Review Article ISSN 3069-9703

International Journal of Mathematic Exploration and Computer Education

Cloud Computing's Data Security and Privacy Issues: A Review of the Problems and Solutions

Sarasij Majumdar*, Shivnath Ghosh

Brainware University, India.

***Correspondence author**
Sarasij Majumdar,
Brainware University, India.

Submitted: 16 Jun 2026; **Published:** 25 Jun 2026; **Published:** 13 Jul 2026

Citation: Majumdar, S. & Ghosh, S. (2026). Cloud Computing's Data Security and Privacy Issues: A Review of the Problems and Solutions. *Int J Math Expl & Comp Edu.3*(2):1-9. DOI : https://doi.org/10.47485/3069-9703.1027

Abstract

As companies shift to cloud computing settings, privacy and security issues become more crucial. With a focus on security and privacy concerns, this study reports and methodically examines a range of cloud computing difficulties and vulnerabilities. This paper analyses potential risks in-depth, ranging from illegal access to data breaches, and evaluates how these issues affect user confidence and data integrity in cloud infrastructure. Furthermore, effective methods and approaches to lower security risks and safeguard user privacy in cloud computing are put up and examined. This study offers practitioners and researchers a useful tool for navigating the changing environment of cloud-based services, while also contributing to the continuing discussion on cloud security and privacy.

Introduction: Overview of Cloud Computing

Cloud computing has become a transformational force in the ever-changing world of modern technology, upending established paradigms for information technology (IT) resource man-agement. The transition from separate systems to shared virtual resource pools has brought about a new era where businesses may readily access services to meet their processing and storage requirements. Our interactions with and usage of information technology have un-dergone a paradigm shift as a result of this integration of computing, software, and storage resources, which has impacted a wide range of fields including education, business, research, consumption, and entertainment. Fundamentally, virtualization, grid computing, and cluster-ing are just a few of the cutting-edge technologies that are integrated into cloud computing.

A popular concept that treats everything provided to consumers as a service is cloud computing. When utilizing a distributed method, it's a convenient and adaptable computing solution that provides a wide range of services, demonstrating its innovative character. With its vast and flexible possibilities, this technology is always changing (Gupta et al., 2021). Cloud technology is not only economical but also removes the logistical difficulties of operating on-site data centers and offers scalability to enterprises, adaptability, and ease of access. It was codi-fied by the National Institute of Standards and Technology (NIST) to the definition of cloud computing in 2006, reflecting the technology's increasing ubiquity (Mell & Grance, 2011).

Its extensive industry usage is proof of its powerful advantages, which include unmatched scalability, seamless processing, and efficient storage. According to Mell and Grance (2011) cloud computing enables demand-driven access to a shared pool of specialized computer resources, as seen in Figure 1, encompassing servers, storage devices, networks, software, and services (Gupta et al., 2021). These resources are quickly released and made available with little involvement from the service provider or administrative work (Gupta et al., 2021). The architecture and cloud service models of cloud computing are depicted in Fig. 2 below. With infrastructure as a service (IaaS), hardware infrastructure is provided by the Cloud Service Provider (CSP), who also gives consumers a virtual interface to host their data. Users carry out tasks by using their own operating systems (OS) and applications. The networking, computing, and storage that their deployed applications require. This architectural design comprises the supply of hardware resources, including bandwidth, memory, CPU, and disk Cloud providers supply all operating systems (OS), apps, and infrastructure under the Software as a Service (SaaS) model. Alternatively referred to as "on-demand software," users can access the program online with a subscription. Reachable through a web browser, business applications, web services, multimedia, and other resources are handled (Sorour & Atkins, 2024).

