Securing Data in Cloud- A Physical Cyber System

K. Pandu Ranga Reddy,
3/4 B.Tech.(CSE) student, Amrita Vishwa Vidyapeetham, Coimbatore

Dr. K. Thammi Reddy,
Professor, Dept. of CSE, GITAM, Visakhapatnam
Thammireddy.konala@gitam.edu, Contact: 9848027456

AUTHOR'S PROFILE:

K. Pandu Ranga Reddy, pursuing his 3rd year Engineering in Computer Science and Engineering at Amrita Viswa Vidyapeetham, Coimbatore. His research interest in cyber Security and pen testing made him to achieve Certification in CEH, RHCE & RHCSA. A Student member of CSI, IEEE.

Prof. K. Thammi Reddy, received M.Tech(CST) from Andhra University and Doctoral degree from JNTUH, in the area of Data mining. Having 25 years of Teaching & Research experience with an expertise in AI, Data Mining & Security. Published good number of papers in the indexed journals. He is working as a Professor, in the Dept. of CSE, GITAM University. Life member of CSI, IETE, IE, ISTE.

Abstract:

Today's networked world, huge amount of data that is being generated by various physical devices for communication. It is due to sudden surge in the use of IoT devices in various sectors like health monitoring, automobile industry, home appliances etc. These data objects are stored in cloud which consists of sensitive data objects along with other information. Cloud storage is a physical cyber system which attracts users from all sectors to store their data in it. Data storing in the cloud is useful to the individual/organizations to save their maintenance cost. Sharing those stored data through cloud makes the organization to improve their business. Though it increases the business it also increases security challenges. Lot of researches has done to provide secure data sharing through cloud storage. Still more mechanisms are requires to fulfill the requirements of secure data sharing. . The possible attacks at cloud storage are Known-ciphertext, Known-Plaintext and Guessing-keyword. Techniques for secure data sharing through cloud Searchable Symmetric encryption (SSE).Public Key Encryption with Keyword Search (PEKS), Attribute Based Encryption (ABE).

Earlier research focus on user attributes for secure data sharing. But, organizations point of view they will have levels of priority to get access of the data. The proposed framework to encrypt the data based on user priority levels before outsourcing the data and allocates credentials based on priority level hierarchy. The data sharing architecture should able to support user attribute revocation as well as the priorities revocation. It should able to provide verifiability regarding accuracy of cloud service provider's search on behalf of data user. In the proposed architecture the index format includes encrypted keyword which is constructed with access policies and time. The user priorities are considered along with attributes.

Keywords: Physical Cyber systems, Security, Cloud, Encryption, keyword search

1. Introduction: In the networked world, huge amount of data that is being generated by various physical devices for communication. It is due to sudden surge in the use of IoT devices in various sectors like health monitoring, automobile industry, home appliances etc. Finally, data from all these different sectors are to be stored in cloud through the internet. But there are instances of intruders controlling devices and stealing data from computer systems. It has become a challenge for the device manufactures to secure the data that is being communicated using public network i.e. internet. The internet usage has been growing at a pace nearly 52% of the world population is having access to it. Next generation is going to witness a new technological shift towards Physical Cyber Systems (PCS) which is going to be a ground breaking field for computer science researchers to develop protocols, standardizing mechanism. Those mechanisms are to be used for monitoring and controlling the users from unauthorized access.

The basic security needs for storing data in the cloud is confidentiality, Integrity and authentication (CIA).Confidentiality means the data should not be revealed during the transmission in the network and during rest in the cloud. Integrity ensures that the data should not be modified by unauthorized users.

Authentication ensures that the data is received by authorized user. The fundamental mechanism to provide confidentiality is encryption. Data owners are required to perform encryption on the data before outsourcing it to the cloud. Whenever user requires the data, he/she can get it from the cloud instead of from the owner. This data sharing needs to prevent users from unauthorized access of data.

