Cloud-Based Data Storage and Sharing using Multi Access Control Mechanism

NALLABATHUNI SOWJANYA, student member, M.Tech(CSE), Dr.Shaik Jaffar Hussain

Associate Professor and Head of Computer Science and Engineering Department,

Sri Venkateswara Institute of Science and Technology,, Kadapa.

Abstract

Cloud-baseddatastorageservicehasdrawnincreasinginterestsfrombothacademicandindustry intherecentyearsdueto its efficient and low cost management. Since it provides services in an open network, it is urgent for service providers to make use ofsecure data storage and sharing mechanism to ensure data confidentiality and service user privacy. To protect sensitive data frombeing compromised, the most widely used method is encryption. However, simply encrypting data (e.g., via AES) cannot fully addressthe practical need of data management. Besides, an effective access control over download request also needs to be considered sothat Economic Denial of Sustainability (EDoS) attacks cannot be launched to hinder users from enjoying service. In this paper, weconsider the *dual access control*, in the context of cloud-based storage, in the sense that we design a control mechanism over bothdata access and download request without loss of security and efficiency. Two dual access control systems are designed in this paper,where each of themis for a distinctdesigned setting. The securityand experimental analysisfor the systems arealso presented

1. INTRODUCTION

A strawman answer to the manipulate of down load request is to leverage dummy cipher texts to In the latest decades, cloud-based storage carrier has attracted great interest from each academia and industries. It may also be extensively used in many Internet-based industrial purposes (e.g., Apple I Could) due to its long-list advantages inclusive of get entry to flexibility and free of neighborhood records management. Increasing range of humans and corporations currently decide upon to outsource their statistics to faraway cloud in such a way that they may additionally decrease the fee of upgrading their neighborhood statistics administration facilities/devices. However, the fear of protection breach over outsourced records might also be one of the major boundaries hindering Internet customers from broadly the usage of cloud-based storage service. In many sensible applications, outsourced information may additionally want to be in addition shared with others. For example, a Dropbox consumer Alice might also share pics with her friends. Without the usage of facts encryption, prior to sharing the photos, Alice wishes to generate a sharing hyperlink and in addition share the hyperlink with friends. Although guaranteeing some degree of get admission to manipulate over unauthorized customers (e.g., these are now not Alice's friends), the sharing hyperlink may additionally be seen inside the Dropbox administration stage (e.g., administrator may want to attain the link).Since the cloud (which is deployed in an open network) is no longer be utterly trusted, it is commonly encouraged to encrypt the information prior to being uploaded to the cloud to make sure records protection and privacy.

One of the corresponding options is to without delay rent an encryption approach (e.g., AES) on the outsourced data To stop shared snap shots being accessed by way of the "insiders" of the system, a simple way is to designate the team of licensed facts customers prior to encrypting the data. In some cases, nonetheless, Alice might also have no concept about who the picture receivers/users are going to be. It is viable that Alice solely has expertise of attributesw.r.t. photo receivers. In this case, traditional public key encryption (e.g., Paillier Encryption), which requires the encryptor to know who the data receiver is in advance, cannot be leveraged. so that Alice makes use of the mechanism to define access policy over the encrypted pictures to assurance solely a team of licensed customers is capable to get entry to the photos. In a cloud-based storage service, there exists a frequent assault that is prevalent as resource-exhaustion attack. Since a (public) cloud might also no longer have any manipulate over down load request (namely, a provider person can also ship limitless numbers of down load request to cloud server), a malicious carrier consumer might also launch the denial-of-service (DoS)/distributed denial-of-service (DDoS) assaults to devour the useful resource of cloud storage provider server so that the cloud provider may want to no longer be in a position to reply truthful users' provider requests. As a result, in the "pay-as-you-go" model, monetary components ought to be disrupted due to greater useful resource usage. The fees of cloud provider customers will upward jab dramatically as the assaults scale up.

This has been regarded as Economic Denial of Sustainability (EDoS) attack. which pursuits to the cloud adopter's financial resources. Apart from financial loss, limitless down load itself may want to open a window for community attackers to examine the encrypted down load information that might also lead to some practicable statistics leakage (e.g., file size). Therefore, an positive manipulate over down load request for outsourced (encrypted) records is additionally needed. In this project, we endorse a new mechanism, dubbed twin get entry to control, to handle the above noted two problems.

