Data Protection Scheme For Cloud Computing Using Attribute And Policy Encryption

Dr. V.Venkatesa Kumar *M.E., Ph.D.,*
Assistant Professor
Computer Science and Engineering
Anna University, Regional Campus
Coimbatore.

V.Kavitha
PG scholar
Computer Science and Engineering
Anna University, Regional Campus
Coimbatore.

Dr.M.Newlin Rajkumar *M.E., Ph.D.,*
Assistant Professor
Computer Science and Engineering
Anna University, Regional Campus
Coimbatore, Tamilnadu.

Abstract--*Cloud computing is increasingly essential for the establishment of services and storage of data on the Internet. Cloud Computing is the next generation architecture of IT Enterprise. However, there are numerous significant challenges in securing cloud Infrastructures. Security is to save data from danger and susceptibility. Various security issues and some of their solutions are explicated and are focused mainly on the public cloud. Data should constantly be encrypted when stored and transmitted. This method is proposed such that the entire data is encrypted along with the cryptographic key. This encryption technique alone is not sufficient for protecting the data. In this paper, an attribute and policy data security protection mechanism is proposed for cloud storage system. The two level encryption is implemented.This process is completely transparent to the sender. Furthermore, the cloud server cannot decrypt any ciphertext at any time.*

Keywords: *key encryption, bilinear, security, GSWO Algorithm, cloud storage.*

I. INTRODUCTION

Cloud storage is an exemplary of the networked storage system where data is stored in pools of storage which are generally accommodated by third parties. There are much remuneration to use cloud storage. The most prominent are data accessibility. Data stored in the cloud can be retrieved at any time from any place as long as there is network access. Storage maintenance tasks, such responsibility of a service provider. Another advantage of cloud storage is data sharing between users. In spite of its recompenses, outsourcing data storage also increases the attack surface area at the same time. When data is circulated, the more locations it is stored the higher threat it contains for unauthorized access to the data. By provision storage and networks with many other users, it is also possible for other unconstitutional users to access your data. This may be due to erroneous actions, faulty equipment, or sometimes because of criminal absorbed. An auspicious solution to offset the risk is to deploy encryption technology. Encryption can protect data as it is being communicated to and from the cloud service. It can further defend data that is stored at the service provider. Even there is an unauthorized antagonist who has gained access to the cloud, as the data has been encrypted, the antagonist cannot get any information about the plaintext. Asymmetric encryption permits the encryptor to use only the public information to make a ciphertext while the receiver uses his/her own secret key to decrypt. This is the most expedient mode of encryption for data transition, due to the elimination of key management existed in symmetric encryption.

A. ENRICHED SECURITY PROTECTION

In a typical asymmetric encryption, there is a single secret key corresponding to a public key or an identity. The decryption of cipher text only necessitates this key. The key is generally stored inside either a personal computer or a trusted server and may be threatened by a password. The security protection is necessary if the computer/server is isolated from an opening network. Awkwardly, this is not what happens in the real life. When being connected with the world through the Internet, the computer/server may grieve from a potential risk that hackers may intrude into it to negotiation the secret key without letting the key owner know. It can be negotiated by some attackers who can access the victim's particular data stored in the cloud system. Therefore, there exists a need to enrich the security protection. In computer networking, cloud computing is computing that involves a huge number of computers linked through a communication network such as the Internet, similar to utility computing. Nowadays cloud computing has occurred as one of the most influential paradigms in the IT industry, and it has fascinated extensive attention from both academia and industry. Cloud computing holds the assurance of providing computing. A public verifier could be a data user (e.g., researcher) who would like to consume the owner's data via the cloud or a third-party auditor who can provide expert integrity checking services.

As cloud computing becomes more established and there will be new applications and storage services provided by the cloud, it is informal to anticipate that the security for data protection in the cloud.They will become more delicate and essential. Actually, we have noticed that the notion of attribute and policy-based encryption, which is one of the encryption trends for data protection, has been spread into some real-world applications. It is really necessary for the era of cloud computing.

II ESSENTIAL SECURITY ISSUES IN THE CLOUD

A. Integrity

Integrity makes sure that data held in a system is a proper depiction of the data envisioned and that it has not been modified by an authorized person. When any application is running on a server, the backup routine is organized so that it is safe in the event of a data-loss incident. Normally, the data will backup to any portable media on a consistent basis which will then be stored in an off-site location.

B. Availability

Availability confirms that data processing resources are not made unavailable by malevolent action. It is the humble idea that when a user tries to access something, it is available to be accessed. This is vigorous for mission critical systems.

