"Enhancing Security of Data in Cloud Computing Using A Novel Approach of Number System"

RICHA SHARMA
RESEARCH SCHOLAR ,COMPUTER SCIENCE
MADHYANCHAL PROFESSIONAL UNIVERSITY,
BHOPAL (M.P.)

How to Cite this Article:

SHARMA, R. (2026). "Enhancing Security of Data in Cloud Computing Using A Novel Approach of Number System". International Journal of Creative and Open Research in Engineering and Management, 02(05). https://doi.org/10.55041/ijcope.v2i5.776

https://doi.org/ 10.55041/ijcope.v2i5.776

Abstract

Due to the increasing number of cyber-attacks and security issues such as data breaches, malware, ransomware, and Distributed Denial-of-Service (DDoS) attacks, cloud computing faces significant challenges in ensuring data confidentiality, integrity, and availability. Recent research highlights a growing emphasis on enhancing cloud security through cryptographic techniques and number system-based approaches. Cryptographic methods such as hash functions, RSA and AES offer robust encryption mechanisms that protect sensitive data from unauthorized access and tampering. A review of various research papers was conducted to identify key problem statements and analyze the methodologies employed in each study to address cloud security concerns.

Keywords:- *cyber-attacks, data breaches, malware, ransomware, Distributed Denial-of-Service (DDoS) attacks etc.*

Introduction

Cloud computing refers to the delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the internet ("the cloud"). These services enable businesses and individuals to access and use powerful computing resources without needing to own or maintain physical hardware or infrastructure.

Key Features of Cloud Computing

1. On-Demand Services: Users can access resources whenever needed without requiring physical installation.
2. Scalability: Resources can be scaled up or down based on demand.
3. Cost Efficiency: Pay-as-you-go pricing eliminates the need for upfront hardware investments.
4. Accessibility: Services are accessible from anywhere with an internet connection.
5. Reliability: Cloud providers often offer data backups, disaster recovery, and high availability.
6. Flexibility: Offers various services such as IaaS, PaaS, and SaaS to cater to different needs.

Cloud computing security is not just about preventing breaches but also about fostering innovation and growth in a secure environment. Cloud computing security encompasses a range of measures, practices, and technologies designed to protect data, applications, and infrastructures hosted in the cloud.

Literature Review

Cloud computing has emerged as a dominant paradigm in the world of computing, and it is now used by a wide range of users across various sectors. Currently, 80% of workloads are handled on the cloud [1]. However, despite its popularity, cloud computing introduces significant security risks. According to the Cloud Security Alliance (CSA), seven primary security threats have been identified:

1. Maltreat and Obnoxious Utilization of Cloud
2. Uncertain API
3. Vicious Infiltrators
4. Distributed Mechanism Challenges
5. Information Drop
6. Unidentified Risk Reports
7. Account, Service, and Traffic Hijacking

In response to these security concerns, IT companies allocate a significant portion of their budgets to safeguard cloud infrastructure. It is reported that 42% of an IT company's funds are spent on cloud security, and a large portion of future spending (around 80%) is expected to be directed towards solving security issues in the cloud.

Researchers have proposed several solutions to enhance cloud security, and these solutions typically fall into three primary categories:

1. Cryptographic Solutions
2. Data Storage Solutions
3. Data Semantics Solutions

This paper reviews the security concerns in cloud computing and explores several proposed models aimed at addressing these security challenges.

In recent years, the expansion of data has accelerated in terms of velocity, volume, and variety, leading to the rise of massive and complex big data[2].

This paper aims to collect and analyze the most common cyber security threats encountered in cloud environments, as well as the mitigation techniques that have been employed. To achieve this, a comprehensive review of published papers from 2019 to 2020 will be conducted. Additionally, a cloud risk assessment case

study will be presented, focusing on an organization based in Saudi Arabia, to provide a practical understanding of the risks and the application of mitigation strategies in a real-world context.

