INTERNATIONAL JOURNAL FOR INNOVATIVE RESEARCH IN MULTIDISCIPLINARY FIELD
ISSN(O): 2455-0620 [Impact Factor: 9.47]
Monthly, Peer-Reviewed, Refereed, Indexed Journal with IC Value : 86.87
Volume - 12, Issue - 7, July - 2026

DOIs:10.2015/IJIRMF/202607019 --:-- Research Paper / Article / Review

SECURING CLOUD COMPUTING DATA USING CRYPTOGRAPHY AND STEGANOGRAPHY

Dinesh Kumar Moriya
Research Scholar, Computer Science
Madhyanchal Professional University, Bhopal (M.P.)

Abstract: *The research presented in these papers highlights a growing emphasis on securing cloud computing data through the integration of cryptographic and steganography techniques. Cryptographic methods such as hash functions, RSA, and AES provide strong encryption to protect data from unauthorized access. Complementing these, steganography adds an additional layer of confidentiality by concealing sensitive information within other media. As cloud computing continues to expand, the adoption of hybrid security models that combine these approaches will be essential in addressing key challenges such as data breaches, unauthorized access, and integrity violations. Various research papers reviewed to find problem statement with methodology used in each research.*

Keywords: *Cryptography, Steganography, Cloud Computing, RSA, AES.*

1.INTRODUCTION :

Cloud computing has emerged as a transformative technology that shifts computing and data management from personal desktops and portable devices to centralized data centers. This technology allows applications and services to be delivered over the internet, rather than relying on local resources. The cloud infrastructure, comprising hardware and system software in data centers, provides the backbone for these services, offering scalability, flexibility, and accessibility to users globally.

The evolution of cloud computing has led to the rise of new security concerns, particularly as more sensitive data is stored in the cloud and transmitted across networks. Data privacy, access control, and protection against cyber threats are critical considerations. As a result, various encryption and data protection techniques have been proposed to secure cloud-based information, ensuring that unauthorized users cannot access or tamper with the data.

Steganography, a technique for hiding information within another medium (such as text, audio, video, or images), has found its application in enhancing the security of data transmitted over networks, including cloud systems. Unlike cryptography, which focuses on making information unreadable to unauthorized parties, steganography conceals the existence of the message itself. This makes steganography a valuable tool for securely transmitting sensitive data in environments like cloud computing, where data privacy is a paramount concern.

2.Literature Review

Cloud computing refers to the delivery of computing services including infrastructure, platforms, and software by a third-party organization known as a cloud service provider (CSP). These services are made available to organizations and individuals over the internet. CSPs dynamically allocate their computing resources based on demand, and these resources are often shared among multiple corporate and private clients. As the number of subscribers to cloud-based services continues to grow, concerns about cloud security have become increasingly significant. Review paper examines current cloud security issues and practices and proposes several innovative solutions aimed at enhancing the security of cloud computing in the future[1]

In recent years, cloud computing has proven its significance, becoming essential for both small and large organizations. Its importance stems from the diverse range of services it offers, one of which is Storage as a Service (SaaS). SaaS enables users to store their data in cloud-based databases. However, a major drawback of this service is the associated security challenges, as data is managed by a third party [2]. Therefore, it is crucial to develop models that enhance data security, ensuring users feel confident storing their information in the cloud.

Image steganography presents a promising solution for protecting data against unauthorized access. It allows users to conceal sensitive information within a cover image, providing an additional layer of security. In the proposed paper, review and compare recent studies that have employed image steganography to secure cloud-stored data. The comparison is conducted in two parts: the first evaluates the models based on the algorithms used, along with their respective advantages and limitations. The second compares the models based on the three primary objectives of steganography: quality (the ability to produce high-quality stego-images), security (how well the hidden data is protected from detection), and capacity (the amount of data that can be concealed).

