International Journal of Academic Information Systems Research (IJAISR)
ISSN: 2643-9026
Vol. 10 Issue 5 May - 2026, Pages: 1-4

Encryption Based on Multilevel Security for Cloud Computing

Masoud Isa Masoud Alagha, Dr. Ahmed Y. Mahmoud

Faculty of Engineering & Information Technology Al-Azhar University-Gaza, Palestine masoud2agha@gmail.com

Abstract: *Cloud computing has become one of the fastest growing fields in Information and Communication Technologies. One of the major challenges in the cloud today is data security in cloud storage, as the cloud can be risky because of the use of the Internet by cloud-based services, which means less control over the stored data. In this paper, we proposed a model to overcome some of the cloud computing security problems related to the client side by using* ***encryption based on multilevel security.*** *The proposed model is implemented using the AES encryption algorithm and Bell-LaPadula model. The data is classified to the following levels: Confidential (C), Secret (S), and Top Secret (TS) according to data sensitivity and importance. The model was implemented using Amazon Web Services (RDS) and Oracle Database, demonstrating that the combination of encryption and multilevel security effectively increases the difficulty for attackers to expose or disclose stored data.*

Keywords—*Cloud Computing; Cryptography; Multilevel Security; Amazon Web Services; Database Security; AES; Bell-LaPadula.*

I. INTRODUCTION

Cloud computing is considered a new technology that moves the computation process from desktop computers to cloud providers through the Internet [1]. This technology decreases the computation cost and makes organizations focus on their businesses. The environment of the cloud is considered public in nature, which requires data security solutions to be protected.

One of the largest security problems that the cloud faces is that the user's data are potentially available to both the hosting agency and hackers [2]. For this reason, security measures must be added to protect data in the cloud. There are many security challenges facing cloud computing security; the important challenge is data protection — how to protect data which places critical information in the hands of a third party. To achieve a solution to this challenge, the data must be encrypted [3].

The second challenge is access control: limiting access to data and monitoring who accesses it, in order to avoid unauthorized access to systems and protect organizational assets. Various access control models and policies have been developed such as Mandatory Access Control (MAC) and Discretionary Access Control (DAC). MAC is defined as Multilevel Security (MLS) [4].

In this paper, we propose a model using the combination of encryption and multilevel security to provide a solution that protects data from any malicious or insider threat. The proposed model is implemented using the AES encryption algorithm and Bell-LaPadula model on Amazon Web Services (RDS) with Oracle Database [5].

II. RELATED WORK

Chakraborty and Roy [6] concentrated on checking and understanding cloud security issues by proposing cryptographic algorithms and powerful measures to guarantee information security in cloud. Different encryption algorithms were discussed along with security aspects of cryptography.

Sara et al. [7] proposed a new idea that gives a higher security level to cloud services. The proposed system depends on a mix of the idea of multilevel security (MLS) and multilevel authentication. The system consists of three levels of security from lowest to highest.

Jeet and Prashant [8] proposed a way to provide data security and data integrity in the cloud. Their approach encrypts the local file using AES-256 encryption algorithm and creates metadata of that file for integrity verification using SHA256.

Alotaibi and Roussinov [9] discussed many security issues related with cloud computing technology and the techniques to protect data in the cloud, finding issues that influence confidentiality, integrity, and availability of data.

Faragallah et al. [10] introduced the concept of multilevel security in the relational database, giving a complete view of an encryption-based multilevel security database model which is a combination of multilevel security for the relational database and encryption system.

Baghel and Theng [11] proposed and implemented data storage security in the cloud environment using Kerberos as a third-party auditor, the RSA algorithm for secure communication, and MD5 for data integrity.

Recent advances include Abualkas and Bhaskari [12], who proposed a hybrid ECC-AES approach for cloud storage combining efficient key management with role-based access control. Zhu et al. [13] presented a dynamic AES encryption system combined with Blockchain-based key management for cloud data security (IEEE Access, 2024), demonstrating the current trend toward adaptive, data-aware encryption frameworks.