An [3] essential and well-defined research direction into the challenges of cloud computing, especially regarding data security and scheduling. It's clear that the key focus areas are:

1. **Challenges in Cloud Computing**:
   - **Security Issues**: Data confidentiality concerns when storing sensitive information on third-party servers.
   - **Scheduling Problems**: Efficient resource allocation in multi-user cloud environments, ensuring fair and optimal distribution of computational resources.
2. **Focus on Data Security**:
   - **Data Confidentiality**: Protecting sensitive data from unauthorized access or breaches.
   - **Data Integrity**: Ensuring data remains accurate, complete, and unaltered during transmission or storage.
   - **Data Availability**: Ensuring that cloud services and data remain accessible to authorized users even in the event of failures.
   - **Encryption and Access Control**: Various methods to secure data, including encryption both at rest and in transit, and fine-grained access control mechanisms to protect sensitive information.
3. **Review and Comparison of Recent Research**:
   - A scientific review would involve identifying and comparing recent studies, examining solutions to the issues of security, scheduling, and resource management.
   - Research might also explore hybrid or multi-cloud approaches, where resources are spread across multiple cloud providers to avoid reliance on a single vendor and to increase data protection.
4. **Recommendations Based on Findings**:
   - Based on your review of the literature, the goal would be to suggest valid, actionable recommendations for improving the security and resource scheduling of cloud computing platforms.

Some key considerations in your approach might include:

- **Cloud Deployment Models**: Public, private, and hybrid cloud models each have unique security and scheduling challenges. The research could address how these models impact data security and resource allocation strategies.
- **Cloud Service Models**: The three common models (IaaS, PaaS, SaaS) have different implications for security and resource management, with varying levels of responsibility for the cloud provider versus the consumer.
- **Security Technologies**: Reviewing encryption techniques (e.g., homomorphic encryption), access control mechanisms (e.g., role-based access control, attribute-based access control), and intrusion detection systems designed for cloud environments.
- **Case Studies**: Reviewing specific case studies of cloud computing security breaches or successful implementations of scheduling and resource allocation systems could provide valuable real-world insights.

This abstract appears to introduce a paper discussing the integration of cryptography and steganography in securing cloud data [4]. It mentions the use of cloud computing for on-demand network access to various computing resources and focuses on how these resources can be protected, particularly in terms of securing sensitive data.

Key Concepts:

1. **Cloud Computing**: The model for providing scalable and flexible computing resources over the internet, which includes servers, storage, and applications. The on-demand access model is emphasized, highlighting convenience and scalability.
2. **Security in Cloud Computing**: The paper addresses the need for securing private and sensitive information stored or transmitted over the cloud. It emphasizes the importance of encryption to ensure that data is unreadable to unauthorized individuals, even if they manage to gain access.
3. **Cryptography and Steganography**:
   - **Cryptography**: The process of securing data by transforming it into an unreadable format using algorithms (in this case, symmetric encryption). This ensures that only authorized parties can decrypt and read the data.
   - **Steganography**: This is the practice of hiding information in another medium, such as embedding data within images or audio files, to conceal the existence of the information. This can be used to add an additional layer of security.
4. **Symmetric Encryption**: The paper mentions the use of symmetric encryption, where the same key is used for both encrypting and decrypting the data. It is presented as a method to enhance the security of the data stored or transmitted in cloud systems.

Possible Areas of Exploration:

- **Symmetric Encryption Algorithms**: The paper may explore various symmetric encryption algorithms like AES (Advanced Encryption Standard) or DES (Data Encryption Standard) to analyze their effectiveness in securing cloud data.
- **Combining Cryptography and Steganography**: The integration of both methods could be explored to see how one could mask encrypted data within other forms of data, such as media files, for added protection. This could prevent detection of the data even if an unauthorized party intercepts it.
- **Practical Implementation**: The paper could provide examples or case studies where these methods are applied in cloud security scenarios, demonstrating their effectiveness in safeguarding sensitive data.

The concept you're describing combines multiple security techniques to provide a multi-layered defence against unauthorized data access during file or data transfer[5]. By combining cryptography and steganography, it can protect data at various levels, ensuring both its confidentiality and integrity.