Cloud computing enables organizations to access computing and storage resources on a rental basis, significantly reducing the need for substantial investments in physical infrastructure. While this model offers numerous benefits, it also introduces critical concerns regarding the security and privacy of data. With the increasing integration of cloud services into smart mobile applications, safeguarding sensitive information has become even more vital[3]. In the paper, author explore how steganography a technique for concealing information within non-suspicious media can be employed to enhance the security and privacy of cloud-stored data accessed by mobile applications. Our proposed approach embeds a secure key within an image, alongside the data, creating an additional layer of protection against unauthorized access.

Cloud computing and its associated security concerns continue to be prominent topics within contemporary research. While numerous surveys on cloud security have been conducted, a noticeable gap remains in effectively mapping specific security issues to their corresponding counter measures [4]. Existing surveys often focus on isolated aspects such as virtualization vulnerabilities or access control mechanisms without offering a unified framework that both generalizes cloud security concepts and provides a detailed analysis of its unique requirements. Furthermore, many proposed countermeasures fail to explicitly indicate the specific issues they address, leading to a lack of clarity and coherence. This survey paper aims to bridge these gaps by presenting a comprehensive approach that not only interconnects various security aspects but also clearly aligns each countermeasure with its respective threat. Finally, it outlines a set of open challenges in the domain, offering a roadmap for future research.

Over the past three decades, the world of computation has evolved significantly from centralized systems (such as traditional client-server models) to distributed architectures, and now toward a form of virtual centralization via cloud computing. The location of data and processes plays a crucial role in this evolution. In traditional computing, individuals or organizations maintained full control over their data and processes, typically hosted on premise. In contrast, cloud computing shifts this control to service providers, who manage both the infrastructure and data storage, often obscuring the actual location and operational details from the end user [5].

Cloud computing relies heavily on the internet for communication and service delivery. This raises concerns around data security and privacy, especially since clients typically lack visibility into where their data is stored or how it is processed. To address these concerns, cloud service providers are expected to offer clear assurances regarding security practices through Service Level Agreements (SLAs). These SLAs are essential for organizations that rely on cloud computing as a critical service infrastructure, particularly when handling sensitive or business-critical applications.

However, ensuring data security in the cloud remains a complex challenge. This complexity is compounded by the different service models offered Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) each of which presents unique security challenges. Consequently, SLAs must clearly articulate the security measures and responsibilities associated with each service model to help customers make informed decisions. Establishing standardized SLA formats across providers could further enhance transparency and encourage broader adoption of cloud services by reducing ambiguity around security practices.

Cloud platforms offer a vast array of services, concepts, and applications including storage, processing power, virtualization, connectivity, and data sharing. They enable users to access software applications delivered as services over the internet, as well as the underlying hardware and system software hosted in data centres. With such a broad spectrum of benefits, it's clear that cloud computing is not only here to stay but is poised for significant growth in the future [6].

However, like all powerful technologies, cloud computing is not without its challenges. One of the most pressing concerns is ensuring user privacy and the secure migration of sensitive data. As organizations move data from private clouds to public clouds, safeguarding this information becomes critical. To address this, the proposed system integrates encryption and steganography techniques to ensure secure data migration while preserving confidentiality and integrity.

Cloud computing is predominantly provisioned through three service delivery models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). While these models offer scalability and flexibility, they are also susceptible to a wide range of security attacks, including those unique to cloud environments as well as traditional web-based vulnerabilities. Taxonomies play a critical role in helping system designers systematically understand, identify, and address these security risks. In this research, author collect and classify cloud-based attacks and vulnerabilities according to their respective service models. Furthermore, propose a comprehensive taxonomy of cloud security threats along with potential mitigation strategies, aiming to provide an in-depth understanding of the security requirements within cloud environments. The study also underscores the importance of implementing Intrusion Detection and Prevention as a Service (IDPS) as a key component of cloud security frameworks [7].

