An Efficient Application of Mobile Cloud Using Key Policy Based AES Encryption

Devendra Khare[1], Prof. Harsh Mathur[2]

[1]*M. Tech. Scholar* , [2]*Associate Professor*

Department of Computer Science and Engineering, IES College of Technology, Bhopal

Abstract - Cloud computing is an important technique that enables various uses to send information or shared information over internet. But during the sharing of data or transmission of data security plays a vital role such that the shared information can be prevented from attacks. Since mobile applications implemented today also uses the facility of cloud. The existing technique implemented for the security of these over mobile application using Attribute based encryption is efficient and prevents from various attacks in the mobile application. But the technique implemented so far for the mobile applications suffers from the problem of Escrow and user revocations. Hence an efficient technique is implemented for the removal of these problems using cipher text policy identity based encryption.

Keywords- encryption, decryption, cipher, cloud computing.

I. INTRODUCTION

Protecting networks from computer security attacks is a vital apprehension of computer security. Since the large amount of text is usually uploaded into many sites and thus it need to be secured especially when sensitive information is uploaded. Protecting networks from computer security attacks is a vital apprehension of computer security.

Currently network and computing are more developed technologies. These enable many users to easily share and update their sensitive information with others via online storage. Peoples are usually sharing their life events with friends and family by uploading photographs and other sensitive information in to social networking sites like Facebook, Orkut, twitter etc. As people enjoy the advantages of these new technologies & services, their main concerns about data security and efficient access control also take place. Inappropriate access of the data by the storage server or unauthorized access by outside users could be potential threats to their data [1].Since the data is private and needs to be made secure from un-authorized users in the network. Also the data security is made possible by providing various access policies in the network based n the attributes or identity of the users [2].

It is essential to protected data that is uploaded in to various social sites or stored online. Attribute-based encryption (ABE) is a promising cryptographic method that achieves a fine-grained data access control [3], [4], [5], [6]. It gives a way of defining access policies based on various attributes of the requested user, scenario, or the data object. Particularly, cipher content approach property based encryption (CP-ABE) empowers an encryptor (who scramble information) to characterize the characteristic set over a universe of properties that a decryptor (that decode data) requires to have with a specific end goal to unscramble the ciphertext, and implement it on the substance [3]. In this way, every client with an alternate arrangement of credits is allowed to decode diverse bits of information per the security strategy.

A. Data Sharing

Today's computing technologies have attracted more and more people to store their private data on third-party servers either for ease of sharing or for cost saving. When people enjoy the advantages these new technologies and services bring about, their concerns about data security also arise. Every people want that their data may be secure by the unauthorized user. In this figure we are performing data sharing. We are using three level of sharing key generation center, data owner and user. In data storing center all the data keep store in encrypted form. Whenever user want to access this data then he or she gets a key by the KGC and with the help of this key user gets this data but the user is registered user otherwise he or she will not having this key. So by this we perform data sharing in small level. Figure 1.1 demonstrates the architecture of data sharing.

B. Secret Sharing

Whenever we performing information sharing we need to keep up the information arrangements and time to time overhaul these strategies. One arrangement of this issue is utilizing a strategy which is great in performing encryption that is Cipher text approach attribute-based encryption (CP-ABE). This strategy gives that each client needed to characterize their own particular approach and uphold that arrangement on the information dispersion.

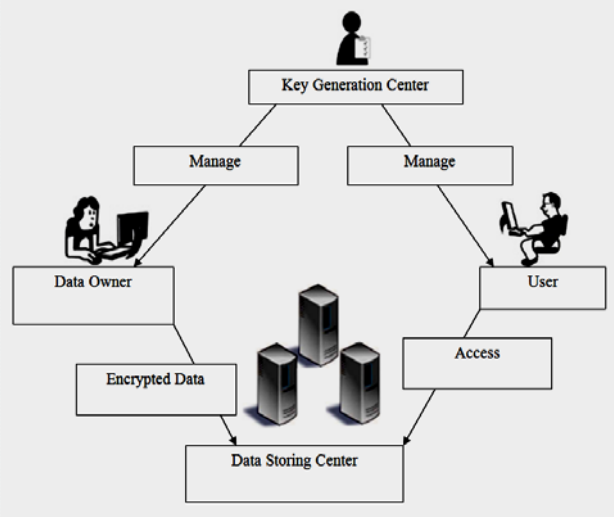

Figure 1.1: Architecture of a data sharing system.

