Article

Cloud Storage Security: Risks and Solutions

Raheba Mohammad Zahir *

Posted Date: 24 November 2025

doi: 10.20944/preprints202511.1778.v1

Keywords: cloud storage; storage security; cloud computing; data breaches; confidentiality

 doi:10.20944/preprints202511.1778.v1

Article

Cloud Storage Security: Risks and Solutions

Raheba Mohammad Zahir

Ala-Too International University COM22; raheba.mohammadzahir@alatoo.edu.kg

Abstract

This paper explains the biggest risks that come with putting information into the cloud and suggests ways to solve them. Although cloud storage is useful because it is cheap and flexible, it means users lose direct control over their files. To keep data safe, we need two things to work together: better technology and better management rules. Better technology means using tools like encryption and making sure only authorized users can see certain files. Better management means training employees well and having clear security plans. The main problems we found are not just about computers; they also involve human mistakes, complicated systems, and making sure the secret encryption keys are managed correctly. We conclude that true cloud security is a balance: we must make protection strong enough to work, but simple enough that people will actually use it. This requires clear communication between the company storing the data and the person owning the data.

Keywords: cloud storage; storage security; cloud computing; data breaches; confidentiality

1. Introduction

If you are an Internet user in 2025, you are most likely using cloud storage to some extent. Companies depend on it for important information, and people use it to store photos, documents, and personal backups. Instead of storing bulky hardware and servers, users can now use on-line data storage using services such as Amazon S3, Google Drive, and Microsoft OneDrive. This flexibility enables teamwork, reduces the total cost of ownership, and provides operational information that is ready to use anytime you have access to the Internet. These advantages explain the growing popularity of cloud data storage among corporations and individuals.

Despite these advantages, security remains the most pressing issue. As soon as the data is uploaded to the cloud, users give up direct control and trust service providers to protect confidential information [1] [2]. Firewalls, authentication, and access control systems can reduce risks, but they cannot eliminate them. Data leaks, insider threats, and even system failures have shown that security incidents are still possible. Encryption provides more reliable protection, but it also introduces new challenges: managing encryption keys is a complex process, and applying it to large datasets can lead to performance and usability problems. These trade-offs show why data privacy, integrity, and availability are still unresolved issues in cloud environments[3] [4] [5].

Addressing these vulnerabilities requires more than just technical solutions. Organizational policies, human behavior, and user practices play an equally important role in ensuring cloud security. A company can invest in advanced tools, but still face risks if employees use unreliable passwords or mishandle files. Similarly, providers can offer secure infrastructure, but they cannot clearly communicate responsibility to their users. These gaps show that cloud storage security is not just a technological issue; it is also a matter of trust, awareness, and coordination [1] [2].

This article examines these issues to provide a clearer understanding of both the risks and possible solutions for securing cloud storage.

The ***goal*** is to analyze how existing methods such as encryption, access control, and authentication work in practice, as well as consider the human and organizational factors influencing the results.

At the same time, the study raises ***important questions***:

 doi:10.20944/preprints202511.1778.v1

- How effective are modern approaches to ensuring confidentiality and accessibility?
- What disadvantages still remain when used in real-world conditions?
- How can users and providers collaborate to provide better protection without compromising usability?

By analyzing these issues, this work contributes to ongoing efforts to transform cloud storage into a more secure and trustworthy foundation for modern digital infrastructure[6].

2. Literature Review

The security of cloud data storage has become one of the most widely discussed topics in cloud computing research. The growing reliance on cloud infrastructure has changed the way enterprises manage, store, and process data. While the cloud offers huge benefits in terms of cost reduction, flexibility, and resource availability, it also creates new forms of security and privacy risks[3][2]. Most studies agree that, despite the convenience and economic benefits, users are still hesitant to store confidential data in the cloud due to the lack of direct control over storage environments and the risks of unauthorized access.

