International Science and Technology Journal
المجلة الدولية للعلوم والتقنية

Volume 37 العدد
Part 1 المجلد

http://www.doi.org/10.62341/aajs3208

Received	**2025/07/28**	**تم استلام الورقة العلمية في**
Accepted	**2025/08/22**	**تم قبول الورقة العلمية في**
Published	**2025/08/24**	**تم نشر الورقة العلمية في**

A Multi-Layered Framework for Enhancing Data Security in Cloud Storage Using Authentication, Encryption, and Integrity Verification

[1]*Alsbara Alasmar Rafea, Jameelah Salam Shuayb[2]

[1]Department of computer Science, Faculty of Science and Arta– Qaminis, University of Benghazi, Benghazi, Libya
[2]Department of computer Technologies Engineering, College of Science and Technology of Qaminis, Libya
*motherstwins2013@gmail.com, Jameelahfathi22@gmail.com

Abstract

Cloud computing has recently played an increasingly important role in the information technology (IT) industry due to its enhanced performance, wide accessibility, low cost, and many other benefits. It provides vast data storage and faster processing for various users over the Internet. Data security in the cloud remains a major ongoing challenge that limits the widespread deployment of cloud computing. The problem addressed in this research is how to enhance data storage security in cloud computing through multiple methods to provide trustworthy and secure cloud data storage services. This study proposes a framework for data security designed to protect data through a combination of double authentication for appropriate data classification and encryption, as well as digital signature verification to ensure data integrity during transmission and retrieval. he Message Authentication Code ensures data integrity during transmission. The proposed framework integrates various techniques and specialized procedures to protect data end-to-end, from the data owner to the cloud and ultimately to the user. The framework employs triple-layer authentication to ensure secure access at all stages: by the user the data owner and the cloud service.

Keywords: Cloud Storage, Encryption Message Authentication Code, Data Classification, Data Retrieval, Public Access, Private Access, Limited Access.

http://www.doi.org/10.62341/aajs3208

إطار متعدد الطبقات لتعزيز أمان البيانات في التخزين السحابي باستخدام المصادقة والتشفير والتحقق من السلامة

الصابرة الأسمر رافع *[1]، جميلة سالم شعيب [2]

قسم علوم الحاسوب، كلية تكنولوجيا الحاسوب – قمينس، جامعة بنغازي ليبيا

قسم هندسة تقنيات الحاسوب، كلية العلوم والتكنولوجيا – قمينس، ليبيا

[1]*motherstwins2013@gmail.com
Jameelahfathi22@gmail.com

ملخص

أصبحت الحوسبة السحابية مؤخرًا تلعب دورًا متزايد الأهمية في صناعة تكنولوجيا المعلومات(IT) وذلك لما توفره من أداء محسّن، وسهولة في الوصول وتكلفة منخفضة والعديد من المزايا الأخرى. فهي توفر سعة تخزين ضخمة ومعالجة أسرع للبيانات لمختلف المستخدمين عبر الإنترنت ومع ذلك، تظل أمان البيانات في البيئة السحابية تحديًا رئيسيًا يعيق الانتشار الواسع للحوسبة السحابية تتناول هذه الدراسة مشكلة تعزيز أمان تخزين البيانات في الحوسبة السحابية من خلال عدة أساليب، بهدف تقديم خدمات تخزين بيانات موثوقة وآمنة. تقترح الدراسة إطار عمل لحماية البيانات يعتمد على المصادقة المزدوجة لتصنيف البيانات بشكل مناسب وتشفيرها إلى جانب التحقق من التوقيع الرقمي لضمان سلامة البينات اثناء النقل والاسترجاع يعتمد النظام على كود تحقق من الرسائل (Message Authentication Code) للتأكد من تسليم البيانات دون أي تغيير أو تعديل. يدمج الإطار المقترح بين تقنيات وإجراءات متخصصة لحماية البيانات من البداية إلى النهاية، بدءًا من مالك البيانات مرورًا بالسحابة وصولا إلى المستخدم النهائي يتم تحقيق مستوى عالٍ من الأمان من خلال المصادقة المزدوجة: واحدة من قبل المستخدم، وأخرى من قبل المالك، وثالثة من قبل مزود الخدمة السحابية. من شأن هذا النهج أن يعزز أداء تخزين البيانات في السحابة، خاصة في مواجهة قضايا مثل تسريب البيانات، والتلاعب بها، والوصول غير المصرح به حتى من قبل مزود الخدمة السحابية نفسه.