1. Cryptographic Techniques (AES, DES, RC2)

- **AES (Advanced Encryption Standard)**: A symmetric encryption algorithm that is widely used for securing sensitive data. It uses the same key for both encryption and decryption, making it fast and secure. AES is efficient and commonly used in modern security systems for its strength.
- **DES (Data Encryption Standard)**: Another symmetric key encryption algorithm that uses a fixed 56-bit key. While DES was once the standard, it is now considered insecure due to its small key size, and modern systems have shifted to stronger algorithms like AES.
- **RC2 (Rivest Cipher 2)**: A variable key-size symmetric encryption algorithm. RC2 provides flexibility in key size, allowing for a balance between security and performance.

These algorithms are chosen because of their ability to securely encrypt and decrypt data using symmetric keys. AES, being the most secure of the three, would likely be the primary encryption algorithm, while DES and RC2 could serve as alternative options for different scenarios.

2. Steganography (LSB Technique)

- **LSB (Least Significant Bit) Steganography**: This technique hides data (typically the encryption key or a smaller file) within an image or audio file by modifying the least significant bits of the data. Since these bits have the smallest effect on the image or audio file, their alteration is often undetectable by the human eye or ear. LSB can be used to securely store the encryption key or other sensitive information within a file that is being transferred, thus hiding the key in plain sight.
- **Key Information Security**: In this system, the LSB technique can be used to hide the symmetric encryption key (used by AES, DES, or RC2) within a harmless-looking image or other file type. Even if the file is intercepted during transfer, the key would remain hidden, and without the right tools to extract the LSB data, the attacker wouldn't be able to decrypt the actual message.

3. Block-wise Security Implementation

- **Block-wise Processing**: This involves breaking the data into blocks (of fixed size) and applying encryption algorithms to each block individually. AES, DES, and RC2 are all block cipher algorithms, meaning they operate on fixed-size blocks of data, typically 128 bits.

The data can be divided into blocks, and each block can be encrypted with a symmetric key. To further strengthen security, the key can be hidden in the LSB of a cover file, as mentioned earlier.

4. Combining Steganography and Cryptography

By combining cryptography (AES, DES, RC2) with steganography (LSB), the system can achieve:

- **Layered Security**: Even if one security method is compromised, the other still provides protection. For example, if an attacker intercepts the encrypted file, they would still need to extract the LSB hidden encryption key (which itself is hidden in an image or audio file).
- **Confusion and Diffusion**: The use of cryptography provides confusion (hiding the relationship between plaintext and ciphertext) and diffusion (spreading the influence of the plaintext over the ciphertext), making it much harder for attackers to deduce any meaningful information.
- **Obfuscation**: The use of steganography ensures that the presence of any sensitive information (such as the encryption key) is hidden. This makes it much harder for attackers to even know there is something valuable being transmitted.

5. Proposed Approach

- **Data Transfer Workflow**:

1. **Step 1**: Data is divided into blocks.
2. **Step 2**: Each block is encrypted using one of the symmetric key algorithms (AES, DES, or RC2).
3. **Step 3**: The encryption key (or a portion of it) is embedded into a cover file (such as an image) using the LSB steganography technique.
4. **Step 4**: The encrypted blocks and the steganographically hidden key are transferred together to the recipient.
5. **Step 5**: The recipient extracts the key from the cover file (using steganographic decoding techniques), decrypts the data blocks using the symmetric key, and reassembles the original message.

This approach ensures that the data is protected not only by encryption but also by the concealment of the encryption key, adding an additional layer of security.

This proposed system, combining cryptographic techniques like AES, DES, and RC2 with stegano graphic methods (LSB), provides a comprehensive security mechanism for the transfer of sensitive data. The system ensures both encryption and the hiding of critical information, which is essential for maintaining confidentiality and integrity during the data transfer process. This multi-layered security approach enhances data protection, making it more resilient to attacks or unauthorized access.

