Secure Data Sharing in Cloud Computing based on Advanced SDBAES with Key Management Technique

A.Banushri[1*], Dr.R.A.Karthika[2]
Department of Computer Science & Engineering,
Vels Institute of Science,Technology and Advanced Studies(VISTAS), Chennai.
[*]banushrics.scs@velsuniv.ac.in

Abstract

Cloud systems can be used to enable data sharing capabilities and this can provide several benefits to the users and organizations, when the data is shared in cloud. Many organizations uses cloud storage to store its critical information rapidly due to its attractive features of cloud computing. Data security is one of the main challenge in cloud computing. Data storage in cloud computing is very difficult now-a-days because internet usage used by the cloud based services have less control in the data. The previous system trust the third-party auditor, who was not doing any illegal actions. But some cases they may involve illegal actions. To overcome such difficulty, the proposed system uses the data sharing which allows the Key Generation Center (KGC) to generate partial private key. The proposed work uses the public and private key for encryption which is formed by the KGC, but the key is accomplished by third party auditor. The whole private key could be gained by the mixture of partial private key and user generated random numbers. The proposed method uses the algorithm, Secure Dynamic Bits Advance Encryption Standard (SDBAES) to design public key cryptography system with key management to offer an authentication against the malicious third-party through public integrity verification scheme. And, also this system overcomes the defense from SQL injection attack, birthday attack and collusion attack in data security cryptography.

KEYWORDS - Public and private key cryptography, SDBAES, Brute Force attack, birthday attack, Collusion attack, SQL injection attack, KGC.

1. INTRODUCTION

In the applications of cloud computing, data are sustained with the usage of central remote server and internet and allow consumers to use the applications without installation and also with the support of internet, the cloud computing permits customers to access their delicate files which are warehoused in some other computer. Today the computing world has attracted lots of organizations as well as individuals to store data on clouds for easily sharing data and thus to reduce the cost of sharing. It is well known that a coin will always have two sides. Even though the advantages of cloud data sharing are a boon, the security of the private data is a serious issue in case of really sensitive data. The private data should be made available only to the users who are authorized to use it. Pervasive data gathering from multiple devices, such as smart phones, personal well-being devices and smart power meters, further intensifies the problem of data security and privacy [1]. The use of cloud as a platform for retrieving, storing, and processing data announces another party in the complex data ecosystem. Malicious actors may compromise cloud systems and cloud applications in order to gain access to private data as well as remove or alter the data, so to destabilize the trust of users toward the data. Research has been very dynamic in planning techniques for data protection over the past 20 years. As a result, many such techniques have been developed ranging from encryption techniques supporting privacy-preserving searches over encrypted data and access control systems supporting the specification and enforcement of access control policies for data sharing, to techniques for trustworthiness assessment of data and integrity techniques for complex data [2] .Key management contracts with the protected generation, dispersal, and storage of keys. It plays a vital role in computer security today as practical attacks on public-key systems are typically aimed at key management as opposed to the cryptographic algorithms themselves [3]. There are different clouds computing services which are follows: 1. Infrastructure as a Service (IAAS) ex: Amazon AWS EC2 2. Platform as a Service (PAAS) ex: Google app 3. Software as a Service (SAAS) ex: flicker 4. Database as a Service (DAAS).

2. LITERATURE REVIEW

Cloud security is one of the dynamic research zone and extensive research work has been carried out in recent years. A number of effective techniques have been proposed by various authors to provide security to cloud data and information. Different cryptographic techniques were used for data sharing security [1]. One trivial solution to achieving secure data sharing in the cloud is for the data owner to encrypt his data before storing into the Cloud, and

hence the data remain information-theoretically secure against the Cloud provider and other malicious users. A collaborative key management protocol to enhance both security and efficiency of key management in cipher text policy attribute-based encryption for cloud data sharing system performs better in cloud data sharing system which serves massive performance-restrained front-end devices with respect to either security or efficiency [2]. Distributed key generation, issue and storage of private keys are realized without adding any extra physical infrastructure and introduced an attribute groups to build a private key update algorithm for fine-grained and immediate attribute revocation. More ever, the storage overhead, the computation and communication cost must be reduced. This scheme is efficient and effective data sharing in cloud application. There are different attacks on data in cloud. This attacks may be initiated by both insiders and outsiders [4]. Outsiders' attacks may be protected by authentication mechanism, but insiders' attacks are very difficult to identify and also very tough to protect. Confidentiality is compromised due to the insiders' attacks on the data stored in the cloud. It is most important to ensure the confidentiality of data in the cloud and also need to develop new technique or mechanism to address the insiders' attacks in the cloud. Based on the relationship deployment in the cloud are differentiated in to public, private and hybrid. The public cloud services are provided by utilizing computing to the public, where in the private cloud it refers to the data centers which is not available to the public.