الكلمات المفتاحية :التخزين السحابي، التشفير، كود تحقق الرسائل، تصنيف البيانات، استرجاع البيانات، الوصول العام، الوصول الخاص، الوصول المحدود.

http://www.doi.org/10.62341/aajs3208

1. Introduction

Cloud computing provides an opportunity for both large-scale enterprises and small businesses to benefit from internet-based services, helping them lower initial investments, cut down on capital costs, and enabling end-users to access services based on a pay-as-you-go model. This allows users to scale their application usage dynamically depending on their operational needs either increasing or decreasing capacity as required (Rountree, 2014). Nevertheless, security concerns remain one of the most critical barriers to the widespread adoption and trust in cloud computing systems. Specifically, issues such as data ownership, privacy assurance, data portability, service level agreements (SLAs), and data confidentiality represent key challenges that hinder the optimal implementation of cloud environments (Krutz, 2010; Zissis, 2012). In recent years, numerous research efforts have aimed to alleviate and resolve the existing security vulnerabilities in cloud computing, in hopes of establishing cloud-based systems as secure, virtual, and cost-effective IT solutions for the future (Subashini, 2011; Chen, 2010). From the end-user's perspective, privacy and data protection remain major concerns and the primary reason behind the reluctance to adopt cloud technologies. Cloud computing has become increasingly significant across various sectors such as education, banking, and healthcare, among others. It delivers a wide range of advantages, including enhanced resource utilization and reduced expenditure on hardware and personnel. Recent studies indicate that cloud adoption can decrease IT operational costs by 30% to 50% Despite the considerable research progress made in cloud security, these concerns continue to persist. Therefore, additional efforts and innovations are necessary to reach a mature and trustworthy level of security in cloud computing infrastructures.

This study aims to investigate and propose an enhanced security framework for cloud computing that specifically addresses unresolved issues related to data protection, privacy, and secure service delivery. Although multiple solutions have been developed in the past, a comprehensive approach that integrates authentication, encryption, and robust SLA compliance mechanisms remains lacking. This research seeks to fill that gap by introducing a multi-layered model that not only enhances data confidentiality but also ensures system integrity and user trust in dynamic cloud environments.

http://www.doi.org/10.62341/aajs3208

Services Provided by Cloud

Figure.1 Cloud Service Types. The cloud computing provides services according to the following levels: Infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS). (Armbrust et al., 2010; Mell & Grance, 2010)

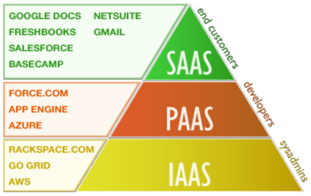

Figure 1. Cloud Service Types

System design

A basic design from through the development and evaluation of a new. Show Figure.2 System Architecture of Proposed Secure Data Cloud Computing Proposal approach as follow:

Phase 1: Identification of the problem domain

Phase 2: Identification of the possible solution approaches

Phase 3: Performance evaluation (Chen, Paxson & Katz, 2010;

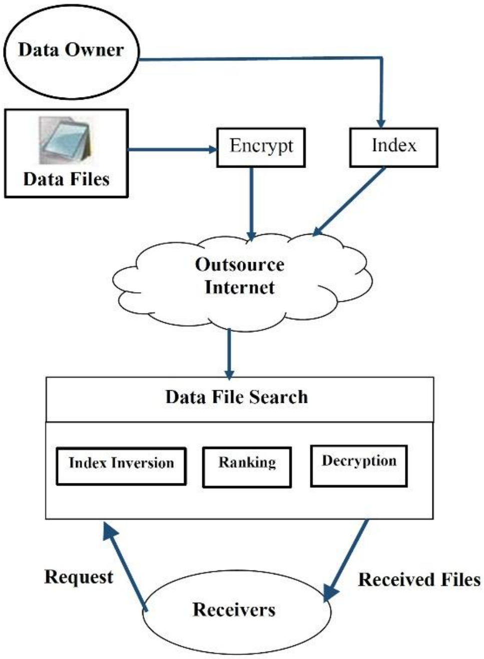

Figure. 2 System Architecture of Proposed Secure Data Cloud Computing Proposal

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

http://www.doi.org/10.62341/aajs3208

Types of Cloud Computing Deployment:

public Cloud: This model is available for use by the general public and is managed by third-party providers. (Carroll, Van Der Merwe & Kotze, 2011)