1. Overview of Cloud Storage and Its Security Concerns

The transition to cloud technologies has given enterprises the opportunity to optimize their IT infrastructures. Instead of maintaining their own servers and software, they can now use cloud providers' resources, gaining flexible access to computing power, storage, and applications, as well as reducing capital and maintenance costs. However, a significant disadvantage of this system is that it involves transferring control over data from the client to the service provider. Once information is hosted in the cloud, users can no longer fully control or guarantee its security[1]. Modern security methods, including virtualization and firewalls, do not always guarantee complete data security in the cloud. The distributed and interdependent nature of cloud ecosystems creates additional risks of cyber attacks, security breaches, and disruptions. Experts agree that the security of cloud services is based not only on technical solutions, but also on a strong relationship of trust between the provider and the user. The loss of this trust caused by incidents such as data leaks, significant disruptions, or poor management inevitably calls into question the very viability of cloud computing[1] [6].

2. Common Threats and Real-World Incidents

The literature highlights several real-life incidents that illustrate how serious cloud storage vulnerabilities can be. For example, even large and reputable providers such as Amazon and Google have experienced service outages and data loss. Amazon Web Services once experienced outages caused by lightning strikes, which caused power generators to malfunction and temporarily shut down their cloud service. Similarly, Gmail users in 2006 reported the loss of all their mailboxes and contacts due to technical problems, and Google was unable to recover the lost data. Another case was the Dropbox incident in 2012, when hackers took advantage of a loophole in the access control system, which led to a serious data leak and leaked user passwords.

These examples show that no provider is completely immune from security vulnerabilities. Threats are usually divided into three main categories: data loss, unauthorized access, and unavailability of services. While some of these incidents are the result of human or system errors, others are caused by deliberate attacks on cloud infrastructure.Importantly, security risks also arise from the configuration of websites that use cloud storage for direct user file uploads, highlighting risks beyond the core CSP infrastructure [6][7].

3. Key Security Objectives and Mechanisms

According to most scientific studies, the security of data stored in the cloud is governed by the same three basic rules that are fundamental to all computer systems: confidentiality, integrity, and accessibility.

Confidentiality requires that access to data be restricted exclusively to authorized parties. Encryption is a typical protection mechanism for this, but this practice can lead to delays due to significant computing power and data transfer costs, especially when working with large amounts of data. The

 doi:10.20944/preprints202511.1778.v1

researchers note that while encrypting sensitive files before uploading them to CSP significantly increases privacy, this process inherently limits the usefulness of the data, making it much more difficult to perform routine actions such as searching or sharing files.

The principle of integrity is aimed at ensuring that data remains complete and unchanged during its storage or transmission over the network. To verify that information has not been tampered with, various reports suggest using cryptographically secure tools such as one-way hash functions or new verification protocols based on blockchain technology.

Accessibility satisfies the user's need for reliable access to their information at all times. Methods such as data replication and comprehensive backup systems are often used to ensure this availability. However, these methods can create additional problems, such as data synchronization conflicts or the additional financial burden associated with paying for duplicate storage space[3] [4] [2].

Achieving all three security objectives simultaneously —confidentiality, integrity, and availability—is a very complex task in practice. For example, increasing confidentiality through encryption often leads to bottlenecks that can reduce system availability or overall usability. For this reason, researchers are constantly working on developing balanced security models that provide robust protection without compromising performance.

4. Encryption and Access Control Approaches

In the field of cloud security, researchers are actively looking for the optimal combination of encryption reliability and ease of use. Although traditional encryption methods protect data well, they can significantly reduce performance due to high computational costs. Some experts believe that encryption is not a panacea, especially considering that the cloud service provider (CSP) retains full control over the infrastructure where your data is stored and processed. Promising technologies such as homomorphic encryption and searchable encryption are currently being actively studied, but at the moment they are too complex and not suitable for widespread practical use in cloud computing [3].