The traditional data receiving process includes 1) user send a search query to the cloud service provider(CSP) 2) CSP decrypts entire data and search for the required data file 3) CSP send data file to the user if it exists. In this case data is revealed to the CSP. Though CSP is a trusted but he/she is curious to know about data and more importantly data owner has no control over the data. The general intension of attackers is to find plaintext data from the ciphertext or gaining secrete key which is used for encryption/decryption. The possible attacks at cloud storage are Known-ciphertext, Known-Plaintext and Guessing-keyword. So many researchers have come up with new techniques for secure data sharing through cloud called searchable encryption techniques.

2. Searchable encryption

Searchable encryption techniques allows the users to recover only required data by searching on encrypted data instead of decrypting entire data. The basic architecture for secure data storing and sharing with searchable encryption is shown in the fig1. In this method data owner prepares a list of keywords for every data file before encrypting the data. Data owner sends encrypted data along with the encrypted keyword list to the cloud data center. Data owner generates information based on access rights given to the data user, which is required for data users to generate a trapdoor. Data user issues this trapdoor to CSP which allows CSP to search on encrypted data. If there is a keyword match occurs then its corresponding data file is issues to user.

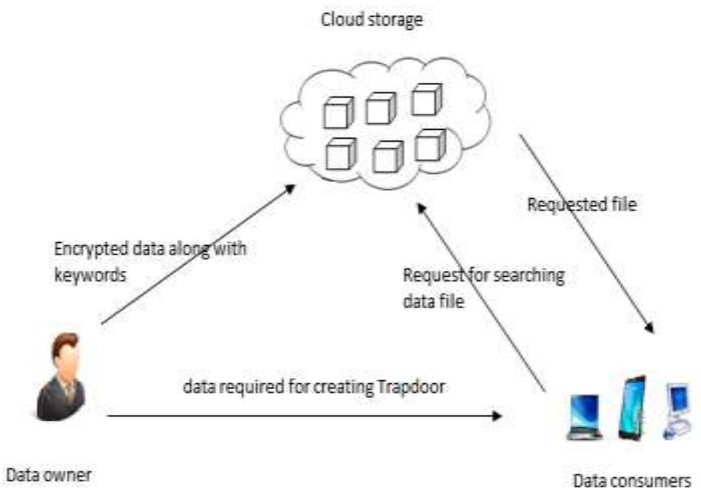
Cloud storage
Requested file
Encrypted data along with keywords
Request for searching data file
data required for creating Trapdoor
Data owner
Data consumers

Fig1: Data storing and sharing architecture in cloud Computing

The searchable encryption allows the cloud service provider to search on encrypted data without knowing (revealing) data and its associated keywords which has been stored in the cloud server. The searchable encryptions are mainly of two types

1) Searchable Symmetric encryption (SSE).
2) Public Key Encryption with Keyword Search (PEKS).

2.1 Searchable Symmetric Encryption: In (SSE) [1] data owner divides the information into equal number of words of equal size. Each word encrypted by an individual key which is generated from pseudorandom generator and pseudorandom function. Data owner stores the encrypted data files along with the encrypted index into the cloud storage space. Whenever user requires the data, he will just send a function of encrypted keyword to the cloud server. Cloud server can search over the encrypted data without compromising confidentiality. SSE is suitable for the architecture where the user is one who sends the data to cloud otherwise there will be a key distribution overhead between the owner and user.

2.2 Public key Encryption with Keyword Search (PEKS): In Asymmetric or public key encryption with keyword search [2], Sender encrypts messages and Set of keywords using receiver's public key and send it to server. Receiver gets the data from the server by sending a trapdoor. Receiver prepares that trapdoor using his private key. Server searches and finds a file whose keyword cipher text is matched to trapdoor.