Private Cloud: Designed for the exclusive use of a specific organization, typically involving several internal users or departments. Figure 3 illustrates the difference between public cloud and private cloud. (Popović & Hocenski, 2010)

Hybrid Cloud: A combination of both public and private cloud infrastructures, allowing data and applications to be shared between them (Sultan, 2010)

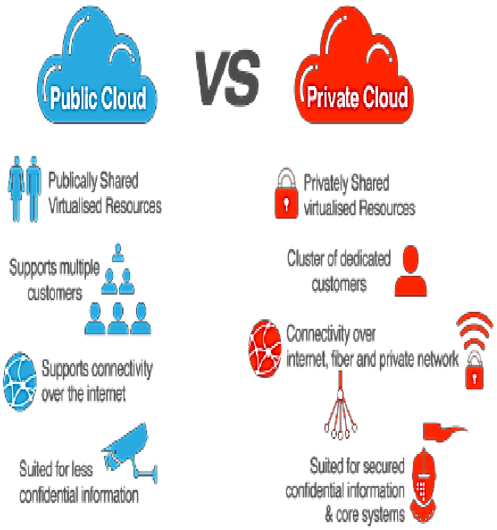
Public Cloud
VS
Private Cloud
Publically Shared Virtualised Resources
Supports multiple customers
Supports connectivity over the internet
Suited for less confidential information
Privately Shared virtualised Resources
Cluster of dedicated customers
Connectivity over internet, fiber and private network
Suited for secured confidential information & core systems

Figure 3. Public Cloud vs. Private Cloud

Methodology

The combined approach of Message Authentication Code (MAC) based data storage and the key-based data retrieval is proposed. The systematic architecture of proposed work is illustrated. Figure 4. structure of the proposed Combined Approach of Data Security. (Kalpana & Singaraju, 2012; Arockiam & Monikandan, 2013)

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

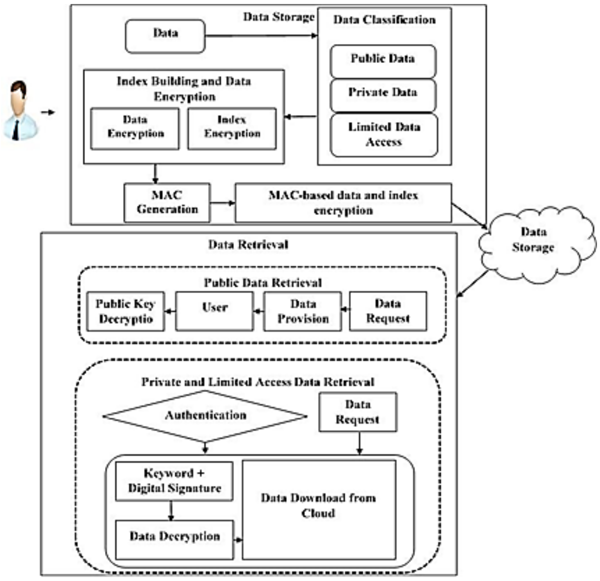

Figure 4. Structure of the proposed Combined Approach of Data Security.

Flowchart of Data Storage Security in Cloud Computing

A seeing in Figure 5 Flowchart of Data Storage Security. The diagram illustrates the logical sequence of the connection between different processes to reach to high level of security of the proposed hybrid secure data storage cloud computing solution.

