IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 12, December 2019, ||Series -III|| PP 14-17

Secure Data Distribution in Mobile Cloud Computing

[1]S. DineshKumar, [2]P Pradheeba,[3]J.Alex Rozario
[1]Assistan Professor Professor, [2]Assistan Professor, [3]Assistant Professor
Department of Computer Science and Engineering
CMS College of Engineering and Technology,
Coimbatore, Tamil Nadu, India

Abstract *- The goal of this research is to make attribute-based encryption (ABE) more suitable for data access control in the cloud.We focus on offering the encryptor complete control over access permissions, allowing for effective key management even in the face of many independent authorities. Cloud computing expansion is hampered by two primary factors: security and privacy. The fact that there are less real-time and business-related cloud applications than consumer-related cloud applications is due to security concerns. A new encryption approach based on Attribute Based Encryption (ABE) has been presented, which includes hash functions, digital signatures, and asymmetric encryption schemes. Our proposed algorithm is a simple but effective technique that can be used in cloud-based applications.*

I. INTRODUCTION

Cloud computing security architecture only allows valid users to upload or share data according to their needs.A valid user can store or upload data into a distributed cloud environment and maintain it for future work thanks to cloud security architecture, which provides a multi-cloud security framework.

The existing approach necessitates a large storage capacity that cannot be met by a desktop computer. This technique employs encryption and decoding.

II. LITERATURE REVIEW

The data in cloud computing is stored at an undisclosed location to the end user. To begin, data in the database must be secure. Virtualization provides a solution for data security. The location of the data centre is kept secret to ensure security and integrity.The question is whether or not to trust an untrustworthy cloud server.We declared it untrustworthy because it involves numerous harmful attacks during data processing.

Brent Waters proposed the cipher text attribute based encryption.The ABE is presented as a solution to the difficult access control method for encrypted data.ABE is a one-to-many encryption based on public keys that decrypts the cipher text only if the user's private key matches the public key and master secret key. The server does the data decryption directly. As a result, effective encryption approaches improve performance.It has a significant disadvantage in terms of decryption costs.[2].

The key policy attribute based encryption was proposed by goyal et al . The KP-ABE has three algorithms. The access structure granted full access to the user. This is major limitation of the key policy attribute based encryption. Full access granted to user creates a lot of problem. The KP-ABE fails the distinguish the necessary access control to the users as the access policy embedded in the decryption key[3].

In 2011 green et al proposed the concept of outsourcing the decryption for ABE ie user has to decrypt the data by him. The ABE with outsourced decryption overcomes the limitation of waters and it assures security from malicious attackers. The cipher text is decrypt only with the public key matches with the user private key[4].

The green et al algorithm modifies the water algorithm with transformation key and retrieving key. The original data is compared with partially encrypted data to achieve confidentiality of the data. The limitation includes non-verifiability of data whether the required cipher text is decrypted. It might produce the previous cipher text or any other cipher that associated with particular file or anything. The other disadvantages include the user has additional work to decrypt the data. Probability of attackers to hack the account is very less[9].

In 2013 Junzuo Lai et al proposed the ABE outsourced decryption . This overcomes the limitation of green et al with verifiable outsourcing of data. The proposed algorithm matches the cipher text with the decrypted cipher text. Thus verification of data is the main advantage of this algorithm. The proxy re-encryption is used for decryption of the ciphers. And size of ciphers also very small in size. The performance of the proposed system is relatively high. Thus cloud is ready for mission critical applications with outsourced decryption of data. The limitation this system includes robustness and scalability. Security and performance measured are relatively varied in real time applications as they have high network traffic and complex access structure. When the number of users increases the performance of the system will be decreased [1].

III. EXISTING SYSTEM

Though the electronic technologies have undergone fast developments in recent years, mobile devices such as smartphones are still comparatively weak in contrast to desktops in terms of computational capability, storage etc, and are not able to meet the increasing demands from mobile users. By integrating mobile computing and cloud computing, mobile cloud computing (MCC) greatly extends the boundary of the mobile applications, but it also inherits many challenges in cloud computing, e.g., data privacy and data integrity. In this paper, we leverage several cryptographic primitives such as a new type-based proxy re-encryption to design a secure and efficient data distribution system in MCC, which provides data privacy, data integrity, data authentication, and flexible data distribution with access control. Compared to traditional cloud-based data storage systems, our system is a lightweight and easily deployable solution for mobile users in MCC since no trusted third parties are involved and each mobile user only has to keep short secret keys consisting of three group elements for all cryptographic operations. Finally, we present extensive performance analysis and empirical studies to demonstrate the security, scalability, and efficiency of our proposed system