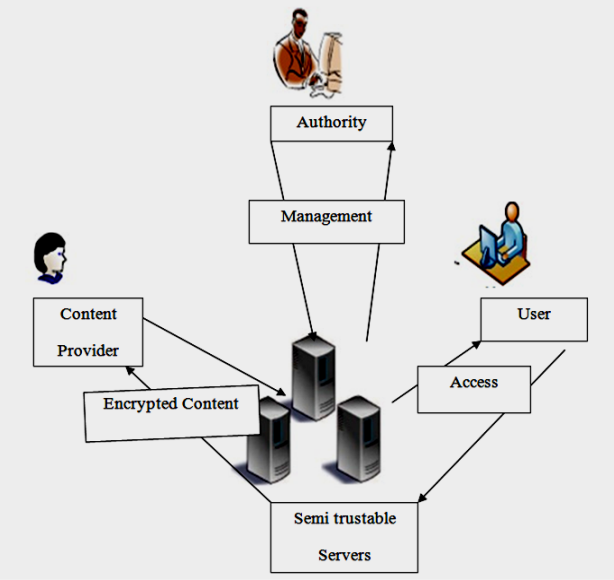

Figure 1.2: An Example of Application Scenario of secret data sharing.

In view of the BRS and SRS, an attainability study ought to be performed to choose the instruments to actualize the information mix framework. Little organizations and ventures which are beginning with information warehousing are confronted with settling on a choice about the arrangement of devices they should actualize the arrangement. The bigger venture or the undertakings which as of now have begun different activities of information mix are in a simpler position as they as of now have involvement and can expand the current framework and endeavor the current learning to actualize the framework all the more viably.

II. GROUP KEY ESTABLISHMENT

In order to benefit of secure group-oriented applications, multiple users need to share a private key, which is obtained as the output of a Group Key Establishment (GKE) protocol. The main goal of GKE is to establish a common key between the authorized members of a group, without disclosing it to other parties. The authorized participants to the protocol are also addressed as qualified, legitimate or privileged. A protocol runs for multiple times, named sessions. Each session is uniquely identified by a session id, which can be computed during the execution of the protocol or given in advance by the environment. We call session key the shared secret derived after one execution of the protocol. It only persists for a short period of time, a natural approach in cryptography (the probability to reveal key increases with its period of usage). To become eligible to take part to protocol sessions, users must first register within the group. After registration, they acquire a long-lived or long-term secret, which they will later use to derive the session keys they are qualified for.

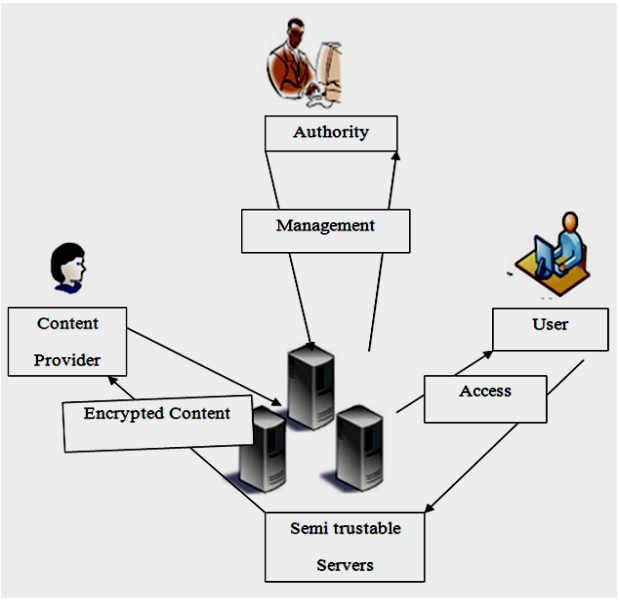

Figure: 2.1 Application Scenarios of Data Sharing.

A. Classification

GKE protocols divide into two classes: Group Key Transfer (GKT) and Group Key Agreement (GKA). The main difference between the two classes derives directly from their definitions: GKT requires the existence of a privileged party to select and distribute the key, while GKA does not, the key being computed as the result of the collaboration of legitimate participants via exchanged messages. Unlike GKA, in which the key is derived only by the cooperation of internal group members, GKT permits the entity that generates the key to be an outsider as well (i.e. not a group member). This entity has various names in the literature, such as: Trusted Third Party (TTP), Key Generation Center (KGC), Key Distribution Center (KDC) or Group Controller [11]. The naming differs according to the precise function it fulfills. For example, it

may exist an entity that generates the key (KGC) and an entity (distinct or not) that distributes it to the authorized members (KDC). For the rest of this work we will mainly refer to the KGC as a single party that performs both key generation and distribution.