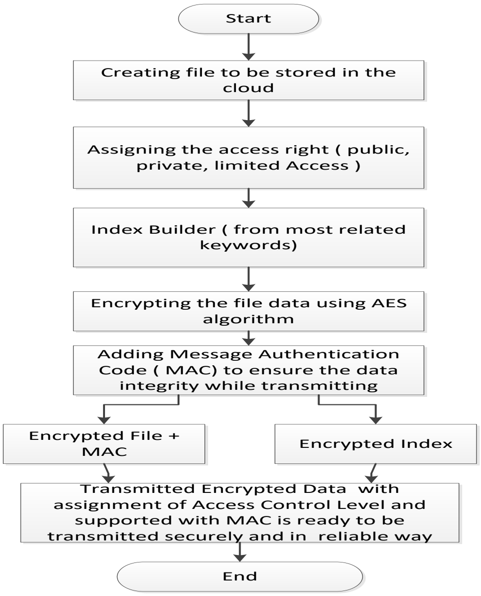
Start
Creating file to be stored in the cloud
Assigning the access right (public, private, limited Access)
Index Builder (from most related keywords)
Encrypting the file data using AES algorithm
Adding Message Authentication Code (MAC) to ensure the data integrity while transmitting
Encrypted File + MAC
Encrypted Index
Transmitted Encrypted Data with assignment of Access Control Level and supported with MAC is ready to be transmitted securely and in reliable way
End

Figure 5. Flowchart of Data Storage Security

Copyright © ISTJ
حقوق الطبع محفوظة
للمجلة الدولية للعلوم والتقنية

http://www.doi.org/10.62341/aajs3208

Data Storage in the cloud

The initial stage in the proposed framework involves storing user-submitted data in the cloud. This process incorporates a range of specialized techniques and mechanisms, including Message Authentication Codes (MAC), index construction, and encryption, before the data is actually stored. Kuyoro, Ibikunle & Awodele, 2011; Kaufman, 2009) Accordingly, this section is divided into three sub-sections, each describing the steps involved in detail.

Data Classification

Confidentiality:

This refers to the level of privacy required at each stage of data handling and processing. (Juels & Kaliski, 2007; Li et al., 2012).

Availability:

This considers how frequently the data is accessed and how promptly it must be made available when requested (Juels & Kaliski, 2007; Li et al., 2012).

Integrity:

Refers to the precision and trustworthiness of data, as well as its resilience against unauthorized access or modification. (Juels & Kaliski, 2007; Li et al., 2012).

Sensitivity rating (SR)

A metric used to evaluate the level of sensitivity of the data. (Juels & Kaliski, 2007; Li et al., 2012).

Formula.

$$SR[i] = (C[i] + \left(\frac{10}{A[i]}\right) + I[i])/2$$

Index construction and Encryption

Data and indexing are secured using 128-bit SSL encryption (Li, Tan, Chen, Wong & Xhafa, 2015), which is implemented through a specific encryption function. Figure 6: Index Builder and MAC-based data storage in cloud R, F represents the original file, F'' denotes the encrypted version of the file, 2 is the encryption key applied during the process.

http://www.doi.org/10.62341/aajs3208

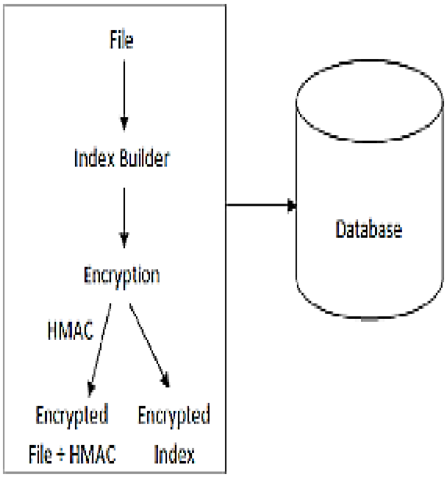

Figure 6: Index Builder and MAC-based data storage in cloud R

Message Authentication Code (MAC)

The Message Authentication Code (MAC) process involves three fundamental cryptographic algorithms:

- **Key Generation (G):** In this phase, a key is randomly selected from the key space using a uniform distribution, ensuring unpredictability and security.
- **Signing Algorithm (S):** This component generates a unique tag by processing the message and the key together. The resulting tag is used to authenticate the message.
- **Verification Algorithm (V):** This algorithm checks the integrity and authenticity of the message by validating the tag against the given key. If the message and tag are found to be untampered, the verification is successful; otherwise, the message is considered invalid. MACs are typically created using cryptographic checksums, providing a secure way to confirm data integrity and authenticity.

