Webology (ISSN: 1735-188X)
Volume 18, Number 6, 2021

Context Aware Matrix-Based Symmetric Algorithm For Data Security In Public Cloud

Dr. D. I. George Amalarethinam[1], Ms. S. Edel Josephine Rajakumari[2]

[1]Bursar & Director (MCA), Associate Professor, [2]Research Scholar

PG & Research Department of Computer Science
Jamal Mohamed College (Autonomous), Affiliated to Bharathidasan University,
Tiruchirappalli – 620020, Tamil Nadu, India.

Abstract

Cloud computing is a trending technological paradigm that attains rapid growth in various domains. Cloud computing is popular for its on-demand services and remote access worldwide. A simple internet connection establishes an interface with the cloud environment and facilitates several services at any time. Technology advancement and changeover of lifestyle make cloud computing an inevitable activity. It includes storing sensitive data subject to serious data privacy and security concerns. In recent days, the untrustworthiness of cloud service providers (CSP) and various data breach have enabled cloud computing as an emerging topic. A novel technique proposed, Context Aware Matrix-based Symmetric Algorithm (CAMSA), a robust cryptographic mechanism that encrypts the numerical data, in a file based on specific criteria before storing it in the cloud. CAMSA performs encryption using the context information with appropriate user tasks. Unless with the decryption key, the original data cannot be retrieved. Most traditional cryptographic systems consume more time for processing encryption and decryption. The proposed CAMSA, a data partitioning mechanism for quick processing, to address this issue. To evaluate the performance of the proposed CAMSA, a comparison is done with the standard symmetric key algorithms and Matrix-based Symmetric Algorithm (MSA). The observation among three algorithms is conducted with encryption time, decryption time and security strength. The experimental works prove on evaluation metrics that the time consumed for proposed execution is minimal and more prominent than the existing cryptography methods.

Keywords: Encryption, Decryption, Cloud service providers (CSP), Cloud Computing, Context Aware Symmetric Algorithm.

1. Introduction

The cloud is a revolutionary innovation and the emergence of internet networking services. Cloud computing has evolved very quickly in recent times. Consequently, noticeable characteristics

include such resources with accelerated flexibility, remote network access, consistent assistance, and quality services. Cloud computing is a developing technology that is increasingly essential for storing and processing data services over the Internet. Popular cloud services include mail, internet transactions, e-commerce, billing, banking, and so on. Cloud storage is popular for its enriched improvements and reduced usage cost, which is outstanding among technological innovations. Cloud storage contains multiple pools, increasing the computing services called "Software as a Service." The remote information center encourages the clients to access the information from everywhere and whenever via huge quality network connection [1].

Conventional storage systems cannot offer huge storage space, but cloud storage avails this facility and can be handled remotely, known as cloud storage. Cloud storage enables clients to utilize any network type with any device or internet access. Cloud storage contains several important characteristics; however, data security is a complex issue. The massive volume of maximized cloud users and their elaborate organizations create data security issues. The outsourced business information might have confidential and private data, for instance, information about credit and debit cards, business confidentiality, banking data, etc. When these kinds of sensitive data are to be stored in third-party's data centers, it becomes highly insecure. Cloud computing obtains a few necessary features such as location-independent services, on-demand information services, permission on the vast network, often versatility, forecasted services, and pay-as-you-go. It also offers multiple advantages with maximized threats in the direction of the deployed information to the cloud users. The cloud comprises external entities called Cloud Service Providers (CSP), a distinct group. It validates the authenticity and stability of stored data files, and the cloud users could get evidence about the stored data on the cloud and evaluate whether it has been modified and deleted. It is still exposed to various risks and internal and external attacks on data integrity [2].

While offering a service to a permitted cloud user, the CSP employs its security procedures. To achieve reliability on cloud storage, the users can store their private information securely; a third-party vendor offers the storage space supplied by CSP. It allows a wide range of threats and a Virtual Machine (VM) side-channel attacks [3]. Information loss is a common problem despite the fact that the cloud structure is constructed with high-security characteristics. These are the persistent problems addressed by the cloud users. These problems queried individual cloud users to utilize the cloud services and depleted the cloud notoriety globally. Cryptography provides numerous techniques for securing the data that are stored in cloud. The data to be stored in the cloud can be classified into normal data and sensitive data, which are in turn stored in different cloud servers. While retrieving the data file from the cloud, the splitted data which are stored in different cloud servers would be merged and sent back to the user [4].

To address these security risks, cryptographic methodologies [5] are mainly used to secure information in the cloud by employing encryption/decryption methods with the support of multiple

keys. The two types of methods which are utilized for data encryption with the assistance of keys are:

- Asymmetric key data encryption
- Symmetric key data encryption

Public-key cryptography is another term for asymmetric key encryption. It includes a pair of keys, that is, public and private keys, for text encryption and decryption, respectively. Moreover, symmetric key encryption is also employed for data security, in which information is encrypted and then decrypted to use a single private key. The private key is utilized to encrypt the text and prevent several activities of the hackers. It has been determined that the complexity in accepting the symmetric cryptographic algorithms has been recognized due to the key size, which must be sufficiently large to guarantee proper security.

Data privacy and security are primary issues in cloud computing. The cloud users store their data with an untrustworthy third party, which requires an effective and capable security technology to make it secure. The information holders do not know where or in which cloud server their information is stored and do not have any physical access to their information. Security and privacy of users' information in a cloud environment are always viewed as critical problems. Users could attain multiple advantages from using the cloud as an external storage medium with minimal cost and easy information access. Still, security concerns must be addressed when transmitting or saving confidential or private information to the cloud.