Proxy re-encryption

- Public key encryption RSA
- AES

Disadvantages:

- It uses too simple algebraic structure.
- Every block is always encrypted in the same way.
- Hard to implement with software.
- proxy re-encryption in counter mode is complex to implement in software taking both performance and security into considerations

IV. PROPOSED SYSTEM

The Cloud computing technique, which enables the resource using latest trend in today IT industry. Data security system is the issue in cloud computing available on the cloud server. The physical control is arising under the privacy and security concerns. The cloud data storage are encrypt on the cloud storage. Here we are using **Hybrid ABE and Homomorphic Encryption**. The **ABE (Attribute based encryption)** is used to encrypt the data and stored the server. The secure the data using the collusion the encrypt system describes under the polices on the users key. The attribute encrypt the data using the traditional access control. The perform the framework using the Homomorphic encryption.

Algorithm Used: Hybrid ABE and Homomorphic Encryption

Advantages:

- It uses too complicated algebraic structure.
- Every block is encrypted in the different way.
- Easy to implement with software.

Hybrid ABE (Attributed Based Homomorphic Encryption)
Algorithm

Cipher-text-Policy Attribute Based Encryption Algorithm: A cipher-text policy attribute based encryption scheme consists of four fundamental algorithms: Setup, Encrypt, Key Gen and Decrypt.

I. Setup: The setup algorithm takes no input other than the implicit security parameter.
It outputs of the public parameters(PK) and a master key(MK).

ii. Encrypt (PK, M, A) : The encryption algorithm gets the input : the public parameters(PK) , message(M) , and structure A over universe of attributes .

The algorithm encrypts (M) and produce cipher text (CT) such that only user that group a set of attributes that convince the access structure to be decrypt the message.

iii. Key Generation (MK, S) : The key generation algorithm takes as input : the master key(MK) and set of attributes(S) that describe the key. It outputs: private key (SK).

iv. Decrypt (PK, CT, SK): The decryption algorithm takes as input: the public parameters PK, a cipher-text CT, which contains an access policy A, and a private key SK, which is a private key for a set S of attributes. If the set S of attributes satisfies the access structure A then the algorithm will decrypt the cipher-text and return a message M.

v. Delegate (SK, S): The delegate algorithm takes as input a secret key SK for some set of attributes S and a set S Ł S. It output a secret key SK for the set of attributes S.

V. SYSTEM IMPLEMENTATION

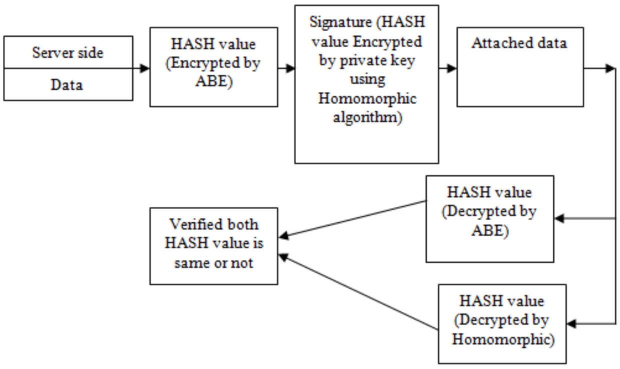
Server side
Data
HASH value (Encrypted by ABE)
Signature (HASH value Encrypted by private key using Homomorphic algorithm)
Attached data
HASH value (Decrypted by ABE)
Verified both HASH value is same or not
HASH value (Decrypted by Homomorphic)

Figure 5.1 Cloud architecture Construction using cloudsim

The CloudSim simulator is a layered architecture. The different layers of cloudsim are shown in the above figure. 1) Network Layer: This layer of CloudSim has responsibility to make communication possible between different layers. This layer also identifies how resources in cloud environment are places and managed. 2) Cloud Resources: This layer includes different main resources like datacenters, cloud coordinator (ensures that different resources of the cloud can work in a collaborative way) in the cloud environment. 3) Cloud Services: This layer includes different service provided to the user of cloud services. The various services of clouds include Information as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). 4) User Interface: This layer provides the interaction between user and the simulator

5.1 Task Creation

In this module, task is created. Since interval scheduling mechanism is used, each task requests service from the cloud platform with a specific start and finish time. Task which has been created is stored for allocation process.