$$MAC = C(K, M)$$

Where:

K – Key
M – Message
C – Cryptographic checksum.

http://www.doi.org/10.62341/aajs3208

Data Retrieval Process

Once data is securely stored in the cloud environment, the retrieval phase involves several essential steps to ensure authorized access and data integrity (Wang, Chow, Li & Li, 2013). These steps include:

- User Registration
- Access Request Generation
- Authentication Procedure
- File Retrieval Operation

Implementation Environment

To evaluate and validate the proposed secure data storage and retrieval framework in cloud computing, a controlled experimental environment was established. The implementation was carried out using Python (Zissis & Lekkas, 2012; Xiao & Xiao, 2013) 3.10 and Java for backend operations including encryption, decryption, and Message Authentication Code (MAC) generation. For the cloud environment simulation, Amazon Web Services (AWS S3) and Google Cloud Platform (GCP) were used to replicate real-world cloud storage scenarios. The cryptographic modules were integrated using libraries such as Crypto, OpenSSL, and Bouncy Castle. The frontend interface was built using HTML5, CSS3, and JavaScript, providing user registration, file upload, and retrieval functionalities. The data used for testing included both real-world documents (text and PDF) and synthetically generated datasets with varying sensitivity levels to evaluate confidentiality, integrity, and availability parameters. The simulation was conducted on a 64-bit Windows 10 machine with Intel Core i7 processor, 16 GB RAM, and stable internet connectivity. Performance metrics such as encryption time, retrieval latency, and integrity validation accuracy were monitored using Wireshark and JMeter tools to ensure comprehensive assessment of the system's security and efficiency.

Security Scenarios

This section analyzes possible security weaknesses that can result in security gaps, such as unauthorized access, alteration of transmitted data, or removal of access privileges that make the data unmanageable or difficult to control. The validation of data throughout the transmission process is a major stage in assuring the effectiveness of the proposed hybrid approaches. During transmission, data is vulnerable to several threats including leakage, modification, privacy breaches, and loss of confidentiality

http://www.doi.org/10.62341/aajs3208

Security Gap: Unauthorized Server Scenario

When data is transmitted to the cloud over a network, attackers may impersonate a legitimate cloud server, leading to data loss or interception. To mitigate this, the proposed system integrates SSL certification and the involvement of trusted Certificate Authorities (CA) before data transmission. This ensures that both the file index and stored files remain encrypted and that the server's authenticity is verified before communication begins.

Limitation & Applicability:

This approach relies heavily on the CA's trustworthiness and may not be suitable in environments where CA compromise or certificate mismanagement is possible (e.g., certain low-regulation regions or private, closed networks without robust PKI infrastructure).

Security Gap: Tampering Scenario

Tampering refers to the unauthorized modification of data during transmission. Even with encryption and SSL in place, sophisticated attackers may attempt to alter data packets. The proposed work addresses this by using MAC (Message Authentication Code) based encryption and decryption.

- The data owner generates a MAC for the original file.
- The MAC is transmitted along with the encrypted file.
- The receiver regenerates the MAC for the received file and compares it with the original to verify integrity

Limitation & Applicability:

The method is effective for detecting changes but does not prevent data modification attempts themselves. In environments with unstable or high-latency networks, MAC verification might introduce processing overhead that affects performance.

Security Gap: CSP Threat Scenario

If a CSP behaves maliciously or acts without the owner's consent, the owner may lose control over the data, increasing the risk of leakage. In the proposed work, this is mitigated through:

Encryption of cloud data storage so the CSP cannot read the raw content. SSL certificate generation to secure private communications over public networks, granting read access only to authorized key holders.

http://www.doi.org/10.62341/aajs3208

Limitation & Applicability:

While encryption prevents unauthorized reading, it does not stop the CSP from deleting data or refusing service. This solution is most applicable in commercial public-cloud settings where encryption can be integrated, but less effective in jurisdictions where CSPs can be compelled to hand over encryption keys.