1.1 Security issues in Cloud Computing

In today's world, security is vital no matter whether it is a physical entity or a logical entity. As information technology advances, information security becomes a matter of contention. Cloud computing provides storage as a service, by which small and medium scale businesses can store their data in the cloud on pay as you go basis. They may contain both the sensitive and non-sensitive data. It becomes vulnerable when the business information is outsourced for storage in the modern digital era. The following are some of the security issues exist in cloud computing:

SQL injection attack: SQL injection is a critical attack that uses web servers' weaknesses to insert malicious code into the system and change the contents of the Customer's databases [6].

Cross-Site scripting attacks: Another major attack is a kind of malware injection attack. It allows hackers to inject malicious scripts and creates vulnerable dynamic web pages [6].

Wrapping attack: In web-based services wrapping attacks are quite common and highly observed in cloud systems. It allows malicious users to duplicate the user's signature and send it to the server. This attack interrupts the cloud server’s services to the cloud users [7].

Virtual Machine (VM) replication is the leakage of cloud data due to an insecure handling system. To maintain data integrity, it is advised that the user correctly deactivates the virtual machines

during duplicating. To restrict the replication of sensitive VMs, VM's movements need to be regulated, infrastructure needs to be managed properly, and appropriate policies should be implemented [8].

VM Rollback: It creates an integrity problem in cloud computing. Rolling back virtual machines can restore previously patched security flaws or allow passwords or accounts that have been disabled [8].

Denial of Service attack: It typically bombards a target service with a massive volume of ambiguous requests and makes the service or data unavailable. It downgrades the cloud services and maximizes the extra computation powers for the cloud computing operating systems [8].

1.2 Problem Statement

Data security is a serious problem that can be hacked through internal or external methods. Various encryption methods are used to secure data transmission over the Internet. But to protect the data, they need big key sizes, large amounts of memory, and a lot of processing power. Typical cryptography techniques cannot solve the following issues:

1) Un-trusted third-party CSP system, which leads to the security breach
2) Higher possibility of security and privacy threats when transmitting sensitive data over an un-trusted or malicious networks
3) Lack of ensuring among the cloud users that their stored data are not pruned to attack
4) Increase in computational cost
5) Increase in time consumption while processing the encryption and decryption.

1.3 Research Motivation

In recent years, several research works have evolved to achieve maximum security in cloud computing. Cryptography is the prominent solution for achieving data privacy and security. The data stored by the user are more sensitive; hence a Context-Aware Matrix-based Symmetric Algorithm (CAMSA) is proposed. The context-aware mechanism understands and interprets the task through user or task context information. In the proposed work, data is classified such as numerical and non-numerical and before processing the encryption and decryption. As a result, it makes the entire execution simpler and more effective.

Organization of this paper: In section 1 introduction, along with research motivation and contributions, are discussed. Several literature works related to cloud security are discussed in section 2. In section 3 proposed workflow and its architecture are discussed in detail. In section 4, observations are discussed, and finally, section 5 contains the conclusion part.

2. Related Work

Fatma Lahmar et al. [9] proposed fuzzy FCA-based Security-aware multi-cloud services. The proposed work combines two effective techniques with a mathematical background: fuzzy formal

concept analysis (fuzzy FCA) and rough set theory (RS). Initially, fuzzy FCA is employed for characterizing multi-cloud environments and eliminating untrusted cloud services. But in some cases, fuzzy FCA cannot satisfy the required policies to achieve the user's security requirements. To overcome this, rough set theory is employed, whereas approximation of RS and fuzzy relations of fuzzy FCA minimize the search space. As a result, disqualified and insecure cloud services are eliminated.

Saba Rehman et al. [10] proposed a Hybrid AES-ECC approach for achieving security on cloud data storage. In this work, the author combines the Advanced Encryption Standard (AES) and Elliptic Curve Cryptography (ECC) to achieve data integrity and authentication. In the proposed hybrid model, AES key generation is performed using the ECC; In order to minimize the key size, the ECC algorithm is employed for key generation, and the AES algorithm is utilized for encryption and decryption. The combined approach establishes a secure and optimized method for data sharing in the cloud with a high level of data integrity and data security.

Yange Chen et al. [11] proposed a threshold hybrid encryption mechanism for data auditing without trust centers. The proposed method is a combined architecture of Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES) with Shamir secret sharing mechanism. AES generated key and users' private key are managed, maintained, and distributed without a trusted center. To achieve this, an advanced integrity auditing and re-signature approach are designed, which authenticates the data integrity and overcomes the cloud collusion questions and revoked users. The Shamir secret sharing applies to several managers in the group for creating and distributing the secret. The multi-managers approach transforms the multi-proxy scenario by minimizing the malicious managers. As a result, the entire approach results in secure and reliable data sharing in the cloud.

Masoud Barati et al. [12] proposed a novel privacy-aware auditing approach for auditing GDPR (General Data Protection Regulation) verification in the online healthcare industry. In this work, the author addresses the leakage of personal data and unauthorized access over cloud ecosystems. The proposed approach is automated and according to which the data operation is logged automatically in the cloud ecosystems. This paper presents a novel technique for monitoring, auditing, and verifying the operation of a user's personal data in cloud computing ecosystems according to the General Data Protection Regulation (GDPR). The recorded information undergoes Smart contracts with GDPR-priority and container-log. The smart contract verification process verifies the trusted third party, linked with Blockchain, responsible for labeling GDPR violations.