Ensuring that only the right people can access the right data is a critically important task, and cloud services generally employ role-based access control (RBAC) most commonly; more recent approaches such as attribute-based access control (ABAC) are gaining traction and allow for fine-grained access decisions based on factors such as where the user is located, when they are attempting to access, or what device they are using. While reliable authentication methods such as multifactor authentication are essential to prevent unauthorized access, experts warn that they should be used judiciously; the most important thing is not to make the process so cumbersome that users look for ways to bypass the security system[2] .

5. **Trust, Compliance, and Shared Responsibility**

Cloud security is a complex issue that requires a comprehensive approach that goes beyond technical aspects. The key elements of successful cloud security are mutual responsibility, trust, and clear rules. Effective data protection requires collaboration between customers and cloud service providers. Users are responsible for aspects such as access control, password protection, and encryption, while vendors are responsible for infrastructure security.

In addition, compliance with data protection laws and regulations is of paramount importance. Organizations that process confidential information, such as financial or personal data, are required to comply with privacy regulations such as the GDPR to protect user rights. Research highlights the importance of openness in data processing practices, regular audits, and transparent service level agreements (SLAs) to build trust between users and cloud service providers [1].

6. Summary

The available scientific papers indicate that the security of cloud storage is a multifaceted task that requires an integrated approach. It includes not only technical solutions, but also organizational measures, as well as compliance with legal norms. Although basic security tools such as encryption, authentication, and access control are important, they do not guarantee complete security. Most researchers agree that a combination of advanced technologies and trusting relationships between

 doi:10.20944/preprints202511.1778.v1

cloud service providers and their customers is needed to ensure data confidentiality, integrity, and accessibility.

The study shows that despite the progress in the field of cloud storage, security issues remain relevant. Solving them requires not only better encryption and access control methods, but also transparency in reporting and increased user awareness of risks [4].Therefore, future research is likely to focus on developing simple, scalable, and user-friendly tools that can effectively protect sensitive data without compromising the performance and flexibility that make cloud computing so attractive.

3. Methodologies

This study uses a comprehensive method that combines two approaches: a thorough analysis of existing scientific publications (a systematic review of the literature) and the study of real cases of data leaks. This allows us to compare the theoretical knowledge gained in the academic environment with practical experience based on recent incidents in the field of cybersecurity. We strive to identify common patterns, evaluate the practical effectiveness of modern security measures, and learn from real-world security incidents to improve existing practices.

3.1. Systematic Literature Review (SLR)

A systematic literature Review (SLR) was conducted by searching leading academic databases (IEEE Xplore, ScienceDirect, SpringerLink, Google Scholar) using keywords such as ”cloud storage security,” ”encryption,” ”authentication,” ”access control,” ”data integrity,” and ”cloud leaks.” Each selected article has been carefully analyzed to identify risks, solutions, and best practices in the field of cloud security.

The data obtained was divided into two categories:

- Technical mechanisms (encryption, access control, authentication).
- Organizational measures (compliance with rules, trust management, user awareness).

This structure enabled a comparative synthesis of how both technical and human factors shape cloud security outcomes.

3.2. Detailed Real-World Incident Analysis

To complement insights from the literature, I also examined recent real-world data breaches reported by reputable cybersecurity news sources. These cases provide practical insight into how cloud security challenges appear in real organizational contexts.

As an example, let us look into another Amazon data leak related to the MOVEit file transfer vulnerability, which Techinformed reported in 2024. Employee information, including phone numbers and email addresses, was compromised in an incident involving a third-party property management service provider used by Amazon. This case demonstrated how dependence on third parties can lead to indirect vulnerabilities, even though personal financial information was not disclosed.

The hack occurred due to a vulnerability in the MOVEit software, which was discovered in 2023 and provided hackers with access to private information bypassing authentication. This vulnerability has been exploited worldwide, affecting major companies such as Canada Post, HP, and HSBC.

According to experts, such incidents highlight the growing danger of attacks on software supply chains, in which vulnerabilities in supplier systems endanger secure infrastructure. Many of the problems mentioned in the literature are reflected in the Amazon example, especially the difficulties with risk management by third-party companies.

