JOURNAL of COMPUTER SCIENCES INSTITUTE

JCSI 26 (2023) 1-6
Received: 10 September 2022
Accepted: 7 November 2022

Augmenting The Cloud Environment Security Through Blockchain Based Hash Algorithms

Ravi Kanth Motupalli[a,*] and Krishna Prasad K.[b]

[a]Research Scholar, Institute of Computer Science & Information Sciences, Srinivas University, Mangalore, Karnataka, India and Assistant Professor, Department of CSE, VNR VJIET, Hyderabad, Telangana, India.
[b]Associate Professor, Institute of Computer Science & Information Sciences, Srinivas University, Mangalore, Karnataka, India.

Abstract
Many techniques and algorithms are developed to enhance the security in the cloud environment. This helps the users to secure their server from malicious attacks. Hence the study and investigation of the performance enhanced security algorithms is a must demanded field in the research industry. When large number users using same server to store their information in cloud environment security is a must needed component to preserve the privacy and confidentiality of every individual user. This can be further strengthened by detecting the attacks in earlier stages and taking countermeasure to prevent the attack. Thus securing the data network without any leakage and loss of the information is a challenging task in the cloud environment. When the attacks or intrusion is detected after the occurrence there may be damage to the data in the form of data damage or theft. Hence it is necessary to predict and detect the attacks before the occurrence to protect the privacy and confidentiality of the user information.

Keywords: Cloud security; Data privacy; Data confidentiality; Hash Algorithm; Substitutional encryption

[*]Corresponding author
Email address: **ravikanth_m@vnrvjiet.in** (Ravi Kanth. M)

©Published under Creative Common License (CC BY-SA v4.0)

1. Introduction

The most preferred technology for the storage of large volumes of data with data privacy and confidentiality is cloud computing. The security risk in the cloud technology may cause collateral damage to the business applications and the numerous number of users. Hence there are many important security policies in the cloud applications like never leaving the cloud server open for other user which may attract the intruders to steal the data, all the security upgrades given by the vendors should be switched in time to prevent risking the data, Basic cyber security steps should be followed to protect the data from user side, use of strong password and efficient password management, Backing up the data to avoid data loss, should not modify the vendor provided permissions, etc.

When a network is designed to protect the user data or host large numbers of users simultaneously, its ability and competence to serve the users is deprived to have an extraordinary approach to its users. Fig.1 illustrates how the cloud environment protects the end user data against the threats and attacks.

It is the responsibility of the cloud service provider to ensure the authentication of the data access through physical path audit controls and the data protection assurance through the strong security algorithms [1]. The data repositories should be consistently watched for their activities and suspicious behaviours. When the service provider provides more services for multiple users there may arise situations where the details about the users will be backed up in the compatible server. During this case it is possible for any user to duplicate the identity of another user [2]. To avoid such damage to the user data two security algorithms using substitution approach and hash algorithm were devised in this study.

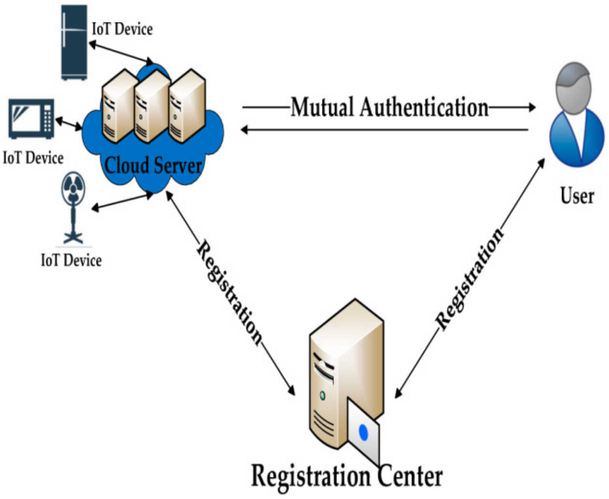

Figure 1: Authentication in Cloud environment.

2. Literature Survey

Many researchers had contributed their study in the cloud security domain. Cloud security involves the confidentiality of the user data and authentication to the user id. It also ensures safety against any type of attacks. Depending upon the applications many type of security algorithms were proposed by different authors and hybrid model of these algorithms were built [3]. Table 1. explains some of the literature work done by different authors on different security algorithm.

