5. System Architecture

Cloud computing, is an emerging computing paradigm, enabling users to remotely store their data in a server and provide services on-demand. In cloud computing cloud users and cloud service providers are almost certain to be from different trust domains. Data security and privacy are the critical issues for remote data storage. A secure user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage.

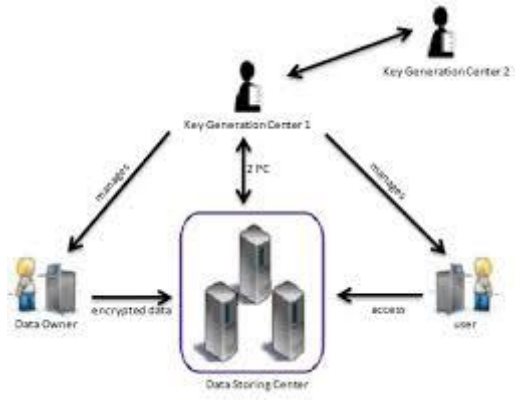

Figure 1: Architecture of Data Sharing

The architecture of data sharing system, which consist of the following entities [1].

1) Key generation center: It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. That is, it will honestly execute the assigned tasks in the system; however, it would like to learn information of encrypted contents as much as possible. Thus, it should be prevented from accessing the plaintext of the encrypted data even if it is honest.

2) Data-storing center: It is an entity that provides a data sharing service. It is in charge of controlling the accesses from outside users to the storing data and providing corresponding contents services. The data-storing center is another key authority that generates personalized user key with the KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control.

3) **Data owner:** It is a client who owns data, and wishes to upload it into the external data-storing center for ease of sharing or for cost saving. A data owner is responsible for defining (attribute-based) access policy, and enforcing it on its own data by encrypting the data under the policy before distributing it.

4)User: It is an entity who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the ciphertext and obtain the data.

6. Algorithm

1)Key Generation: When the KGC authenticates a user u_t, it selects a random exponent $r_t \in R$ for the user. This value is a personalized and unique secret to the user. Then, the KGC and the data storing center engage in a secure 2PC protocol, where the KGC's private input is (r_t, β), and the data-storing center's private input is α. The secure 2PC protocol returns a private output $X = (\alpha + r_t)\,\beta$ to the data-storing center.

2)Encryption: When a data owner wants to upload its data M to the data-storing center for sharing using RSA algorithm
Generate randomly two "large" primes p and q.
Compute $n = pq$ and $\phi = (p-1)(q-1)$.
Randomly public key is generated is
$K_E = (n, e)$.

3)Data Reencryption : Before distributing the ciphertext, the data-storing center reencrypts it by running ReEncrypt(CT, G) using a set of the membership information for each attribute group G that appears in the access tree of CT. The reencryption algorithm enforces user access control per each attribute group.

Given nodes $n_1,\ldots n_N$ each holding an data item d_i
$r_{i,1}+\ldots\ldots+r_{i,N} = d_i$
Now each node n_i simply broadcasts si to all other nodes so that each node can compute:
$T = s_1+\ldots..+s_N$

4)Decryption: Data decryption phase consists of the attribute group key decryption using one-way anonymous key agreement protocol, followed by the message decryption from CT'.

7. Result Analysis

The performance of the project is evaluated with the existing system and suitable graphs are constructed. Parameters like Encryption Time, Decryption time are compared. The results are indicating modified algorithm is performed better than the existing CP-ABE in terms of security and time of encryption and decryption.

