IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Securing Confidential Communications by Employing Encryption and Steganography for Financial Organization

[1] Dr.P.Sumthi, [2] T.Kavya, [3] M.Saheel, [4] V.Saravankumar, [5] V.Raji

[1]Head of the department, [2] Student*, [3] Student*', [4] Student*, [5] Student*
Department of Artificial intelligence and data science,
SNS College of Engineering Coimbatore, India.

***ABSTRACT**:* Cloud-based data storage presents numerous advantages over traditional paper records and client-server systems, particularly concerning image data security. As organizations increasingly turn to the cloud for their image data storage needs, addressing security challenges becomes imperative. This paper proposes a comprehensive security framework integrating cryptography, steganography, and Hadamard transforms to ensure the privacy, confidentiality, integrity, and tamper-resistance of image data in cloud-based storage systems. The system utilizes distributed attribute-based encryption for simplified key management, employs Hadamard transforms to enhance data integrity, and combines multiple cryptographic algorithms such as RC6 with LSB steganography for secure storage of key information within image data. Multithreading techniques are employed during the encryption process to improve efficiency. The proposed system offers a comprehensive approach to securing image data in the cloud, catering to organizations and individuals concerned with data privacy and security

Keywords: Cloud-based storage, cryptography, steganography, Hadamard transforms, image data security, distributed attribute-based encryption, RC6, LSB steganography, multithreading techniques.

INTRODUCTION

The advent of cloud computing has revolutionized data storage and management, blurring the lines between virtual and physical realms. In this digital domain, image data emerges as a linchpin of modernization, driving innovation across industries. However, beneath the veneer of progress lies a shadowy realm of uncertainty, where the security of image data hangs precariously in the balance. Recognizing this challenge, this paper embarks on a journey through the intricate landscape of cloud-based storage systems, guided by the beacon of cryptographic techniques, steganography, and the venerable Hadamard transforms.At its core, this endeavor seeks to fortify the security posture of cloud-based storage, safeguarding the confidentiality and integrity of image data amidst the evolving threat landscape. By integrating advanced cryptographic methods, such as distributed attribute-based encryption, the framework aims to simplify key management and enhance access control. Additionally, the incorporation of Hadamard transforms introduces an extra layer of security, bolstering data integrity and resilience against tampering.Furthermore, the framework harnesses the concealment capabilities of steganography, particularly LSB steganography, to securely embed key information within image files. This ensures that critical encryption details remain hidden from prying eyes, further enhancing the overall security of the system. Through meticulous implementation and optimization, including multithreading techniques for efficient processing, the framework endeavors to establish a robust defense mechanism against cyber threats.In essence, this paper represents a call to arms in the battle for data security within cloud-based storage systems. By leveraging the synergies between cryptographic techniques, steganography, and Hadamard transforms, the framework endeavors to safeguard the sanctity of image data, preserving its integrity in the face of adversity. In doing so, it paves the way for a future where digital innovation thrives within a secure and resilient ecosystem.

EXISTING SYSTEM

In the contemporary landscape of digital data management, the shift towards cloud-based storage solutions has been swift and profound, driven by the allure of scalability, accessibility, and cost-efficiency. However, this transition has brought to the forefront a myriad of security challenges, particularly concerning the protection of image data. While traditional cryptographic methods serve as the cornerstone of data security, the complex nature of cloud environments introduces new complexities that necessitate innovative approaches.

One of the primary challenges organizations face in securing image data within cloud-based storage systems is managing encryption keys. In scenarios where multiple data owners and security domains are involved, the task becomes exponentially more challenging. Coordinating and maintaining encryption keys across disparate entities is a cumbersome process prone to errors and vulnerabilities. Consequently, there is a pressing need for solutions that simplify key management while ensuring granular access control and confidentiality.

To address these challenges, a distributed attribute-based encryption (DABE) scheme is proposed. This scheme allows access to image data from any source using a single key, thereby streamlining key management processes and reducing administrative overhead. By leveraging DABE, organizations can implement fine-grained access control policies tailored to their specific security requirements, thus enhancing the overall security posture of their cloud-based storage systems.

