International Journal of Advanced Trends in Engineering and Management (IJATEM)
Vol. 1(02), July 2022, pp. 22-30

Article Title: **Secured Data Transmission for Cloud Computing using Highly Efficient NTRU Key Management System**

Secured Data Transmission for Cloud Computing using Highly Efficient NTRU Key Management System

K. Sathis Kumar[1], J. Prabula[2]

[1]Department of M.C.A, Lord Jegannath College of Engineering and Technology, PSN Nagar, Ramanathichanputhur, Marungoor, Kanyakumari District, Tamil Nadu 629402, India.

[2]Assistant professor, HOD of M.C.A, Lord Jegannath College of Engineering and Technology, PSN Nagar, Ramanathichanputhur, Marungoor, Kanyakumari District, Tamil Nadu 629402, India.

ABSTRACT

This Project Proposed a Secured Data Transmission For Cloud Computing Using Highly Efficient NTRU Key Management System. Cloud Computing is used for storing and accessing data over the internet without the use of computer's hard drive. The major purposes of a cloudlet are data exchange, data confidentiality and intrusion detection. The data monitored by IOT is stored in cloud with enhanced security. An information about the user that is being captured by wearable technology is encrypted here for the first time using the NTRU method. This information will then be efficiently transferred to the closest cloudlet. The user's medical records are divided into three categories and further secured in a hospital's distant cloud. In this paper, a unique collaborative Intrusion Detection System approach using cloudlet mesh was developed to protect the healthcare system from harmful intrusions. In order to get more reliable functionality, NTRU is employed last. Software called NETBEANS is used to simulate the proposed method.

Keywords: NTRU, Key Management, Cloud Computing, Internet of Things.

1 Introduction

The core concept behind cloud computing is pay per user service delivery. Owners of data can store it in the cloud because storage as a service is easily accessible. Access control, secrecy, and authentication can all be outsourced. Data is a company's most valuable asset. The risk to the data owner arises from a hostile CSP (Cloud Service Provider) or a vulnerability. Utilizing cloud computing because it provides scalable, dependable and expense infrastructures without the expense or difficulty of managing its own hardware, virtual infrastructure offers an alluring alternative to creating applications on top of common physical devices. The benefits of cloud computing, such as lower ownership and operating costs for IT and better resource utilization, are simply too great for the growth of many businesses.

Consumers are finding it is more challenging to domestically retain massive volumes of data due to the fast expansion of data. Consequently, a lot of firms favor cloud storage. So high degree security is required to protect data against malicious attack [1]. In recent years, data sharing in the cloud has become well liked features due to the potential for numerous users to exchange data with one another. Some sensitive information was transmitted in these communications. So, several cryptographic approaches were employed to protect the security

of these data. Nevertheless it is not possible to encrypt the entire shared file in order to conceal sensitive information [2-4]. A significant amount of study was done to offer protection. One of them was the use of virtualization, although it does not keep track of the attacks that evade IDS at tenant virtual machines. [5] A different approach to cloud security also maintains the spatial correlation of the encoded domain using a homomorphic cryptosystem [6-7]. User has both the encryption key and the data embedding key for this crypto scheme. To retrieve the original data, encryption and decryption must be performed more quickly, although this is possible using the suggested approach. It has been suggested that access restriction is a workable strategy for guaranteeing anonymity in cloud computing. [8]. However, it cannot ensure that strangers are reliable. To ensure identity secrecy, the vast majority of traditional systems rely on attribute-based strategies. Correlation analysis of user attribute data, on the other hand, fails to protect user attribute privacy and offers a risk of identity exposure. [9-10]. Additionally, searchable encryption methods that are currently in use were used. [11-12]. It is insufficient in terms of functionality and confidentiality, and it is subject to an inside keyword guessing attack. The use of two servers, public keys, and a keyword search framework to encrypt data outperforms the currently used searchable encryption method [13]. It successfully defeats inside keyword guessing attacks. However, it employs a homomorphic strategy to carry out security against this attack. RSA is a strong existing 1024-bit encryption key, similar to NTRU that provides a high level of security as well as enough resistance to attacks [14]. However, NTRU has a significant advantage in producing small keys and is able to function even when memory is minimal. This suggested technique focuses on creating high level secured data by implementing data masking together with effective encryption based on NTRU in order to get over these problems. The suggested method embeds the original data into another text and saves the positions of each character in a RIF file that is encrypted with NTRU in order to prepare the masked data for cloud storage. [15].After encryption, the recipient receives the original data's hash value, disguised data, and encrypted RIF file. After decrypting the original data and retrieving it. The recovered data is hashed, and the results are compared with the received hash value, to achieve authentication. The proposed work performs more quickly, continues to function even when memory is limited, and tracking data while distributing it across a network is challenging.