In [6], the authors describe how cloud computing has significantly evolved through the adoption of modern technologies. The trend of integrating cloud services into organizational structures is gaining increasing importance. To reduce capital expenditures, companies are encouraged to consider cloud services as a fundamental component of their infrastructure. However, several challenges continue to hinder widespread deployment and adoption. One of the primary drawbacks of current cloud service implementations is their inability to provide a sufficiently high level of security.

In [7], the authors first discuss various security concerns related to cloud computing, including storage security, data security, network security, middleware security, and application security. They highlight the potential use of dense co-processors to enhance security measures. Their work culminated in the implementation of Hadoop. While many new technologies are emerging at a rapid pace each offering technological advancements and the promise of simplifying human life it is crucial to remain aware of the security risks and challenges associated with their adoption.

In [8], the authors examine various cloud architectures based on the services they provide. Data is stored in centralized locations known as data centres, which are capable of housing vast amounts of information. Both data storage and processing take place on servers, requiring clients to trust the service providers for data availability and security. Before migrating data to the public cloud, it is essential to address concerns regarding compatibility and security standards. A trusted monitor installed on the cloud server can serve as an auditor to oversee the server’s operations. To minimize potential trust-related security issues and address governance challenges in cloud computing, an essential control measure is the establishment of a well-defined Cloud Computing Service Level Agreement (SLA).

In [9], the authors focus on an emerging technology that is expected to significantly reduce the cost associated with current systems. Regarding data security, cloud computing introduces both advantages and disadvantages. The overall impact depends on our ability to enhance its strengths while mitigating its weaknesses. Only through this balanced approach can cloud computing improve productivity, deliver real cost savings, and offer a secure platform. Among the various concerns, the most critical is the security of data, whether at rest or in transit. The paper discusses several key security challenges associated with cloud infrastructure. It also outlines essential cloud security considerations that must be addressed to ensure data protection. Finally, the authors propose a secure cloud architecture aimed at safeguarding data against external threats.

In the paper [10], Jyoti Chaurasia and Om Prakash Karada discuss the emerging role of cloud computing in the IT industry, emphasizing its potential to reduce network costs while offering scalable services to clients. In cloud environments, resources are dynamically allocated based on the client's requirements. However, security remains a significant concern, posing a barrier to the full realization of cloud computing’s potential. The authors highlight that while many services are currently provided through cloud systems, the issue of secure authentication still demands robust solutions. To address this, the paper introduces a 3D password generation technique, along with its architecture, algorithms, and user interfaces. The study concludes by analysing the probability of the proposed authentication system being compromised.

Dinesha H. A. [11] highlights that cloud computing is an emerging technology offering software, hardware, infrastructure, and data storage as services. It is widely adopted to enhance business communication and service delivery. In such an environment, a strong password authentication system is essential. Cloud password authentication can be implemented using various methods, including textual, graphical, and 3D passwords. The paper proposes a robust password generation technique called multidimensional password authentication, which incorporates multiple input parameters from the cloud paradigm. The authors present this method along with its supporting architecture, sequence diagrams, algorithms, and user interfaces.

Similarly, Hong Liu [12] addresses the challenge of secure data sharing in cloud computing, where data is stored remotely on online cloud servers and accessed by multiple users who may have shared relationships. The paper proposes a Shared Authority-Based Privacy-Preserving Authentication (SAPA) protocol to enhance privacy and security in such scenarios. The SAPA protocol operates in three stages:

1. **Shared access authority** is established using a suspicious access request identification mechanism that considers authentication, data privacy, user privacy, and forward security.
2. **Attribute-based access control** ensures that users can only access their authorized data fields.
3. **Proxy re-encryption** is performed by the cloud server to facilitate secure data sharing among multiple users.

A theoretical model is also presented to demonstrate the correctness of the SAPA design. This approach supports privacy-preserving access authority sharing and is particularly suitable for multi-user collaborative cloud applications.