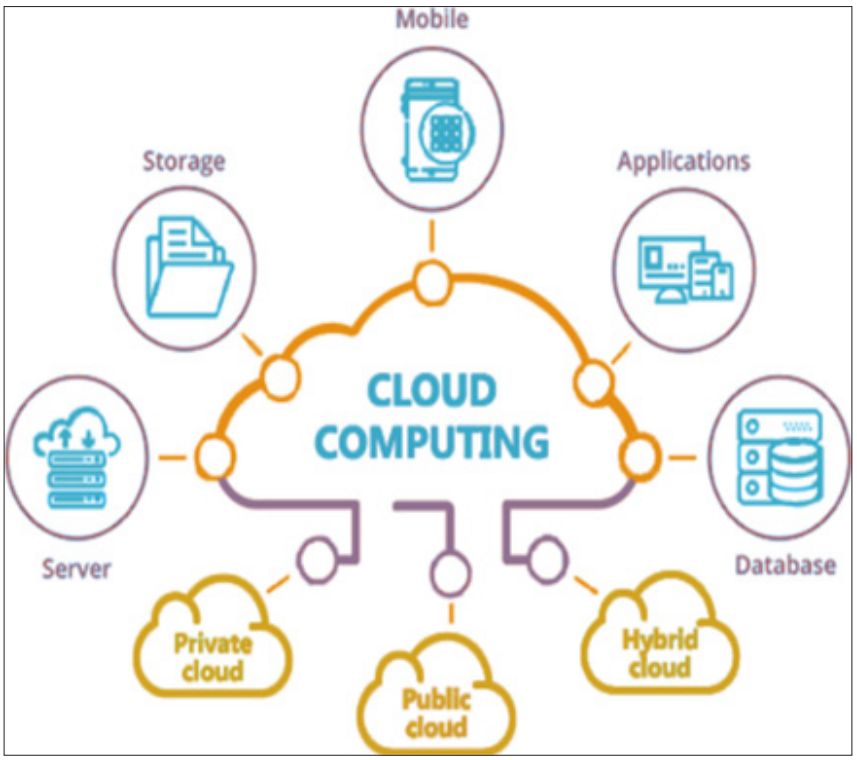

Figure 1: Cloud Computing (Gupta et al., 2021)

As we enter a period marked by exponential growth in data output and a rise in Internet-connected gadgets, the role of cloud computing is becoming more and more significant. Given the massive volume of data generated every second, it is obvious that consumers must use cloud servers for data storage services and storage. This research looks at a number of cloud computing-related topics, including examines the intricate network of technologies that supports it across a range of businesses.

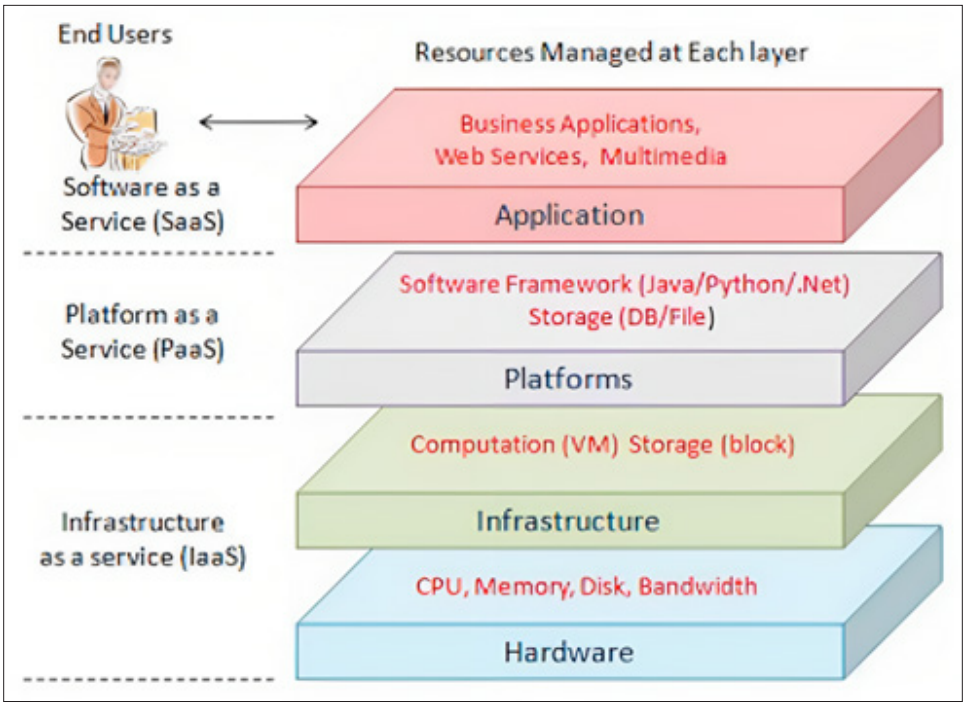

Figure 2: Cloud Computing Architecture and Three Service Models (Sorour & Atkins, 2024)

This paper delves deeper into the constantly changing field of cloud storage. Although cloud services are convenient for users, this study looks at the underlying mechanisms that let end users make the most of cloud computing in their daily lives. Furthermore, a variety of deployment strategies, such as community, and hybrid, whereas both public and private clouds are taken into account, emphasizing their importance and influence on cloud archi-tecture control and regionalization. The ensuing sections provide a thorough analysis of the intricacies of cloud computing, study methods, determining its security and privacy concerns, and the remedies, and difficulties.

Related Studies and Research

A survey about the possible hazards and threats associated with cloud computing was carried out based on the study presented in Ali et al. (2024). The current methods for enhancing cloud security and privacy were also discussed. It describes the idea of cloud computing and goes into additional detail on the advantages and benefits of the cloud service models shown in Fig. 3, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The possible risks, including data breaches, unsecure Application Programming Inter-faces (API), data loss, and account hijacking, are further discussed. Consequently, a number of alternatives, including data anonymization and cryptographic cloud storage, are put out in the discussion.

