International Journal of Pure and Applied Mathematics
Volume 116 No. 9 2017, 261-265
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

KEY-AGGREGATE SEARCHABLE ENCRYPTION (KASE) DATA SHARING VIA CLOUD STORAGE

[1]R.Velvizhi, [2]M.S.Keerthikha
ASST.PROF/CSE,BHARATH UNIVERSITY
[1]velvizhi.cse@bharath.unive.ac.in,[2] keerthika.cse@bharath.unive.ac.in

Abstract: The sharing of the encrypted data to the particular users via cloud storage has many security issues and data leaks may occur in cloud. Our aim is to designing the encryption schemes in the efficient management of encryption keys and sharing any group of selected document with any user securely. In this, the secret keys generated will be sent securely to the particular users. In this, the data owner only needs to distribute single key to a user for sharing large number of documents. Thus, the security analysis and performance evaluation both confirms that our proposed system is secureandefficient.

1. Introduction

Privacy, the usual way is to ensure it is to rely on the server. In recent times, the cloud storage is very popular. Many data outsourcing process are in demand, which is useful in strategic management of corporate data. The cloud is used as the core technology in many online services for many personal applications. Nowadays, creating account for email are free and even can share photo album, file sharing and remote access, with storage size more than 25GB and can even get 1tb for few dollars. In the current wireless technology, we can access all the files and email in any corner Of the world using the mobile phones [1,2]. However, there will be many security issues by this technology. Considering the data enforce the access control for authentication, which means any unexpected privilege will expose all data. In shared cloud computing environment there are many insecurities and things may go worse at any time. The data from different clients may be hosted on separate Virtual Machines (VMS) but they reside on a single physical machine, which may cause data leaks[3,4].The data in the virtual machine is the main target, as when many Virtual Machines are installed in the same machine, the data may be stolen. Based on the availability of the file, there are many cryptographic schemes, which go as far as allowing the third party auditor to check the availability of the files on behalf of the data owner, but cannot view the data. No information will be leaked about the data during this process or without compromising the data owner's anonymity. In the same way, the cloud user will not have a strong belief that the cloud server is doing a good job in terms of confidentiality.The solution for this is given through the cryptosystem concepts, the proven security relied on number-theoretical assumptions are more desirable, when the user is not satisfied or happy with trusting the security of the VM or the honesty of the technical staff. The users are generally asked to encrypt the file before uploading it in the server. The main process in the cloud storage is the data sharing[5,6,7]. transformation verifiability. However, it does not possible to construct the ABE schemes with verified outsourced whichcan be already defined in the existing. Moreover, the method proposed in existing relies on Key Aggregate Searchable Encryption (KASE) model[16]. The KASE model heuristic and a proof of security in KASE model. It does not directly imply about the security of ABE scheme in the real world. It is well known because there exit cryptographic scheme which are secure the KASE. In the KASE algorithm the secure key.

2. Related Works

Should be numerical and the character. However, in this paper we focus on cipher text, as the key
should be in the special In the existing system, there exist ABE schemes for decryption algorithm. It requires only a constant number of character. The design for KASE scheme from both the multi-key searchable encryption scheme and key-aggregate dataairing computations. By solving this problem, newly sharing scheme. Each key is associated with a particular index introduce the notion of ABE with outsourced decryption, it highly eliminates the decryption overhead for users. With the help of ABE existing system, the proposed also concrete with outsourced decryption. A proxy can be operated by a cloud service. The transformation key can be translated

to the cipher text key. User to form a simple cipher text can accept these key. This existing scheme cannot provide the guarantee for transformation to the cloud server. We cannot able to see the encrypted message also. In the cloud service, it has financial incentives to return, it requires the less work and detected by users. In the existing scheme, the repeated file can be saved in the cloud[8,9]. While sharing the data, file will be saved repeatedly in the same cloud. By this processing the file can be occupied more space. Therefore, the data storage space will also be increased. These decrease the processing speed while retrieving the file[10,11]. Of document. In the proposed system the data sharing should be provide securely. While sharing the data, the repeated files cannot be stored in the same cloud. Therefore, the storage space will be reduced. By this process, only the authorized user can view the data.

2.1 Description Of Kase Scheme

In the Key Aggregate Searchable Algorithm (KASE),we make use of the special characters for generating keys. In the present system, we make use of numbers and characteristics. However, in our concept we make use of the characteristics and special characters for generating the secret key. Hence, it would be more secured comparatively. We proposes a concrete KASE scheme as follows[12,13].

2.2 Methods And Material

1) Setup (1_, n): the cloud server will use this algorithm to initialize system parameters as follows:_ Generate a bilinear map group system B=(p,G, G1, e(_; _)), where p is The cloud has to check the correctness of the order of G and 2_ _ p _ 2_+1._ Set n as the maximum possible number of documents which belongs to a data owner. _ Pick a random generator g 2 G and a random _ 2 Zp, and computes gi = g(_i) 2 G for i = f1; 2; _ _ _; n; n + 2; _ _ _; 2ng. _ Select a one-way hash function H: f0; 1g !G. Finally, cloud server publishes the system parameters Params = (B,PubK, H), where PubK = (g; g1; _ _ _; gn; gn+2; :::; g2n) 2 G2n+1.[14,15]

2) Keygen data owner uses this algorithm to generate his/her key pair. It picks a random 2 Zp, and outputs: pk = v = g; msk. Encrypt (pk, i): data owner uses this algorithm.To encrypt data and generate its keyword ciphertexts When uploading the i-the document. To Generate the keyword cipher texts, this algorithm Takes as input the file index i 2 f1; :::; ng, and: _ randomly picks a t 2 Zp as the searchable encryption key ki of this document_ generates a delta _i for ki by computing: c1 = gt; c2 = (v _ gi)t _ for a keyword w, outputs its ciphertext cw as: w = e(g;H(w))t=e(g1; gn)t.