When there is any security breach in the cloud server the corresponding counter action should be taken to compensate the attack [4]. Encrypting the original data before transmission is a preferable choice to avoid the theft or data leak. Hence the service distributor should provide a strong security for the authenticated access of the data [5]. Double encrypted algorithm is the advanced version of the authentication algorithm to improvise the secure access [6].

Cloud security assures the susceptible cloud server against any type of attacks and intrusions that leads to the malicious attacks [7]. Hence it is responsibility of the service provider to ensure the secure authentication to the data access and assuring the data confidentiality of the user data. This model proposes a hybrid model of substitution algorithm to provide authenticated access and hash algorithm to protect the data confidentiality and avoid data loss or damage.

Table 1: Literature study on Security algorithms

	Focus/ Constructs	Reference
Cloud computing security algorithms	DES algorithm is the first devised algorithm for encryption. But due to weak cipher this is prone to many attacks	Hui et al,2019[8]; Srisakthi et al, 2020[9].
	The new AES algorithm was devised to tackle the brute force attacks.	Namasudra et al, 2020[10].
	AES algorithm is simple and rapid.	Sivakumar et al,2019[11].
	TDES algorithm is the customized version of the DES for triple protection. But the complexity of this algorithm makes it impossible to implement for larger data.	Gowtham et al,2021[12]; Kumar et al , 2017[13].
	Blowfish algorithm is a 64 bit block cipher algorithm known to be strong against any type of attacks. This algorithm was not patented and is owned by anyone to use in their application.	Yassein et al, 2017[14]; Bhuvaneshwaran et al, 2019[15].
	Homomorphic algorithms make use of two different public and private symmetric keys. Losing any one key may cause loss data in decryption.	Yahyaoui et al, 2018[16].
	RSA algorithm is also a symmetric key algorithm which generates two large prime numbers which are multiplied to produce private and public keys.	Mahmood et al, 2018[17]. Gayatri et al, 2020[18].

2.1. SECURITY CHALLENGES IN CLOUD COMPUTING

In cloud servers many users are being served with different services. Hence there arises many different issues in the security of the cloud server and user data. Data issue is considered as the foremost issue where the service provider is responsible for the confidentiality of the user data in the server [19]. Data audit should be conducted through automated algorithms to ensure the confidentiality of the data by avoiding data breach and data corruption.

Privacy of data is another issue in the cloud servers. More number of users being served at the same instance there is a chance of a data backlog that leads to the cross access of another user's data. In order to avoid this data breach and to maintain data privacy each user access should be verified using a two way authentication approach [20].

Security issue is a must addressable issue that avoids data tampering and data theft. The cloud server should nor be vulnerable to the external attacks and must ensure to detect the data attack at the early stage and avoid data damage or loss [21].

3. Objectives

The main objective of this research is to find an effective security algorithm to protect the data confidentiality and privacy of every individual user in the cloud environment using blockchain based Hash algorithm and to compare the performance analysis of the hash algorithm against the substitution algorithms.

i. The first and foremost objective of this study is to identify the security challenges in the cloud environment.

ii. Designing and developing the computational process for the substitution algorithm and hash algorithm.

iii. Comparing the performance evaluation of the hash algorithm against other substitutional algorithms in terms of time taken for the execution, amount of memory used and the throughput.

4. Proposed Methodology

Many researchers had contributed their study in the cloud

The flow chart representation of the proposed model to authenticate and protect the cloud data is illustrated in the Fig.2. Initially the user is registered to the cloud service provider through an authenticated server. Then the identification of the user was protected using the substitution algorithm. The user data in the cloud network is protected using the secure hashing algorithm. The change in the hash value is monitored to detect the data damage and data loss to secure the data.

4.1. Substitutional Algorithm

Caeser Cipher Substitution algorithm is considered to be the outstanding substitution algorithm in assuring security to the cloud networks. In this method the secret key is always given in numbers and the decrypted format of the cipher text is saved in the cloud server. This method is considered as a conventional and simplest method of encryption. In this encryption technique the shift method is used for the formation of the cipher text.

In the proposed substitutional technique double encryption of the dataset for the enhanced security is done. In order to generate the cipher text an obsessed numerical value is needed, which is termed as the shift value. Based on the numerical value of the shift the alphabets of the cipher are moved exactly shift times to generate the encrypted text.