IOT data is saved in the cloud using higher security measures. The information about the user that is being captured by wearable technology is encrypted here for the first time using the NTRU method. This information will then be efficiently transferred to the closest cloudlet. The user's medical records are divided into three categories and further secured in a hospital's distant cloud. In this paper, a unique collaborative Intrusion Detection System approach using cloudlet mesh was developed to protect the healthcare system from harmful intrusions. In order to get more reliable functionality, NTRU is employed last.

2 Proposed Work

In the modern era, corporate environment is growing at a very fast rate, so our basic objective is to acquire trustworthy information from any source. Distributed database plays a key part in day to day life. Since a database is spread, data is located in many places geographically, which ultimately makes it easier to retrieve our vital and precious data. A suggested design that combines cloud database services with data integrity, the ability to perform several actions simultaneously on encrypted data and cloud database services. It is a system that enables geographically dispersed clients to establish a direct connection to a cloud database that is encrypted and to carry out concurrent and independent activities, including those that alter the database's structure. Concurrency control and security concerns are the main objectives of the evolving distributed database method. In this research project, a cryptographic NTRU-based Key management system is used to increase data security. Different keys are utilized in an asymmetric key technique for both the encryption and decryption of plaintext. Public and private keys are the names given to these keys. Key management system based on cryptography and NTRU. Hashing algorithms that are quick and secure will increase system security in terms of throughput and processing speed. Its primary traits include low memory and computational needs that offer a high level of security. It is a public-key cryptosystem that is very well organized.

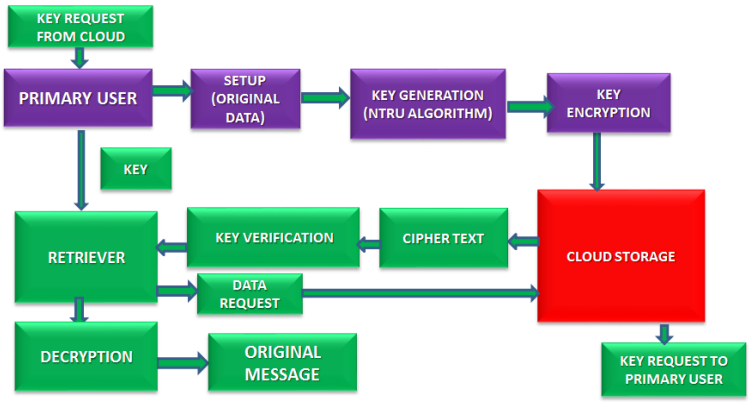

Figure 1: *Proposed system block diagram*

2.1 Parameters Involved In NTRU

In order to complete this operation, NTRU also needs the inputs N, P, and q. P and Q are used to reduce the polynomial coefficients; p and q should be lower than q without a common divisor. N stands for the degree of the polynomial at major N-1.

2.2 Key Generation

A private key must be created in addition to a public key in order to secure a message while it is being transmitted between two nodes. A key pair of two polynomials, f and g, are formed with coefficients that are lower than q's with degree at major N-1 and with coefficients in the

range of {-1, 0, 1}. The polynomial f that was chosen must satisfy the requirement for inverse modulo p and modulo q.

2.3 Encryption

Cloud encryption is the process of transforming and encrypting data before uploading it to the cloud. Using mathematical techniques, this procedure turns plaintext data into unintelligible cypher text, shielding it from unwanted and potentially dangerous users. In the event of a breach, cloud encryption offers a quick and easy way to stop access to sensitive cloud data. Even if the data is ultimately stolen, criminals are unable to access the encrypted files' contents. Many experts believe that encryption is a successful and practical method for ensuring strong data security.