Parvaneh Asghari et al. [13] proposed a Privacy-aware mechanism with Quality of Service (QoS) optimization in the Internet of Things. The primary goal of this work is to enhance the QoS factors in cloud based-IoT environments. To achieve this, a combination of IoT-based cloud service composition conceptual model, privacy level computing model, a hybrid evolutionary algorithm using shuffled frog leaping algorithm (SFLA), and genetic algorithm (GA) referred to as SFLA-

GA is proposed. The proposed system implements various aggregated QoS factors as a fitness value, enhancing the proposed service composition. It further suggests the user choose a perfect composite service that satisfies a higher level of privacy-preserving factors.

Imran A. Khan et al. [14] proposed Elliptic curve cryptography for securing the data in a cloud environment. The proposed work was carried out over the adaptable data sharing among the clients. Because of data redistribution, it is complex to share the decoding keys among the approved clients. A Private Key Generator is implemented to overcome this issue by using elliptic curve cryptography. It generates a unique private key for each user without considering the usage. It shows a better outcome than the traditional security models.

Maria Selvam et al. [15] proposed a Polynomial Based Hashing and Elliptic Curve Cryptography method for data security and cloud authentication. This work proposes a hybrid approach by combining the hybrid algorithm PHECC (Polynomial based Hashing and Elliptic Curve Cryptography) with PH with ECC security algorithms. PH (Polynomial based Hashing) algorithm verifies the authentication against unauthorized access. The ECC-based algorithm enables data encryption between the user and server, where the server is the only entity for recomputing the secret key and obtaining the user information.

Astuti et al. [16] proposed combining cryptography and steganography to enhance cloud security. In this work, the author concentrated on improving the security of the JPG file in cloud storage. The AES 128 algorithm is used for message scrambling, and the least significant bit (LSB) is applied to hide the message via steganography.

Wasan S. Awad et al. [17] proposed a framework for enhancing the information storing cloud computing. In an existing storage system, migrating storage services and data transition results in various vulnerabilities. The proposed framework effectively organizes information systems and security models. It helps to design, customize and manage the security process according to the organization's requirements.

Sumit and Joshi [18] have provided a unique hybrid method to improve cloud storage security by incorporating AES and RSA algorithms with digital signatures. The researchers clearly illustrated the mixture of these three algorithms. However, the AES and RSA algorithms are employed in this journal to produce private keys. After that, the digital signature is utilized on the private key, which offers information authentication in the cloud region. The RSA algorithm with a public key of 1024 bits is utilized for validation. Correspondingly, the suggested algorithm's performance is measured concerning time conservation and contrasted to existing methods, illustrating that the suggested methodology uses considerably less time. But it is utterly irrelevant to large quantities of information.

Shantha et al. [19] introduced ECC Algorithm for achieving security in Lightweight devices. In this work ECC algorithm over Galois Field GF (2^3) generates smaller private keys compared to the other algorithms.

Urszula Ogiela et al. [20] proposed a cognitive cryptography mechanism for achieving security in cloud computing. This work uses hybrid CAPTCHA codes to verify user authentications.

3. Proposed Methodology

3.1 Working principle

This work proposes Context-Aware Text Cryptography using MSA, a robust cryptographic mechanism. This figure 1 illustrates the hierarchy of the three main entities in the proposed system as well as the communication between them: user, Cloud Service Provider (CSP), and cloud server. The initial process begins with user registration with the cloud service provider. In which a unique id and authentication credentials are provided to the users. These authentical details are the primary medium for communication between the user and CSP in accessing the cloud server. Whenever the user accesses the cloud server, the request is sent to the CSP. The CSP validates the user credentials, and authorized users are only allowed to access the server. The file is encrypted using the CAMSA algorithm before storing it in the cloud. The input file is classified as numerical and non-numerical data. Each non-numerical data is encrypted and stored in the allocated space provided by the CSP. The stored files are in ciphertext format, which is not readable. Suppose the user wants to retrieve the original data, the request will be sent to CSP. After validating the user's credentials, by providing the secret key, the user can download and view the original file. Figure 1 illustrates the workflow of the proposed system.