Geetanjali Choudhury and Jainul Abudin [13] explain that cloud computing is a concept that interconnects multiple computers in a real-time network, such as the Internet. It enables IT services to be provided to customers over a network on a rental basis to meet various requirements. Cloud computing also facilitates the sharing of distributed resources and services among different organizations. In private cloud systems, data is shared exclusively among authorized users. The authors propose a new authentication mechanism for cloud computing platforms based on Encrypted One-Time Passwords (EOTP). In this approach, the one-time password is encrypted using the user's public key to generate the EOTP, enhancing authentication security.

Similarly, Deepak G [14] discusses cloud computing as a revolutionary technology aimed at providing services over the Internet. The main objectives are to reduce computational costs and expand storage capacity. This paper focuses on addressing the challenge of user authentication in cloud environments. The author proposes a secure mobile cloud-based authentication algorithm, where the user's mobile phone acts as a verification tool. A one-time encrypted password is generated for the user and later decrypted based on the proposed algorithm, reinforcing secure access to cloud services.

Monika Agarwal [15] Textual Content Steganography Techniques proposed three different text steganography methods:

- **Missing Letter Puzzle Method**:
  - Each character of the secret message is hidden by removing one or two letters from words in a sentence.
  - The position and number of missing letters are based on the ASCII value of the character being hidden.
- **Word List Method**:
  - A list of words is constructed where the first letter and length of each word are based on the ASCII value of the secret character.
  - The secret is encoded in the structure of each word (starting letter + word length).

- **Cover File Method**:
  - Uses a pre-existing meaningful English text (not generated like the first two).
  - Secret bits are hidden using start and end letters of words in the cover text.

2. Mohit Garg [16] – HTML-Based Text Steganography

- Proposes a different type of text steganography using HTML files.
- The secret message is:
  - Encrypted using the Playfair cipher, then
  - Converted to binary, and then
  - Embedded in an HTML file structure.
- This adds both encryption and steganography for enhanced security.

3. Vishal Kolhe et al. [17] 3D Password Authentication

- A multifactor authentication system using a 3D virtual environment.
- Users create a 3D password by:
  - Navigating through a virtual space,
  - Interacting with virtual objects in a specific sequence.
- Each sequence and interaction forms a unique password, making it highly secure and difficult to replicate.

Paul A. J., Varghese Paul, and P. Mythili [18] discuss the use of various encryption standards such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), and EES (Escrowed Encryption Standard) which are widely adopted to secure communication over insecure channels. These encryption techniques are fundamental to ensuring data confidentiality and integrity during transmission in cloud environments.

Grover Aman and Narang Winnie [19] propose a 4-D password authentication system, which incorporates multifactor authentication by combining biometrics, graphical elements, and textual passwords. This method also includes gesture recognition and time tracking, providing enhanced security and making it a more robust authentication technique compared to traditional methods.

Richa Chowdhary and Satyakshma Rawat [20] focus on the implementation of One-Time Passwords (OTP) for authenticating access to services across multiple cloud platforms simultaneously. The paper begins with a detailed explanation of cloud computing and the use of multi-cloud environments in organizations. It then addresses the security challenges faced in cloud systems and emphasizes the role of OTP in mitigating these concerns.

Conclusion

The cloud, while offering flexibility and scalability, also introduces new vulnerabilities and threats to data integrity and privacy. The primary security concerns in cloud systems include data breaches, insecure interfaces, account hijacking, and inadequate data protection mechanisms. These threats have escalated the need for robust research focused on identifying vulnerabilities and developing mitigation strategies to address them. The rapid growth has brought significant challenges in terms of storage, management, analysis, and security. As a response to these challenges, many organizations have increasingly turned to cloud systems to handle their big data needs. However, a lack of awareness regarding the security and privacy risks associated with cloud systems has resulted in the neglect of critical practices and techniques that should be implemented to secure these environments.