4. Results

The results presented in this section are derived from our systematic literature review (SLR) conducted in Section II, specifically synthesizing the findings of the technical and organizational mechanisms and structured to directly answer the three research questions posed in the introduction:

 doi:10.20944/preprints202511.1778.v1

1. How effective are modern approaches to ensuring confidentiality and accessibility?

Modern security methods are very effective in theory, but how well they work in real life depends on balancing security needs with how fast and easy they are to use. The ultimate test is whether they successfully meet the goals of Confidentiality, Integrity, and Availability (CIA) [4] .

A. Keeping Data Private (Confidentiality)

The research review confirms that client-side encryption is the main technical tool for keeping data private, especially when you don't fully trust the cloud provider (CSP) [3]. Modern encryption goes beyond basic scrambling:

- **Advanced Encryption:** Homomorphic Encryption represents the best possible way to keep secrets because it theoretically allows the cloud to perform complex computations or mathematical operations on encrypted data without ever having to decrypt or view the original file. This is often considered the "holy grail" of cloud privacy, as it completely separates the data's utility from its visibility. However, the research shows that HE is currently too complex and computationally expensive to be used widely in large-scale cloud environments due to significant performance overhead. While promising for future adoption, the practicality of HE is still limited [8] [6].
- **Secure Searchable Encryption (SSE):** Since traditional encryption makes core cloud functions like searching and indexing extremely difficult, SSE is considered a highly effective and practical compromise. It allows users to search files that are still encrypted without revealing the search query or the content of the files to the cloud provider. This solves the crucial problem of maintaining data usability while ensuring strong confidentiality, a key balance for effective cloud security. Different SSE schemes, such as those based on trapdoors or index structures, are constantly being refined to improve efficiency and maintain privacy [8] [2] [9].
- **Adaptive Access Control:** To manage exactly who can see protected information, new methods such as Attribute-Based Access Control (ABAC) work really well. Instead of easier Role-Based Access Control (RBAC), which just looks at a user's job or set position, ABAC uses changing details like where the user is, when they're trying to get in, what kind of device they're using, or certain details about the information to make a very exact choice about who gets access based on the situation. This level of detail is very important for company cloud setups where private information is used by different groups that have different security levels and needs depending on the situation. [10].

B. Keeping Data Correct and Available (Integrity and Accessibility)

Data must be correct and always available, despite the risk of system failures. This is mostly secured using special checks:

- **Verifiable Proofs:** Tools like Proofs of Retrievability (PoR) let clients remotely verify that their data is stored correctly, has not been tampered with, and is fully accessible without the massive overhead of having to download the entire file for verification. This is critical for achieving accountability and ensuring the CSP adheres to its promises regarding data durability. Different PoR mechanisms, such as those based on erasure codes and homomorphic tokens, are used to guarantee that the client can efficiently audit the remote data state [4] [7] [11].
- **Enforceable Accountability:** The technical proofs have a major organizational and legal benefit: systems like CloudProof allow users to not only detect when their data has been compromised (integrity violation) but also to generate verifiable cryptographic evidence of the violation that can be presented to a third party or a court. This evidence is crucial for making security promises official, legally binding parts of the Service Level Agreements (SLAs). By transforming security from a matter of blind trust into one of clear, contractually enforceable accountability, these mechanisms fundamentally change the relationship between the client and the CSP [10].

 doi:10.20944/preprints202511.1778.v1

2. What disadvantages still remain when used in real-world conditions?

Even with great theoretical tools, research and real-world incidents show ongoing problems that hurt security in daily use.