This systematic literature review (SLR) examines the intersection of Machine Learning (ML) and Cloud security, analyzing 63 relevant studies to understand how ML is applied to tackle security challenges in the Cloud. [8]

3.Key Findings:

1. Three Core Research Areas:
    - Types of Cloud security threats
    - ML techniques used to address these threats
    - Performance outcomes of these techniques
2. Security Focus Areas (11 in total):
    - Most addressed threats include:
        - Distributed Denial-of-Service (DDoS) – 16%
        - Data privacy – 14%
3. Machine Learning Techniques:
    - 30 ML techniques identified
    - Use of hybrid and standalone models
    - Support Vector Machines (SVM) is the most popular ML technique
4. Performance Evaluation:
    - 60% of papers benchmark their models against others
    - 13 different evaluation metrics identified
        - Most common: True Positive Rate
        - Least common: Training Time
5. Datasets:
    - 20 datasets mentioned across studies
    - Most commonly used: KDD and KDD CUP’99

According to Khorshed et al. [9], gaps in Cloud computing primarily stem from trust issues between customers and Cloud service providers. Customers are often concerned about the lack of transparency, particularly regarding hidden policies that may affect data security or service reliability. Conversely, Cloud providers fear that customers may misuse their services for malicious purposes, such as launching cyber-attacks. The decision to select a particular Cloud provider is largely influenced by organizational expectations and the specific services or capabilities offered by the provider.

According to Modi et al. [10], vulnerabilities are defined as security loopholes in the Cloud that adversaries can exploit to gain unauthorized access to the network and other infrastructure resources. A Cloud threat, on the other hand, refers to a potential adverse event, which may be either intentional (malicious) or unintentional (accidental).

The expert discusses the growing popularity of cloud computing services, which bring both benefits and security challenges. Specifically, the paper focuses on the risks related to the high concentration of data on the cloud, making it a prime target for security attacks such as Denial of Service (DoS), data theft, and privacy breaches. It also highlights the issue of cloud providers potentially failing to meet their performance, availability, and security commitments as per Service Level Agreements (SLAs). [11]

The main point of the paper is the need for secure and efficient mechanisms that allow users to transparently move and copy their data between different cloud providers. The authors explore state-of-the-art techniques for inter-cloud data migration, particularly in the context of the Hadoop Distributed File System (HDFS), a widely used system for managing big data across clusters of computers. The paper proposes an inter-cloud data migration mechanism that promises better security and faster response times for migrating large-scale data files in cloud database systems.

The authors validate the performance of their proposed mechanism by measuring its impact on response time and throughput, comparing it to other techniques in existing literature. The results show that their approach significantly improves the performance of HDFS, outperforming other methods.

In summary, this work aims to enhance the security and efficiency of data migration across cloud platforms, offering an improved solution for handling large-scale data migration in cloud environments.

The issue of live migration of virtual machines (VMs) across different cloud providers with different hypervisors, which currently face challenges related to performance, flexibility, and security. Here's a breakdown of the key points from the paper: [12]

1. **Current Challenges**:
    - Cloud providers typically use proprietary hypervisors to manage their VMs, which creates tight coupling between VMs and the underlying hardware. This coupling hinders the ability to migrate VMs between different providers or environments efficiently.
    - Existing solutions from both academia and industry have attempted to address this issue but face challenges in three major areas:
        - **Performance**: The migration process often leads to downtime, which affects the VM's availability.
        - **Flexibility**: The VM's tight integration with the underlying hardware prevents seamless migration between different platforms.
        - **Security**: Ensuring secure migration of VMs while maintaining the integrity of data and application functionality.
2. **Proposed Solution - LivCloud**:
    - **LivCloud** is proposed as an open-source cloud orchestrator designed to address the limitations of existing migration approaches.
    - Key components of **LivCloud** include:
        - **Developed Transport Protocol**: For efficient communication during migration.
        - **Overlay Network**: A virtual network layer that abstracts the underlying physical network, allowing more flexibility.
        - **Secured Migration Channel**: Ensures secure transfer of VMs across different environments.
3. **Evaluation**:
    - The paper also includes an initial evaluation of live migration in a LAN (Local Area Network) environment, with a focus on:
        - **Nested Virtualization Environment**: This is a setup where virtualization is used inside other virtualized environments.