C. Confidentiality

Confidentiality certifies that data is not disclosed to unauthorized persons. Confidentiality loss occurs when data can be observed or read by any personalities who are unauthorized to access it. Loss of confidentiality can arise physically or electronically. Physical confidential loss revenues place through social engineering. Electronic confidentiality loss earnings place when the clients and servers aren't encrypting their communications.

III. EXISTING SYSTEM

In cloud computing services, customers are worried about moving their sensitive data and applications from their own private computing environments to a cloud environment which is shared by different users and which is usually accessible via a public network. Data stored in the cloud can be retrieved at any time from any place as long as there is network access. By partaking storage and networks with many other users it is also possible for other unauthorized users to access the data. This may lead to felonious act. To solve the problem of leverage two different encryption technologies: one is IBE and the other is traditional Public Key Encryption (PKE).The resulting work ciphertext can be decrypted by a valid receiver with secret key and security device. A trivial combination of IBE and PKE cannot achieve the goal. To support revocability, employ re-encryption technology such that the part of cipher-text for an old security device can be updated for a new device if the old device is revoked. Meanwhile, need to generate a special key for the above cipher-text conversion. Also guarantee that the cloud server cannot achieve any knowledge of message by accessing the special key, the old ciphertext, and the updated ciphertext. Further use hash-signature method to "sign" ciphertext such that once a component of cipher-text is tempered by the adversary, the cloud and ciphertext receiver can tell.

A. LIMITATIONS IN THE EXISTING SYSTEM

The popularity and prevalent use of Cloud have brought great convenience for data sharing and Data storage.The data sharing with a huge number of participants take into account issues like data integrity, efficiency, and confidentiality of the owner for data. In cloud storage services one critical challenge is to manage the security of data storage in the cloud. To make data management more scalable in cloud computing field, we have to improve more security level.

It arises as user's sensitive data are susceptible to both attacks insider and outsider.

The main problem addressed in the previous methods includes:

- Basic encryption techniques are used.
- Key management and backup services not effective.
- Cipher-text based security may not provide the best solution to all time.
- Security issues are not efficient into account.
- High computation overload.
- Provides very low throughput

IV. PROPOSED SYSTEM

Generally in distributed systems the user should be able to access data if a user has a certain set of authorizations or attributes. At present, the only method for implementing such policies is to employ a trusted server to store the data and facilitate access control. Proposed work deals with attribute policy based control. Attribute-policy based access control defines an access control paradigm whereby access rights are established to users through the use of policies which attributes together. The policies can use several types of attributes like user attributes, resource attributes, object, environment attributes etc. It is a security machinery that uses some policies to guide an authorization decision.

This research work is proposed for realizing complex access control on encrypted data that call attribute-policy based encryption. By using procedures encrypted data, which can be kept confidential even if the storage server is untrusted; furthermore, our methods are secure against collusion attacks. In our system attributes are used to define a user's credentials, and a party encrypting data regulates a policy for who can decrypt. In this method, every secret key is connected with a set of attributes, and every ciphertext is connected with an access structure on attributes. Decryption is empowered if and only if the user's attribute set fulfills the ciphertext access structure. Thus, our methods are abstractly closer to traditional access control methods.This is done by implementing the GSO algorithm.

A. WORKING PRINCIPLE OF THE PROPOSED SYSTEM

Proposed work deals with the GSO algorithm, each glowworm distributes in the objective function definition space. These glowworms carry own luciferin respectively to cluster the pseudo-documents based on the similarity between the pseudo-documents is evaluated as the cosine similarity score and has the respective field of vision scope called local-decision range (cosine similarity score). Their brightness concerns within the position of objective function value (cosine similarity score). The glow seeks for the neighbor set in the privacy value, in the set, a brighter glow (pseudo document) has a higher attraction to attract this glow toward this negotiate, and the flight direction each time different will change laterally with the choice neighbor. Moreover, the privacy value size will be influenced by the neighbor quantity, when the neighbor density will be low, glow's policy-making radius will extend favors seeks for more neighbors, diversely, the policy-making radius reduces. Finally, the majority of glowworm return gathers at the multiple optima of the given cosine similarity score.

B. ADVANTAGES OF THE PROPOSED SYSTEM

- It may try to decrypt the ciphertext stored in the cloud storage.
- Proposed work assumes that an honest system user will not expose his/her secret key.
- It supports factor revocability
- Attribute and policy-based security provide the best solution to all time,
- It increases the security level and needs less computation time, no need re-encryption procedure.