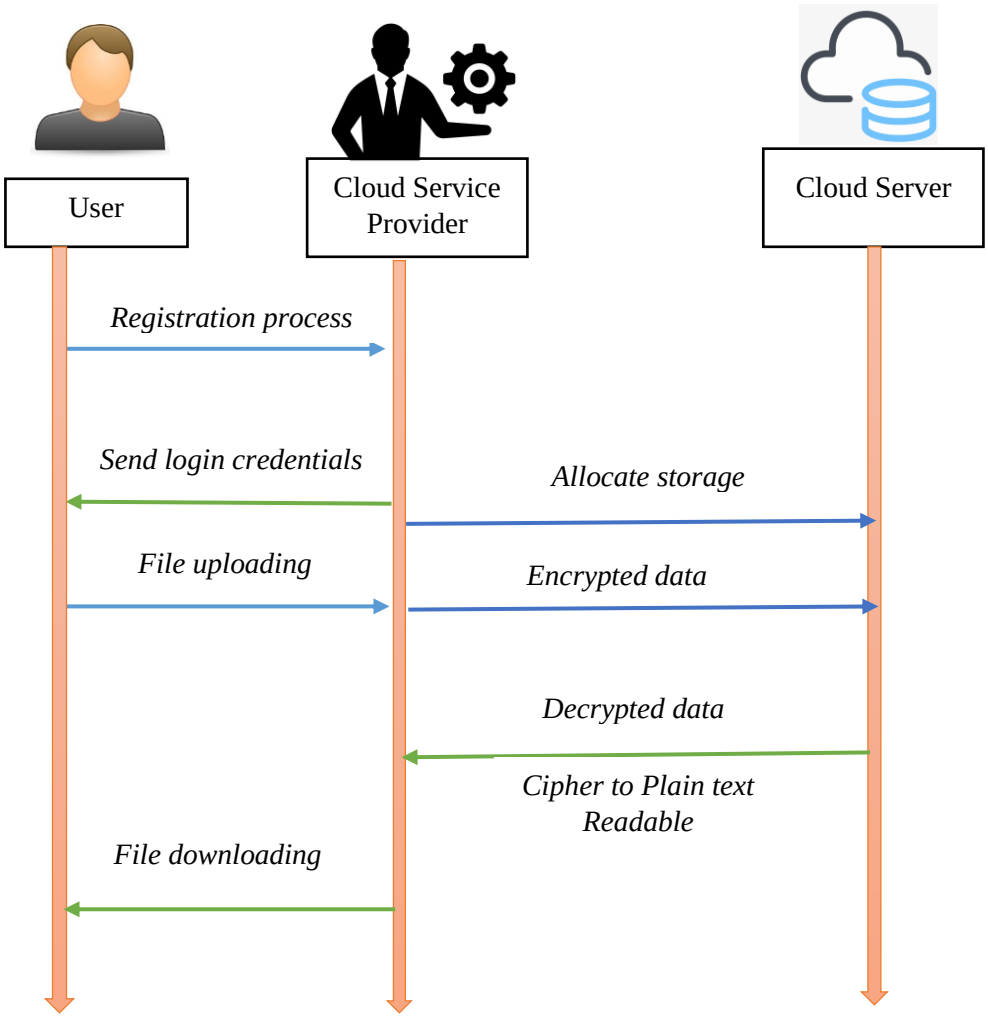

Figure 1. Workflow of the Encrypted Data Storage and Retrieval in Cloud

3.2 Proposed Architecture

Figure 2 illustrates the proposed CAMSA architecture; The cloud user has to register or create an account with the CSP; the user has to login with the username and password to access the cloud. Once the data file uploaded by the cloud user it is classified and uploaded in the cloud. The proposed architecture is executed under three components: data classification, encryption, and decryption.

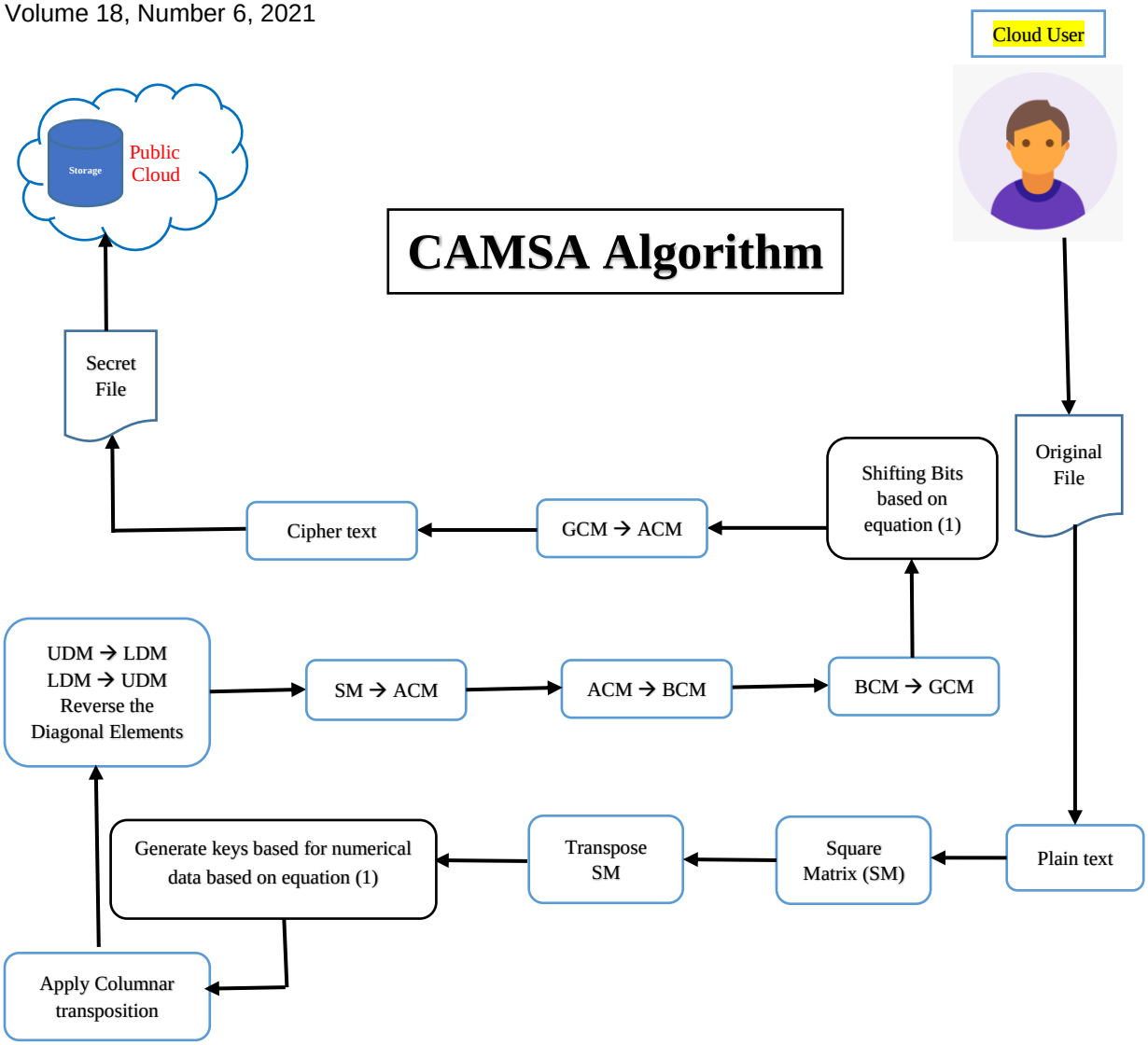

Figure 2. Context-Aware MSA

Data Classification: Data classification is an essential task in the encryption process. It is described as classifying the input file as numerical and non-numerical data before storing the file into cloud. As a result, the numerical data will be encrypted with special keys and stored in cloud that are highly secured. In this way, the file's most sensitive numerical information is protected.