        - **Migration between Different Hypervisors**: Moving VMs between hypervisors from different vendors.
    - The evaluation measures the impact of live migration on several factors:
        - **Network Throughput**: The amount of data successfully transferred across the network during migration.
        - **Network Latency**: The delay in data transmission during migration.
        - **CPU Utilization**: The amount of CPU resources consumed during migration.
    - The results showed that optimization is needed in LAN environments to improve the performance of live migration.

Overall, the paper highlights the need for a solution like LivCloud to improve the performance, flexibility, and security of VM migration in cloud environments, addressing the limitations of existing methods.

Research paper focused on cloud security, particularly the security concerns related to data migration between different cloud environments. The paper proposes a mechanism to address these concerns and includes a prototype implementation based on Hadoop Distributed File System (HDFS). Here's a summary of the key points discussed in the text:[13]

1. **Cloud Security Concerns**: While much of cloud security research focuses on securing operating systems, virtual machines, and data storage within a cloud system, this paper shifts attention to the security of data migration between clouds.
2. **Threats during Data Migration**: The paper identifies potential threats that may arise when migrating data between different clouds, though it doesn't detail them in the provided excerpt.
3. **Proposed Security Mechanism**: The authors propose a security mechanism to address these threats during data migration. This includes:
    - **SSL Negotiation**: Secure Sockets Layer (SSL) negotiation to ensure a secure communication channel.
    - **Migration Ticket Design**: A system to control and authenticate data migration requests.
    - **Block Encryption**: Encrypting data blocks to protect sensitive information during migration, with support for distributed file systems and parallel computing in a cluster environment.
4. **Prototype and Evaluation**: The paper mentions designing a prototype to implement this security mechanism, utilizing Hadoop Distributed File System (HDFS) as the underlying system. A series of tests are conducted to evaluate the prototype's effectiveness in securing data migration.

The advantages and challenges of migrating to Cloud Computing, as written [14] focus is on how Cloud Computing offers a range of benefits, including:

- **On-demand services**
- **Agility**
- **Scalability**
- **Reduced IT overhead**
- **Greater flexibility**
- **Cost reduction**

However, despite these advantages, the migration to Cloud Computing is not without its challenges, especially around security and other potential barriers. The paper likely dives deeper into the specific hurdles organizations face when making the transition to cloud infrastructure.

The growing adoption of cloud computing and the security concerns associated with migrating legacy systems to the cloud. Here's a breakdown of the key points:[15]

1. **Cloud computing as a Paradigm**: The first part of the passage highlights cloud computing as a modern paradigm that combines multiple computing concepts and internet technologies. This provides a more agile and cost-effective platform for business applications and IT infrastructure.

2. **Increasing Adoption of Cloud Computing**: It mentions the steady growth in cloud computing's adoption, suggesting that the technology is becoming more accepted and is maturing over time.
3. **Security Concerns**: A significant concern raised by consumers when moving their data and applications to the cloud is security. This is a common theme when discussing cloud adoption, as businesses worry about the safety and privacy of their data in a third-party environment.
4. **Security in Legacy System Migration**: The passage transitions to focus on the migration of legacy systems to the cloud. The key motivation for discussing security here is the need to address potential risks, requirements, and concerns that arise during this process.
5. **Approach to Security in Migration**: The author mentions carrying out an approach related to security in migration processes, which involves identifying the needs, concerns, and opportunities regarding security in moving legacy systems to the cloud. This is crucial for ensuring that the migration is successful while maintaining data security.