According to, the authorized users can decrypt cipher text and perform write operation to collaborate with each other by using a data collaboration scheme. The access and write permissions of user can be guaranteed based on CP-ABE (cipher text Policy-Attribute based encryption) and ABS (Attribute based system) respectively. These methods are efficient and suitable for resource constrained devices [5]. Another method called an attribute-based secure data sharing scheme with efficient revocation encrypts data using symmetric encryption method and then decrypts based on CP-ABE, which not only guarantees the data security, but also achieves fine-grained access control [6]. This scheme also achieves immediate attribute revocation which guarantees forward and backward security, and incurs less computation cost on users. In, Attribute Based Proxy Re-Encryption Scheme with Keyword Search (ABPRE-KS) supports flexible and secure data access control among users and it is very suitable for providing big data secure sharing in cloud environments [7]. A recent research on single clouds and multi-clouds using secret sharing algorithm used to address the security risks and solutions using Shamir's Secret Sharing algorithm. These algorithms generate their own secret sharing schemes and use secure channels to distribute shares among themselves. So, the migration to multi clouds due to its ability to decrease security risks that affect the cloud computing users.

Shamir's secret reconstruction scheme can obtain the secret when there are more than't' participants in Shamir's secret reconstruction. So, a secure secret reconstruction scheme is obtained and used it to design a secure multi-secret sharing scheme with unconditional security [9]. These schemes are simple modification of Shamir's (t, n) secret sharing scheme. Most of the research done in this field has focused on providing efficient data access control mechanisms between data owners and data users and cloud storage. The data owners encrypts the data and access control policies locally and upload the data to the cloud and provide secret keys to users it want to share with and authorization to cloud the task of handling the access control without have entrance to any keys. Most of the research done in this field has focused on the following technique that is using cryptographic primitives from different encryptions techniques for the purpose of data confidentiality. The most famous technique for providing data storage security is utilizing the homomorphic token with distributed verification of erasure-coded data and Verifying correctness of data storage by using data integrity techniques as in [12]. Conversely, this model of access control is not possible in cloud-based file sharing service where there is no direct interaction between the data owners and the data users. This means that most of the research has focused on data security in terms of access control in cloud storage models where the data owners can directly interact with data users. On the other hand, small amount of research is done about ensuring the data security cloud-based file sharing service where there is no direct interaction between data owners and data handlers.

3. RESEARCH METHODOLOGY

In the present system uses the public and private key for encryption which is formed by the KGC, but the key is managed by third party auditor. The previous system trust the third-party auditor was not doing any illegal actions. But some cases they may involve illegal actions. To overcome such difficulty the proposed system uses the data sharing which allows the KGC to generate partial private key. The complete private key could be gained by the mixture of partial private key and user generated random numbers.

3.1 Proposed SDBAES algorithm

The proposed system uses the algorithm, Secure Dynamic Bits Advance Encryption Standard (SDBAES) are as follows:

- AES having 3 bits level encryption & decryption such as 128bits, 192bits and 256bits.
- File owner upload a file to cloud in background secure architecture will pick one level of bit level (128 or 192 or 256) then converted into byte.
- Based on byte value Random generator will generate public key of AES input Key. Then using public key to encrypt the file and upload to cloud.
- Same as generate secret key of uploaded file then synchronize secret key to every user`s uniquely. Secret key could valid only for those responsive user`s.
- File=>Pub Key=>Encrypt=>Private Key=>Pub Key=>Decrypt=>File

Using this algorithm the key size could be randomly chosen, so the size of the key is not able predicted by the attacker, the random guess on this method is impossible because the attacker needed to choose an key size and to do all the random guess is to be contingent on the key size. The key size is 128, 192 and 256 bits so brute force attack of this approach in cloud environment is impossible.

3.2 Security attacks in cryptography

3.2.1 SQL (Structured Query Language) injection attacks

SQL injection is an attack in which the SQL code is inserted or appended into application/user input parameters that are later passed to a back-end SQL server for parsing and execution. Any procedure that constructs SQL statements could potentially be vulnerable, as the diverse nature of SQL and the methods available for constructing it provide a wealth of coding options. The primary form of SQL injection consists of direct insertion of code into parameters that are concatenated with SQL commands and executed. A less direct attack injects malicious code into strings that are destined for storage in a table or as metadata.

