ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Confidential and Conformable Scheme Based On Improved NTRU for Big Data Storage in Cloud

Sudhir Jaiswal[1], Subham Jha[2], Naveen Ghorpade[3], K S Jagadeesh Gowda[4]

U.G. Student, Department of Computer Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore India

U.G. Student, Department of Computer Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India

Assistant Professor, Department of Computer Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India

Professor & HOD, Department of Computer Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India

ABSTRACT: Big data has a large set of data which make it so [composite] that general processing and accessing software are inadequate to deal with them. The two critical challenge while storing and accessing the big data in cloud was its security and verification of user. Earlier approaches completely ignores the data confidentiality and issue of access policy update. Access policy update important for enhancing the security and dealing with dynamism caused by user join and leave activities. In this paper, we propose a confidential and conformable scheme based on improved NTRU for big data storage in cloud server. we propose an improved NTRU cryptosystem to overcome the decryption failure of the original NTRU.The proposed system can secure the data stored in the cloud by the data owner and also verify the user while accessing the data to prevent from cheating and collusion attacks.our scheme allow the cloud server to update the ciphertext based on our new policy provided by the data owner.Our scheme facilitate to provide a key to each user in order to make verification of the right user by the data owner who can access the data from the cloud server.

I. INTRODUCTION

Big data is data sets that are so voluminous and complex that traditional data-processing software is inadequate to deal with them. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, querying, visualization, updating, information privacy and data source. There are five dimensions to big data known as **volume, variety, velocity** and the recently added **veracity** and **value.**

Volume
The quantity of generated and stored data. The size of the data determines the value and potential insight- and whether it can be considered big data or not.
Variety
The type and nature of the data. This helps people who analyze it to effectively use the resulting insight.
Velocity
In this context, the speed at which the data is generated and processed to meet the demands and challenges that lie in the path of growth and development.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

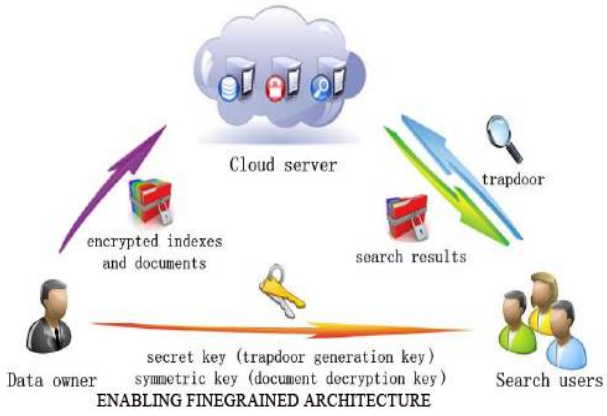
Variability
Inconsistency of the data set can hamper processes to handle and manage it.
Veracity
The data quality of captured data can vary greatly, affecting the accurate analysis.[32]
Most existing approaches for securing the outsourced big data in clouds are based on either attributed-based encryption (ABE) or secret sharing. **Attribute Based Encryption**provides flexibility to the data owner to predefined the set of user who are eligible for accessing the data. **Secretsharing** provide the flexibility of distributing the secret data to be shared among users who are verified from the data owner. There are some challenges in the existing system while outsourcing the data to the cloud.
1.It is a challenging issue to dynamically and efficiently update the access policies according to the new requirements of the data owners in secret sharing approaches.
2.Another challenging issue is how to verify the legitimacy of the users accessing the outsourced data in clouds.
3. Multiple users need to mutually verify each other using multiple RSA operations, such a procedure has a high computational overhead.
The challenges mentioned above motivate us to develop a secure and verifiable access control scheme for big data storage in clouds by the following secret services:
• **Security**: The proposed scheme should be able to defend against various attacks such as the collusion attack. Meanwhile, access policy update should not break the security of the data storage, disclose sensitive information about the data owner, and cause any new security problem.
• **Verification:** When a user needs to decrypt a stored ciphertext, its access legitimacy should be verified by other participating users and the secret shares obtained from other users must be validated for correct recovery.
• **Authorization:** To reduce the risk of information leakage, a user should obtain authorization from the data owner for accessing the encrypted data.