A. Slowdowns and High Cost

The biggest downside is the speed and money required for strong security:

- **Performance Slowdowns:** It's very hard to achieve all three CIA goals at once. Making data more private with encryption often slows the system down, which reduces availability. Rigorous verification systems add a noticeable delay (latency) to reading and writing files, around a 15 percent overhead [10]. This slowdown is a major issue for big companies that handle huge amounts of data [8].
- **High Redundancy Costs:** To make sure data is always available, service companies use many backup systems, such as automatic saving, spreading data across locations, and copying data to different data storage buildings. While this backup system works well to lower risks from broken machines or area problems (like the one Amazon had), it means users have to pay more money [12].Users usually have to pay for double or triple the storage space to make sure there are enough backup systems, which is a real money problem, even though it is something they must pay to keep data safe and keep their businesses running.

B. Usability, Complexity, and Outside Risks

Human factors and a complex security perimeter are bigger problems than technical flaws:

- **Key Management is Too Hard:** Taking care of the secret cryptographic keys that scramble data on the user's end is a very hard task for the user to handle. This difficulty makes security much worse since people may try to make things easier, which means they might use simple passwords, not change codes regularly, or keep codes where they are not safe. This shows a key idea: if a security system is too hard to use right, people—who are the easiest to trick—will be taken advantage of, and the whole security setup will not work. Handling codes well is still a big issue that needs special, focused programs. [2] [1]
- **Supply Chain Risks:** The real-life incident analysis of the MOVEit flaw shows a crucial outside risk: relying on software from third-party vendors creates security holes that are outside the cloud provider's main control. This shows a big gap in the shared responsibility model [6].
- **Website Configuration Risks:** A less obvious, but growing, risk comes from websites that allow users to upload files directly into cloud storage via loosely configured API integrations. This proves that the way a website's developers configure the communication and authorization pathways with the cloud storage service can introduce substantial security risks that the cloud provider might not even be aware of, or responsible for, under the shared responsibility model. These misconfigurations can inadvertently expose user files or allow unauthorized access [7].

C. Trust and Legal Issues

The non-technical problems center on lack of control and conflicting rules:

- **Loss of Trust:** Giving up direct control means users have to trust the provider's employees, which brings the risk of insider misuse. When major outages occur, this loss of trust puts the entire idea of cloud computing into doubt [11] [1].
- **Conflicting Laws:** Because cloud data can be stored in many places around the world, it is subject to different laws and rules (like GDPR). Navigating these conflicting legal frameworks remains a tough and costly disadvantage for global companies [12].

3. How can users and providers collaborate to provide better protection without compromising usability?

Overcoming residual disadvantages requires a paradigm shift towards a collaborative security model that emphasizes shared responsibility, verifiable assurance, and usability-driven design.

 doi:10.20944/preprints202511.1778.v1

A. Policy and Trust-Building Initiatives

Teamwork must start with clear rules and verifiable proof:

- **Clear Shared Responsibility:** Working together goes smoothly when everyone knows what they need to take care of. Cloud companies handle keeping the cloud safe (like the buildings, main software, and computer security). But, people using the cloud need to protect things like sorting data, coding, managing keys, who can access what, and keeping online traffic safe. These differences should be explained and set in the service agreements. The cloud company has to be open about how they keep things secure, check security often, and have easy-to-understand contracts for fixing problems. This separation helps make sure things are watched over and lowers the chance of security holes happening because people don't understand.[11].
- **Standardized Accountability:** Trust in the provider's security statements must be supported by technical and measurable guarantees. It is no longer enough to require customers to have blind faith; providers must cooperate, allowing customers to ensure that their data is intact, properly stored and processed in accordance with the Service Level Agreement. The literature suggests using technical verification tools to back up service contracts. Solutions such as CloudProof, for example, are designed to allow customers not only to detect integrity and availability violations, but also to generate cryptographically sound evidence of these violations, which can be presented to a third party or an auditor. This evidence-based system is crucial for ensuring accountability, as it holds suppliers accountable for their service guarantees and provides customers with a specific mechanism to take legal action. This verifiable guarantee transforms the relationship between the user and the service provider from a passive trust into an active, visible partnership based on the integrity of the data and the conformity of the services provided. [10] [4].
- **Global Standardization:** To ensure the scalability of the security system and simplify global operations, different countries and regions need to work together to standardize data protection rules. The existing system of diverse regulations (such as GDPR, HIPAA and various national standards) creates significant difficulties for both suppliers and users. Policy makers and regulators were strongly encouraged to develop standardized pan-regional cloud strategies that would guarantee users adequate protection while promoting innovation. The alignment of security protocols and compliance allows vendors to create universally secure systems, reducing transaction costs and complexity, as well as ensuring the protection of user data regardless of their geographical location.[12].