III. PROPOSED METHODOLOGY

The proposed methodology consists of the following stages:

- If any user wants to send data to the other user in mobile clouds.
- The user must choose a valid attribute and generate a public and private key pair.
- The user then encrypts his data using AES-256 encryption and send to the central repository.
- Here in the storage panel at central repository the data storage is in the form of attribute and their respective encrypted data.
- The receiver when needs to access the data through central authority needs to be authenticated on the storage panel.
- As soon as the receiver authenticates it will send the attribute and hence on the basis of which the respective encrypted data is fetch from the CA.
- The receiver then decrypts the data using AES-256.

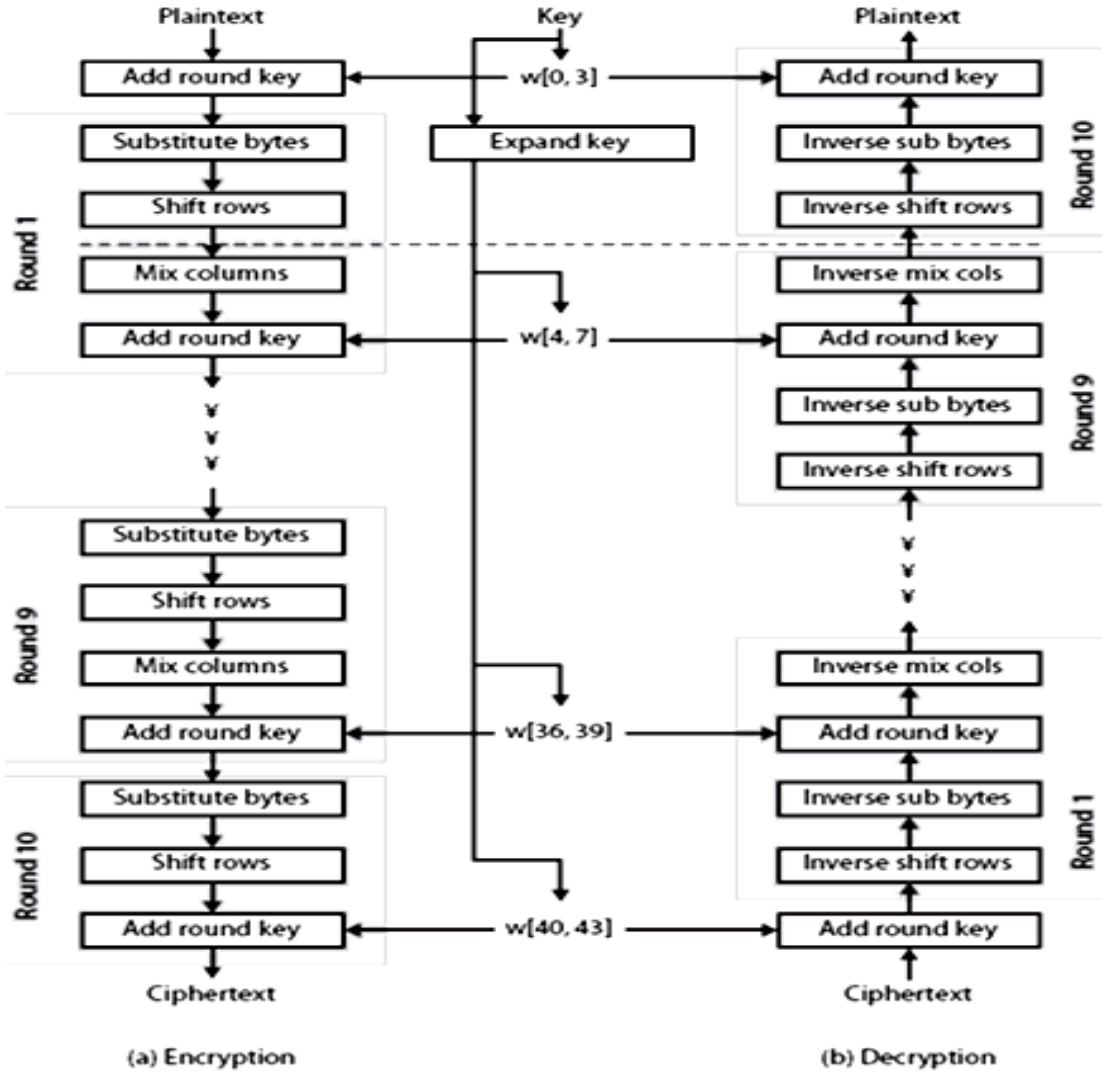

Figure 3.1 Proposed systems.

