"ACHIEVING PRIVACY OF BIG DATA IN MOBILE CLOUD USING DYNAMIC DATA ENCRYPTION STRATEGY (D2ES)"

[1]Madhuri D. Alhat, [2]Prof. Sonali A. Patil,
PG Student[1], Assistant Professor[2], Department Computer Engineering, JSPM's BSIOTR Wagholi, Pune, India-412207[1, 2]

ABSTRACT: Technology is enhancing each and every day especially in the field of Information Technology and data is very momentous elements. Due to the reasons such as the rapid growth and spread of network services, mobile devices, and online users on the Internet leading to a remarkable increase in the amount of data. Almost every industry is trying to cope with this huge data. Big data phenomenon has begun to gain importance. However, it is not only very difficult to store big data and analyze them with traditional applications, but also it has challenging privacy and security problems. So we proposed system will classify the files in two main categories i.e. hot files and Cold files. To avoid bottleneck at server end the replicas of hot file will created and stored on different servers. This accession is drafted to magnify privacy protection scope within liquidate time constraints. Proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints.

***Index Terms:* Big Data Storage; Access Control; the NTRU Cryptosystem; Secret Sharing; Access Policy Update; Cloud Computing.**

I INTRODUCTION

Big data is a high volume, and/or high velocity, high variety information asset, which requires new forms of processing to enable enhanced decision making, insight discovery, and process optimization. Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues. In this project, DROPS methodology, divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaning-ful information is revealed to the attacker. Data access control is a challenging issue in public cloud storage systems. Cipher text-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Clients might be stuck in the sitting tight line for a long stretch to get their mystery keys, along these lines bringing about low-proficiency of the framework. In spite of the fact that multi expert access control plans have been proposed, these plans still can't conquer the disadvantages of single-point bottleneck and low effectiveness; because of the way that each of the specialists still autonomously deals with a disjoint characteristic set. We propose a novel heterogeneous framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism. Our system utilizes various credit experts to share the heap of client authenticity check. In the interim, in our plan, a CA (Central Authority) is acquainted with create mystery keys for authenticity checked clients. Not at all like other multi specialist get to control plots, each of the experts in our plan deals with the entire quality set exclusively. To enhance security, we also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure. Examination demonstrates that our framework ensures the security necessities as well as makes awesome execution change on key generation.

II LITERATURE SURVEY

Data access control is a challenging issue in cloud storage. Cipher text-Policy Attribute-based Encryption (CP-ABE) is a potential cryptographic technique to address the above issue, which is able to enforce data access control based on users permanent characteristics. However, in some scenarios, access policies are associated with user's temporary conditions (such as access time and location) as well as their permanent ones. CP-ABE cannot deal with such situations commendably. In this paper, we focus on the scenario where user's access privilege is determined by their attributes, together with their locations. To cope with this data access control requirement, we propose a location-aware attribute-based access control mechanism (LABAC) for cloud. In LABAC, we uniquely integrate CP-ABE with location trapdoors to make up access policies. In this way, data owners can flexibly combine both user's attributes and locations to implement a fine-grained control of their data. A competitive advantage of LABAC is that it requires no any additional revocation mechanisms to revoke location-aware access privilege when user location changes. Security and performance analysis are presented which show the security and efficiency of LABAC for practical implementations [4].

The datasets usually are encrypted before outsourcing to preserve the privacy. However, the common practice of encryption makes the effective utilization difficult; for example, search the given keywords in the encrypted datasets. Many schemes are proposed to make encrypted data searchable based on keywords. However, keyword-based search schemes ignore the semantic representation information of user's retrieval, and cannot completely meet with users search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, we proposed an innovative semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. More specifically, our scheme first indexes the documents and builds trapdoor based on the concept hierarchy. To further improve the search efficiency, we utilize a tree-based index structure to organize all the document index vectors. Our experiment results based on the real world datasets show the scheme is more efficient than previous scheme. We also study the threat model of our approach and prove it does not introduce any security risk [2].