References:-

[1] Riddhi Doshi, Vivek Kute, "A Review Paper on Security Concerns in Cloud Computing and Proposed Security Models", Computer Engineering Department St. Vincent Pallotti College of Engineering and Technology Nagpur, India vivekkute@rediffmail.com,2020

[2] Roaa Al Nafea, Mohammed Amin Almaiah et.al, "Cyber Security Threats in Cloud: Literature Review", International Conference on Information Technology (ICIT),2021

[3] Faya Safar, Raddad Al King, "Data Security in Cloud Computing", Syrian university International Journal of Wireless and Ad Hoc Communication (IJWAC) Vol. 07, No. 01, PP. 50-61, 2023

[4] Faluyi Bamidele Ibitayo et al, "Securing Cloud Computing Contents with Cryptography and Steganography", International Journal of Science and Engineering Applications Volume 11-Issue 06, 76 - 88, 2022, ISSN:- 2319 – 7560 DOI: 10.7753/IJSEA1106.1002 www.ijsea.com 76, Department of Computer Science, Osun State College of Technology, Esa-Oke. Nigeria

[5] K Annsheela1 , S Habeeb Mohamed Sathak Amina, "Establishing a Secure File Transfer Using Hybrid Cryptography and LSB Stenographic Techniques", International Journal of Science and Research (IJSR) ISSN: 2319-7064 SJIF (2022): 7.942 Volume 13 Issue 5, May 2024 Fully Refereed | Open Access | Double Blind Peer Reviewed Journal www.ijsr.net

[6] Osama Harfoushi, "Data Security issues and challenges in Cloud Computing: A Conceptual Analysis and Review", Communications and Network, 2014, 6, 15-21

[7] P.Radha Krishna Reddy, "The Security Issues of Cloud Computing over Normal & IT Sector", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 3, p. 4, March 2012.

[8] Geethu Thomas," Cloud Computing Security using encryption technique", https://arxiv.org/ftp/arxiv/papers/1310/1310.8392.pdf , 2013

[9] Manas M N, "Cloud Computing Security issues and Methods to Overcome", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 4,p. 3, April 2014.

[10] Jyoti chaurasia & Om Prakash Karada "Three-Dimensional Password Generation Technique for Accessing Cloud Services" ISSN (Print) : 2319 – 2526, Volume-2, Issue-4, 2013 International Journal on Advanced Computer Theory and Engineering (IJACTE)

[11] Dinesha H A and Dr.V.K Agrawal, "Multi dimensional password generation techniques for accessing cloud services", International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.3, June 2012 DOI : 10.5121/ijccsa.2012.2304 31

[12] Hong Liu, Huansheng Ning, Qingxu Xiong and Laurence T. Yang, "Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing", DOI 10.1109/TPDS.2014.2308218, IEEE Transactions on Parallel and Distributed Systems

[13] Geetanjali Choudhury, Jainul Abudin, "Modified Secure Two Way Authentication System in Cloud Computing Using Encrypted One Time Password", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4077-4080,www.ijcsit.

[14] Deepak G, Dr. Pradeep. B. S , Shreyas Srinath , "Dynamic Key Generation Algorithm for User Authentication at Mobile Cloud Environment" International Journal of Science and Research (IJSR), 2014

[15] Monika Agarwal, "Text steganographic approaches : A comparison" , International Journal of Network Security & Its Applications (IJNSA)", Vol.5, No.1, January 2013 DOI : 10.5121/ijnsa.2013.5107 91

[16] Mohit Garg, "A Novel Text Steganography Technique Based on Html ",International Journal of Advanced Science and Technology Vol. 35, October, 2011 129

[17] Vishal Kolhe, Vipul Gunjal, Sayali Kalasakar, Pranjal Rathod ,"Secure Authentication with 3D Password", Volume 2, Issue 2, page no. International Journal of Engineering Science and Innovative Technology (IJESIT) March 2013

[18] Paul. A.J*, Varghese Paul, P. Mythili, "A fast and secure encryption algorithm for message communication", International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007),

[19] Grover Aman, Narang Winnie,"4-D password: Strenting the authentication scene", volume 3 Issue 10, International Journal of Scientific and Research Publications, October-2012, ISSN 2229-5518

[20] Richa Chowdhary Satyakshma Rawat, " One Time Password for Multi-Cloud Environment ", Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering Research Paper Available online at: www.ijarcsse.com