A. Proposed Encryption Algorithm

In the proposed work the propelled encryption standard (AES 256) scheme algorithm is utilized All of the cryptographic calculations have some issue. The prior ciphers can be broken easily on current algorithm frameworks. The DES calculation was softened up 1998 utilizing a framework that cost about $250,000. It was likewise unreasonably moderate in software as it was created for mid-1970's equipment and does not deliver effective software code. Triple DES then again, has three circumstances the same number of rounds as DES and is correspondingly slower. And also this, the 64 bit square size of triple DES and DES is not extremely effective and is faulty with regards to security.

B. The AES Cipher

Like DES, AES is a symmetric piece cipher. This implies it utilizes a similar key for both encryption and decryption. Nonetheless, AES is very not the same as DES in various ways. The square and key can in actuality be picked autonomously from 128,160,192, 224, 256 bits and need not be the same. Be that as it may, the AES standard expresses that the algorithm can just acknowledge a square size of 128 bits and a decision of three keys - 128,192, 256 bits. Contingent upon which adaptation is utilized, the name of the standard is changed to AES-128, AES-192 or AES-256 separately. And additionally these distinctions AES varies from DES in that it is not a feistel structure. Review that in a feistel structure, half of the information square is utilized to adjust the other portion of the information piece and afterward the parts are swapped. For this situation the whole information piece is handled in parallel amid each round utilizing substitutions and changes.

A number of AES parameters rely on upon the key length. For instance, if the key size utilized is 128 then the quantity of rounds is 10 while it is 12 and 14 for 192 and 256 bits separately. At present the most widely recognized key size liable to be utilized is the 128 piece key. This depiction of the AES algorithm in this manner portrays this specific execution.

Figure 3.1 demonstrate the architecture of the proposed system. proposed system have two stages left hand encryption and right hand side decryption of plane text.

IV. RESULTS AND DISCUSSION

The simulation of the proposed cloud project is done on the Netbeans using JAVA and the cloud application is tested for various parameters as it is done in the previous work. The following symbols are used: μ is the sample mean, σ is the sample standard deviation, and LB and UB are the lower and upper bounds, respectively, of the 95% confidence interval, for each set of runs using each of the baseline and proposed algorithms. 100 runs were executed using each technique, and all operations were performed using a single-attribute policy. The data holder performed a union operation on encryption in all cases, with no help, which accounts for its slower action.

The tasks include the main operations related to cryptography runs on all platforms like mobile and desktop. The tasks are explained as follows:

Owner Setup:

Owner setup is the task when system needs to initialize the admin account for performing operations on data. The initialization covers all the necessary steps like set parameters for controllers which handles re-encryption operation and simultaneously communicates with the manager known as trusted authority and he also provides the private group keys. The controller simultaneously communicates with user directly and also through manager.

Manager Setup:

Manager setup task includes the key initialization operation from already available private group key store and coordinate with the user to complete the re-encryption task.

Keygen:

This task is the generation of random keys to re-encrypt data received from the user and store into the Data Store. The keygen operation has facility to generate random keys not repeated at all, and this can be possible due to functioning behind random variable which is based on the date and time to maintain uniqueness regardless whatever and how many keys are generated.

Owner Encryption:

This operation involved the encryption process on the data created by the data owner and the after encryption of the data it will be stored in the data store.

Cloud Encryption:

This process performs the on the cloud the encrypt data as well as encryption key itself.

Decryption:

This process is reverse operation of encrypted data to be visible to the user, which involves first to decrypt the encryption key and then using this key decrypt the data being accessed.

Re-encryption Setup:

Initializing the keys for re-encryption of key to encrypt data provided by data owner.

Re-encryption:

The keys are being re-encrypted after encryption of data for enhancing the security of cloud storage.

Table 1: Benchmark Results of Different Tasks and Their Respective Timing Comparison with Existing Work

Algorithm	**Task**	**Timing in ms**

		μ	LB	UB
Existing Work	Owner Setup	37.6	0	89.8
	Manager Setup	18.8	16.4	21.2
	Keygen	70	63	77
	Owner Encryption	60.8	56.3	65.2
	Cloud Encryption	18.6	16.6	20.5
	Decryption	42.8	38.6	47
	Reencryption Setup	21.6	19.7	23.5
	Reencryption	7.5	6.2	8.8
Proposed Work	Owner Setup	27.3	0	72.5
	Manager Setup	14.5	12.5	15.8
	Keygen	62	56	65
	Owner Encryption	48.4	48.3	52.3
	Cloud Encryption	16.3	12.8	15.8
	Decryption	36.1	27.4	38
	Reencryption Setup	16.8	14.5	19.2
	Reencryption	3.5	3.1	4.3

Table 2: Different Tasks and Their Timing Comparison with Existing Work

	Communication Cost in bits	
Time in hours	**Existing Work**	**Proposed Work**
10	900	400
20	1100	638
30	1285	817
40	1486	938
50	1649	1228
60	1729	1421
70	2438	1726
80	2747	1820
90	3064	1917
100	3422	2137

The entire task and their respective comparison has been explained previously and the other comparison of costs in terms of bits are shown in the Table 2. This comparison shows the time in hours with respective cost in bits for existing and proposed work. The communication cost is shown in bits and it represents the resource constraint utilization and this should be minimized. The graphical comparison of the communication cost is shown in the figure 4.1.