Security Concerns in Legacy System Migration:

When moving legacy systems to the cloud, several security concerns should be addressed:

- **Data Integrity and Confidentiality**: Ensuring that sensitive data is protected and not tampered with during migration.
- **Compliance with Regulations**: Ensuring that the migration process complies with industry regulations (e.g., GDPR, HIPAA).
- **Risk of Data Breaches**: Safeguarding against unauthorized access and data breaches during the transfer of legacy systems to the cloud.
- **Access Control and Authentication**: Implementing strong access controls to ensure that only authorized personnel can access the system.
- **Data Backup and Recovery**: Ensuring that robust backup and disaster recovery processes are in place during and after migration.

Benefits of Addressing Security in Migration:

- **Reduced Risk**: Addressing security early in the migration process reduces the chances of data breaches or loss.
- **Increased Trust**: By taking the necessary security measures, organizations can build trust with customers and stakeholders.
- **Regulatory Compliance**: Ensuring that the migration adheres to relevant laws and regulations can prevent legal issues.

The author, [16] emphasizes that cloud computing is particularly appealing to business vendors because it eliminates the need for users to plan resource allocation in advance. Instead, organizations can start with minimal resources and scale up as demand increases.

A model proposed by Ebrahim et al. that combines encryption and steganography to secure data in the cloud. Let me break it down: [17]

1. **Phase 1: Hashing and RSA Encryption**
    - The secret data first undergoes a hashing process using SHA-256 to generate a unique fixed-size hash value.
    - Then, RSA encryption is applied to both the hash value and the session key, ensuring secure transmission and storage of the key and the integrity of the data.
2. **Phase 2: AES Encryption**
    - The actual secret data is then encrypted using AES-256. AES is a symmetric encryption algorithm, and AES-256 is considered highly secure, using a 256-bit key to protect the data.
3. **Phase 3: Steganography**

- The encrypted data is then embedded into a cover image using the Least Significant Bit (LSB) algorithm. This step ensures that the data is hidden in plain sight, making it less likely to be detected.

Evaluation and Results:

- The authors evaluated their proposed model and compared it with others in terms of security and performance.
- Security against cryptanalysis and steganalysis attacks: Their model was found to be secure against common methods used to break encryption and detect hidden data in steganography.
- Statistical changes: The model also made sure that there are minimal statistical changes to the stego image, ensuring that the hidden data is less likely to be discovered by analyzing patterns in the image.
- High-quality stego image: Despite embedding data, the final image retains its quality, which is crucial to prevent suspicion or detection.

Overall, this model seems to offer a comprehensive approach to securing cloud data by integrating encryption with steganography, providing both confidentiality and un-detectability.

The technique described by Seshubhavan et al. in the reference that have mentioned (presumably) proposes a hybrid method combining steganography and genetic algorithms to securely store data in the cloud. Here's a breakdown of the approach outlined:[18]

4. Key Steps:

1. **Image Conversion to Grayscale**:
   - The technique works specifically on grayscale images. If the cover image is colored, it must first be converted into grayscale. This is done to simplify the processing by reducing the complexity of color channels.
2. **Bit-Level Representation**:
   - The least significant bit (LSB) and most significant bit (MSB) of the grayscale image are extracted. These bits are crucial because the LSB often carries minimal visual information, making it ideal for hiding secret data without significantly altering the image's appearance.
   - Both the LSB and MSB are converted into binary arrays (0's and 1's).
3. **AES Encryption**:
   - The secret data (likely the message or file to be hidden) is encrypted using the AES (Advanced Encryption Standard) algorithm. This encryption is done using the key, which has also been converted into a 0's and 1's array (as the encryption key itself is likely a binary sequence).
4. **Combining Arrays**:
   - The binary arrays representing the image's LSB, MSB, and the AES-encrypted secret data are combined. This merged sequence forms the "payload" that will be embedded in the cover image.
5. **Genetic Algorithm Application**:
   - The combined binary data is split into two blocks: the R Block (Right block) and the L Block (Left block).
   - A genetic algorithm is used on these blocks to produce an address block. The address block is essentially a map of where in the cover image the secret data will be embedded.
6. **Embedding Data into the Image**:
   - The address block generated by the genetic algorithm is used to modify the pixel values of the cover image. The secret data is embedded into the image in such a way that the least significant bits of selected pixels are replaced with the encrypted binary data.
7. **Stego Image Creation**:
   - The modified image, which now contains the secret data, is referred to as the stego image. This stego image is then stored in the cloud database. Since the changes to the image are subtle (as only the LSB is modified), the stego image looks visually identical to the original cover image, ensuring that the hidden data remains secure and difficult to detect.