The encryption equation based on the given shift is formulated as follows:

$$E_i(x) = (x + i)\ mod\ 26 \qquad (1)$$

Where x represents the alphabetic character in the original data and n refers to the shift. Similarly the decryption equation of the cipher text is given as follows:

$$D_i(x) = (x - i)\ mod\ 26 \qquad (2)$$

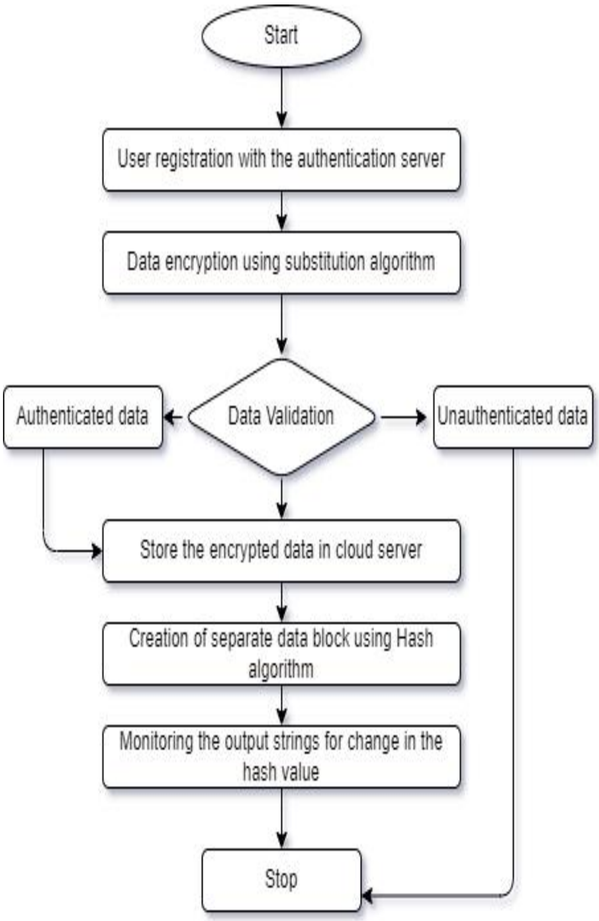
Start
User registration with the authentication server
Data encryption using substitution algorithm
Data Validation
Authenticated data
Unauthenticated data
Store the encrypted data in cloud server
Creation of separate data block using Hash algorithm
Monitoring the output strings for change in the hash value
Stop

Figure 2: Block diagram of the proposed model.

During decryption the alphabets in the cipher text are shifted based on the number of shifts done in the encryption. The steps involved in the double encryption algorithm is explained as follows:

Encryption Algorithm

Step1: *The plain text to be encrypted is obtained from the user.*

Step 2: *The shift number 1 is given as the secret key 1 to the encryption.*

Step 3: *The number of shifts based on the secret key 1 is done to generate the cipher text 1.*

Step 4: *Now for the double encryption secret key 2 is given for the second encryption.*

Step 5: *Cipher text 1 is shifted based on the secret key 2 to generate the cipher text 2, which is the exact cipher text of the double encryption method.*

Decryption Algorithm

Step 1: *Two secret keys 1 and 2 with the known cipher rows are given for the decryption.*

Step 2: *Using secret key 1 first decryption is done and using the secret key 2 second decryption is done.*

Step 3: *The output of the second decryption is the original data given by the user.*

Through the double encryption substitution technique secure user authentication is done with less permutational complexity. This approach produces an output that is impossible to crypt analyse and the method is simple. But the complexity of the proposed substitutional algorithm is higher than the simpler Caesar algorithm with double approach in encryption and decryption. Multiple keys are involved in this procedure which should not be mixed up to produce the original data. In order to ensure the protected authentication in the cloud environment the password of each user is encrypted using the substitutional technique which avoids the storage of the original password in the cloud server.

4.2. HASH ALGORITHM

To protect the data in the cloud server against damage and loss due to malicious attacks and intrusions Hash algorithms are used. In this approach the arbitrary data block of the data set is processed to produce a standard string of the output. With the changes in the hash value damage or data loss can be identified.