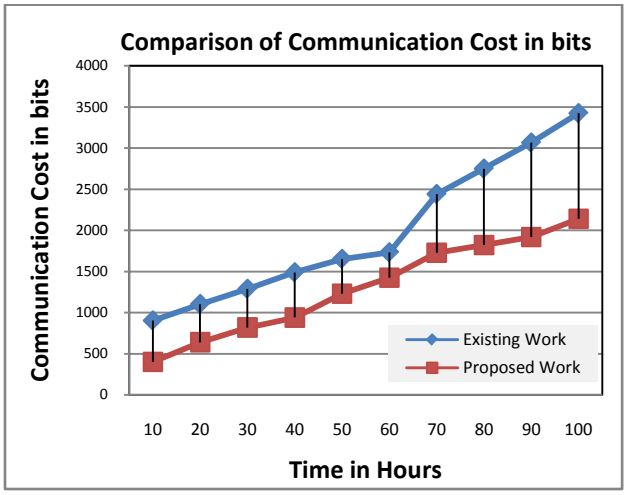

Figure: 4.1 Communication cost of proposed and existing work

V. CONCLUSION

Today's computing technologies have attracted more and more people to store their private data on third-party servers either for ease of sharing or for cost saving. Data confidentiality on the shared data against outside users who have not enough attributes can be trivially guaranteed. There is a trend for sensitive user data to be stored by third parties on the Internet. The proposed methodology implemented here for the secure mobile communication over cloud provides not only provides security from various attacks but also provides an additional authentication. The methodology also reduces the computational cost as well as communication overhead and time.

REFERENCES

[1] Piotr K. Tysowski and M. Anwarul Hasan," Hybrid Attribute- and Re-Encryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds", IEEE 2013.

[2] Yu, Jiadi, Peng Lu, Yanmin Zhu, Guangtao Xue, and Minglu Li. "Towards Secure Multi-Keyword Top-k Retrieval over Encrypted Cloud Data," IEEE transactions on dependable and secure computing, vol. 10, no. 4, pp. 239- 250, July/August 2013.

[3] Pankaj Arora, Rubal Chaudhry Wadhawan and Er. Satinder Pal Ahuja "Cloud Computing Security Issues in Infrastructure as a Service", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, vol. 2, issue 1, Jan. 2012.

[4] Song, Dawn, Elaine Shi, Ian Fischer, and Umesh Shankar. "Cloud data protection for the masses", In IEEE Computer, vol. 45, no. 1, pp. 39-45, 2012.
[5] Priya, P. Shanmuga, and R. Sugumar. "Multi Keyword Searching Techniques over Encrypted Cloud Data", International Journal of Science and Research (IJSR), ISSN: 2319-7064, vol. 3, issue 3, pp. 410 -412, March 2014.
[6] Hur, Junbeom. "Improving security and efficiency in attribute-based data sharing", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October 2013.
[7] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing", IJARCCE November 2013.
[8] Sanjam Garg Craig Gentry Shai Halevi Amit Sahai Brent Waters," Attribute-Based Encryption for Circuits from Multilinear Maps", 2012.
[9] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Attribute based data sharing with attribute revocation." In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270. ACM, 2010.
[10] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt '05), pp. 457-473, 2005.
[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,"Proceedings of ACM Conference on Computer and Communication Security, pp. 89-98, 2006.
[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-PolicyAttribute Based Encryption," Proceedings IEEE Symposium Security andPrivacy, pp. 321-334, 2007.
[13] A.Abdul-Rahman, S Hailes, "Supporting trust in virtual communities," in Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Jan.2000.
[14] H.Sato, A.Kanai, S.Tanimoto, "A Cloud Trust Model in a Security Aware Cloud", 2010 10th IEEE/IPSJ International Symposium on Applications and the Internet, Seoul July.2010, IEEE P.121, ISBN 978-1-4244-7526-1.
[15] J.H.Yao, S.P.Chen, W.Chen, D.Levy, J.Zic, "Accountability as a Service for the Cloud", 2010 IEEE International Conference on Services Computing (SCC), Miami July.2010, IEEE P.81, ISBN 978-1-4244-8147-7.