III. BACKGROUND

A. AES Encryption Algorithm

In cryptography, the Advanced Encryption Standard (AES) [14] is one of the symmetric-key encryption algorithms. Each of the ciphers has a 128-bit block size and having key sizes of 128-bit, 192-bit and 256 bits. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Table I shows the differences between AES types.

TABLE I: DIFFERENCES BETWEEN AES TYPES

AES Type	Key Length (bits)	Block Size (bits)	Rounds
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

B. Multilevel Security and Bell-LaPadula Model

Multilevel Security (MLS) [15] is the system that confirms that a user only obtains the information at or below its level — the user reads the information at or below its level and can write at its level. The Bell-LaPadula model is the basic model that illustrates the concept of multilevel security. This model depends on definitions of objects and subjects.

Every object is assigned to a security level (classification), and every subject is assigned to a security level (clearance). Bell-LaPadula rules are described as follows:

• The simple property (No Read Up): A subject is allowed to read an object if the subject's security clearance level is greater than or equal to the object's security classification level.

• The star property (No Write Down): A subject is allowed to write to an object if the object's security classification level is greater than or equal to the subject's security clearance level.

• Strong star property: A subject is allowed to write to an object if the subject's security clearance level is equal to the object's security classification level.

C. Cloud Computing

Cloud computing [16] is a model for convenient, on-demand network access to a shared pool of configurable computing resources (networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. There are several service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Deployment models include Public Cloud, Private Cloud, and Hybrid Cloud.

One of the major security issues in the cloud is data protection. Since the user's data is placed in the hands of a third party (cloud provider), it is essential to ensure the security of data. To achieve this, the data must be encrypted at rest and in transit [17].

IV. PROPOSED MODEL AND METHODOLOGY

The methodology used in this paper depends on storing data securely at rest in the cloud database. To achieve this objective, we proposed a new model based on encryption and multilevel security. We used Amazon Web Services (RDS) and chose Oracle as a relational database management system.

The proposed model is divided into three parts:

• **Security level (1) — Confidential (C):** Data is encrypted using AES-128 algorithm.

• **Security level (2) — Secret (S):** Data is encrypted using AES-192 algorithm.

• **Security level (3) — Top Secret (TS):** Data is encrypted using AES-256 algorithm.

Table II shows the mapping between data classification levels, encryption algorithms, and the user clearance required to access each level.

TABLE II: DATA CLASSIFICATION AND ENCRYPTION MAPPING

Level	Class.	Algorithm	User Clearance
0	Unclassified	None	Any User
1	Confidential (C)	AES-128	C or above
2	Secret (S)	AES-192	S or above
3	Top Secret (TS)	AES-256	TS only

The proposed model workflow is as follows. The user enters their username and password. After credential validation, the system checks the clearance level. If the clearance level is below C, only unclassified data is visible. If clearance equals C, unclassified data is shown and C-level data is decrypted using AES-128. If clearance equals S, C and S level data are decrypted using AES-128 and AES-192 respectively. Otherwise (TS clearance), all data including TS-level is decrypted using AES-128, AES-192, and AES- 256.

A. AES Algorithm Selection

The choice of AES is dedicated to the following factors [14]: it is not reported to be vulnerable to any known attack; it uses higher length key sizes (128, 192, and 256 bits), making it more strong against attacks; it is implemented in both hardware and software; and it is the most widely used security protocol. Using AES-128 requires 2^128 attempts to break, making it very hard to penetrate.

B. Amazon Web Services (AWS)

Amazon Web Services (AWS) is a cloud computing platform from Amazon that provides customers with many types of cloud services including EC2, Amazon S3, and Amazon Relational Database Service (Amazon RDS) [18]. RDS is a relational database service that supports Oracle, SQL Server, and MySQL. Amazon automatically backs up the databases every 24 hours, with a maximum retention

period of 35 days.

