A DISCUSSION OF KEY AGGREGATE CRYPTOSYSTEMS AND DECOY TECHNOLOGY USED FOR SECURE DATA SHARING IN THE CLOUD

Mali Nilesh Dattatray
Research Scholar
Department of Engineering
Sunrise University, Alwar, Rajasthan.
nileshdmali@gmail.com

Dr. Rathod Sunil Damodar
Research Guide
Department of Engineering
Sunrise University, Alwar, Rajasthan.

Abstract

A crucial feature of cloud storage is data sharing. I demonstrate how to use Decoy technology in secure cloud storage to transfer data effectively, efficiently, and flexibly. I discuss novel public-key cryptosystems that generate constant-size cipher texts, making it feasible to efficiently delegate decryption rights for any collection of cipher texts. It's unusual to be able to combine any collection of secret keys into something that is as little as a single key while yet having the full power of all the individual keys.

In other words, the owner of the secret key may share an aggregate key of constant size for a flexible cipher text set in cloud storage, but the other encrypted files outside of the set stay private. This little aggregate key may be transmitted to others easily or kept on a smart card with a very small amount of safe storage. So, using the standard paradigm, I present a formal security analysis of our methods. I go on to outline further uses for our systems. Our approaches provide the first patient-controlled public-key encryption for flexible hierarchy, which previously unknown.

Keywords: *Cloud storage, data sharing, key-aggregate encryption, patient-controlled encryption.*

Introduction

In recent years, the internet has become more popular. It offers consumers a variety of services. The cloud computing service is one of the crucial ones. An on-demand computing method known as cloud computing provides customers with access to resources over the internet as a service. In cloud computing, protecting files or data from unauthorized users is the key issue when it comes to security.

Any solution that prevents an unwanted invader from accessing your cloud-based files or data has security as its primary goal. Cloud storage is a key service offered by cloud computing. Local users have the option of storing their data on distant cloud storage servers, from which they may access it from any location in the globe. However, using a third party cloud system to store your data might compromise its secrecy. The data is encrypted before being stored in the storage server to prevent this problem. In the case of a generic encryption system, the data owner uses cryptographic methods to encrypt the data before storing it on a cloud storage server. Data secrecy is provided, however strong security and dynamic data change are not. The unauthorized user may get the data during its passage from the data owner to the cloud server or he may obtain the cryptographic keys necessary to decode the data straight from the cloud server.

Then, the hacker may make some changes to the stolen data and deposit it once again on the storage server in the role of the data owner. Users of the cloud and the data owner are unable to recognize data hacking. The information seems to be the real thing. Data originality, data origin authentication, security, and data integrity

are all impacted by the receiver's perception that the data originated from the data owner. Symmetric and asymmetric (public) encryption keys are also available.

With symmetric encryption, the user must provide the encryptor with her secret key if she wants the data to seem to have come from a third party; clearly, this is not always a good idea. In contrast, public key encryption uses two distinct keys for encryption and decoding. Public-key encryption provides our apps additional freedom. For instance, in corporate settings, any employee may upload encrypted data to the cloud storage server without access to the master-secret key of the organization.

Cloud computing is Internet-based computing where virtual shared servers provide PCs on a pay-per-use basis access to software, infrastructure, platforms, devices, and other resources. Users may use these services that are accessible in the "internet cloud" without any prior experience with resource management. As a result, users may focus more on the essential business processes rather than having to spend time learning about the tools required to manage those operations. While residing on a single physical system, data from several customers may be housed on many virtual machines.

By creating a second VM that is coresident with the target one, data in the target VM may be stolen. Regarding file availability, there are a number of cryptographic techniques that even enable a third-party auditor to verify file accessibility on the data owner's behalf without disclosing any information about the data or jeopardizing the data owner's identity. These users are encouraged to encrypt their data using their own keys before submitting it to the server.

Literature Survey

A group of interconnected, virtualized computers make up the cloud, a market-oriented distributed computing system. Users of cloud computing may utilize the Internet to outsource their processing and storage to servers. The science of cryptography focuses on methods for securely transmitting data. Enabling a message's intended receivers to receive it safely is the aim of cryptography. The goal of cryptography is to make the communication unintelligible to listeners. Plaintext refers to the message in its native format.

