Performance Evaluation of Cryptographic Security Algorithms on Cloud

Madhavi Karanam[1*], *Sahithi* Reddy S[1], *Abhinav* Chakilam[1], and *Srinu* Banothu[2]

[1]Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad, India.
[2]Department of Computer Science and Engineering, Vignan Institute of Technology and Science, Hyderabad, India.

Abstract. Cloud computing is a cost-effective approach to provide on demand computing and data storage solutions. Data storage is one of the key services provided by the cloud. Cloud offers improved efficiency, flexibility, and scalability, but all these advantages can be overturned if security is not taken into consideration. It is the cloud vender's responsibility to keep the data safe with highly secure cloud services, which helps them earn the trust of the customers. Today, cloud security is critical since most organizations are already using cloud computing in alternate forms. There is always a concern that the highly sensitive business information and intellectual property may be exposed or misused due to increasingly sophisticated cyber threats. This research paper provides a distributed architecture for cloud data security which is independent of the underlying platforms. A cloud security architecture provides written and visual model to define how to configure and secure operations within the cloud. This paper compares the performance of RC4 against AES-256. The performance of the proposed encryption algorithms is evaluated on a widely used database MySQL. This paper provides a better solution to ensure the security of cloud databases by using two encryption algorithms.

1 Introduction

Cloud computing is a technology that provides remote services on internet to store, manage, and access data online. It is a cost-effective method as it reduces the cost and maintenance burden on the user. There are various types of services provided by the cloud such as Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), Database-as-a-Service (DaaS). In SaaS, the host provides the user with a fully functional application hosted in a cloud and accessible through web browser or mobile application.

[*] Corresponding author: bmadhaviranjan@yahoo.com

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

In PaaS, the host provides the user with a platform or a framework where they can develop, run, and maintain their own applications, without having to build the whole infrastructure. And in IaaS, the host provides the user with cloud-hosted resources, such as storage space and virtualization. DaaS provides data storage services where the user can store the data and files on the internet through a cloud provider. The user can access the stored data from anywhere anytime on any device connected to internet. The storage is scalable, durable, and easily accessible. Cloud storage is cost effective, users can pay only for what they use. They can scale up the storage as and when the requirement grows.

This study examines the issue of data security in cloud data storage. A client or customer that has a database outsources it to a cloud service provider and has faith in them to protect their data. The client is constantly worried about the integrity and confidentiality of their data. It is the duty of cloud service providers to prevent data loss and misuse due to security flaws and unauthorised access. Techniques for data distribution and data encryption can assure the security of the data. The performance of two widely used database encryption algorithms, RC4 and AES-256, is examined in this research. The MySQL server is used to implement the algorithm. Both database encryption and decryption techniques effectiveness is assessed. The database is divided vertically into two or more parts with columns and kept in various databases on the same cloud server. The same database is used for both the RC4 and AES-256 algorithms. By doing this, the database's security is improved because the data is spread and encrypted concurrently. As the data is spread over numerous databases rather than just one, the risks of a data breach and misuse are greatly decreased. Additionally, the databases' security is increased via encryption.

2 Related Work

Poonam Jindal and Brahmjit Singh [1] studied about the RC4 encryption algorithm. RC4 is considered as simple, fast and efficient algorithm. The paper demonstrates a survey which includes the cryptanalysis of RC4 stream cipher including its weaknesses such as key collisions, biased bytes, and key recovery attacks specifically on WEP and WPA. RC4 is largely deployed in wireless network and internet protocols. Future scope is to investigate the issues in RC4 such as the non-random behaviour of bytes in the state permutation, and to develop a new, more efficient and effective RC4 encryption algorithm.

Scott Fluhrer, Itsik Mantin and Adi Shamir [2] presented several weaknesses in the key scheduling algorithm of RC4 and described their cryptanalytic significance. There are large number of weak keys but a small number of key bits are enough to determine many state and output bits with non-negligible probability. These weak keys are used to construct new variants for RC4 to overcome related key attacks with practical complexities. It concludes that RC4 is insecure in a common mode of operation which is used in the widely deployed Wired Equivalent Privacy protocol. It fixes secret key along with known IV modifiers in order to encrypt different messages. The paper elaborates on the invariance weakness and provides various approaches to overcome it. It presents various theorems and their contributions.