V. IMPLEMENTATION

The implementation was carried out from two sides: the cloud provider side using Amazon Web Services (AWS) with RDS, and the client side using Oracle Forms Developer Suite 10g, SQL*Plus Release 11.1.0.6.0, and SQL Developer.

A. Database Design

Three tables were created on Amazon RDS Oracle Database version 11.2 using Oracle SQL Developer:

• Employee table (EMP): Contains fields for employee number, name, salary, and other data. Each field has a corresponding classification field (0=Unclassified, 1=Confidential, 2=Secret, 3=Top Secret).

• Multilevel Security table (MULTI_LEVEL): Contains the classification number and classification name.

• Users table (USERS): Contains User_ID, User_Name, Password, and Clearance_User fields.

B. AES Functions

Six AES functions were created within the Oracle database using PL/SQL:

AES-128 encryption, AES-128 decryption, AES-192 encryption, AES-192 decryption, AES-256 encryption, and AES-256 decryption. These functions are called at data insertion time to encrypt fields according to their classification level, and at query time to decrypt fields based on the user's clearance level.

C. Application Forms

Three application forms were designed using Oracle Forms Developer Suite 10g:

Insert Form: Allows insertion of sample data with field-level classification. Each field is individually classified, and the corresponding AES function encrypts the data before storing it in Amazon Cloud.

Login Form: The user enters their username and password to access the application. Credentials are validated against the USERS table.

Main Form: Allows the user to query and update data according to their clearance level. Fields with higher classification than the user's clearance appear with null values, and an access denial message is displayed according to the No-Read-Up rule.

VI. RESULTS AND DISCUSSION

The proposed model was tested with sample employee data classified at different levels. The results confirm that the model enhances security due to the combination of encryption and multilevel security (TS, S, C). The encryption quality depends on the used encryption algorithm.

A user with Top Secret (TS) clearance can view and decrypt all data across all classification levels. A user with Secret (S) clearance can view unclassified, Confidential, and Secret data, but TS-level fields appear as null. A user with Confidential (C) clearance can only view unclassified and Confidential data. Users below Confidential level can only view unclassified data.

The encrypted data is stored on Amazon RDS in ciphertext form. Even if an attacker gains direct access to the database, the data remains protected by AES encryption. The combination of field-level classification with user clearance enforcement through the Bell-LaPadula rules provides a layered security approach that significantly reduces the risk of unauthorized data exposure [11][13].

TABLE III: COMPARISON WITH RELATED APPROACHES

Work	Encrypt.	MLS	Cloud	Class.
Chakraborty [6]	Yes	No	Yes	No
Sara et al. [7]	No	Yes	Yes	Part.
Faragallah [10]	Yes	Yes	No	Yes
Baghel [11]	RSA	No	Yes	No
Abualkas [12]	ECC	No	Yes	No
Proposed	AES	Yes	Yes	Yes

VII. CONCLUSION AND FUTURE WORK

In this paper, we proposed a model for securely storing data in the cloud to protect it from malicious attacks. We used encryption based on multilevel security to increase security and make it difficult for attackers to expose data. We used the AES algorithm for data encryption and the Bell-LaPadula model for multilevel security, depending on the clearance of users and the classification of data based on sensitivity (Top Secret, Secret, and Confidential). The model was implemented using Amazon Cloud (RDS) and Oracle tools.

As a final conclusion, the proposed model enhances the security due to the combination of encryption and multilevel security. The encryption quality depends on the used encryption algorithm. The results indicate that the model increases security and makes it difficult for attackers to expose or disclose data.

The work can be extended to use multilevel authentication to increase the security of the approach. The future work will provide an additional layer of security: the user at level (C) has a single textual password; the user at level (S) has two passwords (textual and biometric); and the user at level (TS) has three passwords (textual, biometric, and image sequencing). Additionally, integration with Blockchain-based key management [13] represents a promising direction for securing the encryption keys themselves in cloud environments.

