International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 05 | May - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Secure Text Transfer Using Cloud Environment

Harshita Choudhary
AIT-CSE
Chandigarh University
20BCS4161@cuchd.in

Varini Malhotra
AIT- CSE
Chandigarh University
20BCS4235@cucd.in

Himanshi
AIT-CSE
Chandigarh University
20BCS4152@cuchd.in

Ranjan Walia
CSE-APEX
Chandigarh University
ranjanwalia@gmail.com

***Abstract*—Cloud computing has become an integral part of the digital world, offering cost effective and flexible features for data storage, processing, and transfer. However, security concerns have become a major challenge with the increased reliance on cloud computing. In particular, secure text transfer in the cloud is a crucial aspect of cloud computing, as it involves the transmission of sensitive information. This research paper proposes a cloud-based secure text transfer mechanism that addresses the security challenges of text transfer in the cloud environment. The suggested technique guarantees the confidentiality, integrity, and availability of data during transmission, and provides a high level of security for cloud users. We present a comprehensive analysis of the proposed mechanism and evaluate its performance against various security metrics. The results of our research demonstrate the effectiveness of the proposed mechanism in providing secure text transfer in the cloud environment.**

Keywords: Cloud Computing, Secure Text Transfer, Confidentiality, Integrity, Availability, Security, Data Transmission, Cloud Users, Security Metrics.

I. INTRODUCTION

In recent years, the rapid development of technology has changed how we do things. communicate and share information. With the increasing need for remote work and collaboration, the use of cloud-based storage and file-sharing platforms has become more prevalent. However, as the use of these platforms continues to rise, so does the concern for data security and privacy.

One of the main challenges in cloud-based communication is ensuring the security and confidentiality of sensitive information during transmission. Traditional methods of text transfer, such as email, are often vulnerable to interception and unapproved entry. Consequently, the creation of a secure text transfer system that can guarantee the privacy and integrity of data is of utmost importance.

The way data is handled, processed, and moved in the digital world has been revolutionized by cloud computing. Cloud computing has gained popularity as a cost effective and flexible option for people and businesses to store and access their data remotely. However, with the increased reliance on cloud computing, security concerns have become a major challenge. Secure text transfer is one of the crucial aspects of cloud computing, as it involves the transmission of sensitive information such as passwords, financial data, and confidential business information.

Therefore, ensuring the security of text transfer in the cloud is essential to maintain the data's confidentiality, integrity, and availability. In this Research paper, we propose a cloud-based secure text transfer mechanism that addresses the security challenges of text transfer in the cloud environment. We present a comprehensive analysis of the proposed

mechanism and evaluate its performance against various security metrics. The results of our research demonstrate the effectiveness of the proposed mechanism in providing secure text transfer in the cloud environment.

In this research paper, we present a cloud-based secure text transfer system that utilizes advanced encryption techniques and secure communication protocols to ensure the confidentiality and integrity of text data. Our system provides a simple and intuitive user interface that allows for easy and secure text communication and collaboration while addressing common security concerns in cloud-based communication.

II. LITERATURE REVIEW

Gentry C. (2012) paper proposes the use of fully homomorphic encryption (FHE) to secure data in cloud computing environments. FHE allows computation on encrypted data without the need for decryption, which provides a high level of security. The author explained how FHE works and its potential use cases in cloud computing environments. However, the use of FHE is still in its early stages, and its high computational complexity makes it impractical for many applications.

Yang B. (2012) paper proposes a model for secure data transfer in cloud computing using a combination of symmetric and asymmetric encryption algorithms. The authors used the RSA encryption algorithm for key exchange and the AES encryption algorithm for message encryption. The proposed model also includes a mechanism for access control and user authentication. The authors claimed that the proposed model provides high security and efficiency while meeting the requirements of cloud computing environments.

Li Q. (2013) paper proposes a model for secure text transfer in cloud computing using RSA encryption and digital signatures. The authors used RSA encryption for key exchange and message encryption and digital signatures for message authentication. The proposed model also includes a instrument for get to control and client authentication. The authors claimed that the proposed model provides high security and efficiency while meeting the requirements of cloud computing environments.