In this proposed work, the SQL injection attack lets the attacker to generate changes in the database by SQL statement. But the planned algorithm uses the approach of data blocking which does not let any source to changes its data. SQL Injection attack is also a harmful attack in the data security, it cause the direct change in the database. This attack has causes a great problem in web application's data layer. This could be overcome by the proposed system's novel algorithm [10].

3.2.2 Collusion attack

In cryptography, a crash assault on a cryptographic hash tries to discover two information sources delivering similar hash esteem, i.e. a hash impact. As opposed to a pre-image assault, the hash esteem is not indicated. There are approximately two sorts of impact assaults.

- Crash assault: Discover two distinct messages m1 and m2 with the end goal that hash (m1) = hash (m2).
- Picked prefix crash assault: Given two diverse prefixes p1, p2 discover two extremities m1 and m2 to such an extent that hash (p1 ‖ m1) = hash (p2 ‖ m2) (where ‖ is the connection operation).

The key scope of this data is randomly chosen so injecting the misbehaving packet inside the data is not done by using this approach. So, the proposed approach could overcome the issue of collusion attack. Collusion attack is injected some fake details to the network data and cause harm to the data. Attacker choses the weak link for injecting the fake data to the network. This kind of issue is overcome by this approach.

The integrity verification of the stored data is an essential thing; the present system uses Third Party Auditor (TPA) to manage the user certificates, which is not safe. So to reduce this problem, the planned approach allow the TPA to check the truthfulness of the data without managing user's certificate [11].

3.2.3 Birthday attack

Birthday attacks is another important attack in the cryptography which could abuse the communication between the more numbers of parties, this attack is same as the random attack. But it uses the mathematical calculations for the attack. This attack is also talented to overcome by this proposed system.

The birthday attack can be utilized to find collisions with an optimal complexity of $2^{n/2}$ for any function f with output size n. In more detail, choosing N randomly distributed, distinct inputs to the function f, the possibility that two outputs are equal and collide can be approximated by,

$$P(N) \approx 1 - e^{-\frac{N^2}{2^{n+1}}} \quad (1)$$

But the proposed SDBAES uses the 128, 192, 256 bit key size which makes the less possibility of attacks.

The key based cryptography cause the issue of illegal action of third-party authority. This will results a serious issue. Because, the key which is needed to decode the data is maintained and shaped by the third-party authority. The illegal access of data by authority may cause the serious issue. This will be overcome by cryptography. In cryptography, monitoring the third-party auditor is a significant thing to verify the integrity of the outsourced data [8]. Because partial private key is formed by the KGC (Key Generation Center). The illegal actions may result the affected data.

3.2.4 Brute force attack

Brute force attack is a significant data security problem. The attackers could make a random guess of the data security parameters and breaks those security parameters. This could be lead to the serious issue, in this proposed system can overcome this security issue by novel algorithm, the Elgammal uses the asymmetric encryption technique [12]. It uses the receiver public key for encryption and receiver private key for decryption. The public and private key produced by KGC (Key Generation Center). This may lead to the chance of data leak, because the third-part auditor could hold the private key of the user for verification purpose [8]. In some case, the illegal activity of third party authority leads to the huge issue. To overcome those problems, this method uses certificate-less cryptography based on Elgammal. The major issue of the data security attacks could be avoided by the SDBAES algorithm was discussed in the above section. The proposed framework is shown in Figure 1.