Security Gap: Loss of User Identity and Password

If a user’s identity and password are lost or exposed, the security of stored data is at risk. The proposed system adds an extra layer of authentication through security questions, allowing better distinction between authorized and unauthorized users.

Limitation & Applicability

Security questions can be guessed or socially engineered, especially if answers are based on publicly available information. This method is better suited for personal or small-business environments but should be paired with multi-factor authentication (MFA) for high-security applications.

Results and Analysis

The implementation of security measures including Message Authentication Codes (MAC), data classification, indexing and encryption is evaluated with results presented in Figure 7. The comparison demonstrates that while MAC and classification offer a baseline level of security, indexing and encryption significantly enhance the overall protection of cloud-stored data. These results support our initial hypothesis that combining MAC with classification and encryption enhances performance while reducing latency. The improved security is achieved without sacrificing computational efficiency, which confirms the feasibility of integrating multiple layers of protection in a scalable cloud environment.

Figure 8 compares the time efficiency between the existing scalable Identity-Based Encryption (IBE) scheme proposed by Boldyreva, Goyal, and Kumar (BGK) which incorporates revocation through Key Generation Center (KGC) broadcasts and the newly proposed method. The evaluation, using $\log_2 N$ to represent the number of users, shows that the proposed approach incurs a lower time cost, indicating improved scalability and responsiveness.

This finding aligns with the study’s hypothesis that the proposed revocation mechanism would outperform traditional BGK models in terms of time efficiency, particularly in large-scale systems. It confirms that optimizing revocation through the proposed method yields substantial performance gains in cloud-based identity management.

Figure 9 assesses the system's performance in verifying both the cloud audit and storage servers. The x-axis represents the scale of the system (parameter s), while the y-axis shows the corresponding time cost in milliseconds. The results reveal an increase in the time cost on the storage server due to the computational effort required for exponentiations across each data block's tag.

These results validate the hypothesis that while verification introduces some overhead, particularly on the storage server, it remains within an acceptable range for large-scale deployments. The tradeoff between auditability and time cost remains favorable when compared to systems lacking verification capabilities.

Figure 10 illustrates the time involved in both complete and lazy revocation processes across varying data sizes. The findings suggest that the proposed technique yields superior performance in terms of both efficiency and effectiveness.

This confirms the study's hypothesis that implementing lazy revocation can significantly reduce operational overhead without compromising data consistency or user revocation integrity. It also highlights the technique's suitability for dynamic environments where frequent user changes occur.