An approach to execute SQL queries over encrypted data was presented in [3]. The main security issue addressed here is when the provider is not completely trustable with the security of the data. They implemented as many queries and possible without having to decrypt the data at the provider's site. Decryption and query processing was done only at the client's site. An algebraic frame work is presented to split the query and minimize the computation for the client. The paper explains the partition functions and identification functions to access the data. The SQL query is split into two parts, the server query, and the client query. Thus, partial execution of the query takes place at the provider end without decryption and sent to the client. The correct result is obtained by decrypting the data using the client query at the client's site. This way the privacy of the client can be maintained.

Various encryption algorithms in SQL server were presented by Sourav Mukherjee [4]. It analyses which algorithm best suits for the given requirement. The data security playing a crucial role in the paper, it explores the trends and possibilities to provide the best possible security. Various encryption tools are used to for various types of data systems and environments. Choosing the right methods is necessary in order to safeguard the data. The study provides a detailed explanation of various combinations and their results.

Ahmed Albugmi, Madini O. Alassafi, Robert John Walters and Gary Wills [5] presented security of data in cloud services. Different aspects related the cloud security are discussed. Paper also gives information about commonly various methods to ensure maximum protection and security of the data. Various approaches to reduce risks and threats are also described. Cloud is a widely used technology with great benefits but the security of the data stores is at risk. The data is exposed to third parties and is vulnerable. The data may be at risk when a guest OS whose reliability is unknown is run over a hypervisor. The paper also presents data security aspects for both Data-in-Transit and Data-in-Rest. The threats caused in public cloud and multitenancy is also discussed. The paper gives a detailed explanation about the security threats and encryption methodologies to ensure security. An overview of block cipher, stream cipher and hash function are proposed for different types of data at rest and transit.

Ako Muhammad Abdullah [6] presented Advanced Encryption Standard (AES) algorithm for Encryption. Since the exchange of digital data is increasing rapidly, the data must be protected from intrudes and unauthorised access. It is a symmetric block cipher algorithm which is most used for encryption and decryption. It has a unique structure to encrypt and decrypt sensitive data and provide security. It can be applied in both hardware and software. AES is a very reliable algorithm and makes it very difficult for the hacker to get the original data. AES can be performed with three different keys sizes such as AES 128, 192 and 256 bit and each ciphers has 128-bit block size. The paper gives a detailed explanation of the AES encryption algorithm and its structure. The data can be encrypted under different parameters. It presents certain crucial features of AES which makes it a better approach compared to DES, 3DES, Blowfish etc.

The paper proposed by Nishtha Mathur and Rajesh Bansode [7] is a hybrid encryption scheme that combines the Advanced Encryption Standard (AES) with Elliptic Curve Cryptography (ECC) to improve security and performance. The proposed scheme uses AES with a 128-bit key length and 10 iterations, and aims to defend against cache timing attacks by using a combination of public-key and private-key encryption. The goal of the proposed scheme is to increase security and minimize any potential drawbacks of AES or ECC when used alone.

3 Proposed Architecture

Two databases that are hosted in the cloud make up the architecture of the suggested methodology. The raw data is kept in a master database and needs to be divided and encrypted [12]. Using the data security protocols mentioned above, the database's individual records are first encrypted. The master database's encrypted data has now been evenly divided into two different tables. Half of the columns in the actual database are contained in the first table, while the other half are present in the second table. The cloud platform "cloudcluters.io" that allows databases to be hosted in the cloud was used in this implementation. The data is divided and kept in several tables across many databases. The encrypted records from the various databases are concatenated to create the real data record when getting the data from the tables. The record is decrypted and shown to the user after it has been fully fetched from the two cloud databases.