Key Size for different Context: When the user wants to store the business documents which include sensitive numerical data such as mobile number, bank account number, credit card number, zip code, Patient's file number, etc., The context sensitivity can be described as the following equation:

$$\textbf{Category } (\delta) = \begin{cases} \alpha & \textbf{if } n(c) \leq 6 \\ \beta & \textbf{if } n(c) > 6 \;\&\&\; n(c) \leq 10 \\ \gamma & \textbf{Otherwise} \end{cases} \qquad \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

If the data file consists of numerical data like zip code which contains 6-digits or lesser than 6 digits, then the key size (α) for the zip code is 2^6 bits. The numerical data which contains digits more than 6 and less than or equal to 10 (eg. Mobile number), the key size (β) specifically generated for this kind of numerical data is 2^7 bits. For other numerical data which contain digits greater than 10, the key size (γ) is 2^8 bits. Thus, the numerical data of cloud user's file can be encrypted more securely.

Encryption: An effective and efficient cryptographic system is needed to store and manage the outsourced data securely on the cloud. Cryptography is the process of encryption and decryption. Data classification makes the encryption stronger, and the files are encrypted using MSA algorithm. MSA is a symmetrical block cipher algorithm with a small bit key size. The same secret key is used for both encryption and decryption. The encrypted files are stored in the cloud as cipher text in non-readable format. In case any malicious user or CSP tries to access the original data, cannot be retrieved without the secret key.

Decryption: Decryption converts the cipher text into an original text in a readable format. When an authenticated cloud user requests for the encrypted data file stored in the cloud, the user credentials will be verified and the requested data file will be sent to the intended user. The cloud user can decrypt the file using the appropriate keys.

3.3 Proposed CAMSA Algorithm

Input: Plain Text
Output: Cipher Text

Steps:

1. PT ← Plain Text
2. Construct a square matrix SM with the PT from left to right.
3. If(m==n)
   encrypt (PT)
   end if
4. If(m!=n)
   FC = rand (fillers)
   append (FC)
   construct a square matrix S
   end if

where
PT ← Plain Text
SM ← Square Matrix
m ← number of rows
n ← number of columns
FC ← Filler Character

Figure 3. MSA Algorithm

encrypt (PT)
Steps:

1. T ← Transpose(S)
2. ***Generate keys based on the equation (1)***
3. ColTrans = ctrans(T)
4. Split the matrix ColTrans into UDM, LDM and DM
5. For each char i, apply ASCII code in the matrix.
6. Convert the ASCII Code Matrix (ACM) into Binary Code Matrix (BCM)
   BCM ← ACM
7. Convert the Binary Code Matrix (BCM) into Gray Code Matrix (GCM)
   GCM ← BCM
8. ***Generate keys based on the equation (1) for shifting the bits***
9. ***Shift each element in GCM based on the keys generated by equation (1).***
10. Convert the GCM into ACM
    ACM ← GCM
11. Convert the ACM into alphabets / symbols.
12. CT ← Read the resultant matrix by row.

Where
T ← Transpose Matrix of S
Rand1() ← Generate Random number 1
ctrans() ← Columnar Transposition of T
CTrans ← Result of Columnar Transposition
DM ← Diagonal Matrix
LDM ← Lower Diagonal Matrix
UDM ← Upper Diagonal Matrix
i ← each element in the matrix

Figure 4. Encryption Process

Figure 3 and Figure 4 explain the steps for encrypting the data file uploaded by the cloud user. The proposed algorithm is different from MSA (Matrix-based Symmetric Algorithm). Specifically increasing the key size for numerical data in MSA algorithms makes it more strongly encrypted and it is called Context-Aware Matrix-based Symmetric Algorithm (CAMSA).

4. Experimental Results

In this section, the performance of the proposed system with the existing approaches is discussed. Several cryptographic approaches are available in the industry, but each has advantages and disadvantages. Most of the approaches are available with larger private keys, which maximize the memory space and execution time. Time consumption is a serious issue that leverages the overall user experience in the cloud environment. To evaluate the efficiency of the proposed system, a comparison work is conducted among the proposed Context Aware MSA and standard Symmetric Key Encryption Algorithms. The algorithms are executed and the results are compared with encryption time, decryption time and the strength of Security. The values obtained by the respective algorithms are tabulated and plotted graphically for better understanding.

4.1 Encryption time

Table 1. Encryption Time

Data (MB)	**DES (ms)**	**AES (ms)**	**Blowfish (ms)**	**MSA (ms)**	**CAMSA (ms)**
1	2471	2883	2124	2925	2064
2	4503	5194	3499	5276	3796
3	7022	8100	5567	8238	5915
4	9438	11022	7713	11206	7886
5	11920	13865	9869	14084	10029

The symmetric algorithms DES, AES, Blowfish and MSA and the proposed CAMSA algorithms are executed in a public cloud environment and the obtained results are tabulated. Table 1 shows the results for encryption time of proposed DES, AES, Blowfish, MSA and CAMSA algorithms for different file sizes. Compared to other algorithms, the encryption time of CAMSA is significantly reduced.