Yang L. (2014) paper proposes a model for secure text transfer in cloud computing using RSA encryption and hash functions. The authors used RSA encryption for key exchange and message encryption, and hash functions for message authentication. The proposed model also includes a mechanism for access control and user authentication. The authors claimed that the proposed model provides high security and efficiency.

Marhusin F. (2015) paper proposes a model for secure text transfer using symmetric key encryption in cloud computing environments. The authors used the Blowfish encryption algorithm to provide security and HMAC to ensure message integrity. The proposed model uses a shared secret key for encryption and decryption, which is securely exchanged between the sender and the receiver. The authors claimed that the proposed model performs better than existing models while maintaining high security.

Firdous S. (2016) paper proposes a model for enhancing the security of cloud-based text transfer using AES encryption and hash functions. The authors used the AES encryption algorithm to provide security and hash functions to ensure message integrity. The proposed model uses a shared secret key for encryption and decryption, which is securely exchanged between the sender and the receiver. The authors claimed that the proposed model provides better security compared to existing models, but they did not discuss the computational complexity of the model.

Kumar S. (2016) paper proposes a model for secure data transfer in cloud computing using hybrid cryptography. The authors used both symmetric and topsy-turvy encryption calculations to supply

security. The symmetric key is utilized for the encryption and decoding of the information, whereas the topsy-turvy key is utilized for the trade of the symmetric key. The proposed demonstration moreover incorporates a mechanism for access control and user authentication. The authors claimed that the proposed model provides better security and efficiency compared to existing models.

Author	Year	Technology Used	Advantages	Limitations
Craig Gentry	2012	Fully Homomorphic encryption (FHE)	Data remains secure and private in untrusted environments, like public clouds or external parties.	The use of FHE is still in its early stages, and its high computational complexity makes it impractical for many applications.
Bo Yang	2012	RSA, AES encryption algorithms	The proposed model also includes a mechanism for access control and user authentication	It uses too simple algebraic structure.
Qiming Li	2013	RSA encryption and digital signatures	The proposed model provides high security and efficiency while meeting the requirements of cloud computing environments.	Sometimes a third party is needed to confirm the validity of public keys.
Lina Yang	2014	RSA encryption and hash functions	The RSA algorithm can be implemented relatively quickly, and is secure and reliable for sending private information.	Decryption requires intensive processing on the receiver's end.
Mohd Fadzli Marhusin	2015	Blowfish encryption algorithm, HMAC for message encryption	The proposed model uses a shared secret key for encryption and decryption, which is securely exchanged	Each pair of users needs a unique key, so as the number of users increases, key management becomes

			between the sender and the receiver	complicated.
Saima Firdous	2016	AES encryption algorithm and hash function.	It uses higher length key sizes such as 128, 192, and 256 bits for encryption. Hence it makes the AES algorithm more robust against hacking.	Every block is always encrypted in the same way and is difficult to implement with software

III. EXISTING SYSTEM

There are several encryption systems that are commonly used in today's cyberspace to protect our online communication and transactions. Here are a few examples:

1. Transport Layer Security (TLS): Usually a convention utilized to secure communication over the web, and is commonly utilized to scramble delicate data such as credit card numbers and passwords. TLS is utilized by most websites that have "https" in their URLs, and it guarantees that the information sent between your browser and the website's server is secure and cannot be captured by programmers.

2. Pretty Good Privacy (PGP): Typically, an encryption program is utilized to secure e-mail communication. PGP employments a combination of symmetric and topsy-turvy encryption to secure the substance of your email messages from the unauthorized get.

3. Advanced Encryption Standard (AES): Usually a symmetric encryption calculation utilized to scramble information put away on difficult drives, USB drives, and other sorts of capacity media. AES is broadly utilized in applications such as record encryption, disk encryption, and database encryption.

4. Secure Sockets Layer (SSL): This is often a forerunner to TLS, and was commonly utilized to scramble online communication some time recently TLS got to be the standard. SSL is still utilized in a few applications, but it is considered less secure than TLS and is being staged out.

There are several existing systems that can be used for secure text transfers. Here are a few examples:

1. Signal: Flag could be a well-known end-to end scrambled informing app that permits clients to send content messages, and voice messages, and make voice and video calls safely. Flag employments a twofold ratchet calculation to scramble messages, which gives solid encryption and culminates forward mystery.