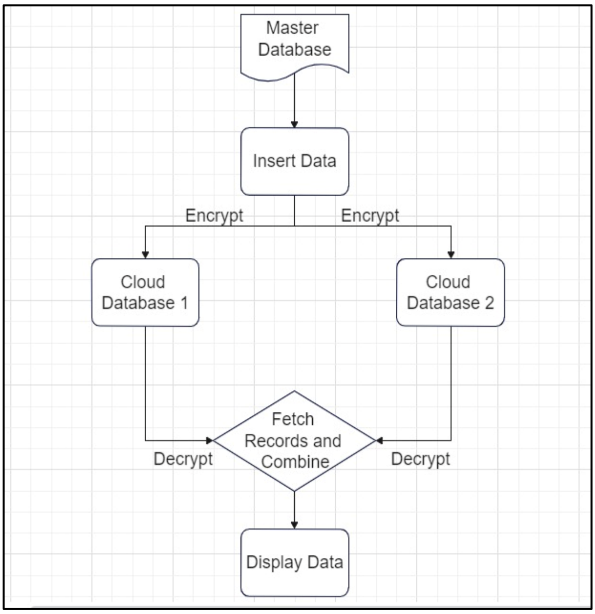


Fig. 1. Architecture of Proposed Methodology

4 Methodology

4.1 *RC4*

A symmetric key stream cypher, also referred to as RC4, is Rivest Cypher 4. Byte by byte, RC4 processes a stream of data. Symmetric key encryption is used. The same key is used for encryption and decryption in symmetric key encryption. Long plain text encryption makes frequent use of RC4. Through S-Box construction, plain text is replaced with the cypher text [8]. RC4 employs a variety of keys, including ones with 64- or 128-bit key widths. RC4 is frequently used in many protocols, including the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols for web communication and the WPA wireless encryption standard. It doesn't take much energy to use RC4.

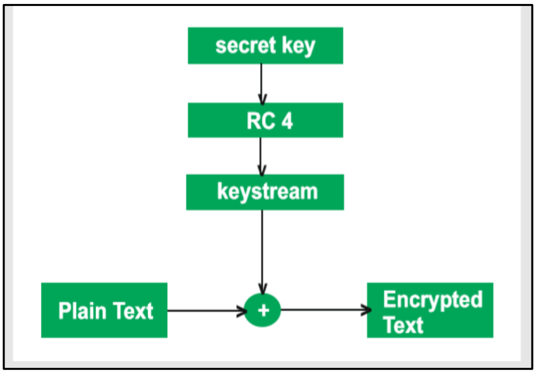


Fig. 2. RC4 Block Diagram [11]

The user enters a secret key and plain text as input. By conducting a bit-wise exclusive-or (XOR) operation on the pseudo-random keystream created by RC4 using a secret key, the plaintext is encrypted. The ciphertext is decrypted using the same keystream and the same XOR technique. Key-scheduling and pseudo-random generation algorithms (KSA and PRGA) are used to create the keystream.

4.1.1 Key scheduling algorithm (KSA)

A variable-length key from 1 to 256 bytes is used to initialize a 256-byte state vector S, with elements S[0] to S[255]. The key-scheduling algorithm (KSA) uses this key to set up the initial state of the algorithm. The key is used to permute the elements in the state vector S in a pseudo-random fashion.

4.1.2 Pseudo-random generation Algorithm (PRGA)

The pseudo-random generation algorithm (PRGA) generates a stream of bytes, one at a time, by selecting one of the 255 entries in S in a systematic fashion, and then permuting the elements in S again. This stream of bytes is then used as the keystream for encryption and decryption by performing a bit-wise exclusive-or (XOR) operation with the plaintext or ciphertext.

ALGORITHM

STEP 1: Plain text and a secret key are given as inputs.

STEP 2: The Keystream is generated using the KSA and PRGA algorithm.

STEP 3: The plain text is XOR with the keystream. This process is done byte by byte and encrypted text is produced.

STEP 4: The encrypted data is sent to the cloud and stored.

STEP 5: The user can access the data whenever required by decrypting the data.

STEP 6: Decryption is done by performing the byte wise X-OR operation on the cipher text to get the original text.

4.2 AES-256

Different countries have chosen the Advanced Encryption Standard (AES), a symmetric block cypher encryption technique, for their data security. A block cypher is AES. AES keys can be 128 bits, 192 bits, or 256 bits in size. It receives input of 128-bit plain text and outputs 128-bit cypher text. The substitution-permutation network idea underlies how AES operates. It is carried out utilising a sequence of interconnected operations. The cypher is formed after the plain text has been changed and mixed internally.

There are three basic components to the AES algorithm. They are Key Expansion, Cypher, and Inverse Cypher. The simple text is altered by cypher into an unintelligible format. At one moment, 128 bits of the input data are processed. A key schedule, which is a collection of derived keys used in the encryption and decryption process, is created during the Key Expansion step. The round function, which consists of the four transformations SubBytes, ShiftRows, MixColumns, and AddRoundKey, is used by both the cypher and the inverse cypher. While ShiftRows and MixColumns randomly shuffle the text, SubBytes perform the substitution [9].

ALGORITHM

STEP 1: Plain text and a secret key are given as inputs.

STEP 2: The Round keys are created.

STEP 3: The plain text is substituted with SubBytes to convert into cipher text.