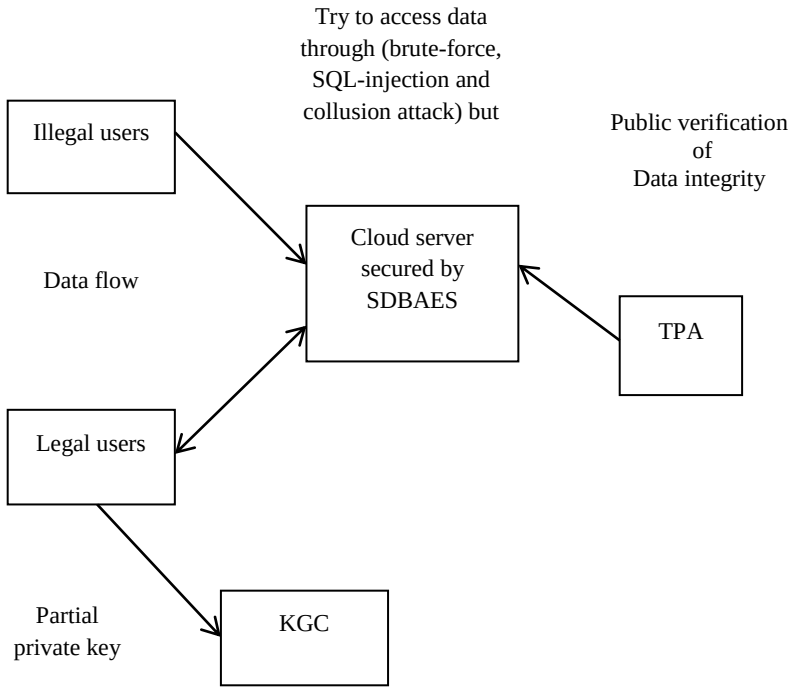

Figure 1.Proposed framework

The above figure depicts the proposed system, where the TPA (Third Party Authority) not have rights to manage the user certificate, instead that it verifies the honesty of the data which is kept in cloud server. The cloud server is secured by the SDBAES algorithm so illegal users can't able to get the details from the server. Only legal user can get the data through server using partial private key made by KGC and the random generated numbers.

4. RESULTS AND DISCUSSION

4.1 SQL injection attacks (SQLIA)

SQL scan's narrow-focused approach to vulnerability scanning differs from that of most commercial products, making it difficult to find an exact match, with which to compare scan results in table 1.

No. of SQL	Total no. of	Average no.	No. of	No. of	Total time	Average time per

statement	tokens	of tokens per second	valid query	SQLIA	required (Millisecond)	query (nanosecond)
1500	14678	15	982	130	500	620

Table 1. Performance analysis

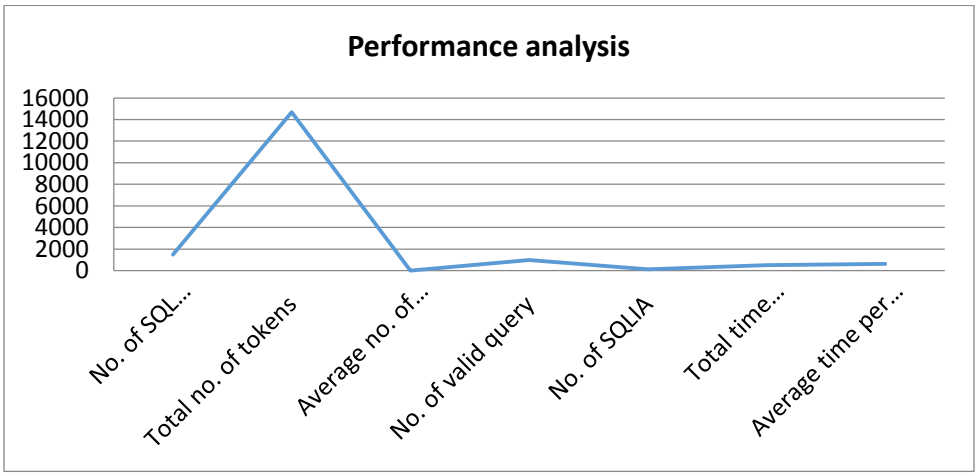

Figure 2. Performance analysis of SQL injection attacks

4.2 Collusion attacks

Experimental results show that the method can generate much better protection than traditional methods. This method reduces the computational complexity compared to the Elliptic Encryption Method. The method also reduces the manual work and performs automatic computations without much involvement of the users.

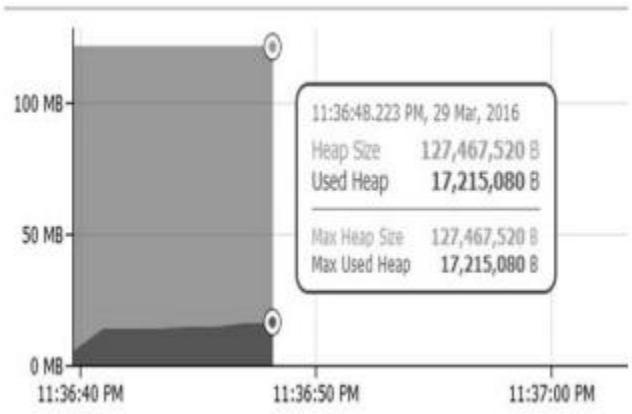

Figure 3. Memory usage

The heap is memory fixed separately for dynamic allocation. Unlike the stack, there is no prescribed pattern to the allocation and deallocation of blocks from the heap. One can allocate a block at any time also cannot free it at any time. The memory heap graph shows a flat usage of memory which means that there are very few short lived objects in the memory, Very less garbage collection happening and there are no memory leaks in the program.