In addition to traditional cryptographic methods, the integration of Hadamard-based techniques presents an opportunity to further bolster the security of image data in the cloud. Hadamard transforms, renowned for their applications in signal processing and data compression, offer a unique approach to encrypting and protecting image data. By incorporating Hadamard transforms into the security framework, organizations can introduce an additional layer of security and data integrity, thereby mitigating the risk of unauthorized access and tampering.

Furthermore, the proposed system adopts a comprehensive approach to image data security by combining multiple cryptographic algorithms with steganography. Steganography, particularly least significant bit (LSB) steganography, is utilized to securely store key information within images. This ensures that critical encryption details, including the algorithms used and their respective keys, are concealed within the image files themselves, further enhancing the confidentiality and integrity of the data.

During the encryption process, the image undergoes transformation using Hadamard transforms and is then split into two parts, each encrypted simultaneously using different encryption algorithms. Multithreading techniques are employed to optimize performance and efficiency, enabling parallel processing of image data across multiple cores or threads.

In conclusion, the proposed comprehensive security framework offers a holistic approach to addressing the security challenges associated with image data in cloud-based storage systems. By leveraging distributed attribute-based encryption, Hadamard transforms, steganography, and multithreading techniques, organizations can enhance the privacy, confidentiality, integrity, and tamper-resistance of their image data, thus ensuring robust protection against evolving cyber threats.

PROPOSED SYSTEM

In today's digitally interconnected society, where information inundates every aspect of our lives, the importance of robust security measures cannot be overstated. The omnipresence of technology has not only transformed the way we interact but has also made our personal finances vulnerable to exploitation by hackers. Consequently, safeguarding sensitive military intelligence from such threats becomes not just a priority but an imperative in the realm of national security.

Unfortunately, the demand for information manipulation services has given rise to a nefarious underworld of malicious actors who exploit vulnerabilities for personal gain. This harsh reality has spurred the proliferation of cryptographic and steganographic techniques aimed at fortifying communication channels and protecting sensitive data from unauthorized access.

Cryptography, a cornerstone of modern information security, involves the complex art of encoding information in a manner that renders it indecipherable to anyone without the proper decryption key. By employing sophisticated algorithms and encryption keys, cryptography ensures that data remains secure during transmission and storage, even in the face of determined adversaries.

In parallel, steganography has emerged as a clandestine method for concealing sensitive information within innocuous digital artifacts, such as images or audio files. By embedding data within the pixels of an image or the silence of an audio track, steganography enables covert communication while evading detection by prying eyes or automated surveillance systems.

Together, these sophisticated methods form the backbone of modern information security, serving as indispensable tools in the ongoing battle against cyber threats. Whether safeguarding personal finances or protecting classified military intelligence, cryptography and steganography play a pivotal role in ensuring the confidentiality, integrity, and availability of critical data in an increasingly digital world.

As cyber threats continue to evolve and grow in sophistication, the importance of leveraging cryptographic and steganographic techniques to safeguard sensitive information becomes more apparent than ever. By staying vigilant and proactive in our approach to information security, we can mitigate risks and ensure the continued protection of our most valuable assets in the digital age

OBJECTIVE AND SCOPE

Objective:

In the rapidly evolving landscape of digital data management, characterized by the exponential growth of data volumes and the proliferation of cloud-based storage solutions, the objective of this study transcends the conventional boundaries of data security. It aspires to establish a fortified bastion against the ever-looming specter of cyber threats within cloud-based storage systems, aiming not merely to safeguard but elevate the security paradigm surrounding image data stored within these environments. The proposed comprehensive security framework endeavors to amalgamate cutting-edge cryptographic techniques, steganography, and the formidable Hadamard transforms into an integrated defense mechanism.

By doing so, the framework aspires to erect an impenetrable fortress, ensuring the sanctity of image data through enhanced privacy, confidentiality, integrity, and tamper-resistance.

At its core, this objective encapsulates a holistic approach towards mitigating the multifaceted security challenges inherent to cloud computing environments. It seeks to transcend the limitations of traditional security frameworks, embracing innovation and adaptation as cornerstones of resilience. By fostering a symbiotic relationship between technological advancement and security consciousness, the objective aims to instill confidence and tranquility

among stakeholders reliant on cloud-based storage solutions, fostering an environment conducive to digital innovation and progress.

