International Multidisciplinary Research Journal Reviews (IMRJR)

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 9, September 2025
DOI 10.17148/IMRJR.2025.020908

Data Security Enhancement In Cloud Using Magic Square Obfuscation

Dr. B. Fathima Mary

Assistant Professor, Department of Commerce CA, St. Joseph's College (Autonomous), Tiruchirappalli, India

Abstract: A distributed collection of related and connected systems with additional resources made available on a pay-per-use basis is known as cloud computing. It has more to do with other computing technologies, such as autonomous computing, grid, and utility computing, among others. Because of its virtualization technology, the Cloud differs from other platforms, particularly the Grid. Cloud service providers (CSPs) like Google, Amazon, Salesforce.som, Microsoft, and others store and manage client data in their data centres. Cloud computing is entirely internet-dependent technology. CSP is in charge of keeping an eye on and maintaining the data that is outsourced. Data leaks, insecure interfaces, resource sharing, data availability, and insider attacks are just a few of the security risks and problems that can arise from having little control over the data. Security, availability, performance, lack of standards, higher usage costs, and difficulty integrating with on-premise IT resources are the first problems. Because they don't know where their data will be stored, when it will be available to them, or how it will be processed by others, many customers don't fully rely on the cloud environment. For these reasons, a large number of researchers focus on the cloud's "security." This study proposes a technique of confidentiality called Magic Square Obfuscation (MSO) to enhance data security and add complexity to the obfuscated text.

Keywords: cloud, data security, CSP, confidentiality, obfuscation.

I. INTRODUCTION

One of the hottest terms in the ICT sector right now is cloud. A network that offers resources as services is called a cloud. There are two types of cloud services: software and hardware. The cloud offers on-demand services like servers, storage, software, and networks [1]. According to service level agreements (SLAs) for their products, a lot of IT vendors guarantee to deliver computing, storage, and application hosting services [2]. Cloud services are readily available over a network; you only pay for the services you use, and you can start or stop the service as needed. Therefore, similar to metering, CSP charges for usage only [3][4]. A straightforward and expandable method of storing, retrieving, and sharing data via the Internet is cloud storage.

The network-connected hardware and software are owned and maintained by cloud storage providers, and you use a web application to provision and use the necessary resources [5]. It assists in lowering the investment and upkeep costs of the IT necessary for small and medium-sized businesses (SMEs). It offers Everything (X) as a Service (XaaS), where "X" stands for operating system, hardware, storage, software, and servers, among other things [4]. For the majority of businesses, data protection is an essential security concern [6]. Data security is the biggest problem with cloud computing. When moving data to storage, outsourcing raises concerns about cloud security. Data confidentiality is made possible by effective cryptography and obfuscation techniques[7]. Encryption techniques are used in cryptography to convert plain text into a coded format. Hence, the privileged users only can access the data. The process of obfuscation involves concealing the initial value of data. Obfuscation is the foundation of the proposed technique[8].

A. Data Masking or Data Obfuscation

In order to prevent unwanted access, data obfuscation is a technique for data concealment in which information is deliberately mixed up. Obfuscation results in obscured or unintelligible data [9]. For security purposes, data obfuscation makes it difficult to decipher the plaintext. Though it makes use of programming logic or mathematical computations, it is comparable to encryption. This method prevents unwanted access to personal information and modifies the original data. To stop access to data stored in the cloud, data obfuscation techniques are employed. It's part of the company's data security plan [10]. Recently, this technique has become more and more popular for protecting data stored in cloud storage [11]. Data obfuscation techniques are used to provide de-identified, de-sensitized, and anonymised data for application users, business intelligence, application testing, and outsourcing. Data masking technology protects data by replacing sensitive data with a non-sensitive pattern and creating an output that can look and work like the original [12][13].