4.3 Birthday attacks

Birthday attacks are a class of brute-force techniques used in an attempt to solve a class of cryptographic hash function problems. These methods take advantage of functions which, when supplied with a random input, return one of k equally likely values. Given user prepared to sign a valid message x

- opponent generates $2^{m/2}$ variations x' of x, all with essentially the same meaning, and saves them
- opponent generates $2^{m/2}$ variations y' of a desired fraudulent message y
- two sets of messages are compared to find pair with same hash (probability > 0.5 by birthday paradox) have user sign the valid message, then substitute the forgery which will have a valid signature

$$\prod_{k=1}^{m}[1-K/N] \approx e^{-(\sum_{k=1}^{m}k)/N} \approx e^{-m^2/2N} \approx \frac{1}{2} \qquad (2)$$

If $m \approx 1.2\sqrt{N}$ .....So ,if $m \approx \sqrt{N}$, probability of a clash is about $\frac{1}{2}$

k	0	10	20	30	40	50	60
P(365,k)	0	0.11	0.45	0.75	0.85	0.95	1.15

Table 2. Performance analysis of birthday attacks

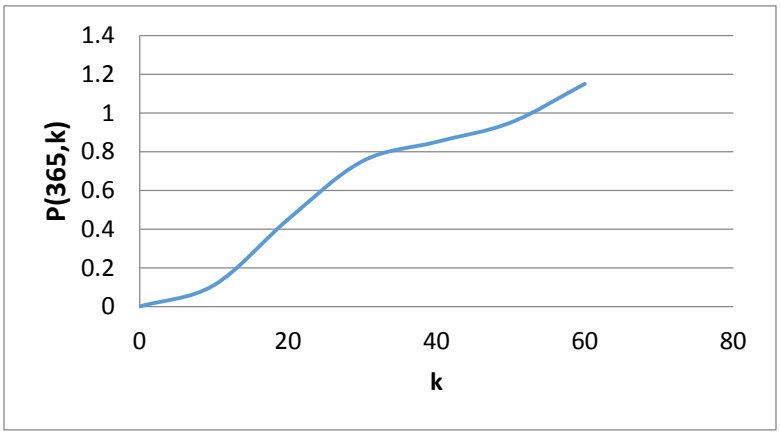

Figure 4. Birthday attacks

5. CONCLUSION

Data Security along with key management is the toughest part to manage in cryptosystems. In the cloud platform, there is always a chance of insider or outsider attack. Keys can be retrieved or stolen by attackers without the awareness of end users. Security for data and keys which is stored in cloud systems was discussed and implemented

here. It gives better data security and key management in cloud systems. The proposed technique also provides better security against brute force attacks, SQL injection attacks and data modification attacks.

REFERENCES

1. Patil Madhubala R, "Survey on Security concerns in Cloud Computing", IEEE, 2015
2. Aditi Tripathi,Mayank Deep Khare,Predeep Kumar Singh,"A review of Scalable Data Sharing Techniques for Secure Cloud Storage", IEEE, 2015
3. R.Swathi,T.Subha, "Enhancing Data Sharing Security in Cloud using Certificateless Public Auditing",IEEE 2017
4. Shenoy H.Nagesh,K.R.AnilKumar,K.T.Rajgopal, "Cloud Architecture Encountering Data Security and Privacy Concerns-A Review",IEEE 2017
5. Mayur N.Ghuge,Prashant N Chatur, "Collaborative key Management in Ciphertext Policy Attribute Based Encryption for Cloud",IEEE,2018
6. YoShiko yasumura,Hiroli Imabayashi,Hayato Yamana,"Attribute-based Proxy re-encryption method for Revocation in Cloud Data Storage",IEEE,2017
7. Hanshu Hong,Zhixin Sun, "Towards Secure data Sharing in Cloud computing using Attribute based Proxy Re-encryption with Keyword Search",IEEE,2017
8. Nida,Bhupendra Kumar Teli, "An Efficient and Secure means for Identity and Trust Management in Cloud",IEEE,2015
9. Sumedh.N.Pundkar,Narendra Shekokar, "Cloud Computing Security in multi-Clouds using Shamir's Secret Sharing Scheme",IEEE,2016
10. Kuisheng Wang,Yan Hou, "Detection Method of SQL Injection Attack in Cloud Computing Environment,IEEE,IMCEC,2016
11. Zhongma Zhu,Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud,IEEE,2016
12. Khalid El Makkaoui,Abderrahim Bemi-Hssane,Abdellah Ezzati, "Cloud-ElGamal:An efficient homomorphic encryption Scheme",IEEE,2016