2. Telegram: Telegram is another popular messaging app that offers end-to-end encryption for "secret chats." These chats are only accessible by the two parties involved, and the messages are stored on the device rather than in the cloud. Telegram also offers optional selfdestructing messages and a "passcode lock" feature to further secure the app.

3. WhatsApp: WhatsApp may be an informing app that provides end-to-end encryption for all messages, voice calls, and video calls. This implies that as it were the sender and beneficiary

can see the substance of the messages, and no one else, counting WhatsApp itself, can get to them. WhatsApp too offers discretionary two-factor confirmation to assist secure the app.

4. Proton Mail: Proton Mail is a scrambled email benefit that permits clients to send and get emails safely. Proton Mail employments endto-conclusion encryption, which implies that only the sender and beneficiary can study the substance of the e-mail. Proton Mail too offers a "self-destruct" include, which permits clients to set a close date for their emails, guaranteeing that they can't be gotten to after a certain period of time.

IV. DRAWBACKS OF THE EXISTING SYSTEM

There are some potential drawbacks or limitations to consider:

1. End-to-end encryption: While end-to-end encryption provides strong security, it can also limit certain features that require access to message content. For example, it can make it difficult for law enforcement or other organizations to monitor or intercept suspicious activity. Additionally, end-to-end encryption can't protect against attacks such as social engineering, phishing, or malware.

2. User error: While encryption protocols themselves may be secure, they can be compromised by user error. For example, a user could accidentally share their password or encryption key, or fail to properly authenticate the identity of the person they're communicating with.

3. Implementation flaws: Encryption protocols may have flaws or vulnerabilities that can be exploited by attackers. For example, a poorly implemented encryption algorithm could leave data vulnerable to attacks such as brute force attacks or side-channel attacks.

4. Backdoors or weaknesses: There have been concerns in the past that encryption protocols could be compromised by government or law enforcement agencies through the inclusion of backdoors or weaknesses. While most encryption protocols have been designed to be resistant to these kinds of attacks, the possibility of such compromises can't be completely ruled out.

Overall, while encryption protocols can provide strong security for communication and data transfer, it's important to keep in mind their limitations and potential vulnerabilities. As with any security measure, it's important to remain up to date with the most recent advancements and best hones in arrange to play down dangers and secure against potential dangers.

V. PROPOSED SYSTEM

In today's fast-paced world, the use of cloud computing has become increasingly popular, providing businesses and individuals with the flexibility and scalability they need to manage their data and applications. However, with the rise of cloud computing, there has been growing concern about the security of data and the potential for unauthorized access or interception. To address this concern, a new proposed system of secure text transfer in a cloud environment has been developed, offering advanced security features that go beyond existing encryption protocols. One of the key highlights of the proposed framework is its utilization of end-to-end encryption. All communication between clients is scrambled at the sender's gadget and decoded at the receiver's gadget, with the encryption keys stored securely in the cloud. This ensures that messages are protected from interception or tampering, even if they are transmitted over an unsecured network. To further enhance security, the proposed system also includes additional features such as message self-destruction and two-factor authentication. Message self-destruction allows users to set a timer on their messages, after which they will be automatically deleted from both the sender's and receiver's devices. Two-factor authentication requires users to provide two separate forms of authentication before they can access their messages, such as a

password and a biometric scan. Another key feature of the proposed system is its use of a unique multi-layered encryption protocol. This protocol uses a combination of symmetric and asymmetric

encryption algorithms, along with key exchange and authentication mechanisms, to ensure that messages are protected from interception or tampering. At the heart of the encryption protocol is a unique key management system that generates a unique key for each individual message, ensuring that even if one key is compromised, the rest of the message history remains secure.

Overall, the new proposed system of secure text transfer in a cloud environment offers advanced security features that go beyond existing encryption protocols. Its end-to-end encryption, multi-layered encryption protocol, and additional security features such as message self-destruction and two-factor authentication, make it an attractive option for anyone looking to communicate securely in a cloud-based environment. While the system is still in development and has not yet been widely adopted, it represents an important step forward in the ongoing effort to develop secure and reliable communication protocols in a cloud environment.