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 9, September 2025
DOI 10.17148/IMRJR.2025.020908

B. Data Obfuscation Techniques

Substitution

One of the best ways to apply data masking while maintaining the genuine appearance and feel of the data records is through substitution. It's just switching out one value for another. It enables the masking to be done so that the current value can be replaced with another that looks authentic.

Shuffling

One popular technique for obfuscating data is the shuffling method. Although the substitution set is derived from the same column of data that is being masked, it is comparable to the substitution method. It is a technique for vertically randomizing values that already exist in a data set. If the shuffling algorithm can be figured out, the shuffling method can also be reversed.

Nulling out or deletion

Applying a null value to a specific field is sometimes a very basic masking technique. The only real benefit of the null value approach is that it keeps the data element hidden.

Blurring

Altering an existing value so that it falls within a specified range at random.

Masking out

Another straightforward but incredibly powerful technique to stop sensitive information from being viewed is character scrambling or masking out specific fields. Although there is more focus on maintaining the authenticity of the data and not completely masking it, it is essentially an extension of the earlier nulling out method [14].

II. RELATED WORKS

Lin et al.[15] introducesd EmojiPrompt, an innovative framework designed to protect user privacy when interacting with cloud-based large language models (LLMs). By converting sensitive input data into a blend of emojis, symbols, and linguistic cues, EmojiPrompt effectively obscures private information without sacrificing task accuracy. The authors demonstrate its robustness across multiple datasets and benchmark it against existing obfuscation methods, showing comparable or superior performance.

To improve cloud data security, Renuka et al. [16] introduced a strong hybrid encryption method that combines the RSA and AES algorithms. The suggested approach creates a double-layered protection model by using AES for quick and effective data encryption and RSA for secure key exchange. Using actual datasets and thorough performance analysis, the authors validate their method, demonstrating gains in security, resilience to different cyberattacks, and encryption effectiveness.

Kamal et al.[17] proposed a novel multilayer encryption model, MDSMTRSA, created to improve public cloud storage data security. The proposed method integrates matrix transformation with an enhanced RSA algorithm that uses ten prime numbers for public key generation and an additional prime for the secure private key.

The SLT-DSA, a multi-layered security framework created to improve data security in cloud computing, was first presented by Vinnarasi et al. [18].It incorporates three encryption layers scrambling with binary operations, dynamic and secret key generation, and secure hash-based signature generation. Susmitha et al.[19] suggested a hybrid encryption model to address security and data storage issues in cloud computing by combining Secure Hash Algorithm-3 (SHA-3) and Fully Homomorphic Encryption (FHE). The method enables secure operations on encrypted data while preserving data integrity through SHA-3 hashing.

To tackle the main security issues with cloud computing, Tajinder et al. [20] proposed the Three-Layered Security Access (TLSA) model. Three key elements are integrated into the model: Intrusion Detection Systems (IDS) for detecting and stopping malicious activity, Role-Based Access Control (RBAC) for controlling user permissions, and AES encryption for data confidentiality.

To improve confidentiality in cloud storage, Fathima et al. [21] proposed a novel data obfuscation technique. Because it obfuscates plaintext data line-by-line and word-by-word without requiring encryption keys. This method is used to convert words to numbers with the combination of randomly generated magic square numbers which is known as obfuscated text.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 9, September 2025
DOI 10.17148/IMRJR.2025.020908

III. METHODOLOGY

The current obfuscation method employs blurring, shuffling, redaction or nullification, and substitution. Through the integration of substitution, transposition, and ASCII values, the MSO Technique enhances traditional obfuscation techniques. This technique is used to hide the original value of data and should not be reversible. Initially the Word (W) lists are generated from the plain text. In the corresponding words, characters(C) are converted to ASCII value and that ASCII(ASC) value is multiplied with that character position where it appeared in the word. After that, the multiplied value of individual character is added with another character value and it produces a Numerical Code(NC) to the corresponding word. The word and the associated Numerical code value, which is obtained from the plain text, are preserved. The Modulo Operation (MO) is used to multiply NC by 64 in order to determine the remainder and quotient value. Modulas (M) are used to generate the Magic Square, which has numerical values in it. Lastly, numbers are calculated based on the remainder and quotient of NC. Finally, using magic square, the obfuscated text (OT) is obtained.