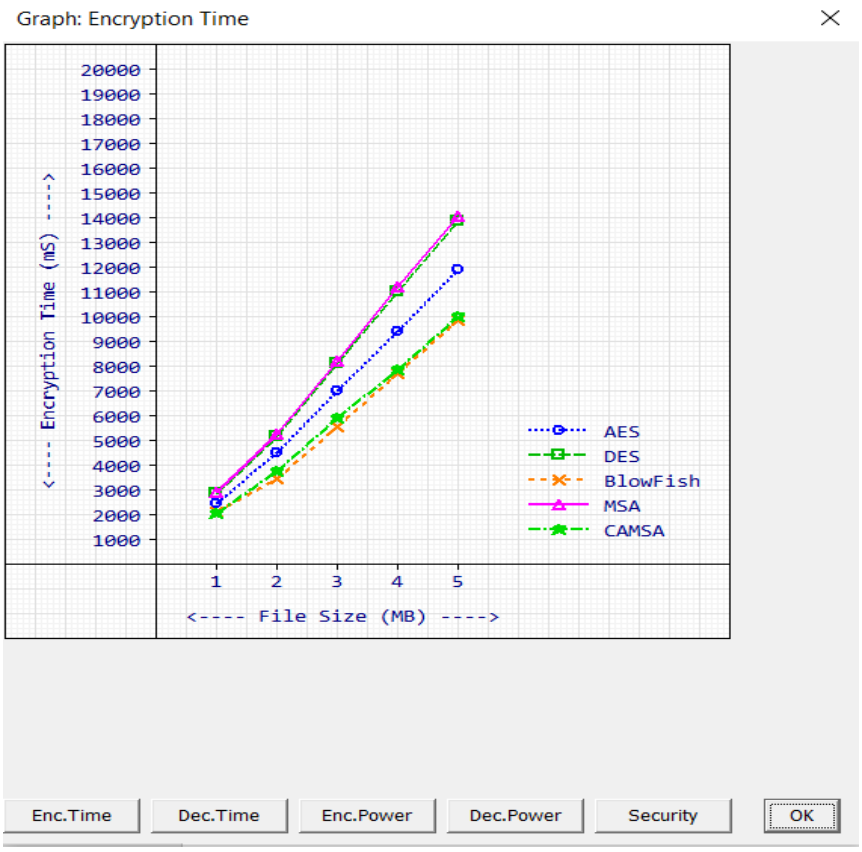

Figure 5. Encryption Time

Figure 5 shows the comparison result concerning encryption time taken for several file sizes. The x-axis shows the file size in megabytes (MB), and the y-axis shows the encryption time in milliseconds. Each iteration increases the file size gradually with a count of 1MB. The results are tabulated and plotted graphically. The proposed CAMSA takes 2064ms for encrypting 1MB files, 3796ms for encrypting 2MB files, 5915ms for encrypting 3MB files, 7886ms for encrypting 4MB files and 10029ms for encrypting 5MB files. The comparison graph shown in Figure 5, proves that the performance of the proposed CAMSA is more efficient than the existing other symmetric encryption algorithms.

4.2 Decryption time

Table 2 shows the results of decryption time, the process of converting the ciphertext into the plaintext. The decryption time is calculated for DES, AES, Blowfish, MSA and the proposed CAMSA algorithms. The results are tabulated in Table 2 and it shows that, the decryption time of CAMSA is considerably reduced compared to other algorithms.

Table 2. Decryption Time

Data (MB)	DES (ms)	AES (ms)	Blowfish (ms)	MSA (ms)	CAMSA (ms)
1	2475	2889	2210	2838	2005
2	4533	5276	3587	5196	3713
3	7046	8173	5782	8038	5741
4	9503	11068	7981	10849	7763
5	11999	13967	10247	13737	9676

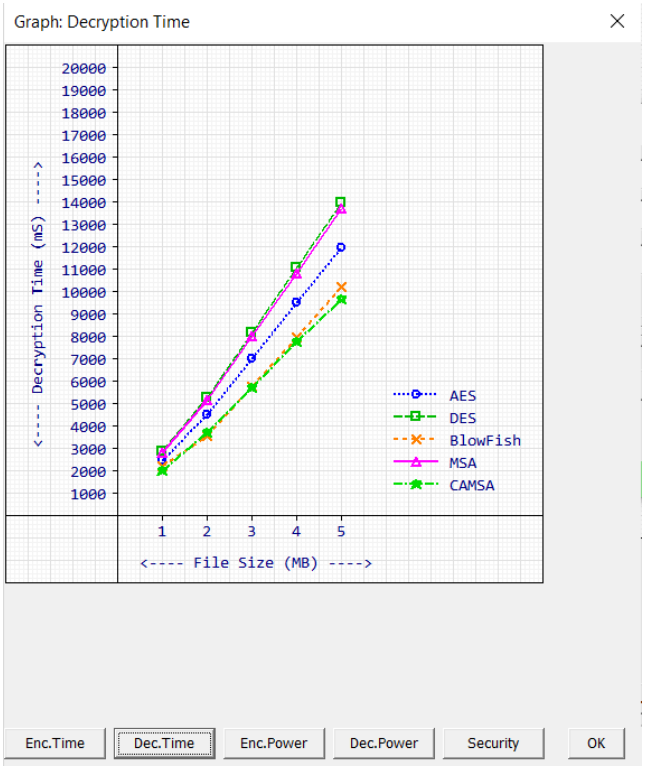

Figure 6. Decryption Time

Figure 6 shows the comparison result concerning decryption time taken for several file sizes. The x-axis shows the file size in megabytes (MB), and the y-axis shows the encryption time in milliseconds. Each iteration increases the file size gradually with a count of 1MB. The proposed CAMSA takes 2005ms for decrypting 1MB files, 3713ms for decrypting 2MB files, 5741ms for decrypting 3MB files, 7763ms for decrypting 4MB files and 9676ms for decrypting 5MB files. The comparison graph shows the performance obtained by the proposed CAMSA is more efficient than the existing other symmetric encryption algorithms.