ACKNOWLEDGMENT

The authors would like to express their deepest gratitude to Dr. Ahmed Y. Mahmoud for his excellent

guidance, patience, and support throughout this research. This work is dedicated to the Palestinian people.

REFERENCES

[1] J. W. Rittinghouse and J. F. Ransome, Cloud Computing: Implementation, Management, and Security. CRC Press, 2016.

[2] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[3] S. Shweta, N. Tabrez, and S. Ankita, "Cloud computing: Security issues and solution," International Journal of Computational Intelligence Research, vol. 13, no. 6, 2017.

[4] S. Bawan and T. Deepti, "Multilevel security model for cloud third-party authentication," in Emerging Research in Computing, Information, Communication and Applications. Springer, 2016.

[5] Gururaj R., Mohsin I., and Farrukh A., "A comprehensive survey on security in cloud computing," Procedia Computer Science, vol. 110, pp. 465-472, 2017.

[6] R. Chakraborty and S. Roy, "Cryptography in cloud computing: A basic approach to ensure security in cloud," International Journal of Engineering Science and Computing, vol. 7, no. 5, 2017.

[7] S. Almutairi, A. Younas, and M. Binsawad, "Multilevel authentication scheme for cloud computing," International Journal of Grid and Distributed Computing, vol. 9, no. 9, pp. 205-212, 2016.

[8] J. Vora and P. Mehta, "Providing confidentiality and integrity on data stored in cloud," International Journal of Advance Research in Engineering, Science & Technology, vol. 4, no. 5, 2017.

[9] S. Alotaibi and W. Roussinov, "Data security, privacy, availability and integrity in cloud computing," International Journal of Advanced Computer Science and Applications, vol. 7, no. 4, 2016.

[10] O. S. Faragallah, E. M. El-Rabaie, F. E. Abd El-Samie, A. I. Sallam, and H. S. El-Sayed, Multilevel Security of Relational Databases. CRC Group, 2015.

[11] S. Baghel and D. Theng, "Multilevel security model for cloud third-party authentication," in Emerging Research in Computing, Information, Communication and Applications. Springer, 2016.

[12] Y. M. A. Abualkas and L. Bhaskari, "Hybrid approach to cloud storage security using ECC-AES encryption and key management techniques," International Journal of Engineering Trends and Technology, 2024.

[13] M. Y. Zhu et al., "Dynamic AES encryption and blockchain key management: A novel solution for cloud data security," IEEE Access, vol. 12, pp. 26334-26343, 2024. doi: 10.1109/ACCESS.2024.3351119.

[14] M. Gupta, S. Mathur, and A. Pandey, "Implementation of 128, 192 & 256 bits advanced encryption standard on reconfigurable logic," International Journal of Engineering Trends and Technology, vol. 50, no. 6, 2017.

[15] W. Stallings and L. Brown, Computer Security: Principles and Practice, 3rd ed. Pearson, 2015.

[16] P. Mell and T. Grance, "The NIST definition of cloud computing," NIST Special Publication 800-145, 2011.

[17] Z. Ghanbari, "A literature review on cloud computing security issues," International Journal of Information, Security and Systems Management, vol. 6, no. 1, 2017.

[18] Amazon Web Services, AWS Whitepapers. [Online]. Available: https://aws.amazon.com/whitepapers, 2018.

[19] S. Bauskar, "Advanced encryption techniques for enhancing data security in cloud computing environment," SSRN Preprint, 2023. doi: 10.2139/ssrn.4987321.

[20] B. Balamurugan et al., "Scalable and secure access control policy for healthcare system using blockchain and enhanced Bell-LaPadula model," Journal of Ambient Intelligence and Humanized Computing, Springer, 2020. doi: 10.1007/s12652-020-02346-8.