Scope:

The expansive scope of this study extends far beyond the confines of traditional security frameworks, delving deep into the intricacies of cloud-based storage systems, where image data reigns supreme as a cornerstone of digital transformation. Within this vast and dynamic realm, the development and implementation of a bespoke security framework tailored explicitly for the guardianship of image data emerge as the focal point of inquiry.

With a laser-like focus, the framework embarks on a multifaceted journey encompassing not only the streamlining of key management processes but also the fortification of data integrity mechanisms and the establishment of impregnable citadels for secure key storage within the very fabric of image files. It traverses the intricate landscapes of encryption, steganography, and signal processing, weaving together disparate threads of technology into a cohesive tapestry of security.

The purview of this study extends its benevolent wings to encompass a diverse array of stakeholders, ranging from enterprises grappling with the complexities of data governance to governmental entities entrusted with safeguarding national security interests, and individual users seeking to protect the privacy of their personal images. United in their quest to safeguard the sanctity of their image data within the boundless expanse of cloud environments, these stakeholders form the backbone of the framework's user base, guiding its evolution and shaping its impact on the digital landscape.

As the digital frontier continues to expand and evolve, so too does the scope of this study, adapting and evolving in lockstep with the ever-changing landscape of cloud-based storage solutions. Through continuous innovation and collaboration, it seeks to push the boundaries of what is possible, forging new paths towards a future where security and resilience are not merely aspirations but fundamental principles of digital existence

SOFTWARE REQUIREMENTS

Programming Language: The implementation of the framework is underpinned by the versatility and robustness of Python, a dynamic and high-level programming language known for its simplicity and readability. Python's extensive libraries and frameworks make it an ideal choice for orchestrating intricate cryptographic operations, image processing tasks, and system-level manipulations within the framework.

Cryptographic Libraries: To fortify the framework's cryptographic capabilities, OpenSSL and PyCryptodome libraries are integrated seamlessly. OpenSSL, a robust open-source toolkit, provides a wide range of cryptographic functions, including encryption, decryption, key generation, and hashing, ensuring the confidentiality and integrity of data.

PyCryptodome complements OpenSSL with its comprehensive cryptographic modules, enhancing the framework's defenses against potential security breaches.

Image Processing Libraries: OpenCV, a powerful computer vision library, and PIL (Python Imaging Library) are the cornerstones of the framework's image processing capabilities. OpenCV offers a plethora of image transformation and analysis tools, enabling the framework to navigate the intricate corridors of image manipulation with precision and efficiency. PIL further enhances the framework's image processing capabilities, providing a rich set of functions for image enhancement, manipulation, and conversion.

Steganography Tools: Within the clandestine realm of steganography, StegHide and OpenStego emerge as indispensable tools for concealing sensitive information within digital imagery. StegHide, a command-line steganography tool, and OpenStego, a versatile steganography software, enable the framework to embed cryptographic keys and metadata covertly within images, ensuring the confidentiality and secrecy of sensitive data.

Integrated Development Environment (IDE): Thonny, a user-friendly integrated development environment (IDE) for Python, serves as the crucible for developing and testing the framework. With its simple and intuitive interface, Thonny provides a conducive environment for writing, debugging, and executing Python code, streamlining the development process and facilitating rapid iteration and prototyping of the framework's architecture. Thonny's built-in debugger and code editor features enhance developer productivity, making it an ideal choice for implementing and refining the framework's functionality.

HARDWARE AND SOFTWARE SETUP

Operating System: The framework is designed to be platform-agnostic, supporting deployment on Windows, Linux, or macOS operating systems. This cross-platform compatibility ensures that the framework can be seamlessly integrated into diverse computing environments, offering flexibility and accessibility to users across different platforms.

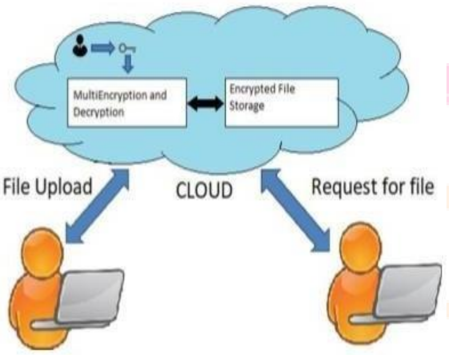
Cloud Storage Provider: The framework's compatibility extends to all major cloud service providers, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. Whether deployed on AWS's robust infrastructure, GCP's scalable cloud platform, or Azure's comprehensive suite of services, the framework ensures

universal access to cloud-based storage solutions, empowering organizations to leverage their preferred cloud provider for data storage and management.