There are many secure hashing algorithms which are designed one way to provide strong security. Thus this algorithm is strong enough to detect the intrusion or attack done on the data This algorithm is combined with the block chain technique which generates the hash value to protect the data. The hashing algorithm used in this model is SHA-512. Hash algorithm is notable for exhibiting overwhelming results. The algorithm works on the basic principle of the simpler modification made in the input block creates a complex impact on the output string and the distant blocks produce a comparable hash value. The hashing of the 512 bit block in the input is formulated as follows:

$$Ha(512) = \sum 512 \ \ p(x)(x \, mod \, y) \, (x - i) \qquad (3)$$

Where the Ha(512) represents the hash function of the 512 bit block and the p(x) represents parole with mean y. In this algorithm initially the input block is segregated as the fragments with 1024 bits. 64 bit hash value and the rounding constants are generated. This algorithm comprises 80 iterations where the message array is organized as 80 words, each with 64 bits. The iterating loop is scheduled from the 16th bit to 79th bit. The results and performance analysis of the hash algorithm is discussed in the following section.

5. RESULTS AND DISCUSSION

Cloud computing framework is notable for its harmless yield since its implementation in the market. With the advancing approaches and the technical methodologies the security and authentication of the user data and the user is augmented. Thus the added benefits of the advanced cloud computing servers are the perseverance of the user authentication and data confidentiality.

Cloud encryption by Caesar's algorithm provides an encounter model to the mutual and scheduled architecture which is prone to the security breaches. The Caesar's substitution technique used in the proposed model gives more effective security against two attacks namely dictionary attacks and rainbow attacks. These attacks are made to eavesdrop the data exchange, creating a fake browser and stealing the passwords of the users. When the cloud network is in active state, a protocol analyzer is used in the analysis of the activity of the end users. When the user is vulnerable to any attack the admin of the cloud server alerts the users.

As double key is used in the double encryption based Caesar's cipher method enhanced security is achieved. The processing speed is fast as the technique is not computationally complex, also requires less time to encrypt and decrypt making this as the time consuming algorithm. As the data size of the encrypted cipher is same as that of the original message, lesser storage space is required when compared with the other substitutional techniques. The key exchange process in this technique is simpler without any challenging issues.

The Hash algorithm 512 encryption is used in the cloud server to protect the data. In this model the user data is hashed by the string of hash values. Variance in these values detects the modification or loss of user data and alerts the user for the same. The Hash 512 algorithm proposed in this model highly contributes to the fake browser problems which detects the attacks in the early stage and prevents them. The output parameters of the single key Ceaser model, SHA 512 model and the proposed model are compared in Table 2.

5.1. Execution Time:

A process is defined as the end user application running at the user system which comprises single or multiple executions. The average time taken for the execution of a single process and the amount of energy spent on the execution of the process is calculated to find its efficiency. In the proposed model 1813 kbps of execution speed and 5813 kbps of the application running speed is obtained making it more efficient than the individual models.

5.2. Throughput:

Throughput is the measure of the productivity of the processors responding to any algorithm. It is measured as the amount of data exchanged between the users. The throughput of the file uploading process should be high enough to upload all the data and the throughput of the usage should be small enough to be computationally simple and fast. The proposed model exhibits highest throughput for file upload and lowest for the application usage.

5.3.Memory Utilization:

This denotes the amount of field taken by the respective algorithms to complete their processes.

Table 2: Output attribute comparison

Output Parameters	Caeser's model	SHA 512 model	Proposed model
Execution speed (kbps)	322	1743	1813.45
Application running speed (kbps)	580	632	5813
Throughput (file upload) (kbps)	150	157	194
Throughput (Application Usage)(kbps)	75	62	45
Memory Utilization (kbps)	240	225	180

In comparison with the other model the proposed model take only 180 kbps to complete the execution of the process making this encryption model more effective and rapid enough

6. CONCLUSION

In the communication era huge data are being transacted through cloud servers. All these transactions are demanded to be secure and perfect. To ensure this data security and confidentiality certain security algorithms were developed. In this series, a hybrid algorithm comprising of double encrypting substitutional approach and Hash algorithm is implemented. This algorithm is proved to be more efficient in providing data security and data confidentiality in effective way than the existing algorithms. This algorithm is implemented to prove to overcome the security limitations in the cloud network by suppressing the risks like unauthorized data access, data damage, data theft and data leaks. Thus this study has achieved all the objectives outlined and the comparative analysis done with the existing algorithms proves the same.