B. Making Security Simple (Usability-Focused Technical Design)

Providers must help by making strong security features easy to use so people don't try to bypass them:

- **Simplifying Key Management:** The most important job for providers is to hide the complexity of key management from the user. They must design user-friendly tools that manage the keys automatically and securely in the background. This removes the main reason why users compromise their own security [2] [8].
- **Adaptive Authentication:** Collaboration on login security means using systems like Adaptive MFA. Instead of asking for a complex login every time, this system only increases security checks (like asking for a code) when the access attempt seems risky (like logging in from a new country). This keeps security strong while making the user experience easier [10].
- **User-centered security dashboards and feedback systems:** If everyone is going to help with security, people need to easily understand the dangers they face. Companies work together to create security tools that change hard-to-understand computer data and danger scores into easy-to-read signals like "green, yellow, red." Instead of saying there is a problem with the firewall, the system might say: "Your Project X sharing options let too many people in. You need to: only let people on the team see it." This removes confusing computer words, makes it easier

 doi:10.20944/preprints202511.1778.v1

to understand and allows the user to fix settings, which is usually why cloud systems fail[6]. This change from just telling people about problems to helping them fix things makes the user go from someone who is helpless to someone who actively helps with security.

- **Simplified and decentralized access control (attribute-based encryption - ABE):** Everyone knows that controlling who can see a certain file, called access control, is not easy. Ways to share, such as attribute-based encryption (ABE), make working together easier. ABE lets the user set rules for who can see something based on what they are like (for example, ”Anyone who is a”manager”” and works in”HR”can open this file”). When the user locks the file, they set the rule once and a trusted person gives out the key to open it based on what the user is like right now, not just a list of names. This makes things much easier for the user — they don’t have to control lots of different keys or change lists every time someone on the team changes jobs; the system handles access automatically, which makes it easier to use and manage.

5. Conclusions

The study shows that keeping data safe in the cloud is a hard job, and it needs both tech skills and people to understand it. New tools like keeping data secret, managing who can see it, and checking things seem good when planned, but real events show that mistakes, system problems, and flaws in other programs can still put data at risk. The study also makes clear that keeping things safe is not just up to cloud companies; users must carefully handle their passwords and secret codes, and also follow the safety rules.

At the same time, being easy to use is really important. If a safety plan is too hard to use, it might cause errors or people to avoid safety steps, which then makes the whole system less safe. Simple rules, being clear, and splitting up responsibilities between sellers and users are key for building trust and ensuring data is always easy to get access to. In the end, following laws and rules is a top priority, especially when data is kept in different countries.

The findings also point out that both those who use and those who offer services must pay attention, as dangers become more complex each year. This implies that safety measures need to be refreshed often, and staff need continuous learning to keep away from basic yet damaging errors. Simple talking between cloud firms and those who use them also matters a lot, as it stops misunderstanding about where each side’s safety roles stop and the other’s start. Moreover, carefully following global rules and how data is managed is very important, most of all when information goes across countries and different legal areas. This shared method, mixing strong tech with a plain awareness of what people do, is key for keeping confidence and ensuring data stays safe and easy to get to. To sum up, this study shows that cloud safety is a team effort that joins tech, smart rules, and working together to protect private information while keeping systems useful and easy to use.

