International Journal of Control and Automation
Vol. 12, No. 6, (2019), pp. 789-794

Attribute Based Encryption for Secure Deduplication in Cloud Computing

Nipun Chhabra[a], Manju Bala[b]
[a]*Ph.D. Research Scholar, I. K. Gujral Punjab Technical University, Kapurthala (Punjab), India.*
[b]*Director, Khalsa College of Engineering & Technology, Amritsar , (Punjab), India.*

***Abstract**:*

With the wide usage of cloud services, the volume of data stored at cloud servers has also increased. As a result, most of the valuable storage space is being wasted due to duplicacy or redundancy of data and which deteriorates the Quality of Service and underutilises the cloud storage resources. To address this issue various deduplication techniques are used which ensure that a single instance of the data is uploaded and other instances are allocated with a reference pointer for future use. It has been observed that this movement of data from user to storage servers is not secure enough and it creates a lacuna in the reliability of cloud service providers. Many encryption techniques were rendered for providing security to data across the network. This paper presents a deduplication technique coupled with attributes based encryption for providing a secure data transfer between user-end to cloud servers without compromising on data security.

***Keywords**: Secure Deduplication, Attributes Based Encryption with Secure Deduplication, Access Policy in Cloud Storage, Data Deduplication, Secure Access of Data, Encryption Policies in Deduplication, Data Privacy, Cloud Computing, Secure Deduplication Techniques, File Encryption Scheme in Cloud Computing, Proof of Ownership.*

1. Introduction

With the advent of cloud technology many enterprises are opting to get rid of the heavy data management work and are concentrating on their main business. Large cloud service providers have launched industrial cloud platforms for facilitating large volume of data for industrial enterprises. Many organisations want to migrate their data to these platforms but the only apprehension is the security and privacy of data [1]. The need of the hour is to make the storage and access of data to be more secure and less prone to the leakage. Moreover, hosting data to the third-party platforms adds new problems as the security and privacy of the data is dependent on the credibility of the third-party.

To provide desired security, encryption provides the necessary security and assurance to the users. Encryption is the process of encoding information in such a way that only authorized person can access it. In this technique special encryption algorithms are deployed to encrypt user's plain text in to encoded cipher text and which can be decrypted only with the corresponding decryption technique. Traditional Encryption and decryption techniques are far from providing optimal solution to the current problem therefore many researchers are delving out for highly secure and personalised encryption strategies. In this paper, Attribute-based encryption (ABE) coupled with deduplication has been proposed for providing secure access of data, data confidentiality and optimal usage of storage capacity in cloud computing.

2. Literature Survey

Shamir, A **et al [2]** introduced a novel concept of sharing a key which is split into a set number of parts and decryption is possible only when all the set number or more parts of the secret key are available failing which reconstruction is infeasible. Authors have further researched this technique and coined a new identity based encryption based on unique cryptographic scheme where no exchange of public or private key was required for the secure exchange of data. The unique identity of recipient is used to encrypt the message. With this technique, decryption of the message is only possible through the user with the corresponding

ISSN: 2005-4297 IJCA

identity. Sahai A. **et al [3] have** presented the Attribute-based Encryption (ABE) scheme for secret sharing and to regenerate the key IBE was used. This technique provides a promising strategy for encryption and access based restriction on data. A fine-grained access control ABE technique was introduced by Goyal, V.**et al**. [4] for proving additional security to the access of data. Bethencourt, J. **et al. [5]** have presented an improvement of ABE over the previous model which distributes the authority and accountability in encryption used in Cloud environment. Lewko, A. **et al**. [6] proposed the decentralized multi authority CPABE, but user's attributes can be found easily through global identifier. Ostrovsky, R. **et al.[7] have p**roposed an access structure with key policies based on non-monotone formulas but it was having an additional computational overhead. Yan, Z **et al.[8]** proposed a new access structure, ordered binary decision diagram which improved the performance and efficiency but it does not supported revocation mechanism. Emura, K. **et al. [9]** proposed a new scheme with constant cipher text length and constant number of bilinear pairing operations. Secure convergent encryption key was introduced by Chen et al. [10] which ensures data privacy. Yun, A et al. [11] proposed a universal hash based mac scheme to ensure secure file encryption at low cost

3. Existing System

With the growing need of storage and facilities like virtualization & resource sharing, the organizations prefer to store data in cloud storage. It has been observed that users are storing multiple copies of the same data sometimes accidentally and others for the safety of the data. In both the cases the valuable online storage capacity is getting consumed unnecessarily, which can be avoided by using various deduplication techniques where only a unique copy of data is uploaded on the cloud storage and the owners are provided with references to this unique copy whenever they need an access [12]. Moreover, the data being stored on the cloud storage is available to the third party i.e. cloud service provider.