Interne Connectivity Astable internet connectionis essential for the framework's operation, enabling seamless communication with cloud-based storage systems and expediting the transfer of encrypted image data. With reliable internet connectivity, users can securely access and manipulate image data stored in the cloud, ensuring uninterrupted workflow and efficient data transmission

Virtualization Software: Thonny IDE, coupled with libraries like NumPy, Matplotlib, and OpenCV, provides a powerful development environment for building and testing the framework. Thonny's user-friendly interface and built-in debugger simplify the development process, while libraries like NumPy facilitate efficient numerical computations, Matplotlib enable data visualization, and OpenCV empower advanced image processing tasks. Additionally, virtualization software such as Docker or Kubernetes can be used to create isolated development environments, allowing developers to test the framework in virtualized settings and ensure compatibility across different deployment scenarios.

SYSTEM DESIGN



METHODOLOGY

The proposed security framework represents a comprehensive and multifaceted approach to enhancing the security of data, particularly image data, within cloud-based storage systems. By integrating distributed attribute-based encryption (DABE), cryptographic algorithms such as RC6, LSB steganography, and Hadamard transforms, the framework aims to address key security challenges and ensure the confidentiality, integrity, and availability of sensitive information.

Distributed attribute-based encryption (DABE) serves as the cornerstone of the proposed framework, offering a sophisticated solution to the complex task of key management in cloud environments. DABE simplifies the management of encryption keys by allowing access to data based on user attributes rather than specific keys. This eliminates the need for maintaining and distributing multiple encryption keys, thereby streamlining the key management process and reducing administrative overhead. By implementing DABE, organizations can establish fine-grained access control policies tailored to their specific security requirements, enhancing overall data security within cloud-based storage systems.

In addition to DABE, the proposed framework leverages cryptographic algorithms like RC6 to ensure secure data transmission and storage. RC6, a symmetric key block cipher, offers robust encryption capabilities, making it well-suited for securing sensitive information in transit and at rest. By encrypting data using RC6, organizations can protect against unauthorized access and data breaches, thereby safeguarding the confidentiality of their information assets.

Furthermore, the integration of LSB steganography adds an additional layer of security to the framework. LSB steganography involves concealing key information within the least significant bits of digital images, making it virtually undetectable to the naked eye. By embedding encryption keys or other sensitive information within images, organizations can enhance the security of their data while maintaining a low profile. This covert communication technique adds an extra dimension of security to the framework, ensuring that critical information remains protected from prying eyes.

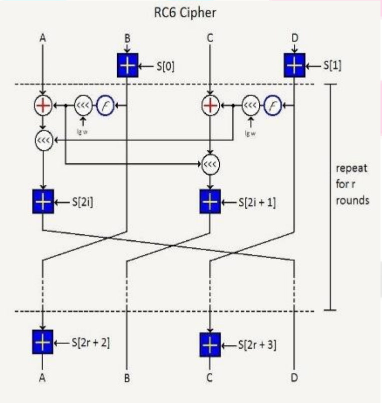
Moreover, Hadamard transforms are employed to enhance data integrity within the proposed framework. Hadamard transforms, known for their applications in signal processing and data compression, offer a powerful mechanism for detecting and correcting errors in encrypted data. By applying Hadamard transforms to encrypted image data, organizations can verify the integrity of their information assets and detect any unauthorized modifications or tampering attempts. This proactive approach to data integrity ensures the trustworthiness and reliability of data stored within cloud-based storage systems.

To optimize performance and efficiency, the proposed framework utilizes multithreading techniques during the encryption processes. Multithreading enables parallel processing of data across multiple threads or cores, allowing for faster encryption and decryption times. By harnessing the power of multithreading, organizations can maximize the throughput of their encryption processes

while minimizing latency and resource utilization.

In conclusion, the proposed security framework offers a comprehensive and robust solution for enhancing the security of data within cloud-based storage systems. By integrating distributed attribute-based encryption, cryptographic algorithms like RC6, LSB steganography, and Hadamard transforms, the framework addresses key security challenges and ensures the confidentiality, integrity, and availability of sensitive information. With its focus on key management simplification, secure data transmission, covert communication, data integrity enhancement, and performance optimization, the proposed framework provides organizations with a powerful toolset for protecting their valuable information assets in today's digital age.