IV. ILLUSTRATION

Sample text is used to test the MSO technique. The process of the experiment is carried as follows.
Step 1: Examine the original text "Jamal" that follows.

Step 2: The ASCII value of each individual character is multiplied by its position to convert the word to the Numerical Code (NC).

Word	ASCII	Position	NC
Jamal	J a m a l 74 97 109 97 108	1 2 3 4 5	74x1+97x2+109x3+97x4+108x5=1523

Step 3: The quotient and remainder values are obtained by applying the modulus operation by 64 to the relevant numeric codes.

NC	Quotient	Remainder
1523	23	51

Step 4: MS is created based on the mod value. Mod is eight.

1	63	62	4	5	59	58	8
56	10	11	53	52	14	15	49
48	18	19	45	44	22	23	41
25	39	38	28	29	35	34	32
33	31	30	36	37	27	26	40
24	42	43	21	20	46	47	17
16	50	51	13	12	54	55	9
57	7	6	60	61	3	2	64

Step 5: Lastly, the quotient and remainder values are used to extract numerical values from the MS.
Step 6: The encrypted text is “41 13”

Based on the random number generation, secret key is generated.
The features of the MSO techniques are

1. Magic square is generated based on the modular value.
2. Increases the complexity of cipher text such as character to number conversion using position value along with ASCII.
3. Matrix size is changed based on modular value.
4. Cipher text is generated based on quotient and remainder.
5. It improves the efficiency by using magic square.

The proposed MSO technique is applied on both numeric and non numeric data. It guarantees data confidentiality and maintains the security. Therefore, when data is stored in the cloud, there is no need to be concerned about it being obfuscated.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 9, September 2025
DOI 10.17148/IMRJR.2025.020908

V. CONCLUSION

Cloud storage offers both individuals and organizations affordable services. It offers a vast amount of space for cloud data outsourcing. Businesses and organizations lack the complete infrastructure necessary to keep their data on site. Maintaining their data in cloud storage is made easier with the aid of data outsourcing. There are numerous ways for users to attack their data while it is being stored in the cloud. The confidentiality-enabled obfuscation method known as MSO is covered in this paper. To sum up, the proposed method uses magic square to increase the complexity of the cipher text. Since quotient and remainder are used in text scrambling, the original text may become significantly jumbled. The sample text used in this work has been jumbled. Therefore, it is impossible to anticipate the pattern of scrambling that hackers will employ. The suggested MSO technique improves data security when compared to current encryption methods. The application of this suggested method is the focus of the upcoming work.