While data anonymization is a method that allows the analysis of the data, cryptographic cloud storage can safeguard data from security breaches and guarantee that the data is under user control. Data protection allows for more beneficial uses of the information. To ensure that the CSP offers consumers dependable and secure services, a few issues must be resolved, such as the suggested secure and dependable services. Next, in order to protect the data throughout storage, transmission, and sharing on the cloud, encryption needs to be put into place.

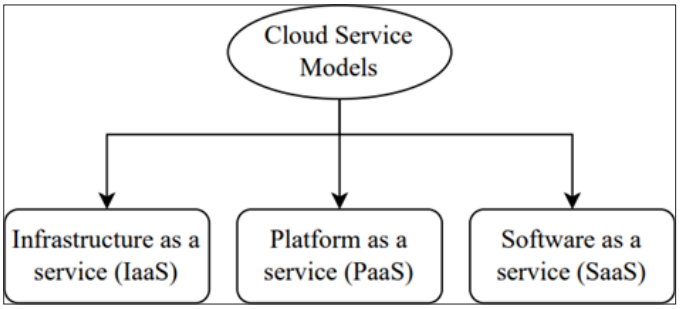

Figure 3: Cloud Service Models

Furthermore, the research in Sun (2020) illustrates the debates and difficulties surrounding cloud computing security and privacy protection. It describes the fundamental ideas of cloud computing and how it provides end users with adequate resources. This study, like the one in Ali et al. (2024), also provides an explanation of its models, which are shown in Fig. 2. This study finds that due to the vast volumes of data being uploaded to the cloud, the intricacy of the cloud computing service model, and the constrained resources of terminals, a range of security-related issues need to be investigated and evaluated by cloud computing.

As a result, the research in Sun (2020) concentrates on the several crucial technologies, such as access control, attribute-based encryption, and trust. This study indicates that there are multiple ways to guarantee privacy and security when using cloud computing. The first is cloud computing privacy security protection, which is separated into two sections: a privacy security risk and a privacy protection network. Conventional access control has a unique function in preventing unauthorized users from accessing information, permitting authorized users to access information, and preventing approved users from accessing information.

Attribute-based Encryption (ABE), an encryption method suited for cloud computing, is also covered in the paper in reference (Sun, 2020). This method can safeguard user information and fine-tune data access management. Since searchable encryption (SE) technology is very compatible with maintaining the confidentiality of cloud privacy data, searchable encryption is one of the security and privacy strategies that is also covered in the Sun (2020) paper. It also provides cipher text retrieval based on keywords. Nonetheless, there are certain difficulties that require better approaches. Among the difficulties are the various attack methods used to pilfer confidential information. Scholars' ought to be mindful of and focus more on attacks on virtual machines that occur during cloud migration. As a result, new directions are still being discussed, and a framework for future development has been suggested.

In the context of edge, cloud, and fog computing, privacy and security concerns are examined in the research conducted by Sorour and Atkins (2024). This paper defines cloud computing as externalized data storage and processing. But despite all of the benefits of cloud computing, one of the most important things to consider is cloud security. As a result, the conversation delves deeper into the subject by describing a few cloud computing threats, including Injection of cloud malware, Denial of Service (DoS) assaults, and Communication interception. This work also elaborates on service kinds, which include IaaS, PaaS, and SaaS in Fig. 3, in a manner similar to the discussions in Ali et al. (2024) and Sun (2020). As a result, this paper lists the security vulnerabilities in each service.

An additional research paper in Lalitha et al. (2023) examines cloud-based data security challenges and solutions. In this study, the paradigm of cloud computing is described as one that prioritizes computation and data sharing among a scalable network of nodes. The reasons why data needs to be protected, problems with cloud data storage, different cloud computing security concepts, and current security solutions for data security and privacy protection are thus covered in the discussions that follow. Security and privacy concerns with cloud computing are covered in research in George and Pramila (2021). According to this report, cloud computing is a collection of hard-ware and software resources that are remotely made available to customers via the internet. This

study also examines cloud service models, which, as Fig. 3 illustrates, are comparable to those of the earlier research mentioned above. The three types of cloud deployment models shown in Fig. 4 are the topic of discussion moving forward. These include hybrid clouds, private clouds, and public clouds.