2.3 Attribute Based Encryption (ABE): When individual/organizations required data sharing with different users, access control is required along with the confidentiality [3].In 2006 Goyal et al [4] proposed Attribute Based Encryption (ABE) to provide fine grained access control mechanism for secure data sharing in the cloud. Here encryption keys are prepared based on the user attributes. So that the data can be decrypted by the user whose attributes are matched. In the users are authenticated with their attributes. The two variants of ABE are ciphertext-policy ABE and Key-policy ABE. In CP-ABE user’s decryption key is associated with the user attributes where as in KP-ABE user’s decryption key is associated with the access policy.

3. Related Works

Many other researchers have done their work towards secure data sharing through cloud storage. The details of the existing works listed in the table1.

In 2012 Alok Kumbhare et al [5] designed a secure Cloud storage repository called Cryptonite. With this mechanism data owner encrypts (symmetric) his data and do signature on that before outsourcing in to cloud. It uses Broad Cast Encryption to prevent unauthorized access of data. BCE allows the owner to prepare a single common sharable key based on user’s public keys (U_1,U_2,….U_n). Data owner use this key to securely distribute encryption key and signature key to the users. Then users use their private key to know the encryption key and signature key. Data users use this encryption key to prepare search query and get the required data. In 2014 Tang [6] introduced a secure and scalable multi-party searchable encryption scheme (MPSE). Here index includes the encrypted keyword and some authorization information which allows only the authorized users to access the data. Other authors in [7] & [11] also introduced methods to support the multi-user and multi-contributor architecture.

The Keyword Guessing Attack (KGA) [8] addresses in Traditional PEKS Framework. Trapdoor is generated using Receiver's public key. Here verification performed by two servers called front and back servers. The servers are trusted and cannot learn anything except the test results. Security relies on secret value P. It does not explicitly discussed about secure communication between front and back servers. Liu, J. in 2016 [9] introduces a two-factor data encryption to share data through cloud. In this, encryption performs in two levels. First level is conducted by data owner and second level is conducted by cloud server. Data owner encrypts the data based on user’s identity in the first level and then sent it to cloud server. Cloud server performs second level encryption corresponding to security device. The encrypted data can only be decrypted by the user who is having two secret keys (two factors). If either one is not available user cannot decrypt the data which is downloaded from the cloud server. If user lost one of the factors, this system allows the user for security device revocability. To support revocability, it performs re-encryption when the security device is changed.

Method	Encryption Technique	Access control policy(Index)	User revocation	Verifiability
Alok Kumbhare et al [5]	SE	Broadcast encryption	Y	N
Tang, Q. [6]	SE	Asymmetric	N	Y
Chen, R et al [8]	ASE	Key distribution	N	N
Liu, J. K. [9]	ASE	IBE on data	Y	N
Cui, B [10]	SE	Aggregate key	N	N
Sun, W etal [11]	SE	ABE	Y	Y
Shen.z et al [12]	SE	HPE	Y	N

Table 1: summary of mechanisms for Securing Data at Cloud Storage

[10] Cui, B proposed key aggregate scheme to outsource the data. In this data owner only needs to distribute a single key to a user for sharing a large number of documents and user only needs to submit a single trapdoor to the cloud for querying the shared documents. Recently Shen.z et al [12] uses hierarchical predicate encryption to encrypt the files. According to the property of HPE, the index information includes the specified access policy, the representative keywords, and the symmetric key which is used to encrypt/decrypt the file.

All the Previous works done based on user attributes for secure data sharing. But, organizations points of view there are some levels of priority to get access of the data. We are trying to encrypt the data based on user priority levels before outsourcing the data and allocate credentials based on priority level hierarchy. The data sharing architecture should able to support user attribute revocation as well as the priorities revocation. It should able to provide verifiability regarding accuracy of cloud service provider's search on behalf of data user. In the proposed architecture the index format includes encrypted keyword which is constructed with access policies and time .The user priorities are considered along with attributes.