II. RELEATED WORK

In cloud storage system Attribute Based Encryption (ABE) [3] is used and it is known as one of the most suitable technologies, it has two forms ABE (KP-ABE) and Cipher text policy ABE both are effective for a ABE. Policies are building into user's secret keys in a KP-ABE. While in other form means in CP-ABE attributes are used to describe the user's attribute and the access policies over there attributes are attached to the encrypted are attached to the encrypted data. In fine-grained access control of encrypted data process key policy based encryption and also discussed how to change policies on keys. In Dynamic credentials & cipher text delegation for attribute-based encryption's author proposed a cipher text delegation method which is used to update the policies of cipher text. In" "Privacy preserving cloud data access with multi-authorities," author proposed any valid user's can cipher text re-encrypted by decrypting it first, thus a new outsourced policy updating method is desired for ABE system's.

III.MODEL AND PRELIMINARIES

SYSTEM MODEL



Cloud server:-A cloud server provides spaces for data owners to store their outsourced ciphertext data that can be retrieved by the users. It is also responsible for updating the ciphertexts when the data owner changes its access policy.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Owners:-A data owner designates the access policy or its data, encrypts the database don the access policy before outsourcing the data to the cloud server, and requests the cloud server to update the encrypted data when a new access policy is adopted. It can also check whether the ciphertext at the cloud server is correctly updated.
Users:-Each user is assigned with a sub-key for an encrypted data that the user is eligible to access. In order to decrypt the ciphertext, the user's eligibility must be verified by at least t−1 other users that are also eligible to access the data. The information provided by the t − 1 verifiers must be validated by the user for correct message decryption based on the (t,n)-threshold secret sharing.

IV. PRELIMINARIES

We introduce two crypotographicprimitive: **NTRUcrypotosystem** and **secret sharing**

THE NTRU CRYPTOSYSTEM

The NTRU cryptosystem is based on the shortest vector problem (SVP) in a lattice that makes it lightning fast and resistant to quantum computing attacks. It has been proved to be faster than RSA.
The arithmetic of NTRU depends on three integer parameters (N, p, q). Let Zq = Z/qZdenote the ring of integers modulo q. The operations of NTRU took place in the ring of truncated polynomials P = Zq[X]/ XN − 1 . In this ring, a polynomial f is defined by its coefficients in the base 1, X, X2 , . . . , XN−1 as
f = (f0, f1, . . . , fN−1) = f0 + f1X + . . . + fN−1XN−1
The addition of two polynomials f and g is defined as pairwise addition of the coefficients of the same degree
f + g = (f0 + g0, f1 + g1, . . . , fN−1 + gN−1),
and multiplication, noted " ∗ " is defined as a convolution multiplication
f∗ g = h = (h0, h1, . . . , hN−1), with hk = X i+j≡k (mod N) figj .
The Euclidean norm or the length of a polynomial f = (f0, f1, · · · , fN−1) is defined as
kfk = vuut N X−1 i=0 f 2 i
Let B(d)) be the binary set of polynomials defined for a positive integers d as the set of polynomials of R with d coefficients equal to 1 and all the other coefficients equal to 0. The set B(d)) can be written as
B(d) = (f(X) = N X−1 i=0 fiXi∈ P | fi ∈ {0, 1}, N X−1 i=0 fi = d)
Different descriptions of NTRUEncrypt, and different proposed parameter sets, have been in circulation since 1996. The 2005 instantiation of NTRU is set up by six public integers N, p, q, df , dg, dr and four public spaces Lf , Lg, Lm, Lr.

- N is prime and sufficiently large to prevent lattice attacks.
- p and q are relatively prime numbers.
- q is much larger than p.
- Lf = B(df) is a set of small polynomials from which the private keys are selected.
- Lg = B(dg) is a similar set of small polynomials from which other private keys are selected.
- Lm = Zp[X]/ XN − 1 is the plaintext space. It is a set of polynomials m ∈Zp[X]/(XN − 1) that represent encryptable messages.
- Lr = B(dr) is a set of polynomials from which the blinding value used during encryption is selected. The key generation, encryption and decryption primitives are as follows:

1. Key generation

- Randomly choose a polynomial f ∈ Lf such that f is invertible in P modulo p and modulo q.
- Compute fp ≡ f −1 (mod p) and fq ≡ f −1 (mod q).
- Randomly choose a polynomial g ∈ Lg.
- Compute h ≡ g ∗fq (mod q).
- Publish the public key (N, h) and the set of parameters p, q, Lf ,Lg, Lr and Lm.
- Keep the private key (f, fp).