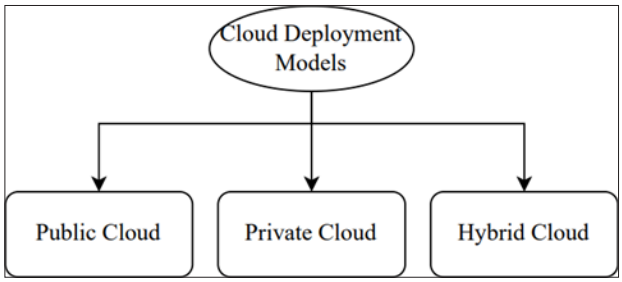

Figure 4: Cloud Deployment Models

Several cloud security challenges, including data confidentiality, data availability, data integrity, data security, and data localization issues, were also included in the study in George and Pramila (2021). Additionally, several threats have been identified, including denial of service, unsafe interfaces and APIs, traffic hijacking, and many others. This paper also offers solutions to the security problems associated with cloud computing, including recovery facilities, encryption algorithms, and backup facilities. The topic of cloud computing privacy is discussed in more detail. Among the problems mentioned are data boundaries, access control, loss of control, and improper storage.

The architecture, features, and models of cloud computing are covered in the research paper in Alharthi et al. (2024). This work describes the models as illustrated in Fig. 2, which is similar to the papers discussed in the aforementioned studies. The deployment models are illustrated in this study in the same way as in Fig. 3, but Community Cloud is a new model that was included. Additionally, a few security-related concerns have been highlighted in this work, including insider attacks, logical storage segregation and multitenancy, key and cryptography management, and identity management challenges.

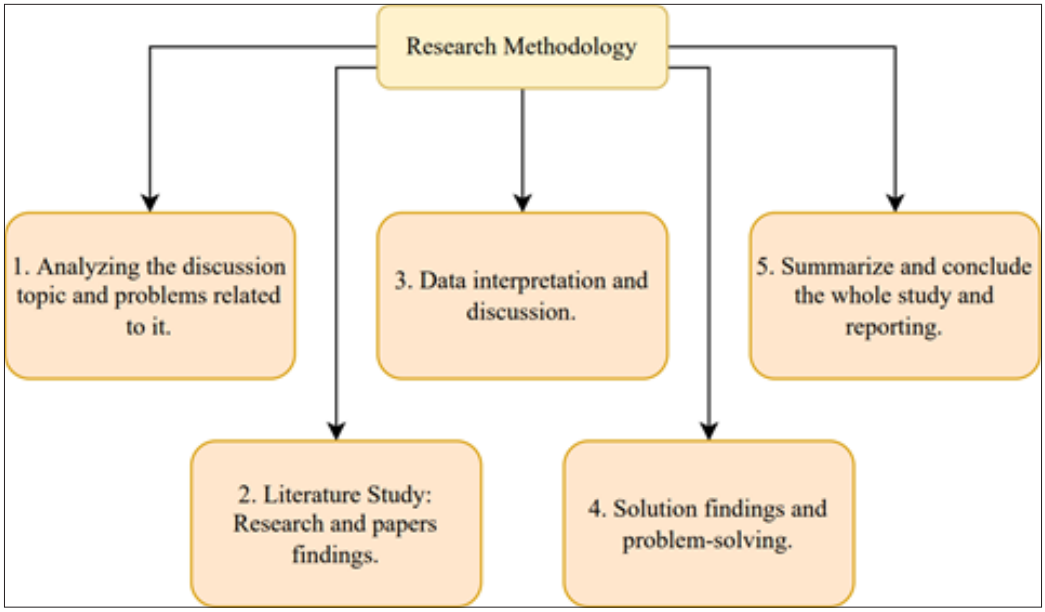

Figure 5: Research Framework

The study in Gupta et al. (2021) highlights the cloud computing services that are comparable to Fig. 1 and addresses the cloud services, deployment model, and security problems in cloud computing. Subsequently, the research work in Alharthi et al. (2024) is paralleled by an explanation of cloud deployment methods in this study. This study mentions a number of security issues, including account and traffic hijacking, insecure APIs and services, incorrect cloud computing deployment, and malpractice. The solutions offered for each of the aforementioned problems include the need for user registration to go through extensive authentication processes, the recommendation that cloud providers' APIs use a strong authentication security model, and the necessity of forbidding the sharing of account credentials between users and services.

Research Methodology

Discussing and Analysing the Topic and its Related Problems

While analysing a topic for discussion, this research tries to break down the problem elements and has researched the topic more thoroughly. In order to comprehend and recognize the fun-damental issues connected to the subject under discussion, the core problems have also been investigated. This step entails defining the research's parameters and developing a thorough knowledge of the relevant problems. In essence, it involves establishing the framework for the entire investigation to guarantee that the next inquiry is targeted and intentional. In order to concentrate on the topic's finer points, the research scope has also been delineated. Addi-tionally, this stage focuses on laying a strong foundation for the upcoming research. By doing this, this phase will guarantee that the study

is well-guided and that the difficulties are clearly understood. This basically lays the groundwork for focused investigation and guarantees that every action that follows is founded on a thorough comprehension of the issue at hand.