REFERENCES

[1]. Thabit F, Can O, Alhomdy S, Al-Gaphari GH, Jagtap S, A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing, *International Journal of Intelligent Networks*,pp.16–30,2022.
[2]. Sana MU, Li Z, Kiren T, Liaqat HB, Naseem S, Saeed A. A Secure Method for Data Storage and Transmission in Sustainable Cloud Computing, *Computers, Materials & Continua*, pp.2741–2757,2023.
[3]. Gupta M, Ahuja L, Seth A, Security enhancement in a cloud environment using a hybrid chaotic algorithm with multifactor verification for user authentication, *International Journal of Computers and Applications*,pp.680–696,2023.
[4]. Amitabha Yadav, Cloud computing security mechanisms random number authentication, *Edelweiss Applied Science and Technology*,pp.1016-1022,2025.
[5]. Diwakar Ramanuj Tripathi, Data Obfuscation Technique for Security in Cloud Computing, *International Journal of Recent Technology and Engineering*,pp.4239-4244,2020.
[6]. D.I. George Amalarethinam , J. Vinnarasi, Enhancing the data security of cloud computing critical systems using layered encryption technique, *International. Journal of Critical Computer-Based Systems*,pp.194-214,2024.
[7]. Osama Aljumaiah, Mounir Frikha, Model of Protecting Data in the Cloud, *Journal of Theoretical and Applied Information Technology*,pp.1785-1790,2023.
[8]. P Nagaraju, Dr N Nagamalleswara Rao, Obfuscation Techniques In Cloud Computing: A Systematic Survey, *International Journal of Scientific & Technology Research*,pp.1097-1102,2019.
[9]. Dr.D.I.George Amalarethinam, B.FathimaMary, DMUCE- A Confidentiality Enabled Technique To Improve Cloud User Security, *International Journal of Applied Engineering Research*,pp.34103,34108,2015.
[10]. Dr.D.I.George Amalarethinam, B.FathimaMary, eDSSuMRT- Ensured Data Security Strategy using Matrix Random Traversal In Cloud Storage Environment, *International Journal of Applied Engineering Research*,pp.272-279,2015.
[11]. Dr.D.I.George Amalarethinam, B.FathimaMary, Data Security Enhancement in Public Cloud Storage, *Journal of Computing and Intelligent Systems*, pp.1-5,2017.
[12]. Dr.D.I.George Amalarethinam, B.FathimaMary, Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography, *IEEE* Explore,pp.181-184,2016.
[13]. Dr.D.I.George Amalarethinam, B.FathimaMary, Security Enhancement for Public Cloud Storage with Minimum Cost, *International Journal of Pure and Applied Mathematics*, pp.1-9,2018.
[14]. .D.I.George Amalarethinam, B.FathimaMary, Comparative Analysis of Obfuscation Techniques in Public Cloud, *American International Journal of Research in Science, Technology, Engineering & Mathematics*,pp.309-312,2019.
[15]. Sam Lin, Wenyue Hua, EmojiPrompt: Generative Prompt Obfuscation for Privacy-Preserving Communication with Cloud-based LLMs, *Association for Computational Linguistics*,pp.12342-12361,2025.
[16]. Renuka S. Durge,Vaishali M. Deshmukh, Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance,journal of integrated science and technology,pp.1-7,2025.
[17]. M. Kamal , Dr. G. Ravi, A Multilayer Data Security using Matrix Transformation and RSA for Public Cloud Storage, *Journal of Advanced Applied Scientific Research*,pp.30-47,2024.
[18]. J.Vinnarasi, D.I. George Amalarethinam, Advancing Data Security in Cloud Computing: Introducing Secured Layered Technique for Data Security Approach (SLT-DSA), A Multi-Layered Security Framework, *Indian Journal of Science and Technology*,pp.848-860,2025.
[19]. Susmitha Pothireddy, Nikhila Peddisetty, Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability, *Interrnational Journal of Intelligent Engineering and Systems*,pp.159-170,2023.

International Multidisciplinary Research Journal Reviews (IMRJR)
A Peer-reviewed journal
Volume 2, Issue 9, September 2025
DOI 10.17148/IMRJR.2025.020908

[20]. Tajinder Kumar , Purushottam Sharma, Enhanced Triple Layered Approach for Mitigating Security Risks in Cloud, *Tech Science Press*,pp.719-738,2025.

[21]. Dr.D.I.George Amalarethinam, B.FathimaMary, Confidentiality Technique for Enhancing Data Security in Public Cloud Storage using Data Obfuscation, *International journal of control theory and application*,pp.1-11,2016.

[22]. Dr.D.I.George Amalarethinam, B.FathimaMary, Data Security Enhancement in Public Cloud Storage using Data Obfuscation and Steganography, *IEEE* Explore,pp.181-184,2016.

[23]. B.Fathima Mary, Dr.D.I George Amalarethinam, Data security enhancement in public cloud storage using data obfuscation and steganography, *world congress on computing and communication technologies (WCCCT),*pp.181-184,2016.