To tightly closed information in cloud-based storage service, attribute-based encryption (ABE) is one of the promising candidates that allows the confidentiality of outsourced statistics as nicely as fine-grained manipulate over the outsourced data. In particular, Cipher text-Policy ABE (CP-ABE) affords an superb way of statistics encryption such that get right of entry to policies, defining the get admission to privilege of practicable facts receivers, can be specific over encrypted data. Note that we reflect onconsideration on the use of CP-ABE in our mechanism in this paper. Nevertheless, virtually using CP-ABE approach is no longer adequate to diagram an dependent mechanism guaranteeing the manage of each records get right of entry to and down load request. confirm statistics receiver's decryption rights. It, concretely, requires information owner, say Alice, to add more than one "testing" cipher texts alongside with the "real" encryption of facts to cloud, the place the "testing" cipher texts are the encryptions of dummy messages beneath the identical get entry to coverage as that of the "real" data. After receiving a download request from a user, say Bob, cloud asks Bob to randomly decrypt one of the "testing" cipher texts. If a right result/decryption is returned.

2. LITERATURE SURVEY

1. John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute- based encryption. In S&P 2007, pages 321–334. IEEE, 2007.

   In numerous dispensed structures a consumer must solely be in a position to get admission to records if a consumer posses a positive set of credentials or attributes. Currently, the solely approach for imposing such insurance policies is to rent a relied on server to save the facts and mediate get entry to control. However, if any server storing the records is compromised, then the confidentiality of the information will be compromised. In this paper we existing a machine for realizing complicated get right of entry to manipulate on encrypted facts that we name ciphertext-policy attribute-based encryption. By the usage of our strategies encrypted facts can be stored exclusive even if the storage server is untrusted; moreover, our techniques are impervious towards collusion attacks. Previous attribute- based totally encryption structures used attributes to describe the encrypted records and constructed insurance policies into user's keys; whilst in our gadget attributes are used to describe a user's credentials, and a celebration encrypting records determines a coverage for who can decrypt. Thus, our strategies are conceptually nearer to ordinary get right of entry to manage techniques such as role-based get right of entry to manage (RBAC). In addition, we supply an implementation of our device and provide overall performance measurements.

2. Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au.

Improving privateness and safety in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on data forensics and security, 10(3):665–678, 2015. In preceding privacy-preserving multiauthority attribute-based encryption (PPMA- ABE) schemes, a consumer can gather secret keys from a couple of authorities with them understanding his/her attributes and furthermore, a central authority is required. Notably, a user's identification statistics can be extracted from his/her some touchy attributes. Hence, current PPMA-ABE schemes can't completely shield users' privateness as a couple of authorities can collaborate to discover a consumer by using accumulating and inspecting his attributes. Moreover, ciphertext-policy ABE (CP-ABE) is a extra environment friendly public-key encryption, the place the encryptor can choose bendy get right of entry to buildings to encrypt messages. Therefore, a difficult and vital work is to assemble a PPMA-ABE scheme the place there is no necessity of having the central authority and furthermore, each the identifiers and the attributes can be blanketed to be recognized with the aid of the authorities.

In this paper, a privacy- keeping decentralized CP-ABE (PPDCP-ABE) is proposed to limit the have faith on the central authority and defend users' privacy. In our

PPDCP-ABE scheme, every authority can work independently barring any collaboration to preliminary the gadget and trouble secret keys to users. Furthermore, a person can achieve secret keys from a couple of authorities besides them understanding some thing about his international identifier and attributes.

3. Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent aid consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

Frank Mckeen. IntelR software program protect extensions: Epid provisioning and attestation services. White Paper, 1:1–10, 2016. Obligated with the aid of a utility pricing model, Internet-facing internet assets hosted in the public cloud are inclined to Fraudulent Resource Consumption (FRC) attacks. Unlike an application-layer DDoS assault that consumes assets with the intention of disrupting momentary availability, an FRC assault is a extensively greater refined assault that alternatively seeks to disrupt the long-term monetary viability of running in the cloud by using exploiting the utility pricing mannequin over an prolonged time period. By fraudulently eating net sources in adequate quantity (i.e. records transferred out of the cloud), an attacker (e.g. botnet) is capable to incur huge fraudulent prices to the victim. This paper proposes an attribution methodology that the introduced methodology achieves certified success in opposition to difficult assault scenarios.to discover malicious consumers taking part in an FRC attack. Experimental effects demonstrate.

4. Jiguo Li, Xiaonan Lin, Yichen Zhang, and Jinguang Han. Ksfoabe: outsourced attribute-based encryption with key-word search feature for cloud storage. IEEE Transactions on Services Computing.10(5):715–725, 2017.

Cloud computing turns into more and more famous for records proprietors to outsource their statistics to public cloud servers whilst permitting supposed facts customers to retrieve these information saved in cloud. This variety of computing mannequin brings challenges to the safety and privateness of records saved in cloud. Attribute-based encryption (ABE) technological know-how has been used to graph fine-grained get entry to manage system, which affords one suitable technique to Department of CSE Page 4 solve the protection troubles in cloud setting.