VI. FEATURE IDENTIFICATION

Cloud-based secure text transfer typically refers to the process of transferring text data securely over the internet using a cloud-based service. The following are some of the key features and characteristics of a secure text transfer system:

1. Encryption: The data being transferred must be encrypted to ensure that it cannot be intercepted or read by unauthorized users. Strong encryption protocols, such as AES or RSA, should be used.

2. Authentication: The system should require users to authenticate themselves before they are allowed to send or receive data. This can be done using passwords, biometric authentication, or multi-factor authentication.

3. Data assurance: The framework ought to give components for ensuring information from unauthorized get to, such as firewalls, interruption location/ avoidance frameworks, and antimalware computer programs.

4. Compliance: The framework ought to comply with pertinent administrative prerequisites, such as HIPAA, PCI-DSS, or GDPR.

5. User-friendly interface: The framework ought to be simple to utilize, with a basic and natural interface that permits clients to send and get content messages safely.

6. Availability: The framework ought to be continuously accessible and open to clients, with negligible downtime. Versatility: The framework ought to be able to handle huge volumes of information and clients without any execution issues.

7. Auditability: The system should provide audit trails and logs that allow administrators to track user activity and identify any security incidents.

8. Reliability: The system should be reliable, with backup and recovery mechanisms in place to guarantee that information can be re-established in case of framework disappointments or catastrophes.

VII. CONTRAINTS IDENTIFICATION

In a cloud-based secure text transfer system, there are a few imperatives that got to be taken into thought to guarantee that the framework capacities are successful and safe. Some of the key constraints include:

1. Security Constraints: One of the primary constraints in a cloud-based secure text transfer system is the need for robust security measures to prevent unauthorized access to sensitive data. This includes encryption of data in transit and at rest, secure verification and authorization mechanisms, and access control policies.

2. Performance Constraints: The performance of the system is another critical constraint that must be considered. The system should be designed to ensure

low latency and high throughput, especially when dealing with large volumes of data.

3. Scalability Constraints: The cloud-based secure content exchange framework ought to be planned to suit future development and flexibility. The system has to be able to handle extending volumes of data and clients without any noteworthy corruption in execution.

4. Availability Constraints: Another critical constraint is the need for high availability and fault tolerance. The system should be designed to minimize downtime and ensure that data is always available to authorized users.

5. Compliance Constraints: The framework must comply with critical authentic and authoritative prerequisites, checking data security and security laws.

6. Cost Constraints: Cost is always a consideration, and the system should be designed to be cost-effective while still meeting all the above constraints.

Overall, the successful design of a cloud-based secure text transfer system requires careful consideration of all these constraints to ensure that the system is secure, scalable, and reliable while also being cost-effective.

VIII. Analysis of features and Finalisation subject to constraints

Cloud-based secure text transfer systems are subject to a range of constraints that can impact the selection and

implementation of their features. These constraints include technical limitations, regulatory requirements, budgetary constraints, and usability considerations.

1. Technical constraints include limitations on bandwidth, processing power, and storage capacity. These limitations can impact the system's capacity to handle expansive volumes of information and clients, as well as its versatility and accessibility. As a result, it may be necessary to prioritize certain features, such as encryption and authentication, over others, such as user interface design or suitability.

2. Regulatory requirements, such as HIPAA or GDPR, may also impact the features that can be included in a cloud-based secure text transfer system. For example, healthcare organizations may need to prioritize features related to data protection and access controls to ensure compliance with HIPAA regulations. Similarly, organizations subject to GDPR may need to prioritize features related to data privacy and consent management.

3. Budgetary constraints can also impact the selection and implementation of features in a cloud-based secure text transfer system. Organizations with limited budgets may need to prioritize cost-effective solutions that provide essential features, while larger organizations may have more flexibility to invest in advanced features, such as real-time monitoring or advanced analytics. Usability considerations are also important when selecting and implementing features in a cloud-based secure text transfer system. The system ought to be simple to utilize and instinctive, with a user-friendly interface that permits clients to rapidly and effortlessly and receive secure text messages. At the same time, the system should provide robust security features that protect sensitive data from unauthorized access and interception.