In this paper, we propose a scheme to enable the requester to delegate set operations over crowd sourced big data to the cloud. Meanwhile, workers data and identity privacy are preserved, and the requester can verify the correctness of the set operation result. We extend our scheme to achieve data preprocessing, batch verification and data update are also proposed to reduce computational costs of the system. [3]

Because of the intricacy and volume, outsourcing cipher texts to a cloud is considered to be a standout amongst the best methodologies for enormous information stockpiling and access. By and by, confirming the entrance authenticity of a client and safely refreshing a cipher text in the cloud in view of another entrance strategy assigned by the information proprietor are two basic difficulties to make cloud-based huge information stockpiling commonsense and successful. Conventional methodologies either totally disregard the issue of access arrangement refresh or designate the refresh to an outsider specialist; yet practically speaking, get to approach refresh is vital for improving security and managing the dynamism caused by client join and leave exercises.[1]

III EXISTING SYSTEM

Dynamic Data Encryption Strategy (D2ES) Model:

1) Phase I: Sorting by Weights: This is a preparation phase of the model. All data package types are sorted at this phase. The sorting operations consider both execution time and privacy protections; thus two variables are involved, which are PWVs and the corresponding encryption execution time. The sorting operation uses a descending order. The sorting results form a table that is named S Table

2) Phase II: Data Alternatives: This phase is the crucial step of selecting data packages for encryption operations. S Table will be used for providing the reference of protection efficiencies.

3) Phase III: Output: This phase mainly output the results of the Phase II. An encryption plan will be generated at this phase.

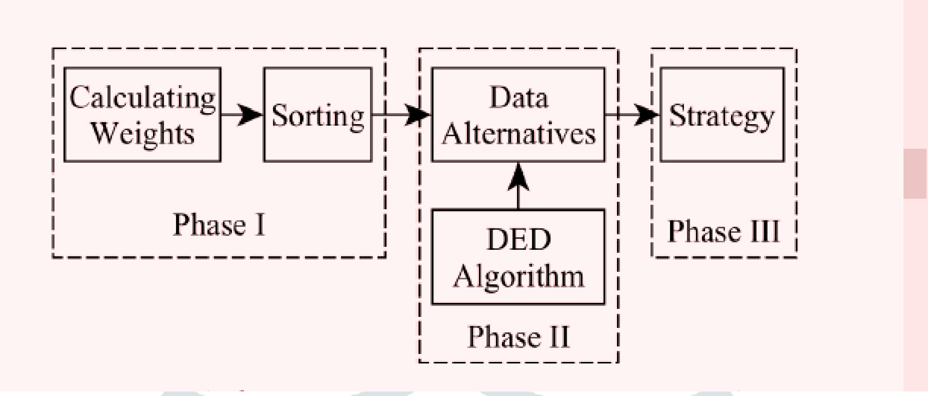


Figure 3.1: Dynamic Data Encryption Strategy (D2ES) Model

IV PROBLEM STATEMENT

"To develop a model that provide privacy to big data in mobile cloud computing and selectively encrypts data packages to maximize the privacy protection level under timing constraints"

V PROPOSED SYSTEM

The data to a cloud is an appropriate approach. Generally speaking, clouds can be classified into two major categories: 1) public clouds with each being a multi-tenant environment shared with a number of other tenants, and 2) private clouds with each being a single-tenant environment dedicated to a single tenant. For example, the IBM cloud was proposed as a public one for the data management of banking. When a bank stores its data in the could server only its legal staff members have the rights to access the stored data. Typically the bank system contains much sensitive and private consumer information. In order to reduce the risk of information leakage, the access right of an employee should be properly restricted, and a single employee should not be allowed to reveal the data by it without obtaining the authorization from other users; that is, recovering the data requires to get the authorization of multiple employees.

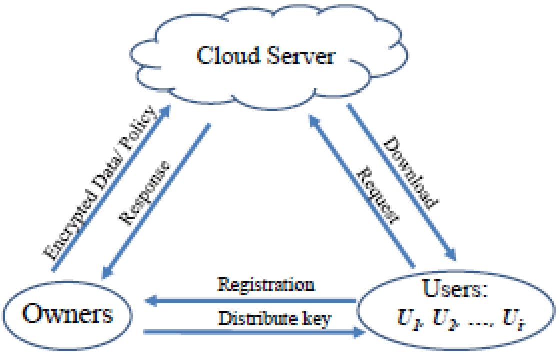


Figure 5.1: System Architecture

VI METHODOLOGY

1. Data Owner Module: A data owner designates the access policy for its data, encrypts the data based on 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 cipher-text at the cloud server is correctly updated.