However, the computation price and ciphertext measurement in most ABE schemes develop with the complexity of the get admission to policy. Outsourced ABE (OABE) with fine-grained get admission to manage gadget can generally decrease the computation value for customers who favor to get entry to encrypted facts saved in cloud by means of outsourcing the heavy computation to cloud carrier issuer (CSP). However, as the quantity of encrypted documents saved in cloud is turning into very huge, which will prevent environment friendly question processing.

To deal with above problem, we existing a new cryptographic primitive known as attribute-based encryption scheme with outsourcing key-issuing and outsourcing decryption, which can put in force key-word search feature (KSF-OABE). The proposed KSF-OABE scheme is proved invulnerable towards chosen-plaintext assault (CPA). CSP performs partial decryption mission delegated via statistics person except understanding whatever about the plaintext. Moreover, the CSP can function encrypted key-word search except understanding something about the key phrases embedded in trapdoor.

5. Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Full verifiability for outsourced decryption in attribute based totally encryption. IEEE Transactions on Services Computing, DOI: 10.1109/TSC.2017.2710190, 2017.

Attribute primarily based encryption (ABE) is a famous cryptographic technological know-how to defend the safety of users' data. However, the decryption price and ciphertext dimension avert the software of ABE in practice. For most present ABE schemes, the decryption price and ciphertext dimension develop linearly with the complexity of get admission to structure. This is undesirable to the units with confined computing functionality and storage space. Outsourced decryption is regarded as a viable approach to limit the user's decryption overhead, which permits a consumer to outsource a giant quantity of decryption operations to the cloud provider issuer (CSP). However, outsourced decryption can't warranty the correctness of transformation accomplished by means of the cloud, so it is crucial to test the correctness of outsourced decryption to make sure protection for users' data. Current lookup often focuses on verifiability of outsourced decryption for the approved users. It nonetheless stays a difficult problem that how to warranty the correctness of outsourced decryption for unauthorized users.In this paper, we recommend an ABE scheme with verifiable outsourced decryption (called full verifiability for outsourced decryption),

3. EXISTING SYSTEM

Although being in a position to assist fine-grained statistics access, CP-ABE, performing as a single solution, is a ways from sensible and wonderful to maintain towards EDoS assault which s the case of DDoS in the cloud setting. Several countermeasures to the assault have been proposed in the literature. But Xue et al. mentioned that the preceding works should now not completely protect the EDoS assault in the algorithmic (or protocol) level, and they in addition proposed a answer to impervious cloud facts sharing from the attack.

However, suffers from two disadvantages. First, the statistics proprietor is required to generate a set of undertaking ciphertexts in order to withstand the attack, which enhances its computational burden. Second, a statistics person is required to decrypt one of the venture ciphertexts as a test, which charges a lots of high-priced operations (e.g., pairing). Here the computational complexity of each events is inevitably extended and meanwhile, excessive community bandwidth is required for the transport of ciphertexts. The enormous computational energy of cloud is now not wholly viewed in .

In this paper, we will current a new answer that requires much less computation and verbal exchange price to stand nevertheless in the front of the EDoS attack. Recently, AntonisMichalas proposed a statistics sharing protocol that combines symmetric searchable encryption and ABE, which permits customers to immediately search over encrypted data. To put in force the performance of key revocation in ABE, the protocol makes use of SGX to host a revocation authority.

Bakas and Michalas later prolonged the protocol in and proposed a hybrid encryption scheme that reduces the hassle of multi-user facts sharing to that of a single-user. In particular, the symmetric key used for facts encryption is saved in an SGX enclave, which is encrypted with an ABE scheme. Similar to , it offers with the revocation hassle in the context of ABE through using the SGX enclave. In this work, we hire SGX to allow the manipulate of the downloadrequest (such that the DDoS/EDoS assaults can be prevented). In this sense, the reason and the approach of ours are specific from that of the protocols in].

Disadvantages

1) The device used to be no longer carried out Ciphertext-Policy Attribute-based-Encryption Method which leads much less protection on outsourced data. 2) The device is less protection due to lack of Authenticated Encryption with Associated Data.

4. PROPOSED SYSTEM

In this paper, we propose a new mechanism, dubbed dual access control, to tackle the above aforementioned two problems. To secure data in cloud-based storage service, attribute-based encryption (ABE) is one of the promising candidates that enables the confidentiality of outsourced data as well as fine-grained control over the outsourced data.

In particular, Cipher text-Policy ABE (CP-ABE) provides an effective way of data encryption such that access policies, defining the access privilege of potential data receivers, can be specified over encrypted data. Note that we consider the use of CP-ABE in our mechanism in this paper. Nevertheless, simply employing CP-ABE technique is not sufficient to design an elegant mechanism guaranteeing the control of both data access and download request.