References

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, Above the clouds: A berkeley view of cloud computing, Technical Report No. UCB/EECS-2009-28, EECS Department, University of California, Berkeley (2009).

[2] N. Fernando, S.W. Loke, W. Rahayu, Mobile cloud computing: A survey, Future generation computer systems 29(1) (2013) 84-106.

[3] C. Yang, Q. Huang, Z. Li, K. Liu, F. Hu, Big Data and cloud computing: innovation opportunities and challenges, International Journal of Digital Earth 10(1) (2017) 13-53.

[4] S. Subashini, V. Kavitha, A survey on security issues in service delivery models of cloud computing, Journal of network and computer applications 34(1) (2011) 1-11.

[5] M.A. Rababaa, M.A. Kofahi, F.A. Saqqar, S.A. Rababavh, Hash algorithms for security on GSM system, International Review on Computers and Software 4 (2009) 698-703.

[6] M. Ali, S.U. Khan, A.V. Vasilakos, Security in cloud computing: Opportunities and challenges, Information sciences 305 (2015) 357-383.

[7] N. Santos, K.P. Gummadi, R. Rodrigues, Towards Trusted Cloud Computing, HotCloud 9(9) (2009) 3.

[8] H. Hui, D. McLernon, Design and Application of a Service Outsourcing Cloud for the Insurance Industry, Proceedings of the 9th International Conference on Information Communication and Management (2019) 1-5.

[9] S. Srisakthi, A.P. Shanthi,Towards the Design of a Stronger AES: AES with Key Dependent Shift Rows (KDSR), Wireless Personal Communications 114(4) (2020) 3003-3015.

[10] S. Namasudra, R. Chakraborty, A. Majumder, Securing Multimedia by Using DNA-Based Encryption in the Cloud Computing Environment, ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) 16(3s) (2020) 1-19.

[11] P. Sivakumar, M. NandhaKumar, R. Jayaraj, A. Sakthi Kumaran, Securing Data and Reducing the Time Traffic Using AES Encryption with Dual Cloud, IEEE International Conference on System, Computation, Automation and Networking (ICSCAN) (2019) 1-5.

[12] A.K. Gautam, R. Kumar, A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks, SN Applied Sciences 3(1) (2021) 1-27.

[13] S.P. Kumar, A. Aswini, M. Kavithadevi, S. Ramya, Improvised dedupication with keys and chunks in HDFS storage, Third International Conference on Science Technology Engineering & Management (ICONSTEM), (2017) 226-230.

[14] M.B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, Y. Khamayseh, Comprehensive study of symmetric key and asymmetric key encryption algorithms, International conference on engineering and technology (ICET) (2017) 1-7.

[15] A. Bhuvaneshwaran, P. Manickam, M. Ilayaraja, K. Sathesh Kumar, K. Shankar, Clustering Based Cybersecurity Model for Cloud Data, Cyber security and Secure Information Systems (2019) 227-240.

[16] A. El-Yahyaoui, M.D.E.C. El Kettani, Data privacy in cloud computing, 4th International Conference on Computer and Technology Applications (ICCTA) (2018) 25-28.

[17] Z.H. Mahmood, M.K. Ibrahem, New fully homomorphic encryption scheme based on multistage partial homomorphic encryption applied in cloud computing, 1st Annual International Conference on Information and Sciences (AiCIS) (2018) 182-186.

[18] R. Gayatri, Y. Gayatri, Detection of Trojan based DoS Attacks on RSA Cryptosystem using Hybrid Supervised Learning Models, IEEE Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (2020) 1-5.

[19] D. Zissis, D. Lekkas, Addressing cloud computing security issues, Future Generation computer systems 28(3) (2012) 583-592.

[20] A.T. Hashem, I. Yaqoob, N.B. Anuar, S. Mokhtar, A. Gani, The rise of big data on cloud computing: Review and open research issues, Information systems 47 (2015) 98-115.

[21] D. Sun, G. Chang, L. Sun, X. Wang, Surveying and analyzing security, privacy and trust issues in cloud computing environments, Procedia Engineering 15 (2011) 2852-2856.