4.3 Security Strength

The IBM Crypto Analytics Tool (CAT) is used for measuring the strength of the security of the algorithm. Attempting various kinds of attacks on the encrypted data, it is proved that the proposed CAMSA algorithm is the best algorithm which is stronger than other symmetric encryption algorithms. Table 3 shows the results of the security strength of existing and proposed symmetric key algorithms in percentage. It is proved that the strength of data security in CAMSA is tremendously increased, compared to other algorithms.

Table 3. Security Strength

Data (MB)	DES (%)	AES (%)	Blowfish (%)	MSA (%)	CAMSA (%)
1	96	94	91	97	99
2	96	92	90	96	96
3	96	92	90	97	97
4	95	92	88	96	97
5	96	91	90	97	97

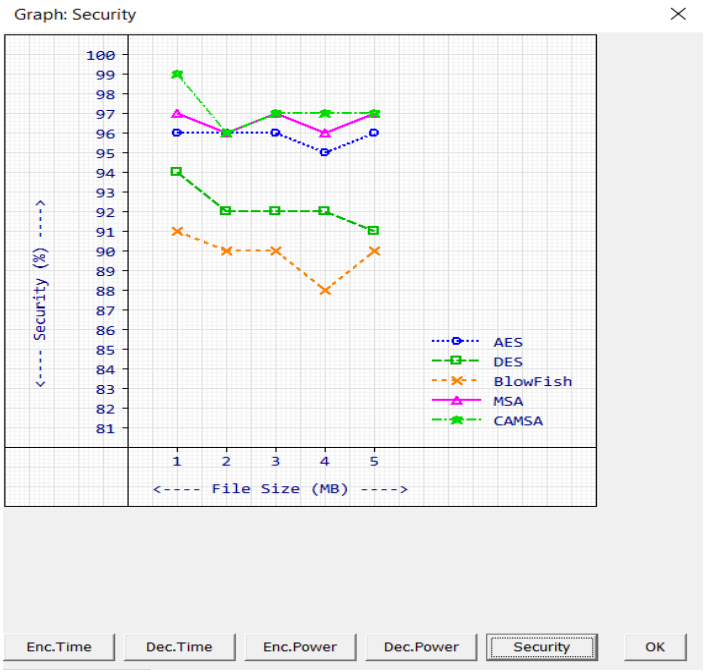

Figure 7. Security Strength

Figure 7 clearly shows that compared to other symmetric key encryption algorithms and MSA, the CAMSA provides 99% security at the maximum to the data stored in public cloud. It is the only algorithm which provides the highest level of security.

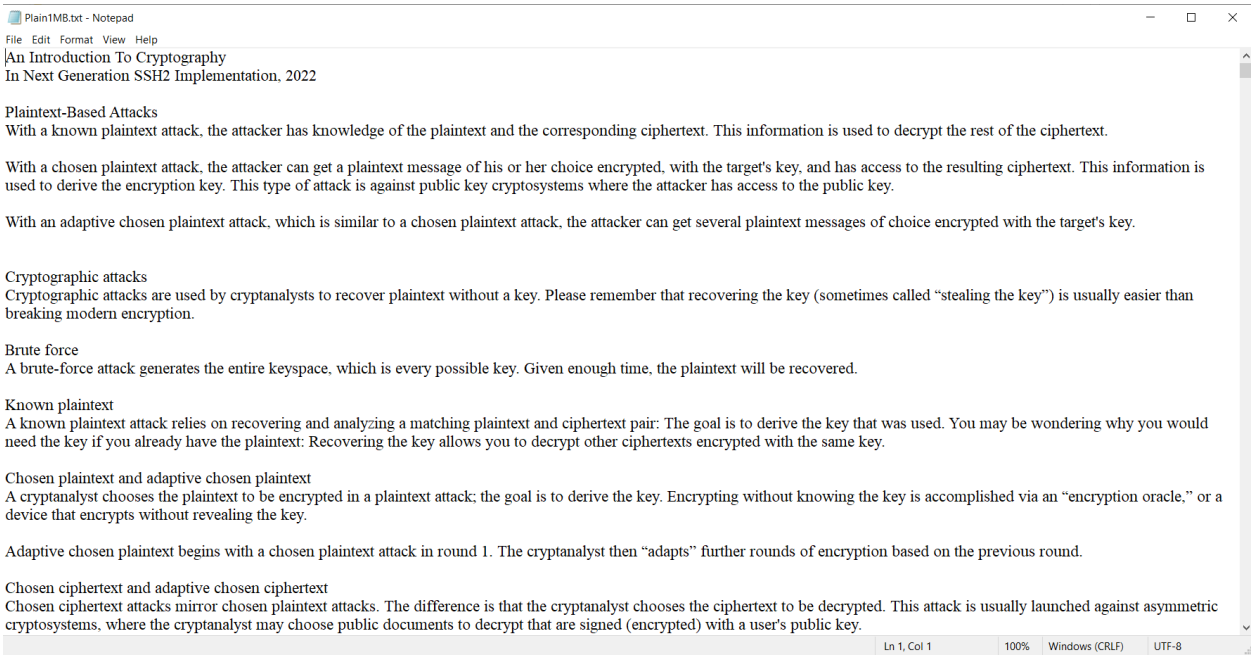

Figure 8. Plain Text (1MB)

Figure 9. Cipher Text (1MB)

Figure 8 & Figure 9 show the Plain text and Cipher text files, before and after the encryption process of CAMSA. The file is 1MB and it is completely unreadable and can be securely stored in Public Cloud. The algorithm is executed on 2MB, 3MB, 4MB and 5 MB files respectively.