Literature Study: Results of Research and Papers

This phase is a journey through already gathered knowledge and discoveries. In this stage, it is often mentioned as literary study, and here, ideas are generated and points must be noted to encourage the ideas to be covered in this research. To comprehend the chosen issue, a number of research articles and studies that have already addressed various facets of it have been evaluated and examined. This stage aims to assess and assimilate the concepts and discoveries in addition to expanding one's knowledge base. The majority of the paper searches are done in MyKM to locate research publications from the Association for Computing Machinery (ACM), ScienceDirect, and the Institute of Electrical and Electronics Engineers (IEEE). This paper, this analysis will not only assist in developing and discovering additional knowledge, but they will also help to comprehend the issue of the core idea at a deeper level. It involves locating and arranging this research material in a way that will allow for original contributions to the current conversation.

Interpretation and Discussion of the Data

Information and data from previous researches are gathered and analysed here. Based on the findings of this investigation, information is systematically retrieved thorough awareness of current knowledge and recommendations from earlier research. In addition to collecting a multitude of data and insights from earlier investigations, information was extracted from different types of research and studies, including journals and research findings, extracting important information to guide the current investigation. This analytical journey entails more than just describing the idea of cloud computing; it also covers a careful analysis of problems, the identification of possible threats, the investigation of potential solutions, and an open discussion of the difficulties that arise from the data and information once they have been gathered and thoroughly examined.

Finding Solutions and Solving Issues

Current study is focused on suggesting solutions based on the data's insights once the data and information have been sufficiently extracted and examined from the research and publi-cations. This phase is actively seeking solutions in addition to understanding and recognizing the issue and problem. Additionally, this level calls for critical thinking, inventiveness, and a thorough comprehension of the implications of the suggested solution. Researchers aim to provide useful answers in this area by creative concepts, policy suggestions, and required interventions. As the study focuses on not only comprehending issues but also actively con-tributing to the development of effective solutions, this stage reflects the synthesis of knowl-edge, critical thinking, and an outlook on the future of data security.

Conclusion after Summarizing the Entire Research and Reporting

The study concludes with a summary of the different findings, conclusions, and discussions. Important discoveries and prior research were mainly highlighted in the conclusions that were derived from the entire previous study. Lastly, the outputs of research are properly recorded to ensure that the study contributes significantly to the body of knowledge on the chosen subject. The results of this study are succinctly and effectively presented in this step, which marks the final stage of the research journey.

Threat Issues

Because of concerns about security and privacy, users can be reluctant to entrust the cloud with their data. If these problems arise, users can believe that the cloud is not entirely depend-able, which could make them fearful that their private information might be compromised. Here is a list of the majority of problems or risks for cloud computing, based on Gupta et al. (2021), Mell and Grance (2011), Sorour and Atkins (2024) , Ali et al. (2024) and George and Pramila (2021):

Vulnerability in API Security

In cloud computing, APIs are essential as connectors. It permits the seamless integration of cloud services with enterprise software while preserving accessibility, scalability, and secu-rity. APIs are crucial for removing hiccups, increasing speed, and enabling a range of API types for effective management in multi-cloud systems (Waseem et al., 2024). The efficacy of the APIs' nu-merous helpful features to safeguard cloud services would be rendered ineffective due to the limited availability of publicly accessible cloud services. Thus, there is an open risk that unauthorized parties will gain access to cloud services. As such, there is a greater chance of being hacked by attackers (Gupta et al., 2021).

Unintended Data Exposure

Inadequate access control to object storage buckets and data stores is a major cause of cloud data breaches (Goel et al., 2024). This allows unauthorized people or entities to access sensitive data stored in object storage buckets. As a result, confidential information may be accessed, changed, or deleted without permission. Moreover, unauthorized individuals or the general public may be given access to sensitive information.

Code Injection Threat

The main threat to SaaS is a virtual assault that involves unauthorized SQL injection on a computer. Because of the badly developed application, SaaS is the most negatively impacted by this attack. The process consists in using an unstable interface to complete the unautho-rized SQL execution of a statement. These assaults aim to obtain personal data not intended for public consumption by gaining unauthorized access (Kaur & Kaimal, 2023). Due to unauthorized access to personal data, people's privacy may be at danger. If the identity of the individuals whose data was exposed is stolen or used fraudulently, they could face legal repercussions.

DoS Attack

When hackers send an excessive amount of data packets over the network or services, they might launch this kind of assault. The server becomes overloaded with connections as a result, and redundant and needless data is thrown into the host's buffer memory. The server won't be able to build any links if the buffer is empty at the end. The IaaS and PaaS levels are the specific targets of this assault (Kaur & Kaimal, 2023). Users who try to access the affected services or resources consequently lose connectivity. Moreover, this assault may create downtime for websites, apps, and even entire systems.