V.SYSTEM ARCHITECTURE

System Architecture diagram which defines the secure cloud storage system supporting privacy preserving data security. In which the data owner upload the data in the cloud server and they are allowed to modify the data using the private key. In this mechanism, the sender only needs to know the identity of the receiver but no other information like a public key. The secret key is stored in the computer. The storage server which is used to store the data which can be generated by the key server. By using attribute-based encryption the key server gives permission to owner and user to access the data stored in the storage server. By this attribute based encryption unauthorized person cannot access data in cloud storage and every time the key will be generated to ensure the security

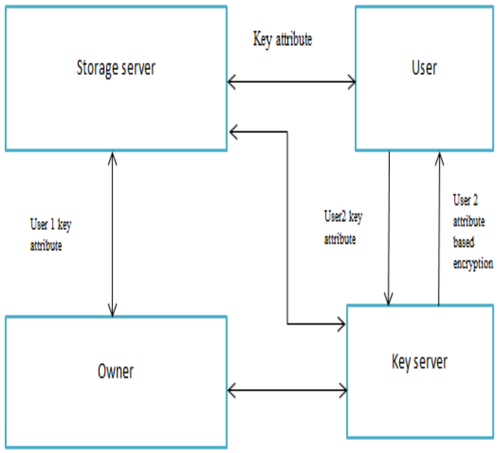

Fig 1. System Architecture

VI. SYSTEM PERFORMANCE AND EVALUATION

To create an account in the cloud by the user, the users store their encrypted data in the cloud by using security key. The Auditor control process of transaction between the user and cloud storage. A PrivateKeyGenerator will respectively generate a secret key for a registered user ID insecure channel such that the user can access the secret key to recover message from its encrypted format. This mechanism is implemented by the Bilinear Diffie-Hellman Assumption.The Diffie–Hellman problem is a mathematical problem suggested by Whitfield Diffie and Martin Hellman in the context of cryptography. The inspiration for this problem is that many security systems use mathematical operations that are wild to compute, but difficult to reveres. Because they enable encrypting a message, but reversing the encryption is problematic. If solving the DHP were easy, these systems would be definitely broken. It contains two phases. In the first phase, a data sender encrypts a data under the identity of a data receiver, and promote sends the encrypted data to the cloud server. In the second phase, the first-level cipher-text of a data from the data sender, the cloud server crafts the second-level cipher-text.

If the user is requested then cloud server will load module to clients end to implement encryption operation. Here client uploads encrypted the file on the cloud server private folder using Public Key Encryption technique. At the time of downloading the encrypted file user will ask to deliver the decryption key if the key is effective then the only file will get downloaded at clients end. This encryption and decryption of data will be completed at client side by making use of a private key. The cipher text is kept on cloud storage while he can download it for decryption. The receiver has a private key which is given by the Private Key generator. The decryption of cipher text required the private key. The attribute and policy can be generated based on the identity of the receiver. It can be decrypted by a valid receiver with a secret key.

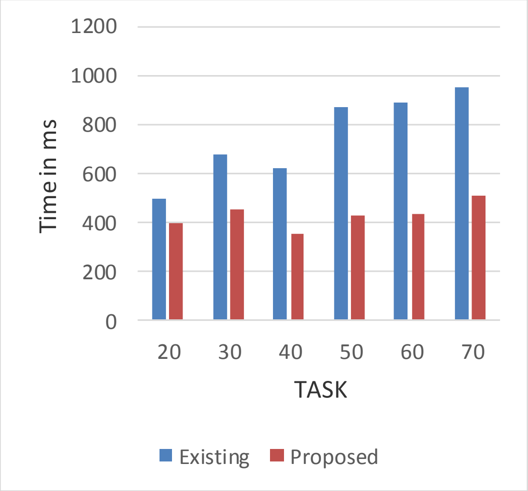

Fig 2. Performance between execution time Verses no of task

As per the Existing system, task percentage is increased by increasing the time where in proposed system task percentage is increased with low time leads to the conclusion that with least amount of time task percentage can be increased.

VII. CONCLUSION

In cloud communication, cloud security is very important but the existing system that uses key encryption is not having sufficient security. Because the key is generated using thread and binary map method which enables the user to download the information by using that key which is not a secure system for users. So, this work includes using GSO algorithm implementation, which results in high security of the transaction. Furthermore, we presented the security proof and efficiency analysis for this system using policy-based encryption. Attribute policy-based data protection mechanism which is used in the proposed system, it proves higher security with less computation time. So, there is no need for multi-level encryption procedure.