2. Encryption

- Represent the message as a polynomial m ∈ Lm.
- Randomly choose a polynomial r ∈Lr.
- Encrypt m with the public key (N, h) using the rule e ≡ p ∗ r ∗ h + m (mod q).

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

3. Decryption

• The receiver computes $a \equiv f * e \pmod q$.

• Using a centering procedure, transform a to a polynomial with coefficients in the interval $-q/2, q/2$.

• Compute $m \equiv fp * a \pmod p$

The decryption process is correct if the polynomial $p * r * g + f * m \pmod q$ is actually equal to $p * r * g + f * m \in Z[X]/(X^N - 1)$, that is without using modulo q. We have

$a \equiv f * e \pmod q$

$\equiv f * (p * r * h + m) \pmod q$

$\equiv f * r * (p * g * fq) + f * m \pmod q$

$\equiv p * r * g * f * fq + f * m \pmod q$

$\equiv p * r * g + f * m \pmod q$.

Hence, if $a = p * r * g + f * m$ in $Z[X]/(X^N - 1)$, then

$a * fp \equiv (p * r * g + f * m) * fp \equiv m \pmod{}$.

AN IMPROVED NTRU CRYPTOSYSTEM

There exist two types of decryption failures in NTRU: the Wrap failure and the Gap failure. In other words, the decryption process of NTRU cannot always output a correct decrypted message. To overcome this problem, we propose an improved NTRU cryptosystem in this section. To proceed, we first analyze the reasons of the decryption failures in the original NTRU. When a ciphertext $e = p\varphi * h + m \pmod q$ is received, it is decrypted according to the following two steps:

1) Compute $a = e * f \pmod q$;

2) Calculate $m0 = a * fp \pmod p$.

As analyzed, the NTRU decryption could correctly recover the plaintext m if $a = (a0, a1, a2, \cdots, aN-1)$ remains unchanged after the module q operation in step 1. This indicates that as long as $ai \in (-q/2, q/2)$, $i = 0, 1, \cdots, N-1$, before the mod q operation, m can be correctly recovered. If there is at least one ai with $|ai| \geq q/2$, the Wrap failure could happen, resulting in $m0 \neq m$ with a high probability; if $\max_{0 \leq i \leq N-1}\{ai\} - \min_{0 \leq i \leq N-1}\{ai\} > q$, the Gap failure could happen, leading to $m0 \neq m$ with a high probability. From the above analysis, one can see that the Gap failure leads to the Wrap failure and thatovercomingtheWrapfailurecanalsogetting rid of the Gap failure.

In order to overcome the Wrap failure, we propose the following improved NTRU decryption algorithm. For $a = e * f = p\varphi * h * f + m * f$, we first figure out $\Gamma = \max\{|\max_{0 \leq i \leq N-1}\{ai\}|, |\min_{0 \leq i \leq N-1}\{ai\}|\}$ in a, and then compute $\tau = b\Gamma q/2c$. If $\tau = 0$, which implies that each $ai \in (-q/2, q/2)$ in a, we can decrypt e to get m via the traditional approach; otherwise, we adjust a to obtain $a0 = a - c(1) - c(2) - \cdots - c(\tau)$, where $c(1), c(2), \cdots, c(\tau)$ are the adjusting vectors and $c(j) = (c(j)\,0, c(j)\,1, \cdots, c(j)\,N-1)$ for $j = 1, 2, \cdots, \tau$.