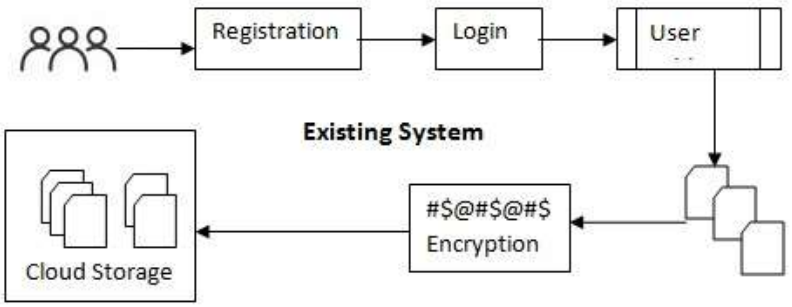

Fig. 1 Diagrammatic Representation of the Existing System.

In the existing system, to secure the shared data on cloud various cryptographic algorithms are used with encryption as the main concept where data is encrypted by individual-user's independent secret key and different user's can encrypt same copies of data with their different secret keys. Hence, different cipher-text will be produced in both cases and desired duplicate data will also be stored [13] [14]. Encryption can be both symmetric and asymmetric. When same key is used for encryption and decryption of data, it is known as symmetric whereas in asymmetric encryption different keys are used for encryption and decryption.

In the existing system many keys are generated for encryption and decryption which is a computational overhead on the system and maintenance of which brings in additional complexity. Moreover, the main drawback of the existing system is that there is no proper verification with the access authority and any users possessing the key can access the confidential data. A solution to this problem can be provided by

using a key which is made unique by using user's personal attributes which give it the name as attributes based encryption [15].

4. Proposed System

The proposed system is based on Attributes based encryption technique which has four main parts viz. Attribute authority, Data owner, Cloud Service Provider and User. For decryption, every user is issued a decryption key on the basis of his attributes by Attribute Authority.

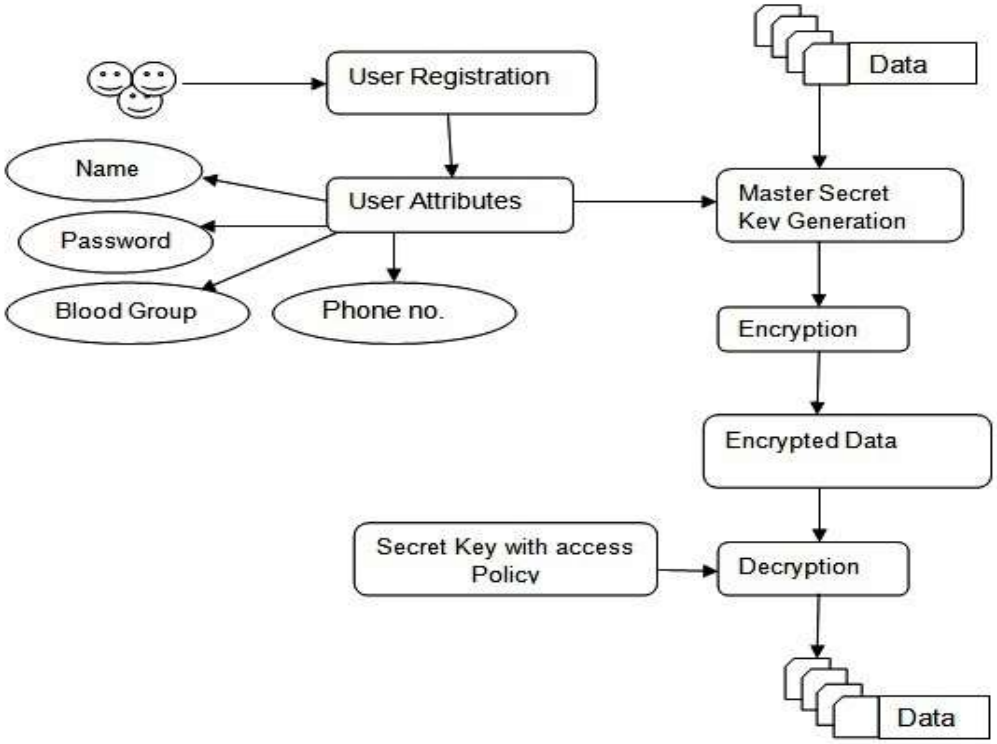

Fig. 2 Diagrammatic Representation of the Attributes Based Encryption.

Registration: Registration module allows the users to register and login for uploading and downloading of data. In this user credentials are used as attributes for the generation of Master Key.
Authentication: In this process, it is checked whether the user is authorised for uploading or downloading of data or not.
Upload File: This module involves the first step of selecting the file to be uploaded and registered users can upload their files on the cloud storage.
Encryption: The selected file is encrypted and then sent to the cloud storage where a hash is computed (deduplication process) to check for a duplicate entry.
Hash Table: The generated hash is checked against the hash table to check whether the file already exists or not.
Cloud storage: If the hash entry is present in hash table then it is not uploaded otherwise new hash entry is included in hash table and file is uploaded on the cloud storage.

The attributes of the user are combined with secret key following which a master key is created for encrypting the data. Data encryption is done at user's end, before the file is sent to the cloud server for storage.

The course of actions to implement the proposed strategy for secure deduplication has been diagrammatically shown in Fig 2 and has been put in a succession as under.