2.4 Decryption

From its Dropbox account's shared folder, the user chooses a file to read or edit. Now, the program running on the customers attempts to decode it. Before evaluating the group names in the file header to see if there is a match between the groups present and the group the user belongs to, the currently open application tries to ascertain whether the login username is contained in the encrypted file header or not (When a user logs in and is a member of a group, the application will automatically flush the user's private key from memory if there is a match between the groups already in use and the group the user belongs to (the user will receive the private key when using it). Information that has been encrypted can be restored to its original form through the process of decryption. While being exchanged or transferred, information is converted throughout the encryption process from its original format, known as plaintext, into an unreadable format, known as cipher text.

2.5 Number Theory Research Units (NTRU) to Perform Encryption and Decryption

The Shortest Vector Problem is used in this technique for the first time in a lattice rather than through factorization or a discrete approach. It is more secure than RSA and ECC because it can withstand a quantum based attack. NTRU may be executed 2000 times quicker than any other cryptographic method in terms of speed. This is as a result of its linear action. It has been formally recognized as IEEE P1363 standard in terms of a standard. In addition, it uses 1/50th of the memory space required by conventional systems. Key creation is remarkably simple due to the speed of NTRU. Because encryption and decryption rely on simple polynomial multiplication, they are quicker than the comparable algorithms.

2.5.1 Algorithm of Proposed Approach is as Follows

i. Two polynomials with coefficients much lower than q, a degree of no more than N-1, and coefficients in the range of {-1, 0, 1} are needed in order to construct the key pair.
ii. The value of f should be selected so that f. fp=1 (mod p) and f. fq=1 (mod q) exist.
iii. Her private keys are f and fp, respectively.
iv. The equation h=pfq.g (mod q) can be used to calculate the public key.
v. Pick a polynomial m with a coefficient of -1,0,1; m stands for the message.
vi. Randomly select an r-polynomial with a low coefficient.
vii. Using the receiver's public key, the message can then be finally encrypted using the formula e=r.h+m.
viii. The encryption text, e, is now transferred securely to the recipient.
The recipient must first multiply the cypher text and the portion of the private key f in order to decrypt the message. A=f.e accomplishes this (mod q).
ix. Using the formula b=a(mod p)=f, determine the value of a mod p. (mod p).
The recipient can reconstruct the original message by multiplying the value of b with the other portion of the private key fp. C=fp performs this action. B is equal to fp.f.m (mod p), therefore c=m (mod p). Here, c represents the sender's initial message.

3 Results and Discussion

The simulation results are examined using a software Netbeans 7.3.