V. DISCUSSION

In our scheme, a data owner maintains the access right to its encrypted data. The advantages of such a policy are listed as follows: • Thedataownersplitstheaccess rightoftheencrypteddata into n pieces, with each legitimate user holding one piece of the access right. This can effectively reduce the risk of information leakage in big data storage. • If a user Ui wants to decrypt the data owner's encrypted data Sj, its legitimacy must be verified by the data owner (by securely and successfully retrieving the message certificate dj from the data owner) and at least $t - 1$ other legitimate users of the data (via the exchange certificate); the information provided by the $t-1$ other users for the message recovery also must be verified by Ui to prevent the user from providing fake information. This verification process can ensure the legality of Ui to access Sj. • The cloud sever only stores the outsourced ciphertext data - it cannot obtain the data owner's original plaintext data. In addition,the data owner updates the access policy while the cloud server updates the encrypted data.No data owner can access the plaintext data outsourced by other data owners in the cloud server. Compared with RSA, at an equivalent cryptographic strength, NTRU performs the costly encryption and decryption operation sat a much faster speed,and its implementationsinbothhardwareandsoftwareareeasierandrequireasmallersizeofmemory;therefore NTRU can be employed in applications involving devices with limitedcomputationpowerandstoragesuchasmobiledevicesand smart-

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

cards.Ontheotherhand,whenourschemeisutilizedinreal worldapplications,anadequatethreshold t needstobeselectedby the data owner before deployment because an unsuitable threshold t would decrease the security of the data if t is too small or have a harmful effect on the flexibility of access control if t is too large. Nevertheless, the selection of a right value for t is not easy. One possible remedy approach is to pick up an initial value of t based on experience and adjust it via access policy update as time goes.

VI. CONCLUSION AND FUTURE WORKS

In this paper, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU and then present a secure and verifiable access control scheme based on the improved NTRU to protect the outsourced big data stored in a cloud. Our scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding outsourced ciphertext to enable efficient access control over the big data in the cloud. It also provides a verification process for a user to validate its legitimacy of accessingthedatatobothdataownerand t−1 otherlegitimate users and the correctness of the information provided by the t−1 other users for plaintext recovery. The security of our proposed scheme is guaranteed by those of the NTRU cryptosystem and the (t,n)-threshold secret sharing. We have rigorously analysed the correctness, security strength, and computational complexity of our proposed scheme. Designing a secure, privacy preserving, and practical scheme for big data storage in a cloud is an extremely challenging problem. In our future research, we will further improve our scheme by combining the (t,n)-threshold secret sharing with attribute based access control, which involves an access structure that can place various requirements for a user to decrypt an outsourced ciphertext data in the cloud. Meanwhile, we will investigate the security problems when a data owner outsources its data to multicloud servers and consider an attribute-based access structure that can be dynamically updated, which is more applicable for practical scenarios in big data storage.

VII. ACKNOWLEDGMENT

This research was partially supported by the National Science Foundation of the US under grants CNS-1318872, CCF-1442642 and IIS-1343976, and the National Natural Science Foundation of China under grants 61672119, 61373027, 61472044, 61272475, 61571049, 61472403, and 61672321, and the Fundamental Research Funds for the Central Universities (No.2014KJJCB32).

REFERENCES

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.
[2] V. Marx, "Biology: The big challenges of big data," Nature, vol. 498, no. 7453, pp. 255–260, 2013.
[3] G. P. Consortium et al., "A map of human genome variation from population-scalesequencing,"Nature,vol.467,no.7319,pp.1061–1073, 2010.
[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.
[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between external users and wireless body area networks," in Proceedingsofthe2ndACMworkshoponHottopicsonwirelessnetwork security and privacy. ACM, 2013, pp. 31–36.
[6] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94– 107, 2016.
[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 89–98.
[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography– PKC 2011, pp. 53–70, 2011.
[9] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 37–46, 2013.
[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT 2011, pp. 568–588, 2011.
[11] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, "An attributebasedsigncryption scheme to secure attribute-defined multicast communications," in SecureComm 2015. Springer, 2015, pp. 418–435.
[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.
[13] M. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multisecret sharing," Computer Standards & Interfaces, vol. 30, no. 3, pp. 187–190, 2008.
[14] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," Information Sciences, vol. 180, no. 15, pp. 2889–2894, 2010.
[15] M. H. Dehkordi and S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes," Information Sciences, vol. 178, no. 9, pp. 2262–2274, 2008.