REFERENCES

1. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou. Privacy preserving public auditing for secure cloud storage. IEEE Trans. Computers 362–375, 2013.
2. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou. Toward secure and dependable storage services in cloud computing. IEEE T. Services Computing, 5(2):220–232, 2012.
3. H. Wang. Proxy provable data possession in public clouds. IEEE T. Services Computing, 6(4):551–559, 2013.
4. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. Hu. Dynamic audit services for outsourced storages in clouds. IEEE T. Services Computing, 6(2):227–238, 2013.
5. H. C. H. Chen, Y. Hu, P. P. C. Lee, and Y. Tang. NC cloud: A network-coding-based storage system in a cloud-of-clouds. IEEE Trans. Computers, 63(1):31–44, 2014.

6. K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie. Dac-macs: Effective data access control for multi-authority cloud storage systems. IEEE Transactions on Information Forensics and Security, 8(11):1790–1801, 2013
7. V. Varadharajan and U. K. Tupakula. Security as a service model for cloud environment. IEEE Transactions on Network and Service Management, 11(1):60–75, 2014.
8. C.-K. Chu, S. S. M. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng. Key-aggregate cryptosystem for scalable data sharing in cloud storage. IEEE Trans. Parallel Distrib. Syst., 25(2):468–477, 2014.
9. L. Ferretti, M. Colajanni, and M. Marchetti. Distributed, concurrent, and independent access to encrypted cloud databases. IEEE Trans. Parallel Distrib. Syst., 25(2):437–446, 2014
10. S. S. Al-Riyami and K. G. Paterson. Certificateless public key cryptography. In ASIACRYPT, volume 2894 of Lecture Notes in Computer Science, pages 452–473. Springer, 2003.
11. M. H. Au, Y. Mu, J. Chen, D. S. Wong, J. K. Liu, and G. Yang. Malicious kgc attacks in certificateless cryptography. In ASIACCS, pages 302–311. ACM, 2007
12. J. K. Liu, M. H. Au, and W. Susilo. Self-generated-certificate public key cryptography and certificateless signature/encryption scheme in the standard model: extended abstract. In ASIACCS, pages 273–283. ACM, 2007.
13. Y. H. Hwang, J. K. Liu, and S. S. M. Chow. Certificateless public key encryption secure against malicious kgc attacks in the standard model. J. UCS, 14(3):463–480, 2008.
14. C. Gentry. Certificate-based encryption and the certificate revocation problem. In EUROCRYPT, volume 2656 of Lecture Notes in Computer Science, pages 272–293. Springer, 2003.
15. J. K. Liu, J. Baek, and J. Zhou. Certificate-based sequential aggregate signature. In WISEC, pages 21–28. ACM, 2009.
16. J. K. Liu, F. Bao, and J. Zhou. Short and efficient certificate-based signature. In Networking Workshops, volume 6827 of Lecture Notes in Computer Science, pages 167–178. Springer, 2011.
17. J. K. Liu and D. S. Wong. Solutions to key exposure problem in ring signature. I. J. Network Security, 6(2):170–180, 2008.
18. J. K. Liu and J. Zhou. Efficient certificate-based encryption in the standard model. In SCN, volume 5229 of Lecture Notes in Computer Science, pages 144–155. Springer, 2008.
19. D. Boneh, X. Ding, and G. Tsudik. Fine-grained control of security capabilities. ACM Trans. Internet Techn., 4(1):60–82, 2004
20. S. S. M. Chow, C. Boyd, and J. M. G. Nieto. Security-mediated certificateless cryptography. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 508–524. Springer, 2006.
21. W.-S. Yap, S. S. M. Chow, S.-H. Heng, and B.-M. Goi. Security mediated certificateless signatures. In ACNS, volume 4521 of Lecture Notes in Computer Science, pages 459–477. Springer, 2007
22. Y. Dodis, J. Katz, S. Xu, and M. Yung. Key-insulated public key cryptosystems. In EUROCRYPT, volume 2332 of Lecture Notes in Computer Science, pages 65–82. Springer, 2002.
23. Y. Dodis, J. Katz, S. Xu, and M. Yung. Strong key-insulated signature schemes. In Public Key Cryptography, volume 2567 of Lecture Notes in Computer Science, pages 130–144. Springer, 2003
24. G. Hanaoka, Y. Hanaoka, and H. Imai. Parallel key-insulated public key encryption. In Public Key Cryptography, volume 3958 of Lecture Notes in Computer Science, pages 105–122. Springer, 2006.
25. B. Libert, J.-J. Quisquater, and M. Yung. Parallel key-insulated public key encryption without random oracles. In Public Key Cryptography, volume 4450 of Lecture Notes in Computer Science, pages 298–314. Springer, 2007.