Procedure: Attribute Based Encryption for Secure Deduplication

Phase I: Encryption and Uploading
Step 1: User 'AA' logs in using his credentials.
// these credentials are further used as attributes in master key creation.
Step 2: A key 'KG' is generated. //for Authentication of user.
Step 3: A file 'm' is selected for uploading on to clod server.
Step 4: The selected file is encrypted and encrypted code E(m) is generated sing Master Key which is the combination of KG and Attributes..
Step 5: This encrypted file E(m) is transferred to cloud server and then a hash value is computed, let say H(E(m))
Step 6: For i=1 to n // n= number of entries in hash table
If H (E (m)) = H (E (m_i)) //employing deduplication
Then: it is a duplicate file
Reference pointer of file m is same as that of file m_i
Else
File is stored in cloud and its reference is added into Hash function table
Step 7: Exit

Phase II: Access Granting and File Sharing

Step1: Customer C Logs in to access any file m in Cloud storage

Step2: File m is selected and a request to access file is sent to user AA through Cloud server.
Step3: If user AA grants access to C on file m, then a random key RK is generated and sent to customer C.
// which checks the authentication of customer
Step4: Reference of the key RK and Customer C id is stored against the requested file m.
Step 5: Exit

5. Conclusion:

With the advances in cloud computing a large number of users are storing their data on cloud servers. In the digital era of internet, users are storing multiple copies of the same data on cloud storage. Deduplication strategies provide an efficient mechanism of storing the single copy of data and passing references to all other instances. It was observed that movement of data form users to servers is highly insecure due to unauthorised access. In this paper, we are proposing an Attributes Based Encryption technique coupled with Deduplication for providing added security feature to data during deduplication. The proposed study pairs key and access policies and gives a very secure, reliable and efficient mechanism. In future biometric attributes can be added as personal attributes for making the key unique resulting in a robust system

ISSN: 2005-4297 IJCA

6. References

[1] Song, Y., Wang, H., Wei, X., & Wu, L. (2019). Efficient Attribute-Based Encryption with Privacy-Preserving Key Generation and Its Application in Industrial Cloud. Security and Communication Networks, 2019, 1–9. doi:10.1155/2019/3249726

[2] Shamir, A. (n.d.). Identity-Based Cryptosystems and Signature Schemes. Lecture Notes in Computer Science, 47–53. doi:10.1007/3-540-39568-7_5

[3]. Sahai A., Waters B. (2005) Fuzzy Identity-Based Encryption. In: Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg.

[4] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th ACM Conference on Computer and Communications Security - CCS '06. doi:10.1145/1180405.1180418

[5] Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. 2007 IEEE Symposium on Security and Privacy (SP '07). doi:10.1109/sp.2007.11

[6] Lewko, A., Okamoto, T., Sahai, A., Takashima, K., & Waters, B. (2010). Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Lecture Notes in Computer Science, 62–91. doi:10.1007/978-3-642-13190-5_4

[7] Ostrovsky, R., Sahai, A., & Waters, B. (2007). Attribute-based encryption with non-monotonic access structures. Proceedings of the 14th ACM Conference on Computer and Communications Security - CCS '07. doi:10.1145/1315245.1315270

[8] Yan, Z., Wang, M., Li, Y., & Vasilakos, A. V. (2016). Encrypted Data Management with Deduplication in Cloud Computing. IEEE Cloud Computing, 3(2), 28–35. doi:10.1109/mcc.2016.29.

[9] Emura, K., Miyaji, A., Omote, K., Nomura, A., & Soshi, M. (2010). A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. International Journal of Applied Cryptography, 2(1), 46. doi:10.1504/ijact.2010.033798

[10] Li, J., Chen, X., Li, M., Li, J., Lee, P. P. C., & Lou, W. (2014). Secure Deduplication with Efficient and Reliable Convergent Key Management. IEEE Transactions on Parallel and Distributed Systems, 25(6), 1615–1625. doi:10.1109/tpds.2013.284

[11] Yun, A., Shi, C., & Kim, Y. (2009). On protecting integrity and confidentiality of cryptographic file system for outsourced storage. Proceedings of the 2009 ACM Workshop on Cloud Computing Security - CCSW '09. doi:10.1145/1655008.1655017.

[12] Chhabra, N., & Bala, M. (2018). A Comparative Study of Data Deduplication Strategies. 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC). doi:10.1109/icsccc.2018.8703363

[13] Wang, W., Li, Z., Owens, R., & Bhargava, B. (2009). Secure and efficient access to outsourced data. Proceedings of the 2009 ACM Workshop on Cloud Computing Security - CCSW '09. doi:10.1145/1655008.1655016

[14] Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2011). Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing. IEEE Transactions on Parallel and Distributed Systems, 22(5), 847–859. doi:10.1109/tpds.2010.183 .

[15] P, P. K., P, S. K., & P.J.A., A. (2018). Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. Journal of Network and Computer Applications, 108, 37–52. doi:10.1016/j.jnca.2018.02.009

ISSN: 2005-4297 IJCA