The key elements of this approach are:

- **Steganography**: Hiding data within the image by modifying the LSB and MSB.
- **Genetic Algorithm**: Optimizing the embedding locations to ensure minimal distortion to the cover image.
- **AES Encryption**: Ensuring that the secret data remains secure by encrypting it before embedding.

This combination of methods enhances both the security (via AES encryption) and the imperceptibility (via steganography) of the embedded data, making it suitable for secure cloud storage where the integrity of the cover image is important.

The research as mentioned by Rahman et al. [19] proposes an innovative approach to enhance data security in the cloud using a combination of encryption and steganography. Here's a breakdown of their approach and key features:

1. **Blowfish Encryption**: The Blowfish algorithm is a symmetric encryption algorithm that Rahman et al. used to encrypt the secret data. It's known for its speed and efficiency, making it a good choice for encrypting data in cloud environments.
2. **E-LSB (Enhanced Least Significant Bit) Steganography**: After the data is encrypted, Rahman et al. used an embedding technique based on the E-LSB algorithm to hide the encrypted data within a cover image. This technique modifies the least significant bits of pixels in the image to embed data in a way that is difficult to detect visually.
3. **SHA-256 for Integrity Preservation**: To ensure the integrity of the stego-image (the image with the hidden encrypted data), they used SHA-256, which is a cryptographic hash function. SHA-256 generates a fixed-size hash of the stego-image, and this hash can later be used to verify whether the image has been altered or tampered with.
4. **Security Analysis**: According to their analysis, the model they propose is resilient to both statistical and visual attacks:
    - **Statistical Attacks**: These involve analyzing the distribution of pixel values and detecting anomalies that could reveal the presence of hidden data. The combination of encryption (with Blowfish) and steganography (with E-LSB) makes it difficult to detect such patterns.
    - **Visual Attacks**: These attacks try to detect any visual distortion in the cover image after embedding the secret data. By using E-LSB, the changes made to the image are minimal and difficult to notice by the human eye, providing a good level of visual security.

5. Conclusion

Despite its potential, cloud computing is still in its early stages and faces several challenges that need to be addressed. The paper focuses on these research challenges, suggesting that while the cloud computing model offers numerous opportunities, particularly to industries reliant on information technology, its widespread adoption and development are still in progress. In summary, while cloud computing offers numerous benefits such as agility and cost-effectiveness, security remains a crucial aspect, especially during the migration of legacy systems. Addressing these security concerns will ensure that businesses can leverage the advantages of the cloud while keeping their data safe.

The approach of combining encryption with steganography and using a hash function to maintain integrity creates a robust security mechanism for cloud data storage, making it resistant to various types of attacks.

References:

[1] Sanjevi Kumar A, A Rajlingam, B Gokila, "Study Analysis of Cloud Security Challenges and Issues in Cloud Computing Technologies", Journal of Science, Computing and Engineering Research (JSCER) Volume-6, Issue- 8, August 2023. DOI: https://doi.org/10.46379/jscer.2023.0608002

[2] Afrah Albalawi , Nermin Hamza, "A Survey on Cloud Data Security using Image Steganography", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 1, 2020