Data Crash

A number of activities can result in data compromise, including modifying or deleting data without making a backup. Cloud data storage is similar to data saved on dubious media. A misplaced key may also result in a data crash (Gupta et al., 2021). Furthermore, data backup is necessary in case of unintentional or purposeful calamities. Regular backups of the data are required under the Content Security Policy to ensure its availability. Actually, backup data should follow security protocols to prevent suspicious assaults like manipulation and unauthorized access (Alrasheed et al., 2022).

Solutions

Numerous challenges or dangers have emerged in the field of cloud computing, prompting research and the development of several solutions to address these issues. Several approaches have been proposed and implemented to address these problems or dangers. The solutions are as follows: Several methods should be followed to enhance cloud computing API security:

Robust API Authentication architecture:

Cloud providers should implement APIs with a robust authenticated security architecture as they improve the security of private data and also reduce the chance of unauthorized access and data breaches.

Safe Transmission of Data

Encrypting data prior to transmission is strongly recommended since it is an essential step in improving data security and protection when information is being transferred. The risk of data breaches is significantly reduced by encryption, as it serves as a barrier against unauthorized access and ensures that only authorized parties can decrypt the sent data using the decryption key.

Secure Key Handling:

Keep the process's keys in a secure location rather than reusing them. This enhances the security of cryptographic operations and fortifies the security scenario by preventing vulner-abilities caused by compromised or reused keys.

API Dependency Chain:

A comprehensive grasp of the API dependency chain is crucial. By identifying potential weak places in their systems, businesses can improve their understanding of risks and fortify their resilience. Common API frameworks such as Cloud Infrastructure Management Interface (CIMI) and Open Cloud Computing Interface (OCCI) must be considered.

Network Level:

This denotes the specific layer of cloud architecture where security protocols and measures are implemented to ensure the availability, confidentiality, and integrity of data during transmission across the cloud infrastructure. This layer focuses on safeguarding data exchanges and communication pathways among various cloud services, components, and external entities. To protect against potential threats and vulnerabilities, here is a list of solutions for these:

Confidentiality:

Ensured by cryptographic methods such as public or private key encryption. Information is stored and transmitted in an encrypted format, guaranteeing that only individuals with the appropriate decryption key can access the data (Prasad et al., 2024).

Private Key (Ghosh et al., 2020)

At the very beginning, the data has to be encrypted using a robust encryption method like Triple DES, RSA, Blowfish, etc., for the creation of the private key. As soon as the data is encrypted, hence the private key is also generated. It's important to mention here that this step is essential to ensure the security of the data.

Salted Hashing

The next phase involves enhancing the security feature of the private key and making it less vulnerable to unauthorized access after it has been created. The method employed to accom-plish this is known as "salted hashing." For salted hashing to function properly, the private key is initially supplemented with a random value (salt). This process results in a hashed out-put that is more intricate and distinct, which makes it further difficult for attackers to calculate the original private key.

Public Key (Kumari et al., 2022)

ABE

ABE is a multi-user public-key encryption technique that provides fine-grained access control and data privacy in cloud computing. In ABE, characteristics are used to encrypt user data, which is then decrypted by the user using a secret key linked to the access policy. Thus, ABE will improve data privacy and access management.

Searchable Encryption

It enables the searching of encrypted data without revealing any details about the plaintext material. By keeping sensitive data from being exposed throughout the search process, this procedure guarantees that the search functionality is carried out with privacy and security in mind.

Re-encryption of Proxy

A cipher text encrypted with a separate key can be encrypted by a proxy using a different key. This guarantees the data's security during the transmission procedure.

Encryption based on DNA

Encryption keys are produced using DNA computing and neural networks. There is less chance of unauthorized access or key compromise. Overall security for privacy will be enhanced.

Dual Encryption and Data Fragmentation

This method combines two different encryption algorithms to encrypt the data. The process of breaking up a piece of data into multiple smaller bits and distributing them across servers or networks is known as data fragmentation. Vulnerabilities in one strategy may be lessened by strengths in another when several approaches are combined.

Homomorphic Encryption

It allows computation over ciphered text without the need for text decoding. Throughout the computing process, the data will be kept confidential to avoid exposure to unauthorized parties. Integrity (Prasad et al., 2024) kept up to date with techniques like digital signatures, message digests, and Message Authentication Code (MAC). These methods guarantee that data is reliable and unmodified through-out transmission and storage.

Access Control (Prasad et al., 2024)

Implemented using established guidelines and rights of access. Resources are made available to users who have the right credentials and follow the rules.