References

1. Vurukonda, N., and Rao, B. T., “A Study on Data Storage Security Issues in Cloud Computing,” *Procedia Computer Science*, Vol. 92, 2016, pp. 128–135. https://doi.org/https://doi.org/10.1016/j.procs.2016.07.335, URL https://www.sciencedirect.com/science/article/pii/S1877050916315812, 2nd International Conference on Intelligent Computing, Communication & Convergence, ICCC 2016, 24-25 January 2016, Bhubaneswar, Odisha, India.
2. Kumar, P. R., Raj, P. H., and Jelciana, P., “Exploring Data Security Issues and Solutions in Cloud Computing,” *Procedia Computer Science*, Vol. 125, 2018, pp. 691–697. https://doi.org/https://doi.org/10.1016/j.procs.2017.12.089, URL https://www.sciencedirect.com/science/article/pii/S1877050917328570, the 6th International Conference on Smart Computing and Communications.
3. Huang, C.-T., Huang, L., Qin, Z., Yuan, H., Zhou, L., Varadharajan, V., and Kuo, C.-C. J., “Survey on securing data storage in the cloud,” *APSIPA Transactions on Signal and Information Processing*, Vol. 3, 2014, p. e7. https://doi.org/10.1017/ATSIP.2014.6.
4. Mohanty, S., Ganguly, M., and Pattnaik, P. K., “CIA triad for achieving accountability in cloud computing environment,” *International Journal of Computer Science and Mobile Applications*, Vol. 6, No. 3, 2018, pp. 38–43.

 doi:10.20944/preprints202511.1778.v1

5. Gulbarga, M. I., and SAYYID, M., "ALATOO ACADEMIC STUDIES," *ALATOO ACADEMIC STUDIES* Учредители: Международный университет Ала-Тоо, , No. 4, 2021, pp. 344–354. https://doi.org/10.17015/aas.2021.214.40.
6. Dilworth, R., "Cloud Computing and Security: An Overview of Vulnerabilities, Cyber Attacks, and AI-Driven Solutions," *Proceedings of the 2024 7th Artificial Intelligence and Cloud Computing Conference*, Association for Computing Machinery, New York, NY, USA, 2025, pp. 615–626. https://doi.org/10.1145/3719384.3719473, URL https://doi.org/10.1145/3719384.3719473.
7. Chen, Y., Li, Y., Lu, Y., Pan, Z., Chen, Y., Ji, S., Chen, Y., Li, Y., and Shen, Y., "Understanding the Security Risks of Websites Using Cloud Storage for Direct User File Uploads," *IEEE Transactions on Information Forensics and Security*, Vol. 20, 2025, pp. 2677–2692. https://doi.org/10.1109/TIFS.2025.3544082.
8. Gupta, I., Singh, A. K., Lee, C.-N., and Buyya, R., "Secure Data Storage and Sharing Techniques for Data Protection in Cloud Environments: A Systematic Review, Analysis, and Future Directions," *IEEE Access*, Vol. 10, 2022, pp. 71247–71277. https://doi.org/10.1109/ACCESS.2022.3188110.
9. Kirubakaramoorthi, R., Arivazhagan, D., and Helen, D., "Survey on encryption techniques used to secure cloud storage system," *Indian J. Sci. Technol*, Vol. 8, No. 36, 2015, pp. 1–7.
10. Popa, R. A., Lorch, J. R., Molnar, D., Wang, H. J., and Zhuang, L., "Enabling security in cloud storage {SLAs} with {CloudProof}," *2011 USENIX Annual Technical Conference (USENIX ATC 11)*, 2011.
11. Yang, P., Xiong, N., and Ren, J., "Data Security and Privacy Protection for Cloud Storage: A Survey," *IEEE Access*, Vol. 8, 2020, pp. 131723–131740. https://doi.org/10.1109/ACCESS.2020.3009876.
12. Nayak, D., "Understanding the Security, Privacy and Trust Challenges of Cloud Computing," *Journal of Cyber Security and Mobility*, Vol. 1, No. 2-3, 2012, pp. 277–288.