ALGORITHM



CONCLUSION

In conclusion, the proposed security framework stands as a beacon of hope amidst the encroaching darkness of uncertainty, serving as a testament to the indomitable spirit of human ingenuity in the face of adversity. By synthesizing cryptographic techniques, steganography, and Hadamard transforms, the framework embarks on a noble journey to safeguard the sanctity of image data within cloud-based storage systems.

Through a holistic approach that encompasses distributed attribute-based encryption, cryptographic algorithms such as RC6, LSB steganography, and the transformative power of Hadamard transforms, the framework fortifies the security posture of cloud environments. By leveraging distributed attribute-based encryption, the framework simplifies key management, while cryptographic algorithms like RC6 ensure secure data transmission and storage. LSB steganography conceals sensitive information within images, and Hadamard transforms enhance data integrity, collectively ensuring the confidentiality, integrity, and tamper-resistance of image data.

This unified effort seeks to redefine the very essence of image data security, ushering in a new era of resilience and tranquility within the boundless expanse of cloud environments. As organizations and individuals navigate the complexities of digital transformation, the proposed framework offers a ray of hope—a promise of security and stability in an ever-changing landscape.

As we stand on the precipice of uncertainty, let us embrace the transformative power of innovation, forging a path towards a brighter, more secure future for image data within cloud-based storage systems. With the proposed framework as our guide, we can navigate the challenges ahead with confidence, knowing that our most valuable assets are safeguarded by the latest advancements in information security. Together, let us embark on this journey towards a safer, more resilient digital world

REFERENCES

[1]Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, “An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography”, IEEE International Conference on Electrical, Computer and Communication Engineering (ECCE), February 209.

[2]o Salim Ali Abbas, Malik Qasim Mohammed, “Enhancing Security of Cloud computing by using RC6 Encryption Algorithm”, International Journal of Applied Information Systems (IJAIS), November 207.

[3]o ShengDun Hu, KinTak U, “A Novel Video Steganography based on Non-uniform Rectangular Partition”, in the 4th IEEE International Conference on Computational Science and Engineering, 20.

[4]o Ako Muhamad Abdullah, “Advanced Encryption Standard (STEGANOGRAPHY) Algorithm to Encrypt and Decrypt Data”, published in Research Gate, 207.

[5]o Dnyanda Namdeo Hire, “Secured Wireless Data Communication”, International Journal of Computer Applications, September 202.

[6]o Xingtong Liu, Quan Zhang, Chaojing Tang, Jingjing Zhao and Jian Liu, “A Steganographic Algorithm for Hiding Data in PDF Files Based on Equivalent Transformation”, in IEEE journal, 2008.

[7]o Xinyi Zhou, Wei Gong, WenLong Fu, LianJingJin, “An Improved Method for LSB Based Color Image Steganography Combined with Cryptography”, in the IEEE International Conference on Computer and Information Science, June 206.

[8]o Nadeem Akhtar, Vasim Ahamad, Hira Javed, “A Compressed LSB SteganographyMethod”, IEEE International Conference on Computational Intelligence and Communication Technology, 207.

[9]o Mohamed abdel hameed M. Hassaballah , saleh aly and ali ismail awad,“AnAdaptiveImage Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques”, in IEEE journal , December 209.

[10] Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, “An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with STEGANOGRAPHY Cryptography”, International conference on informatics, electronics & vision, 204.

[11] o Tapan Kumar Hazra, Rumna Samanta, Nilanjana Mukherjee, Ajoy Kumar Chakraborty, “Hybrid Image Encryption and Steganography Using SCAN Pattern for Secure Communication”, IEEE journal, 207.

[12] o Pooja Yadav, Nishchol Mishra, Sanjeev Sharma, “A Secure Video Steganographywith Encryption Based on LSB Technique”, IEEE International Conference on Computational Intelligence and Computing Research, 203.

[13] o Jaspal Kaur Saini, Harsh K Verma, “A Hybrid Approach for Image Security by Combining Encryption and Steganography”, IEEE Second International Conference on Image Information Processing, 203.