Security Updates and Firewalls (Prasad et al., 2024)

To fix vulnerabilities, operating systems, browsers, and linked apps must receive regular upgrades. One way to defend against Denial of Service (DoS) assaults is through well-configured firewalls.

Legitimate User Access (Prasad et al., 2024)

Only authorized users should be allowed access privileges, and in order to stop unwanted access, these rights must be properly managed.

Transport Layer Security (TLS) (Prasad et al., 2024)

Used to provide a safe channel for data transmission and to safeguard network connection.

Firewalls and intrusion detection systems (IDS) (Prasad et al., 2024).

To identify and stop network assaults, including port scans, IDS and sophisticated firewalls are used.

Domain Name System Security Extension (DNSSE) (Prasad et al., 2024)

Installed to manage DNS attacks, strengthening the Domain Name System's security. Reduce risks that come from the host. Tera Architecture (Prasad et al., 2024).

Tera architecture is proposed as a way to defend virtual machines against full-privileged users. It prevents any modifications from other virtual machines inside the same environment by creating an isolated environment that resembles a closed box. By limiting the actions that users with full access can take, this isolation improves security.

Trusted Virtual Data Centre (TVDc) (Prasad et al., 2024)

TVDc is marketed as a solution that tackles security issues at the management and infras-tructure levels. TVDc allows providers to offer an execution environment that is segregated from other users under the Infrastructure as a Service (IaaS) model. Using the Trusted Cloud Computing Platform (TCCP), this secure setting, giving consumers confidence that the service runs in a reliable setting.

Security Assurance in Software Development Life Cycle (SDLC) (Prasad et al., 2024)

Some companies are mentioned for offering security assurance as part of their SDLC, includ-ing Salesforce.com, Microsoft, and Google. This shows that security concerns are incorporated into the development process, guaranteeing that services and applications are developed with security in mind from the start.

Application Level

It refers to a certain layer of cloud architecture where services and software programs oper-ate. In order to enhance functionality and interoperability throughout the cloud ecosystem, cloud apps frequently interact with other cloud services and resources. Threats could yet materialize, though. This is a list of ways to stop these dangers:

Service Provider's Role in Security (Prasad et al., 2024)

It is the responsibility of the service provider to ensure platform-specific security solutions. This entails putting in place a number of security mechanisms, including support for Trans-port Layer Security (TLS), Secure Socket Layer (SSL), authorization techniques, authentica-tion protocols, and single sign-on (SSO).

Diversity in Security Features (Prasad et al., 2024)

Different PaaS providers may offer different security configurations and features. Platforms such as Google App Engine and Force.com, for instance, offer unique APIs that enable cus-tomers to configure different security parameters according to their own requirements and preferences.

Use of Security Assertion Markup Language (SAML) (Prasad et al., 2024)

In PaaS setups, SAML can be used to facilitate user federation. A foundation for enabling Single Sign-On (SSO) and other security-related features is provided by SAML, a standard for sharing authorization and authentication data between parties. Challenges.

Managing virtual instances in cloud systems poses ongoing issues that need for ongoing investigation, security evaluation, and preventative measures. Central asset management becomes increasingly challenging when cloud workloads are spread across several locations. Here are a few of the difficulties:

Challenges in Securing Cloud Computing (Goel et al., 2024)

Dynamic Environment

Continuous and timely viewing of virtual instances might be difficult due to the elastic nature of cloud environments. It is necessary to regularly examine these environments, assess their security, and take precautionary action.

Creating Boundaries

Central asset management is hampered by the dispersion of cloud workloads across many environments and geolocations. It becomes difficult since it deals with tasks that take place in different surroundings and in different regions of the world. This is comparable to the challenge of managing and managing activities and tasks that are dispersed over various cloud settings and places.

Lack of Authority Regarding Physical Security

When a company loses control over physical security, it becomes the customer's responsibility to safeguard workloads and data throughout the transfer.

Challenges in Protecting Cloud Computing (Sun, 2020)

The cloud infrastructure of system management programs is usually the foundation for all kinds of attacks. To increase operating rights or steal confidential information, a variety of attack methods are employed. The following difficulties arise when developing the solutions:

1. Researchers should focus more on types of attacks on virtual machines during cloud migration, such as malicious theft of private information, to more effectively combat side-channel assaults between virtual machines.
2. Policies for security defences that are not dependent on CSP must be created to effectively prevent privilege abuse. Researchers should focus on the detrimental effects of security defences on public cloud performance.
3. It is necessary to raise the sharing algorithm's privacy protection level. Although further research is needed on the unidirectionality and transitivity characteristics of proxy re-encryption methods, attribute encryption strategies often have low efficiency in dynamic permission management.

