. Miede, H. Yu-Lun, and R. Steinmetz, "Threat as a Service?: Virtualization's Impact on Cloud Security," IT Professional, vol. 14, pp. 32-37.

[9] P. You, P. Yuxing, W. Liu, and S. Xue, "Security Issues and Solutions in Cloud Computing," in 32nd International Conference on Distributed Computing Systems Workshops (ICDCSW), 2012, pp. 573-577.

[10] Abi Tyas Tunggal "What Are Cloud Leaks?" Cybersecurity journal, Feb 23, 2023.

[11] S. Subashini and V. Kavitha, "Review: A survey on security issues in service delivery models of cloud computing," J. Netw. Comput. Appl., vol. 34, pp. 1- 11.

[12] Mr. Avinash Ganne "CLOUD DATA SECURITY METHODS: KUBERNETES VS DOCKER SWARM" e-ISSN: 2582-5208 International Research Journal of Modernization in Engineering Technology and Science (Peer-Reviewed, Open Access, Fully Refereed International Journal) Volume:04/Issue:12/December-2022 Impact Factor- 6.752 WWW.irjmets.com.

[13] Rishabh Gupta, Deepika Saxena, and Ashutosh Kumar Singh "DATA SECURITY & PRIVACY IN CLOUD COMPUTING: CONCEPTS AND EMERGING TRENDS" Department of Computer Applications National Institute of Technology Kurukshetra, India deepika_6180096@nitkkr. August 24, 2021.

[14] Sajid Habib Gill, Mirza Abdur Razzaq, Muneer Ahmad, Fahad M. Almansour, Ikram Ul Haq, NZ Jhanjhi, Malik Zaib Alam, and Mehedi Masud "Security and Privacy Aspects of Cloud Computing: A Smart Campus Case Study" Intelligent Automation & Soft Computing DOI:10.32604/IASC.2022.016597, Received: 06 January 2021; Accepted: 05 May 2021.

[15] Bayan A. Alenizi, Mamoona Humayun, NZ Jhanjhi "Security and Privacy Issues in Cloud Computing" International Conference on Recent Trends in Computing (ICRTCE-2021) Journal of Physics: Conference Series 1979 (2021) 012038 IOP Publishing doi: 10.1088/1742- 6596/1979/1/012038.

[16] Bader Alouffi, Muhammad Hasan, Abdullah Alharbi, Wael Alosaimi, Hashem Alyami, and Muhammad Ayaz, "A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies" Published by IEEE Access. Received March 17, 2021, accepted April 9, 2021,

[17] Date of publication April 14, 2021, date of current version April 21, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3073203.

[18] Isma Zulifqar, Sadia Anayat, Imtiaz Kharal "A Review of Data Security Challenges and their Solutions in Cloud Computing" Govt College Women University Sialkot, Pakistan Received: 12 August 2020; Accepted: 17 November 2020; Published: 08 June 2021.

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023

[19] Lynda Kacha and Abdelhafid Zitouni "An Overview on Data Security in Cloud Computing" Lire Labs, Abdelhamid Mehri Constantine 2 University, Ali Mendjli, 25000 Constantine, Algeria (2018).

[20] Eman M.Mohamed, Hatem S. Abdelkader, and Sherif EI-Etriby "Enhanced Data Security Model for Cloud Computing" The 8th International Conference on INFOrmatics and Systems (INFOS2012) - 14-16 May 2012 Cloud and Mobile Computing Track.

[21] Zahra Ghanbari "A Literature Review on Cloud Computing Security Issues" Department of Information Technology-Computer Network Engineering, Electronic Branch Islamic Azad University Tehran, Iran.

DOI: https://doi.org/10.54216/IJWAC.070105

Received: January 28, 2023 Revised: April 26, 2023 Accepted: May 24, 2023