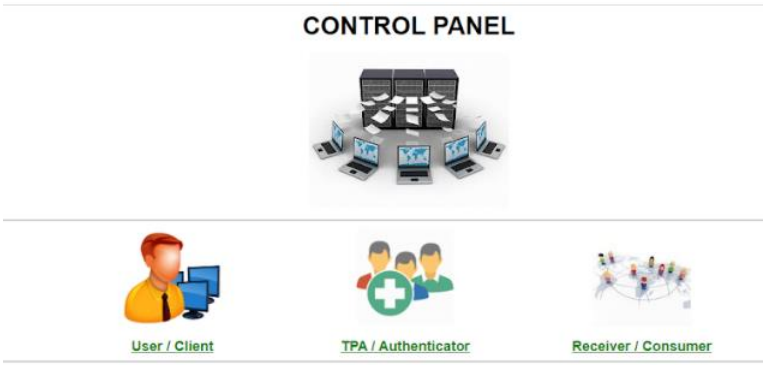

Figure 2: *Control Panel*

Figure 3: *Third Party Auditor Login*

Retriever View File

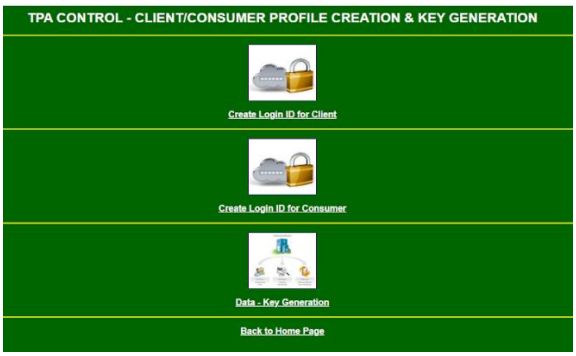

Figure 4: *Key decryption*

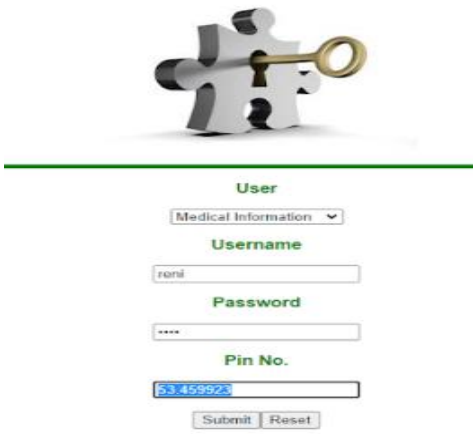

Figure 5: *User Login*

Figure 6: *Login for Consumer*

The figure shows the login page of proposed project work, the user can create login is in this page.

Article Title: **Secured Data Transmission for Cloud Computing using Highly Efficient NTRU Key Management System**

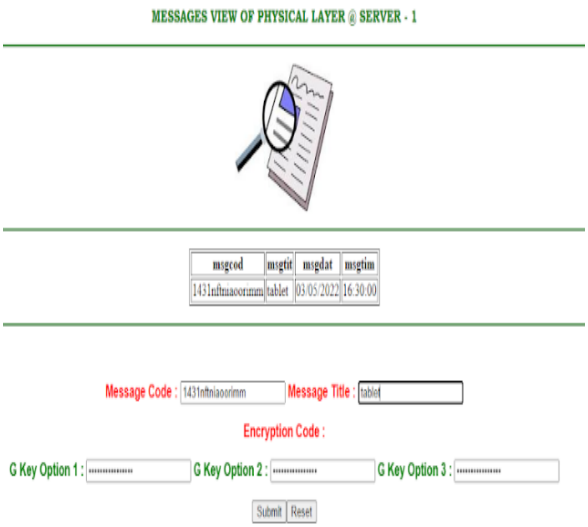

Figure 7: *Messages View of Server1*

Figure 8: *CP-AB Encrypted Messages View*

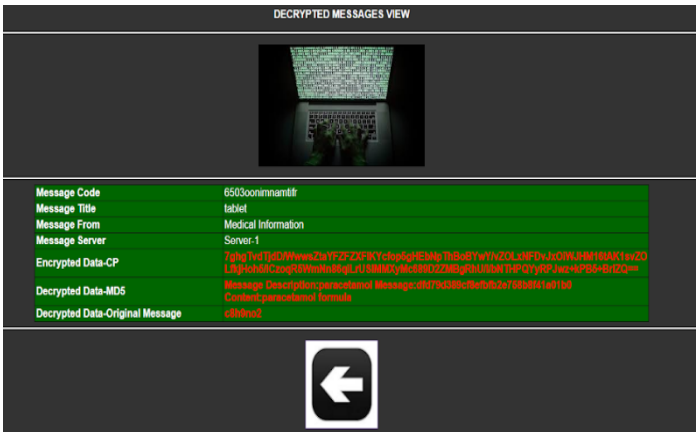

Figure 9: *Decrypted Messages View*

The analysis of NTRU and RSA's performance is shown in the following table:

Table 1: *Performance analysis of NTRU and RSA*

METHOD	RSA	NTRU
Approach	Asymmetric	Asymmetric
Encryption	Slow	Fastest
Decryption	Slow	Fastest
Key Distribution	Easy	Easy
Complexity	O(N^3)	O(NLogN)
Security	Highest	High

4 Conclusion

Security is now one of the most crucial factors in every industry. Every piece of information needs to be protected because any alterations cause very serious issues. The protection of data from harmful attacks and illegal access is necessary. In this study, we mainly focus on distributed database communication, and we address issues with concurrency control and security. In order to secure our sensitive information from unauthorized users, security is crucial to our operation. The Cryptographic NTRU based Key method has been implemented in this dissertation using net beans. In this study, we examined at the Ramp Secret Sharing Scheme, which is now in use for data encryption and decryption and to boost the dependability of distributed de-duplication systems. However, there are significant drawbacks to the RSSS technique that is currently in use. To address these drawbacks, a cryptographic NTRU based Key algorithm is employed. The suggested method takes less time for authentication purposes as well as for encrypting and decrypting data while exchanging files in a distributed database system.