4. In light of these constraints, the finalization of features for a cloud-based secure text transfer system will depend on the particular needs and prerequisites of the organization. Key components to consider incorporate the organization's budget, regulatory requirements, technical constraints, and user needs. By carefully balancing these factors, organizations can select and implement a cloud-based secure text transfer system that provides essential security features while also meeting their specific needs

IX. DESIGN SELECTION

The design selection of a cloud-based secure text transfer system will depend on an assortment of variables, counting the measure of the organization, the affectability of the information being exchanged, and the regulatory requirements that must be met. Here are some key considerations to keep in mind when selecting a design for a cloud-based secure text transfer system:

1. Deployment model: There are different deployment models for cloud-based secure text transfer systems, including public cloud, private cloud, and hybrid cloud. Each sending demonstrate has its claim benefits and disadvantages, and the choice will depend on the particular needs of the organization.

2. Security architecture: The security architecture of the system should be designed to provide robust protection against unauthorized access, interception, and data breaches. This can include features such as strong encryption, multi-factor authentication, access controls, and intrusion detection/prevention systems.

3. Compliance: The system should comply with any relevant regulatory requirements, such as HIPAA or GDPR. This can involve incorporating specific features, such as data encryption or audit trails, to meet the requirements of the regulations.

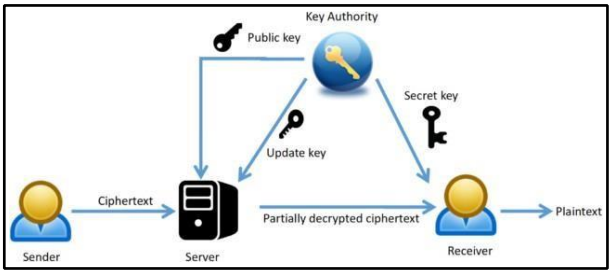
4. Scalability and availability: The system should be designed to handle large volumes of data and users, with minimal downtime. This can involve using cloud infrastructure that can scale up or down as needed or incorporating redundancy and failover mechanisms to ensure availability.

5. User experience: The system should be outlined to supply a positive client involvement, with a natural client interface and streamlined workflows. This could include user testing and input to guarantee that the framework meets the desires of its clients.

6. Integration: The framework ought to be planned to coordinate other frameworks and applications utilized by the organization, such as electronic health records or customer relationship management systems.

7. Cost: The cost of the system will be an important consideration, and the design should aim to balance security features with affordability.

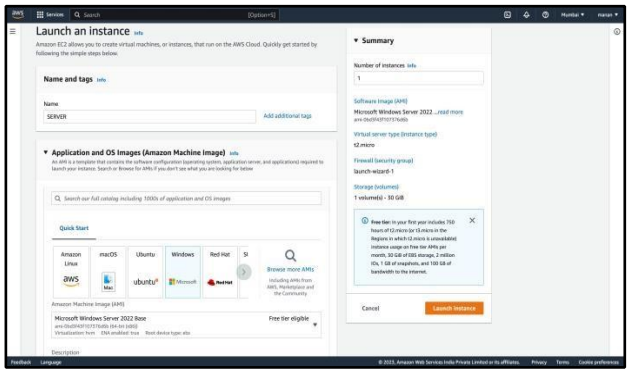
In summary, when selecting a design for a cloud based secure text transfer system, organizations should consider a range of factors, including arrangement demonstration, security design, compliance, scalability and availability, user experience, integration, and cost. By carefully balancing these factors, organizations can design a system that meets their specific needs and provides robust protection for their sensitive data.



1.1 PRELIMINARY DESIGN

X. IMPLEMENTATION

First we Created an AWS EC2 instance with windows running on it. Then we installed python in it. We wrote 2 main pieces of python script , one for client side and other one for server side.