Conclusion

In conclusion, because cloud computing offers a shared virtual resource pool for a range of applications, it is revolutionizing IT resource management. Its ubiquitous use is fueled by advantages including cost-effectiveness, scalability, and accessibility. Nonetheless, there are still security issues that call for robust frameworks. Security-related subjects like unantici-pated data leakage and API vulnerabilities are examined in our study. Among the solutions are enhanced API security, encryption, access control, and state-of-the-art techniques like homomorphic and DNA-based encryption. The dispersed workload and the transient nature of cloud settings present challenges.

Organizations need to proactively evaluate and defend against changing threats. The client is now responsible for protecting data during transmission as physical security control wanes. As physical security control diminishes, customer responsibility for data protection during transfer rises. This paper provides a comprehensive analysis that considers various de-ployment strategies and highlights the importance of security in cloud computing. In a period of exponential data expansion and increasing connectivity, the ideas and findings being pre-sented are meant to contribute significantly to the current discussion on cloud infrastructure security.

References

1. Gupta, S., Gupta, A., & Shankar, G. (2021). Cloud computing: Services, deployment models and security challenges. 2nd International Conference on Smart Electronics and Communication (ICOSEC), pp. 414–418. DOI: https://doi.org/10.1109/ICOSEC51865.2021.9591794
2. Mell, P. & Grance, T. (2011). The NIST definition of cloud computing. National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA (2006). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
3. Sorour, A., & Atkins, A. S. (2024). Big data challenge for monitoring quality in higher education institutions using business intelligence dashboards. *Journal of Electronic Science and Technology, 22*(1), 100233. DOI: https://doi.org/10.1016/j.jnlest.2024.100233
4. Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information security risk assessment methods in cloud computing: Comprehensive review. Journal of Computer Information Systems, 66(1), pp. 1–28. DOI: https://doi.org/10.1080/08874417.2024.2329985
5. Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges. *Journal of Network and Computer Applications, 160*(2), 102642. DOI: https://doi.org/10.1016/j.jnca.2020.102642
6. Lalitha, P., Yamaganti, R., & Rohita, D. (2023). Investigation into security challenges and approaches in cloud computing. *Journal of Engineering Sciences, 14*(8), 2113-2133. https://www.researchgate.net/publication/375610287_INVESTIGATION_INTO_SECURITY_CHALLENGES_AND_APPROACHES_IN_CLOUD_COMPUTING
7. George, S. S., & Pramila, R. S. (2021). A review of different techniques in cloud computing. Materials Today: *Proceedings, 46*(5), 8002. DOI: https://doi.org/10.1016/j.matpr.2021.02.748
8. Alharthi, S., Alshamsi, A., Alseiari, A., & Alwarafy, A. (2024). Auto-scaling techniques in cloud computing: Issues and research directions. *Sensors, 24*(17), 5551. DOI: https://doi.org/10.3390/s24175551
9. Waseem, M., Ahmad, A., Liang, P., Akbar, M. A., Ahmad, L., Setälä, M., & Mikkonen, T. (2024). Containerization in multi-cloud environment: roles, strategies, challenges, and solutions for effective implementation. DOI: https://doi.org/10.2139/ssrn.5151248
10. Goel, A., Prabha, C., Malik, M., & Sharma, P. (2024). Security concerns and data breaches for data deduplication techniques in cloud storage: A brief meta-analysis. *International Journal of Safety & Security Engineering,* 14, 435-446. DOI: https://doi.org/10.18280/ijsse.140211

11. Kaur, M. & Kaimal, A. B. (2023). Analysis of cloud computing security challenges and threats for resolving data breach issues. International Conference on Computer Communi-cation and Informatics (ICCCI), pp. 1–6. https://doi.org/10.1109/ICCCI56745.2023.10128329
12. Alrasheed, S. H., Adubaykhi, S. A., & El Khediri, S. (2022). Cloud computing security and challenges: issues, threats, and solutions. 5th Conference on Cloud and Internet of Things (CIoT), pp. 166–172. DOI: https://doi.org/10.1109/CIoT53061.2022.9766571
13. Prasad, A., Singh, T. P., & Sharma, S. D. (2024). Communication technologies and security challenges in IoT: Present and future. Springer, pp. 107–129. https://link.springer.com/book/10.1007/978-981-97-0052-3
14. Ghosh, S., Singh, A. R., Pandey, G., & Lakhanpal, A. (2020). A novel solution to cloud data security issues. 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 857–860. DOI: https://doi.org/10.1109/ICACCCN51052.2020.9362743
15. Kumari, S., Solanki, K., Dalal, S. & Dhankhar, A. (2022). Analysis of cloud computing security threats and countermeasures. 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 1–6. https://doi.org/10.11091/ICRITO56286.2022.9964632