STEP 4: ShiftRows is done to shift the text multiple times.

STEP 5: Matrix multiplication is done to change the position of each byte within the MixColumns.

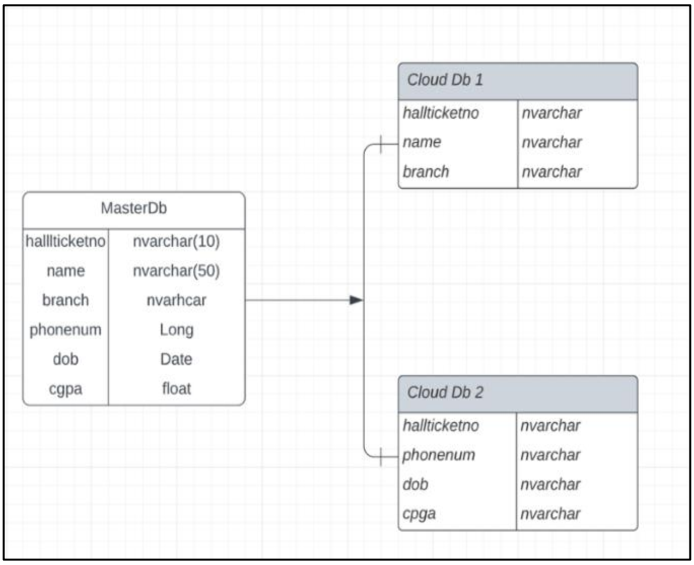
5 Implementation and Results

The proposed methodology is implemented by developing an a program that measures the time taken to encrypt and decrypt the data. The whole program has been written using PHP.

The architecture as mentioned above consists of two cloud databases which are hosted on the cloud. In this application we have used open-source cloud platform called “mycloudcluster.io”. Using this platform there are two database servers hosted in the cloud. The first database consists of a table where half of the columns present in the dataset are encrypted and stored. The remaining columns are encrypted and stored in another database.

The main idea behind using two different databases is to achieve cloud security. Platform independence is another factor which led to usage of two separate databases. The first step is to connect the cloud database to the php program. After a successful connection we retrieve all the data that is stored in the actual existing database. The next step is to encrypt and upload each encrypted record to their respective databases. The splitting of the data is based on sensitivity. The primary key of the database is stored in both the tables as it is later used for retrieving the data. The program also performs the retrieval operation where the actual data of a record is shown. When a query is performed for retrieval the data from each table is combined and decrypted and displayed to the user. The performance of rc4 is evaluated using a function which measures the time to encrypt and upload the data. Another function is also used to measure the time taken to fetch the records.

After we executed the php program, the following results were obtained. A student database of a class is taken and the experiment was performed. The time taken by AES-256 to encrypted and upload database is 19249.11 milliseconds and the time taken by RC4 is 21745.53 milliseconds. The time taken to decrypt the database by AES-256 was 12.23 milliseconds and the time taken by RC4 is 8.44 milliseconds. The results may vary depending on the database. The performance of the algorithms purely depends on the type of data in the table and the size of the database.



Cloud Db 1	
hallticketno	nvarchar
name	nvarchar
branch	nvarchar

MasterDb	
halllticketno	nvarchar(10)
name	nvarchar(50)
branch	nvarhcar
phonenum	Long
dob	Date
cgpa	float

Cloud Db 2	
hallticketno	nvarchar
phonenum	nvarchar
dob	nvarchar
cpga	nvarchar

Fig. 3. Cloud Data schema

6 Conclusion

The commonly used encryption technique RC4 is quick, effective, and easy to use, making it perfect for a variety of applications. Another safe encryption method with strong performance metrics is AES-256. Their layout and security features are different. Both have advantages and disadvantages of their own. According to the findings of this experiment, both encryption techniques require more time to encrypt and upload data than to retrieve and decrypt it. It is evident that RC4 requires more time to upload and encrypt data than AES-256. In contrast, RC4 decryption and retrieval take less time than AES-256. The database being used will have an impact on the outcomes. The conclusion obtained from this experiment is that RC4 is a better algorithm for splitting and encryption of cloud databases. The performance of both methods was compared in this experiment using the same database.

Security algorithms play a crucial role in ensuring the confidentiality, integrity, and availability of sensitive information. These algorithms provide strong protection against unauthorized access, interception, and modification of data. Security algorithms are essential components of modern cryptography for maintaining the security and privacy of sensitive information in various applications, including e-commerce, online banking, and communication systems. Thus, implementing the best cryptography methods available to ensure security is essential. The experiments performed in this paper consist of only two databases. But for larger databases and larger tables the splitting can be done in more than two databases. Many other existing security algorithms can also be tested for performance evaluation.