A strawman solution to the control of download request is to leverage dummy cipher texts to verify data receiver's decryption rights. It, concretely, requires data owner, say Alice, to upload multiple "testing" cipher texts along with the "real" encryption of data to cloud, where the "testing" cipher texts are the encryptions of dummy messages under the same access policy as that of the "real" data. After receiving a download request from a user, say Bob, cloud asks Bob to randomly decrypt one of the "testing" cipher texts. If a correct result/decryption is returned (i.e. indicating Bob is with valid decryption rights), Bob is authorized by Alice to access the ”real” data, so that the cloud allows Bob to download the corresponding ciphertext.

Benifits

(1) Confidentiality of outsourced data. In our proposed systems, the outsourced data is encrypted prior to being uploaded to cloud. No one can access them without valid access rights.

(2) Anonymity of data sharing. Given an outsourced data, cloud server cannot identify data owner, so that the anonymity of owner can be guaranteed in data storage and sharing.

(3) Fine-grained access control over outsourced (encrypted) data. Data owner keeps controlling his encrypted data via access policy after uploading the data to cloud. In particular, a data owner can encrypt his outsourced data under a specified access policy such that only a group of authorized data users, matching the access policy, can access thedata.

(4) Control over anonymous download request and EDoS attacks resistance. A cloud server is able to control the download request issued by any system user, where the download request can set to be anonymous. With the control over download request, we state that our systems are resistant to EDoS attacks.

(5) High efficiency. Our proposed systems are built on the top of the CP-ABE system. Compared with [36], they do not incur significant additional computation and communication overhead. This makes the systems feasible for real-world applications.

5. MODULES

Data Owner

In this module, the data owner uploads their data in the cloud server. For the security purpose the data owner encrypts the file and then store in the cloud. The data owner can have capable of updating and deleting of a specific file. And also he can view the transactions based on the files he uploaded to cloud.

End User

In this module, receivers logs in by using his/her user name and password. After Login receiver will Search for files and request for secret key of a particular file from Authority, and get the secret key. After getting secret key he is trying to download file by entering file name and secret key from cloud server.

Authority

In this module, the authority helps to check transaction of files and also. If receiver exists and the profile. Authority also view the requests from the receivers and generates the secret key and send to the requested data receivers.

Cloud Server

The cloud service provider manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with Remote

User. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Data Encryption and Decryption

All the legal receivers in the system can freely query any interestedencrypted and decrypted data. Upon receiving the data from the server, the receiver runs the decryption algorithm Decrypt to decrypt the cipher text by using its secret keys from different Users.

Attacker Module

In Data Receiver module, while downloading files if receiver enters wrong secret key for particular file, then cloud servers treats him as attacker and moves to attacker list.

6. CONCLUSION

We addressed an interesting and long-lasting problem in cloud-based data sharing, and presented two dual access control systems. The proposed systems are resistant to DDoS/EDoS attacks. We state that the technique used to achieve the feature of control on download request is “transplantable” to other CP-ABE constructions. Our experimental results show that the proposed systems do not impose any significant computational and communication overhead (compared to its underlying CP-ABE building block). In our enhanced system, we employ the fact that the secret information loaded into the enclave cannot be extracted. However, recent work shows that enclave may leak some amounts ofits secret(s) to a malicious host through the memory access patterns or other related side- channel attacks. The model of transparent enclave execution is hence introduced in. Constructing a dual access control system for cloud data sharing from transparent enclave is an interesting problem. In our future work, we will consider the corresponding solution to the problem.

BIBLIOGRAPHY

1. Joseph A Akinyele, Christina Garman, Ian Miers, Matthew W Pagano, Michael Rushanan, Matthew Green, and Aviel D Rubin.Charm: a framework for rapidly prototyping cryptosystems. Journal of Cryptographic Engineering, 3(2):111–128, 2013.
2. Ittai Anati, Shay Gueron, Simon Johnson, and Vincent Scarlata.Innovative technologyfor cpu based attestation and sealing. In

Workshop on hardware and architectural support for security and privacy(HASP), volume 13, page 7. ACM New York, NY, USA, 2013.

3. Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute-based encryption,symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.
4. Amos Beimel. Secure schemes for secret sharing and key distribution.PhD thesis, PhD thesis, Israel Institute of Technology, Technion,Haifa, Israel, 1996.
5. John Bethencourt, Amit Sahai, and BrentWaters. Ciphertext-policy attribute-based encryption. In S&P 2007, pages 321–334. IEEE,2007.
6. Victor Costan and Srinivas Devadas. Intel sgx explained. IACR Cryptology ePrint Archive, 2016(086):1–118, 2016.
7. Ben Fisch, Dhinakaran Vinayagamurthy, Dan Boneh, and Sergey Gorbunov. IRON: functional encryption using intel SGX. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, pages 765–782, 2017.
8. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In Advances in Cryptology-CRYPTO 1999, pages 537–
9. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters.Attribute-based encryption for fine-grained access control of encrypted data. In ACM CCS 2006, pages 89–98. ACM, 2006.