5.2 Hybrid Abe And Homomorphic Encryption.

Hybrid Attribute based encryption to provide better solution for access control. It used user identities as Attributes and these attributes play important role in encryption and decryption. The primary ABE used a threshold policy for access control, but it lacks expressibility. ABE schemes are further classified into key-policy attribute based encryption. We say that a homomorphic encryption scheme *E* is fully homomorphic if it compactly evaluates all circuits We say that a family of homo-morphic encryption schemes *fE*(*d*) : *d 2* Z+*g*islevelled fully homomorphic if, for all *d 2* Z+,they all use the same decryption circuit, *E*(*d*) compactly evaluates all circuits of depth almost *d* (that use some specified set of gates), and the computational complexity of *E*(*d*)'algorithms is polynomial in *d*, and the size of the circuit *C*.

5.3 Hybrid ABE and Homomorphic encryption.

Hybrid Attribute based encryption to provide better solution for access control. It used user identities as Attributes and these attributes play important role in encryption and decryption. The primary ABE used a threshold policy for access control, but it lacks expressibility. ABE schemes are further classified into key-policy attribute based encryption. We say that a homomorphic encryption scheme *E* is fully homomorphic if it compactly evaluates all circuits We say that a family of homo-morphic encryption schemes *fE*(*d*) : *d 2* Z+*g*is levelled fully homomorphic if, for all *d 2* Z+,they all use the same decryption circuit, *E*(*d*) compactly evaluates all circuits of depth almost *d* (that use some specified set of gates), and the computational complexity of *E*(*d*)'algorithms is polynomial in *d*, and the size of the circuit *C*.

VI. CONCLUSION AND FUTURE WORKS

The current state of attribute-based encryption in cloud computing was examined, along with its benefits and drawbacks.We've also classed cloud applications based on the danger they pose, taking into account a variety of factors.A thorough examination of attribute-based encryption is carried out.We also classed the cloud application depending on the risk it poses, and we classified it using appropriate encryption mechanisms.Finally, we present a new ABE-based encryption technique that includes hash functions, digital signatures, and asymmetric encryption.Microsoft Azure is currently being moved entirely to the cloud.Cloud computing has numerous benefits.As a result, the cloud's utility should not be diminished in the future.As a result, cloud computing must progress to the next level by being applied to applications such as healthcare.

REFERENCES:

[1]. JunzuoLai,Deng, R.H, Chaowen Guan, JianWeng,.Attribute-Based Encryption With Verifiable Outsourced Decryption Information Forensics and Security, IEEE Transactions on , vol.8, no.8, pp.1343,1354, Aug. 2013.

[2]. B. Waters. Ciphertext-policy attribute-based encryption:An expressive, efficient, and provably secure realization in Proc. Public Key Cryptography, 2011, pp. 53–70.

[3]. VipulGoyal, OmkantPandey, AmitSahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06).ACM, New York, NY, USA, 89-98.

[4]. Matthew Green, Susan Hohenberger, and Brent Waters. 2011. Outsourcing the decryption of ABE ciphertexts. In Proceedings of the 20th USENIX conference on Security (SEC'11).USENIX Association, Berkeley, CA, USA, 34-34.

[5]. Dropboxnews.https:// www.dropbox.com/news.

[6]. RafailOstrovsky, AmitSahai, and Brent Waters. 2007. Attribute-based encryption with non-monotonic access structures. In Proceedings of the 14th ACM conference on Computer and communications security (CCS '07). ACM, New York, NY, USA, 195-203.

[7]. S. Chatterjee and A.Menezes. On cryptographic protocols employing asymmetric pairings—The role of revisited,‖DiscreteAppl.Math., vol. 159, no. 13, pp. 1311–1322, 2011.

[8]. Patrick P. Tsang, Sherman S. M. Chow, and Sean W. Smith. 2007. Batch pairing delegation. InProceedings of the Security 2nd international conference on Advances in information and computer security (IWSEC'07), Atsuko Miyaji, Hiroaki Kikuchi, and Kai Rannenberg (Eds.). Springer-Verlag, Berlin, Heidelberg, 74-90.

[9]. Rosario Gennaro, Craig Gentry, and Bryan Parno. 2010. Non-interactive verifiable computing: outsourcing computation to untrusted workers. In Proceedings of the 30th annual conference on Advances in cryptology (CRYPTO'10), Tal Rabin (Ed.). Springer-Verlag, Berlin, Heidelberg, 465-482