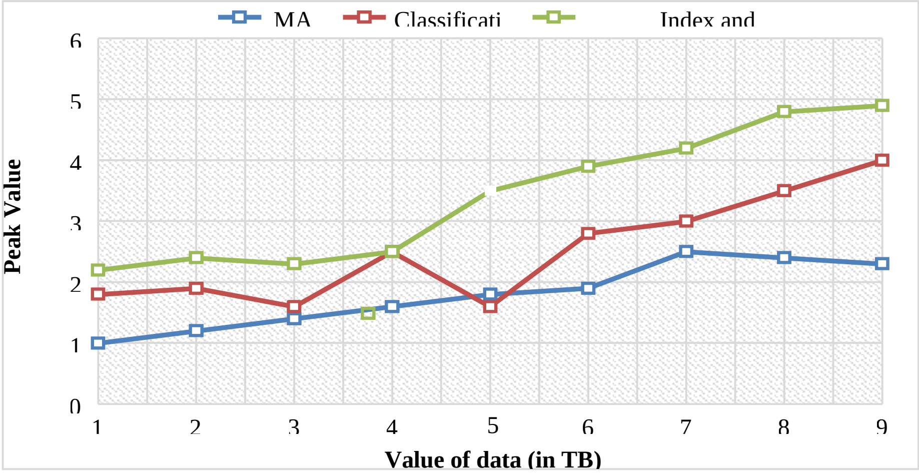

Figure 7. Security evaluation

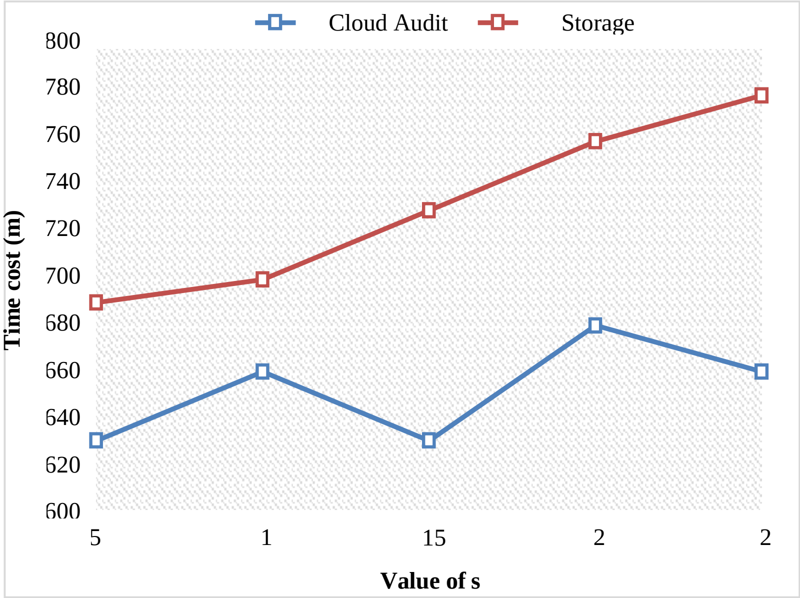

Figure 8. Time cost of existing and proposed techniques

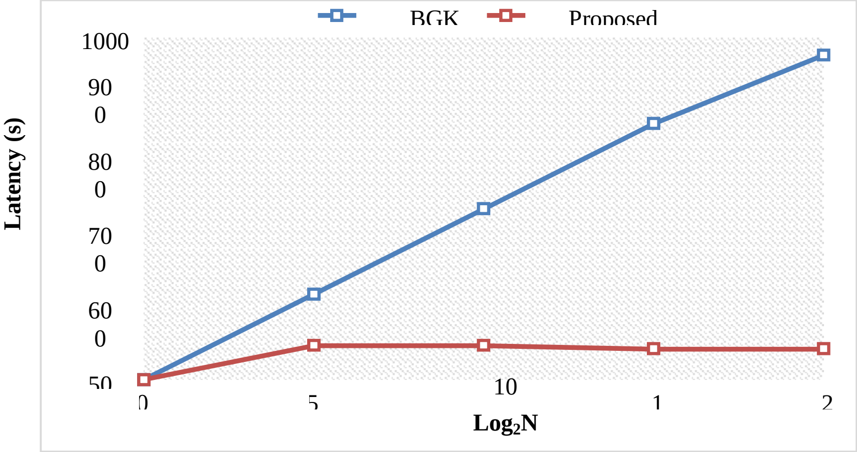

Figure 9 Verification Tim

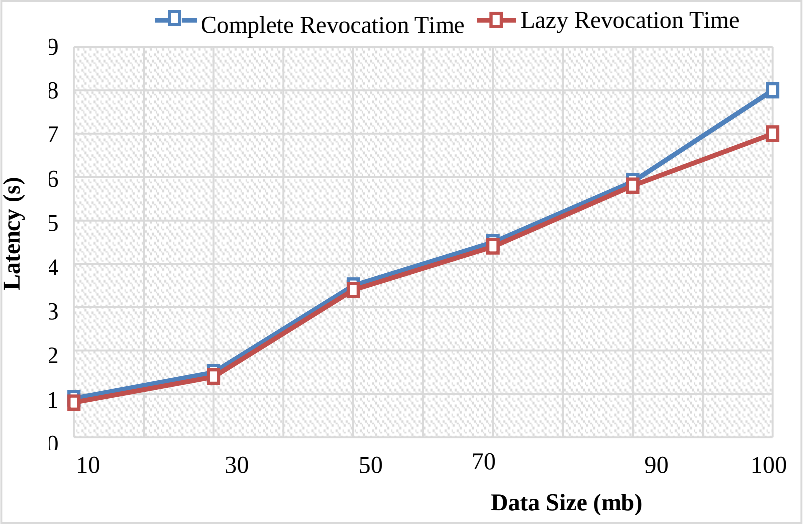

Figure 10. Execution time

Conclusion

A novel data security framework has been developed for cloud computing that enhances protection through the integration of dual authentication and digital signature verification. This framework incorporates a range of advanced techniques and specialized procedures to ensure end-to-end data security. A key feature of the system is its implementation of dual authentication, which significantly strengthens the protection of cloud storage against various threats.