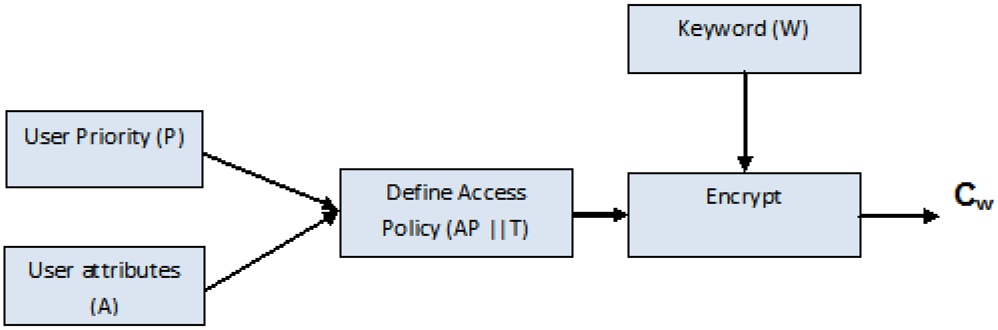

Fig2: Keyword construction in the Index

4. Conclusion

Cloud storage is a physical cyber system which attracts users from all sectors to store their data in it. Data storing in the cloud is useful to the individual/organizations to save their maintenance cost. Sharing those stored data through cloud makes the organization to improve their business. Though it increases the business it also increases security challenges. Lot of researches has done to provide secure data sharing through cloud storage. Still more mechanisms are requires to fulfill the requirements of secure data sharing.

References

[1] Song, D. X., Wagner, D., &Perrig, A. (2000). Practical techniques for searches on encrypted data.In *Security and Privacy,. Proceedings. Of IEEE Symposium* 44-55

[2] Boneh, D, Di Crescenzo, G., Ostrovsky, R., & Persiano, G. (2004). Public key encryption with keyword search. In *International conference on the Theory and Applications of Cryptographic techniques*, Springer Berlin Heidelberg,.506-522

[3] Thilakanathan, D., Chen, S., Nepal, S., &Calvo, R. A. (2014). Secure data sharing in the Cloud. In *Security, Privacy and Trust in Cloud Systems,* Springer Berlin Heidelberg, 45-72

[4] Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, 89-98

[5] Kumbhare, A., Simmhan, Y., & Prasanna, V. (2012). Cryptonite: a secure and performant data repository on public clouds. In *Cloud Computing (CLOUD), 2012 IEEE 5th International Conference*, 510-517

[6] Tang, Q. (2014). Nothing is for free: security in searching shared and encrypted data. *IEEE Transactions on Information Forensics and Security*, *9*(11), 1943-1952.

[7] Zheng, Q., Xu, S., & Ateniese, G. (2014, April). VABKS: verifiable attribute-based keyword search over outsourced encrypted data. In *Infocom, 2014 proceedings IEEE* ,522-530

[8] Chen, R., Mu, Y., Yang, G., Guo, F., & Wang, X. (2016). Dual-server public-key encryption with keyword search for secure cloud storage. *IEEE transactions on information forensics and security*, *11*(4), 789-798.

[9] Liu, J. K., Liang, K., Susilo, W., Liu, J., & Xiang, Y. (2016). Two-factor data security protection mechanism for cloud storage system. *IEEE Transactions on Computers*, *65*(6), 1992-2004.

[10] Cui, B., Liu, Z., & Wang, L. (2016). Key-aggregate searchable encryption (KASE) for group data sharing via cloud storage. *IEEE Transactions on computers*, *65*(8), 2374-2385.

[11] Sun, W., Yu, S., Lou, W., Hou, Y. T., & Li, H. (2016). Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. *IEEE Transactions on Parallel and Distributed Systems*, *27*(4), 1187-1198.

[12] Shen, Z., Shu, J., & Xue, W. (2017). Keyword Search With Access Control Over Encrypted Cloud Data. *IEEE Sensors Journal*, *17*(3), 858-868.