5. Conclusion

In the proposed work, various security issues like unauthorized access, malicious insiders, data confidentiality, cyberattacks in the public cloud environment have been analyzed. It includes various security methods are evolved to protect cloud data. Based on the study, the key size and processing time during cryptography significantly impact cloud performance. To quick process and enhance the security, the Context Aware Matrix-based Symmetric Algorithm (CAMSA) is proposed. The proposed approach includes data classification to make the execution simpler and quicker. The CAMSA algorithm provides additional security to the cloud-stored data using a secret key mechanism. To evaluate the proposed system's ability, the experiments are conducted in public cloud environment and the performance of the proposed CAMSA's performance is compared with the existing standard symmetric cryptography algorithms such as DES, AES, Blowfish and MSA. The results of each algorithm are plotted graphically for comparison analysis. The graphical result proves that the proposed CAMSA is far better than the other existing algorithms on all the evaluation metrics.

References

[1] Felix Bentil, Isaac Lartey, "Cloud Cryptography - A Security Aspect", International Journal of Engineering Research & Technology (IJERT), ISSN. 2278-0181, Vol. 10 (5), 2021.

[2] Deepali Gupta, Kamali Gupta, Naresh Kumar, "Emerging Technologies and Trends in Cloud Computing", COMPUSOFT, An International Journal of Advanced Computer Technology, ISSN. 2320-0790, Vol. 8(6), 2019.

[3] Arockia Panimalars, N. Dharani, R. Aiswarya & Pavithra Shailesh, "Cloud Data Security using Elliptic Curve Cryptography", International Research Journal of Engineering and Technology, ISSN. 2395-0072, Vol. 4 (9), 2017.

[4] LiYibin, KekeGai, LongfeiQiu, MeikangQiu, ZhaoHui, "Intelligent Cryptography Approach for Secure Distributed Big Data Storage in Cloud Computing", Information Sciences, Vol. 387, 2017.

[5] Ashima Narang, Gupta Deepali, AmandeepKaur, "Efficient FragSecure Framework for Data Security and Fragmentation in Cloud Computing", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN. 2278-3075, Vol. 8 (7), 2019.

[6] Srijita Basu, Arjun Bardhan, Koyal Gupta, Payel Saha, Mahasweta Pal, Manjima Bose, Kaushik Basu, Saunak Chaudhury, Pritika Sarkar, "Cloud Computing Security Challenges & Solutions - A Survey", IEEE, 2018. DOI: 10.1109/CCWC.2018.8301700

[7] Jaydip Sen, "Security and Privacy Issues in Cloud Computing", Architectures and Protocols for Secure Information Technology Infrastructures, 2013. DOI: 10.4018/978-1-4666-4514-1

[8] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez, "An Analysis of Security Issues for Cloud Computing", Journal of Internet Services and Applications, Vol. 4 (5), 2013.

[9] Fatma Lahmar, Haithem Mezni, "Security-aware multi-cloud service composition by exploiting rough sets and fuzzy FCA", Soft Computing, ISSN. 5173–5197, Vol. 25 (4), 2021.

[10] Saba Rehman, Nida Talat Bajwa, Muna Ali Shah, Ahmad O. Aseeri and Adeel Anjum, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage", Electronics, 2021.

[11] Yange Chen, Hequn Liu, Baocang Wang, Baljinnyam Sonompil, Yuan Ping & Zhili Zhang, "A threshold hybrid encryption method for integrity audit without trusted center", Journal of Cloud Computing, Vol. 10 (3), 2021. https://doi.org/10.1186/s13677-020-00222-6

[12] Masoud Barati, Gagangeet Singh Aujla, Jose Tomas Llanos, Kwabena Adu Duodu, Omer Rana, Madeline Carr, Rajiv Ranjan, "Privacy-Aware Cloud Auditing for GDPR Compliance Verification in Online Healthcare. IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, 2021.

[13] Parvaneh Asghari, A. Rahmani, H. Javadi, "Privacy-aware cloud service composition based on QoS optimization in Internet of things", Journal of Ambient Intelligence and Humanized Computing, 2020.

[14] Imran A. Khan, Rosheen Qazi, "Data Security in Cloud Computing Using Elliptic Curve Cryptography", International Journal of Computing and Communication Networks (IJCCN), ISSN: 2664-9519, Vol. 1 (1), 2019.

[15] Selvam, J.M., Srivaramangai, P., "Time complexity analysis of cloud authentications and data security: Polynomial based hashing and elliptic curve cryptography", Int. J. Anal. Exp. Modal Anal., 2020.

[16] N R D P Astuti, E Aribowo, E Saputra, "Data security improvements on cloud computing using cryptography and steganography", IOP Conference Series: Materials Science and Engineering, Vol. 821, 2019.

[17] Wasan S. Awad, "A Framework for Improving Information Security Using Cloud Computing", InfoSciRN: Cloud Computing (Sub-Topic), 2020.

[18] Sumit Chaudhary, N. K. Joshi, "Secured Blended Approach for Cryptographic Algorithm in Cloud Computing", International Journal of Pure and Applied Mathematics, Vol. 118 (20), 2018.

[19] A. Shantha, J. Renita, Elizabeth N., Edna, "Analysis and Implementation of ECC Algorithm in Lightweight Device", International Conference on Communication and Signal Processing (ICCSP), 2019. DOI: 10.1109/ICCSP.2019.8697990.

[20] Urszula Ogiela, "Cognitive cryptography for data security in cloud computing", Concurrency and Computation: Practice and Experience", 2021.