2.3 Upload file

The user can upload a file in cloud storage area. The data will get encrypt and then it will be stored into the database.

2.4 Adminlogin

The admin has to login by providing userid and password.

2.5 Issue Password Through Mail

The admin should view the user details and he has to issue the secret keys to the user to access the file through mail.

2.6 Access File

The user can check the mail to see the private password and then can access the file securely 4) Trapdoor (kagg, w): the user uses is lgorithm to generate the trapdoor to perform keyword Search. For all documents which are relevant to the aggregate key kagg, this algorithm generates the only one trapdoor Tr for the keyword w by computing: Tr = kagg _ H(w). Then, the user sends (Tr, S) to the cloud server.

2.7 User Login

The user has to login by providing usernd password.for the first time propose the concept of key- aggregate searchable encryption (KASE) and construct aconcrete KASE scheme. Both analysis and evaluationresults confirm that our work can provide an effectivesolution to building practical data sharing system basedon public cloud storage. In a KASE scheme, the owner only needs to distribute a single key to a user whensharing many documents with the user and the user onlyneeds to submit a single trapdoor when he queries overall documents shared by the same owner.

Figure 1. Architecture diagram

3. Conclusion

Considering the practical problem of privacy preservingdata sharing system based on public cloud storage which requires a data owner to distribute a large number ofkeys to users to enable them to access his/her documents,

4. Future Enhancement

However, if a user wants to query over documents shared by multiple owners, he must generate multiple trapdoors to the cloud. How to reduce the number of trapdoors under multi-owners setting is a future work. Moreover, federated clouds have attracted

References

[1]Udayakumar R., Kaliyamurthie K.P., Khanaa, Thooyamani K.P., Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, v-29, i-14, pp-86-90, 2014.

[2]Kaliyamurthie K.P., Parameswari D., Udayakumar R., QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, v-6, i-SUPPL5, pp-4648-4652, 2013.

[3]Brintha Rajakumari S., Nalini C., An efficient cost model for data storage with horizontal layout in the cloud, Indian Journal of Science and Technology, v-7, i-, pp-45-46, 2014.

[4]Brintha Rajakumari S., Nalini C., An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, v-7, i-, pp-44-46, 2014.[5]Khanna V., Mohanta K., Saravanan T., Recovery of link quality degradation in wireless mesh networks, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4837-4843, 2013.

[6]Khanaa V., Thooyamani K.P., Udayakumar R., A secure and efficient authentication system for distributed wireless sensor network, World Applied Sciences Journal, v-29, i-14, pp-304-308, 2014.

[7]Udayakumar R., Khanaa V., Saravanan T., Saritha G., Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, v-16, i-12, pp-1781-1785, 2013.

[8]Khanaa V., Mohanta K., Saravanan. T., Performance analysis of FTTH using GEPON in direct and external modulation, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4848-4852, 2013.

[9]Kaliyamurthie K.P., Udayakumar R., Parameswari D., Mugunthan S.N., Highly secured online voting system over network, Indian Journal of Science and Technology, v-6, i-SUPPL.6, pp-4831-4836, 2013.

[10]Thooyamani K.P., Khanaa V., Udayakumar R., Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, v-20, i-12, pp-2464-2470, 2014.

[11]R.Kalaiprasath, R.Elankavi, Dr.R.Udayakumar, Cloud Information Accountability (Cia) Framework Ensuring Accountability Of Data In Cloud And Security In End To End Process In Cloud Terminology, International Journal Of Civil Engineering And Technology (Ijciet)
Volume 8, Issue 4, Pp. 376–385, April 2017.

[12]R.Elankavi, R.Kalaiprasath, Dr.R.Udayakumar, A fast clustering algorithm for high-dimensional data, International Journal Of Civil Engineering And Technology (Ijciet), Volume 8, Issue 5, Pp. 1220–1227, May 2017.

[13]R. Kalaiprasath, R. Elankavi and Dr. R. Udayakumar. Cloud. Security and Compliance - A Semantic Approach in End to End Security, International Journal Of Mechanical Engineering And Technology (Ijmet), Volume 8, Issue 5, pp-987-994, May 2017.

[14]Thooyamani K.P., Khanaa V., Udayakumar R., Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, v-20, i-12, pp-2604-2612, 2014.

[15]Udayakumar R., Thooyamani K.P., Khanaa, Random projection based data perturbation using geometric transformation, World Applied Sciences Journal, v-29, i-14, pp-19-24, 2014.

[16]Udayakumar R., Thooyamani K.P., Khanaa, Deploying site-to-site VPN connectivity: MPLS Vs IPSec, World Applied Sciences Journal, v-29, i-14, pp-6-10, 2014.