References

1. Poonam Jindal and Brahmjit Singh, “A Survey on RC4 Stream Cipher”, International Journal of Computer Network and Information Security 7(7):37-45, June 2015.

2. Scott Fluhrer, Itsik Mantin and Adi Shamir. "Weaknesses in the Key Scheduling Algorithm of RC", January 2005.
3. Hakan Hacıgumus , Bala Iyer, Chen Li and Sharad Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model", 2002 ACM SIGMOD International Conference on Management of Data, June 2002.
4. Sourav Mukherjee, "Popular SQL Server Database Encryption Choices", International Journal of Computer Trends and Technology (IJCTT), Volume-**66** Number-1, December 2018.
5. Ahmed Albugmi, Madini O. Alassafi, Robert John Walters and Gary Wills, "Data Security in Cloud Computing", Fifth International Conference on Future Generation Communication Technologies (FGCT), IEEE, Volume: **1**, August 2016.
6. Ako Muhammad Abdullah, "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data", June, 2017.
7. Nishtha Mathur and Rajesh Bansode, "AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection", Procedia Computer Science, Volume **79**, Pages 1036-1043, 2016.
8. Isnar Sumartono, Andysah Putera Utama Siahaan and Nova Mayasari, "An Overview of the RC4 Algorithm", IOSR Journal of Dental and Medical Sciences 18(6):2278-661, December 2016.
9. M.Pitchaiah, Philemon Daniel and Praveen, "Implementation of Advanced Encryption Standard Algorithm", International Journal of Scientific & Engineering Research Volume **3**, Issue 3, 1 ISSN 2229-5518, March 2012.
10. Tharindu Weerasinghe, "An Effective RC4 Stream Cipher", 8th IEEE International Conference on Industrial and Information Systems (ICIIS), December 2013.
11. GeeksforGeeks - RC4 encryption, Updated - October 2021.
12. Srinu Banothu, Govardhan A and Karnam Madhavi, "Performance Evaluation of Cloud Database Security Algorithms", E3S Web Conf. Volume **309**, 2021, 3rd International Conference on Design and Manufacturing Aspects for Sustainable Energy (ICMED-ICMPC 2021), October 2021.
13. Toa Bi Irie Guy-Cedric and Suchithra. R, "A Comparative Study on AES 128 BIT AND AES 256 BIT", International Journal of Scientific Research in Computer Science and Engineering Vol.**6**, Issue.4, pp.30-33, August 2018.
14. Nur Atikah, Mutia Rizky Ashila, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto and Christy Atika Sari, "AES-RC4 Encryption Technique to Improve File Security", Fourth International Conference on Informatics and Computing (ICIC), IEEE, October 2019.
15. Harrison John Bhatti and Babak Bashari Rad, "Databases in Cloud Computing: A Literature Review", International Journal of Information Technology and Computer Science 9(4):9-17, April 2017.
16. Fizza Shahid1, Humaira Ashraf1, Anwar Ghani, 1, Shahbaz Ahmed Khan, Ghayyur1,Shahaboddin Shamshirband 2,And Ely Salwana 3," PSDS–Proficient Security, Over Distributed Storage: A Method for Data Transmission in Cloud" , IEEE Access, VOLUME **8**,Pg.No 118285-118295, 2020.
17. Srinu Banothu, A.Govardhan, Karnam, Madhavi, "Performance Comparison of Cryptographic Algorithms for Data Security in Cloud Computing", Journal of Information and Computational Science, ISSN: 1548-7741, Volume **11** Issue 9 – 2021,Pg. No 1-8.
18. Amjad Alsirhani, Srinivas Sampalli, Peter Bodorik, "Improving Database Security in Cloud Computing by Fragmentation of Data", International Conference on Computer and Applications (ICCA), 978-1-5386-2752-5/17, IEEE, 2017.

19. H. Hacigumus, B. Iyer and S. Mehrotra, "Providing database as a service," Proceedings 18th International Conference on Data Engineering, pp. 29-38, 2002.
20. Elisa Bertino, and Ravi Sandhu, “Database Security—Concepts, Approaches, and Challenges”, IEEE Transactions On Dependable And Secure Computing, VOL. **2**, NO. 1, January-March 2005.