[3] Santosh Kumar Singh , Dr. P.K.Manjhi , Dr. R.K.Tiwari , "Cloud Computing Security Using Steganography", Journal of Emerging Technologies and Innovative Research (JETIR) www.jetir.org 9232019 JETIR June 2019, Volume 6, Issue 6 www.jetir.org (ISSN-2349-5162) JETIR1907G28

[4] Srijita Basu , Arjun Bardhan, Koyal, Gupta, Payel Saha et.al, "Cloud Computing Security Challenges & Solutions-A Survey", Institute of Engg. & Management Kolkata, India, 2018

[5] Balachandra Reddy , Kandukuri Ramakrishna Paturi et.al, "Cloud Security Issues", Advanced Software Technologies International Institute of Information Technology Pune, India, 2009 IEEE International Conference on Services Computing, 2009

[6] Harjot Kaur and Dinesh Kumar, "DATA MIGRATION FROM PRIVATE CLOUD TO PUBLIC CLOUD USING ENCRYPTION AND STEGNOGRAPHY TECHNIQUE", INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY DOI: 10.5281/zenodo.1165928, 2018

[7] Salman Iqbal et al , "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service", Contents lists available at ScienceDirect journal homepage: www.elsevier.com/locate/jnca Journal of Network and Computer Applications Elsevier.2016

[8] ALI BOU NASSIF , MANAR ABU TALIB et. Al, "Machine Learning for Cloud Security: A Systematic Review", OpenUAE Research and Development Group, University of Sharjah,2015

[9] M. T. Khorshed, A. B. M. S. Ali, and S. A. Wasimi, ''Trust issues that create threats for cyber attacks in cloud computing,'' in Proc. IEEE 17th Int. Conf. Parallel Distrib. Syst., Dec. 2011, pp. 900–905, doi: 10.1109/ICPADS.2011.156.

[10] C. Modi, D. Patel, B. Borisaniya, A. Patel, and M. Rajarajan, ''A survey on security issues and solutions at different layers of cloud computing,'' J. Supercomput., vol. 63, pp. 561–592, Oct. 2013, doi: 10.1007/s11227-012-0831-5

[11] Wei Hao, I-Ling Yen and Bhavani Thuraisingham,"Dynamic Service and Data Migration in the Clouds", 2009 33rd Annual IEEE International Computer Software and Applications Conference.

[12] Qingni Shen, Lizhe Zhang, Xin Yang, Yahui Yang, Zhonghai Wu, Ying Zhang, "SecDM: Securing Data Migration Between Cloud Storage Systems",2011 Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing.

[13] Rabi Prasad Padhy, Manas Ranjan Patra,Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) ,Vol. 1, No. 2, December 2011.

[14] Sh. Ajoudanian and M. R. Ahmadi, "A Novel Data Security Model for Cloud Computing", IACSIT International Journal of Engineering and Technology, Vol. 4, No. 3, June 2012.

[15] Rajesh Piplode, Umesh Kumar Singh, "An Overview and Study of Security Issues & Challenges in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.

[16] Kangchan Lee, "Security Threats in Cloud Computing Environments", International Journal of Security and Its Applications, Vol. 6, No. 4, October, 2012

[17] M. A. Ebrahim, I. A. El-Maddah, and H. K. Mohamed, "Hybrid model for cloud data security using steganography," in 2017 12th International Conference on Computer Engineering and Systems (ICCES). IEEE, 2017, pp. 135–140.

[18] M. Seshubhavan, D. Suneetha, and S. A. Varma, "A novel approach for data security for cloud data using image steganography and genetic algorithms." Grenze International Journal of Engineering & Technology (GIJET), vol. 4, no. 3, p. 137, 2018. [Online]. Available: http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=134178986&lang=ar&site=eds-live

[19] M. O. Rahman, M. K. Hossen, M. G. Morsad, and A. Chandra, "An approach for enhancing security of cloud data using cryptography and steganography with e-lsb encoding," IJCSNS, vol. 18, no. 9, p. 85, 2018.