2. User Module: The data consumer (User) is assigned a global user identity Uid by CA. In the proposed system the user send request to the cloud server for accessing the file. Each user is assigned with a sub-key for an encrypted data the user is eligible to access.

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

VII ALGORITHM

NTRU (Nth degree Truncated polynomial Ring Units) is probably the only post quantum public key cryptosystem suitable for practical implementation. Recently, several NTRU based systems have also been shown having property of homomorphic encryption with important application in cloud computing security. In this thesis, several efficient algorithms and architectures for NTRU Encrypt system and for NTRU based homomorphic encryption system are proposed. For NTRU Encrypt system, a new LFSR (linear feedback shift register) based architecture is firstly presented. A novel design of the modular arithmetic unit is proposed to reduce the critical path delay. The FPGA implementation results have shown that the proposed design outperforms all the existing works in terms of area-delay product. Secondly, a new architecture using extended LFSR is proposed for NTRUEncrypt system. It takes advantage of small polynomials with many zero coefficients, and thus significantly reduces the latency of the computation with modest increase of the complexity. Thirdly, systolic array architecture is proposed for NTRU Encrypt. There is only one type of PE (process element) in the array and the PE was designed with optimized arithmetic. The systolic array yields all the output in N clock cycles.

NTRU Algorithm

Operations are based on objects in a truncated polynomial ring R=Z[X]/(X^N-1), polynomial degree at most N-1: $a_0 + a_1 + a_2$ x^2 + · · · + a_{N-1} x^(N−1)

1st step: User B randomly chooses 2 small polynomials f and g in the R (the ring of truncated polynomials). Notes: - The values of these polynomials should keep in a secret. - A chosen polynomial must have an inverse

2nd step: The inverse of f modulo q and the inverse of f modulo p will be computed Properties: f*fq^-1 = 1 (modulo q) and f*fp^-1 = 1 (modulo p)

3rd step: Product of polynomials will be computed: h = p * ((Fq)*g)mod q. Private key of B: the pair of polynomials f and fp Public key of B: the polynomial h.

NTRU Decryption

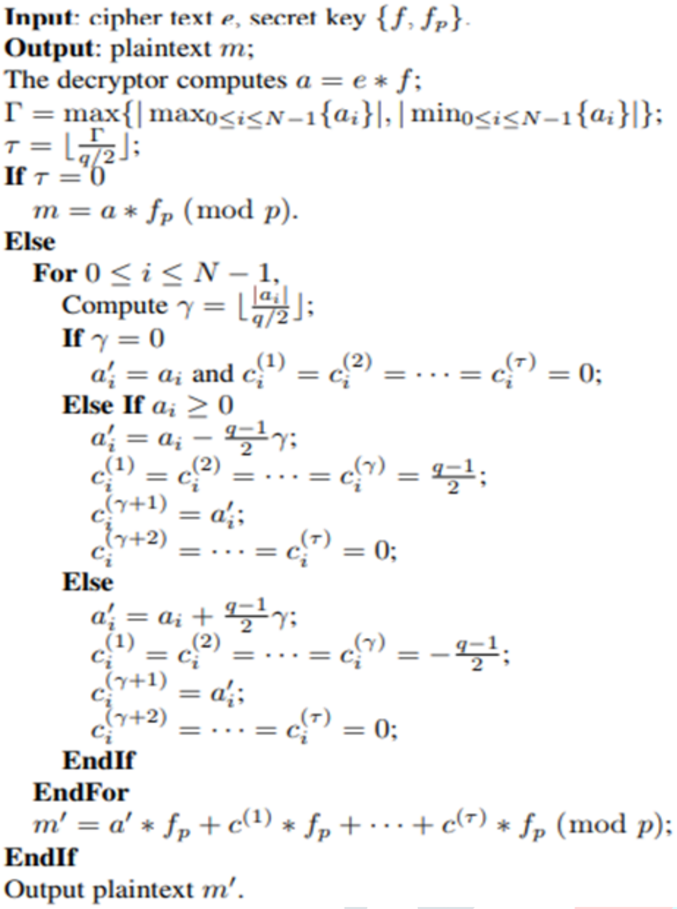
B receives a message e from A and would like to decrypt it.