References

1. Enrico Bacis; Sabrina De Capitani di Vimercati; Sara Foresti; Stefano Paraboschi; Marco Rosa; PierangelaSamarati, Year: 2020, “Securing Resources in Decentralized Cloud Storage”, IEEE Transactions on Information Forensics and Security, Vol. 15, no.5, pp. 286-298.
2. Pan Yang; NaixueXiong; Jingli Ren, Year: 2020, “Data Security and Privacy Protection for Cloud Storage: A Survey”,IEEE Access, Vol.8, no. 7, pp.131724- 131740.
3. Mohsen KarimzadehKiskani; Hamid R. Sadjadpour, Year: 2018, “Secure and Private Information Retrieval (SAPIR) in Cloud Storage Systems”, IEEE Transactions on Vehicular Technology, Vol.67, no. 12, pp. 12302- 12312.
4. Wenting Shen; Jing Qin; Jia Yu; RongHao; Jiankun Hu, Year: 2019,“Enabling Identity-Based Integrity Auditing and Data Sharing With Sensitive Information Hiding for Secure

Cloud Storage", IEEE Transactions on Information Forensics and Security, Vol. 14, no. 2, pp. 331-346.

5. Leyou Zhang; Yilei Cui; Yi Mu, Year: 2020, "Improving Security and Privacy Attribute Based Data Sharing in Cloud Computing", IEEE Systems Journal, Vol. 14, no. 1, pp. 387-397.
6. Kennedy A. Torkura; Muhammad I. H. Sukmana; Feng Cheng; ChristophMeinel, Year: 2020. "CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure", IEEE Access, Vol. 8, no. 7, pp. 123044-123060.
7. Preeti Mishra; Vijay Varadharajan; Emmanuel S. Pilli; UdayTupakula, Year: 2020, "VMGuard: A VMI-Based Security Architecture for Intrusion Detection in Cloud Environment", IEEE Transactions on Cloud Computing, Vol. 8, no.3, pp. 957-971.
8. Ming Li; Lanlan Wang; Jingjing Fan; Yushu Zhang; Kanglei Zhou; Haiju Fan, Year: 2019, "Fidelity Preserved Data Hiding in Encrypted Highly Autocorrelated Data Based on Homomorphism and Compressive Sensing", IEEE Access, Vol. 7, no. 5, pp. 69808- 69825.
9. LizhiXiong; Danping Dong; Zhihua Xia; Xianyi Chen, Year: 2018, "High-Capacity Reversible Data Hiding for Encrypted Multimedia Data With Somewhat Homomorphic Encryption", IEEE Access, Vol. 6, no. 10, pp. 60635-60644.
10. Pauline Puteaux; ManonVialle; William Puech, Year: 2020, "Homomorphic Encryption-Based LSB Substitution for High Capacity Data Hiding in the Encrypted Domain", IEEE Access, Vol. 8, no.6, pp. 108655- 108663.
11. Feng Hu; Bing Chen, Year: 2020, "Channel Coding Scheme for Relay Edge Computing Wireless Networks via Homomorphic Encryption and NOMA", IEEE Transactions on Cognitive Communications and Networking, Vol. 6, no.4, pp. 1180-1192.
12. GuoweiQiu; XiaolinGui; Yingliang Zhao, Year: 2020, "Privacy-Preserving Linear Regression on Distributed Data by Homomorphic Encryption and Data Masking", IEEE Access, Vol. 8, no. 11, pp. 210855-210867.
13. Alabdulatif; Ibrahim Khalil; Albert Y. Zomaya; ZahirTari; Xun Yi , Year: 2020, "Fully Homomorphic based Privacy-Preserving Distributed Expectation Maximization on Cloud", IEEE Transactions on Parallel and Distributed Systems, Vol. 31, no.11, pp. 2668-2681.
14. Hu Xiong; Hao Zhang; Jianfei Sun, Year: 2019, "Attribute-Based Privacy-Preserving Data Sharing for Dynamic Groups in Cloud Computing", IEEE Systems Journal, Vol. 13, no.3, pp. 2739-2750.
15. Yichen Zhang; Jiguo Li; Hao Yan, Year: 2019, "Constant Size Ciphertext Distributed CP-ABE Scheme with Privacy Protection and Fully Hiding Access Structure" IEEE Access, Vol. 7, no. 4, pp. 47982- 47990.