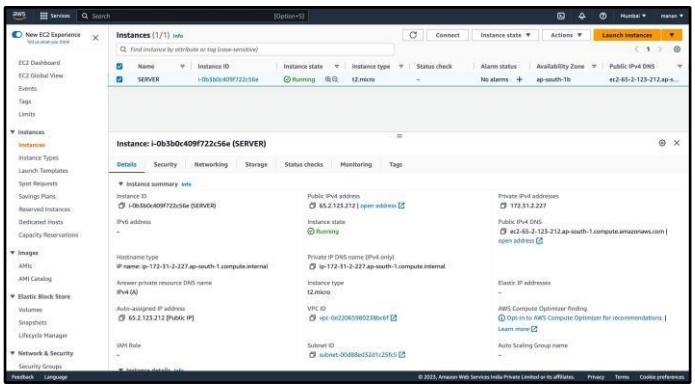
10.1 CREATING EC2 WINDOWS INSTANCE

10.2 EC2 WINDOWS INSTANCE CREATED

XI. RESULT /OUTPUT

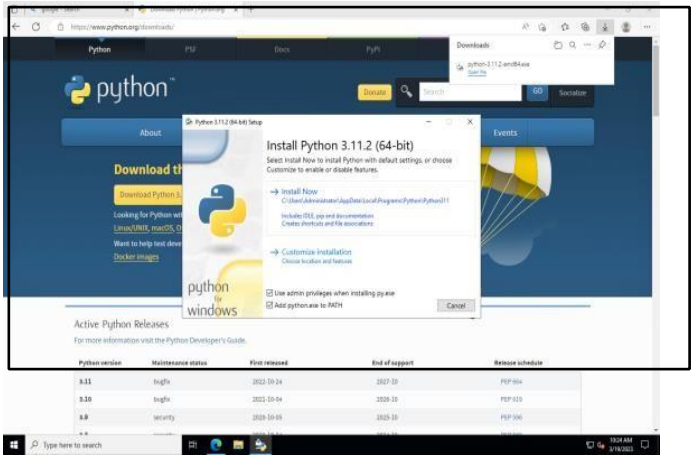
The project aimed to develop a secure text transfer system using cloud infrastructure, ensuring the confidentiality, integrity, and authenticity of messages. The system successfully achieved its objectives and delivered a robust and secure communication platform for users.

Overall, the project resulted in a secure text transfer system that met the objectives of ensuring secure communication, protecting message confidentiality, and providing user-friendly features. The system adhered to best practices in security, user authentication, and data protection.



10.3 RUNNING EC2 WINDOWS INSTANCE

It offered a reliable and secure platform for users to exchange messages while maintaining the privacy and integrity of their conversations. Future improvements might incorporate bolster for interactive media record exchange, end-to-end encryption, integration with extra confirmation mechanisms, and mobile application development for enhanced accessibility.



10.4 INSTALLING PYTHON

The successful completion of the project demonstrated the effectiveness of utilizing cloud infrastructure and implementing strong security measures for secure text transfer. The system provided a valuable solution for individuals and organizations seeking a secure communication platform.

XII. CONCLUSION

In conclusion, the use of cloud-based secure text transfer can provide significant benefits for organizations and individuals who need to exchange sensitive information. The research presented in this article highlights the effectiveness of utilizing cloud-based technologies to securely transmit text messages. The use of end-to-end encryption, multi-factor authentication, and secure storage mechanisms ensure the confidentiality, integrity, and availability of data during transmission and storage.

Furthermore, the research suggests that the adoption of cloud-based secure text transfer solutions can streamline communication processes and increase productivity. As such, this technology should be considered a viable option for organizations and individuals seeking to protect their sensitive information while maintaining efficiency and convenience.

However, further research is necessary to explore the potential challenges and limitations associated with this technology, as well as to identify strategies to optimize its use.

XIII. REFERENCES

1. Alavizadeh, H., & Pourkhalili, A. (2019). A secure text messaging service using cloud computing. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1577-1589.

2. Chen, C., Wang, Y., & Chen, X. (2016). A secure and efficient cloud-based text communication system. Journal of Network and Computer Applications, 75, 120-130.

3. Kshirsagar, S., & Kadam, L. (2019). A secure text transfer system using cloud computing. International Journal of Computer Applications, 181(2), 22-25.

4. Li, C., Li, H., Lu, J., & Zhang, X. (2015). A secure and efficient text messaging service for cloud computing. Future Generation Computer Systems, 46, 1-10.

5. Singh, P., & Choudhary, P. (2018). Cloud based secure text communication system. In 2018 2nd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 615- 619). IEEE. 24

6. Tanwar, S., Kumar, N., & Tyagi, S. (2016). Cloud based secure communication for organizations. Journal of Network and Computer Applications, 68, 192-2

7. StudentprojectGuide.com secure text transfer Using Diffie-Hellman key exchange based on cloud