1st step: Using his private polynomial f he computes a polynomial a= f*e(mod q). B needs to choose coefficients of a that lie in an interval of length q.

2nd step: He computes the polynomial b=a(mod p). B reduces each of the coefficients of a modulo p.

3rd step: B uses the other private polynomial fp to compute c=fp*b(modulo p), which is the original message of A.

NTRU:



```
Input: cipher text $e$, secret key $\{f, f_p\}$.
Output: plaintext $m$;
The decryptor computes $a = e * f$;
$\Gamma = \max\{|\max_{0\leq i\leq N-1}\{a_i\}|, |\min_{0\leq i\leq N-1}\{a_i\}|\}$;
$\tau = \lfloor \frac{\Gamma}{q/2} \rfloor$;
If $\tau = 0$
    $m = a * f_p \pmod{p}$.
Else
    For $0 \leq i \leq N-1$,
        Compute $\gamma = \lfloor \frac{|a_i|}{q/2} \rfloor$;
        If $\gamma = 0$
            $a'_i = a_i$ and $c_i^{(1)} = c_i^{(2)} = \cdots = c_i^{(\tau)} = 0$;
        Else If $a_i \geq 0$
            $a'_i = a_i - \frac{q-1}{2}\gamma$;
            $c_i^{(1)} = c_i^{(2)} = \cdots = c_i^{(\gamma)} = \frac{q-1}{2}$;
            $c_i^{(\gamma+1)} = a'_i$;
            $c_i^{(\gamma+2)} = \cdots = c_i^{(\tau)} = 0$;
        Else
            $a'_i = a_i + \frac{q-1}{2}\gamma$;
            $c_i^{(1)} = c_i^{(2)} = \cdots = c_i^{(\gamma)} = -\frac{q-1}{2}$;
            $c_i^{(\gamma+1)} = a'_i$;
            $c_i^{(\gamma+2)} = \cdots = c_i^{(\tau)} = 0$;
        EndIf
    EndFor
    $m' = a' * f_p + c^{(1)} * f_p + \cdots + c^{(\tau)} * f_p \pmod{p}$;
EndIf
Output plaintext $m'$.
```

VII CONCLUSION AND FUTURE WORK

In this paper 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 cipher-text to enable efficient access control over the big data in the cloud.

REFERENCES

[1] Zhangjie Fu, Xingming Sun and Sai Ji, Towards efficient content-aware search over encrypted outsourced data in cloud IEEE INFOCOM 2016.

[2] Yingjie Xue, Jianan Hong,Wei Li and Kaiping Xue, LABAC: A location-aware attribute-based access control scheme for cloud storage 2016 IEEE.

[3] Gaoqiang Zhuo, Qi Jia, “Privacy-preserving Verifiable Set Operation in Big Data for Cloud-assisted Mobile Crowd sourcing”2017.

[4] Dr. S. Prayla Shyry, “A SECURE AND VERIFIABLE ACCESS CONTROL SCHEME FOR BIG DATA STORAGE IN CLOUDS” Volume 119 No. 12 2018.

[5] Prof.Sonali A. Patil, Dr.Sharmila Sankar, Dr. M. Sandhya “A Servey On Cloud Computing Parameters,” Asian Journal Of Convergence In Technology, volume IV Issue I.

[6] Prof.Sonali A. Patil, Ms.Megha D.Savekar “KNN CLASSIFICATION SCHEME BASED PRIVACY PRESERVING POLICY OVER SEMANTICALY SECURE ENCRYPTED DATABASE, IJARIIE-ISSN(O)-2395-4396, vol-2 Issue-3,2016.

[7] Prof. Sonali A. Patil, Pritam L Mahamane “A Servey On Cloud Data Security And Intrigrity using Sack of Cryptographic Algorithm through Trusted Third Party(TTP), volume 4, Issue 12, December 2016.