The proposed approach effectively mitigates several critical issues, including data leakage, unauthorized access, and data tampering. Based on the analysis conducted, the framework demonstrates strong capabilities in verifying data integrity and user authentication. Performance evaluation has been carried out using metrics such as peak value, processing time, latency, and private key size. The results indicate that the proposed method outperforms existing techniques across these parameters.

Recommendations.

It is recommended that future work explore the adoption of more robust and diverse encryption algorithms tailored to the dynamic

http://www.doi.org/10.62341/aajs3208

nature of data storage and retrieval in contemporary cloud computing environments.

Future Work

Future research could extend this work by addressing more advanced and diverse encryption algorithms, tailored to the varying types of data stored and retrieved in modern cloud computing environments.

References

[1] Armbrust, M., et al. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50–58.
[2] Mell, P., & Grance, T. (2010). The NIST definition of cloud computing. National Institute of Standards and Technology.
[3] Rountree, D. (2014). Cloud computing: Implementation, management, and security. CRC Press.
[4] Krutz, R. L., & Vines, R. D. (2010). Cloud security: A comprehensive guide to secure cloud computing. Wiley.
[5] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.
[6] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11.
[7] Chen, Y., Paxson, V., & Katz, R. H. (2010). What's new about cloud computing security?. Technical Report, EECS Department, University of California, Berkeley.
[8] Carroll, M., Van Der Merwe, A., & Kotzé, P. (2011). Secure cloud computing: Benefits, risks and controls. 2011 Information Security South Africa (ISSA). IEEE.
[9] Popović, K., & Hocenski, Ž. (2010). Cloud computing security issues and challenges. MIPRO 2010, 344–349.
[10] Sultan, N. (2010). Cloud computing for education: A new dawn?. International Journal of Information Management, 30(2), 109–116.
[11] Kalpana, P., & Singaraju, S. V. (2012). Data security in cloud computing using RSA algorithm. International Journal of Research in Computer and Communication Technology, 1(4), 143–146.
[12] Arockiam, L., & Monikandan, S. (2013). Efficient cloud storage confidentiality to ensure data security. International Journal of Computer Applications, 62(10), 0975–8887.

http://www.doi.org/10.62341/aajs3208

[13] Kuyoro, S. O., Ibikunle, F., & Awodele, O. (2011). Cloud computing security issues and challenges. International Journal of Computer Networks, 3(5), 247–255.

[14] Kaufman, L. (2009). Data security in the world of cloud computing. IEEE Security & Privacy, 7(4), 61–64.

[15] Juels, A., & Kaliski, B. S. (2007). Pors: Proofs of retrievability for large files. Proceedings of the 14th ACM Conference on Computer and Communications Security.

[16] Li, J., Wang, Q., Wang, C., Cao, N., Ren, K., & Lou, W. (2012). Fuzzy keyword search over encrypted data in cloud computing. Proceedings IEEE INFOCOM, 441–445.

[17] Li, J., Tan, Y., Chen, X., Wong, D. S., & Xhafa, F. (2015). Effective authentication for mobile devices using cloud-assisted biometric data. Future Generation Computer Systems, 49, 26–37.

[18] Engels, D., Fan, K., Gong, G., Hu, H., & Smith, E. M. (2011). Ultralightweight cryptography for low-cost RFID tags: Hummingbird algorithm and protocol. IACR Cryptology ePrint Archive, 2011, 173.

[19] Wang, C., Chow, S. S., Li, Q., & Li, K. (2013). Privacy-preserving public auditing for secure cloud storage. IEEE Transactions on Computers, 62(2), 362–375.

[20] Xiao, Z., & Xiao, Y. (2013). Security and privacy in cloud computing. IEEE Communications Surveys & Tutorials, 15(2), 843–859.