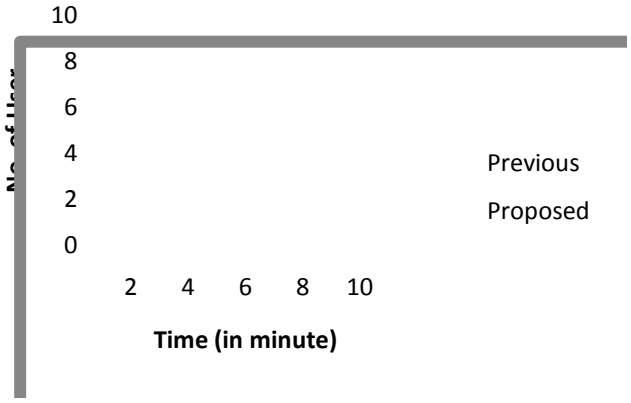

Figure 2: Comparison between previous and proposed system in terms of time and No. of user in data sharing

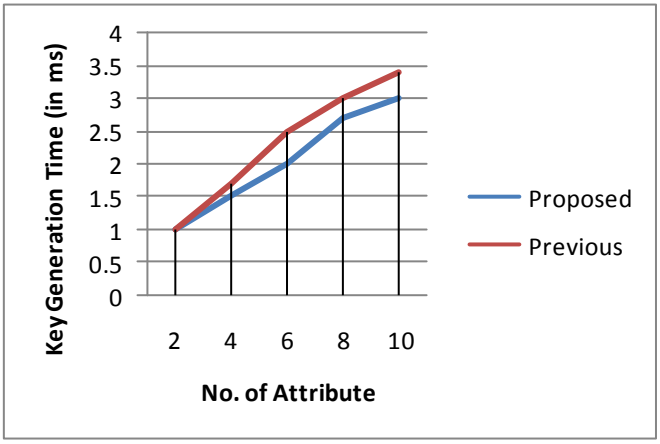

Figure 3: Comparison between previous and proposed system for key generation time with respective No. of attribute

8. Conclusion

Issues such as scalability in key management, flexible access and efficient user revocation, security have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. For improving the security and fine grained access control of stored data on un-trusted server the anonymous id generated for attribute based encryption is introduced. It achieved higher security than the existing system. This scheme also enables dynamic modification of access policies or file attributes. Finally it generates a performance evaluation graph it take less time for encryption compared to the existing attribute based encryption.

9. Future Work

Future work is Alert and Notification System. The system needs an alert and notification system to give both providers and users the ability to track their data. Alerts can help users to prevent any miss-use of their data. Also the alert system can be used to identify suspicious activities.

References

[1] Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing" IEEE Transactions On Knowledge And Data Engineering Vol:25 No:10 Year 2013
[2] M. Chase and S.S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," Proc. ACM Conf. Computer and Comm. Security, pp. 121-130, 2009.
[3] S.S.M. Chow, "Removing Escrow from Identity-Based Encryption," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography (PKC '09), pp. 256-276, 2009.
[4] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[5] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," Proc. ACM Conf. Computer and Comm. Security, pp. 195-203, 2007.
[6] A. Lewko, A. Sahai, and B. Waters, "Revocation Systems with Very Small Private Keys," Proc. IEEE Symp. Security and Privacy, pp. 273-285, 2010.
[7] N. Attrapadung and H. Imai, "Conjunctive Broadcast and Attribute-Based Encryption," Proc. Int'l Conf. Palo Alto on Pairing-Based Cryptography (Pairing), pp. 248-265, 2009.
[8] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.
[9] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably secure and efficient bounded ciphertext policy attribute based encryption," in Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security (ASIACCS '09), pp. 343–352, March 2009.
[10] L. Ibraimi, Q. Tang, P. Hartel, and W. Jonker, "Efficient and provable secure ciphertext-policy attribute-based encryption schemes," in Information Security Practice and Experience (ISPE 2009), pp. 1–12, Springer, Berlin, Germany, 2009.
[11] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.
[12] A. Lewko, T. Okamoto, A. Sahai, and B. Waters, "Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption," in Advances in Cryptology: EUROCRYPT 2010, vol. 6110 of Lecture Notes in Computer Science, pp. 62–91, Springer, Berlin, Germany, 2010.
[13] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 417-426, 2008.

Author Profile

Neeta S. Nipane, pursuing M.Tech 2nd year, Computer Science & Engineering in Nagpur Universty. Two years of experience as an Assistant Lecturer in an engineering college.