A secure system's transmitter will encrypt the plaintext in order to obscure its meaning. Only when the intended receiver makes an attempt to access it will its significance become clear. The result of this reversible mathematical operation is cipher-text, which is an output that is encrypted. The message is encrypted using a cipher algorithm. The user who is not authorized may also attempt to view the data. The study is done to see whether the security of the encryption against unauthorized access is sufficient. The study of cipher cracking is known as cryptanalysis, and cryptanalysts work to undermine the security of cryptographic systems.

It is possible to send cipher-text across an open communications channel. Eavesdroppers who could have access to the cipher-text will ideally be unable to decipher the communication due to its encrypted nature. The communication can only be decrypted, retrieved, and read in plaintext by the intended receiver, who also has the correct key. Cheng-Kang Chu, Jianying Zhou, Wen-Guey Tzeng, Sherman S. M. Chow, In this essay, the

writers discuss how a key concern with cloud storage is how to safeguard users' personal information. Cryptographic techniques are becoming more adaptable with more mathematical tools, and often use many keys for a single application.

I discuss how to "compress" secret keys in public-key cryptosystems that allow delegation of secret keys for various cipher text classes in cloud storage in this post. The delegate may always get an aggregate key of a fixed size, regardless of which class is chosen from the power set of classes. Compared to hierarchical key assignment, which can only save space if all key holders have the same set of rights, our method is more adaptable. Boyang Wang, Hui Li, Ming Li, and Sherman S. M. Chow.

In this study, the authors provide what they see as the best strategy for achieving data anonymity while preserving the integrity of the data, which can be independently verified by the public. Through the employment of a security mediator, their methodology decouples the anonymous protection mechanism from the process for possessing proven data. Their approach reduces the middleman's computational and bandwidth requirements while simultaneously reducing the confidence that is put in it in terms of data privacy and identity privacy. Empirical evidence is also presented to support our system's effectiveness. Jie Zhou, Songzhu Mei, Zhiying Wang, Yong Cheng, Jiangchun Ren, This study introduces a unique method called attributes union for encouraging the use of the CP-ABE algorithm in cryptographic access control systems. I can cut down on the amount of components in ciphertext and private secret keys thanks to attributes unionizing. Additionally, by unionizing characteristics, I can minimize the computational and storage expense to a constraint. Other CP-ABE algorithms that are already in use may be modified using the characteristics union. Since the quantity of characteristics only has a little impact on it, attributes union is quite advantageous to us. R. Saravanan, Ashish Agarwala,The algorithm's operation depends on the well chosen specification of the parameters. The values of p and q should be such that the modulus n is very big. B and R's values should be chosen such that br is much less than n. B and r should both be significantly less than (n) in order for br to be smaller than n. Hu Xiong, Fengli Zhang, and Qinyi Li Here, they compare and analyze the effectiveness of a few revocable ABE systems that are currently in use.

They developed a prototype application in this study to provide the proof of concept of a security method put out by Stolfo et al. The security system focuses on thwarting attempts at insider data theft. By combining two technologies, this is accomplished. User profile management and offensive decoy technology are two terms for them.

Together, these two strategies might thwart attempts at insider data theft. The maintenance of user profiles makes sure that the navigational habits and behavior of authorized users are observed. The decoy technique enables the program to store fake or decoy information in the file system to trick attackers attempting to steal insider data. Decoy information attracts malevolent insiders when they break into the cloud file system.

Table 1: Different types of Concept

Title of the Paper	Authors	Year/ISSN No./Volume Number	Proposed Concept and Details
Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage	Cheng Kang Chu, S.S.M.Chow	February 2014/Vol 25/ No. 2	A new public- key cryptosystems that produce constant-size ciphertext with private keys to decrypt
Storing Shared Data on the Cloud via Security-Middleman	B. Wang, S.S.M. Chow, M. Li, H. Li	(ICDCS)/2013	Security middleman which is able to generate verification signatures for data owners.
Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control	Yong Cheng, Jiangchun Ren, Zhiying	Vol I /Nov 2012/180-186	A novel technique namedn *attributes union*, which can integrate a certain number of attributes into an attributes union
A Public Key Cryptosystem Based on Number Theory	Ashish Agarwala, R.Saravanan	April 2012 /238-241	It is based on number theory and exploits the features of computation - ally hard problems, namely integer factorization, discrete logarithmic problem to name a few.

Proposed Work

Key aggregation policies are used in contemporary cryptography to increase the decryption of a key's strength by enabling the decryption of numerous cipher texts without growing the key's size. a particular kind of key-aggregate cryptosystem used for public-key encryption.

Users of KAC encrypt messages using both a public key and a class-based ciphertext identification. The master-secret key is a master-secret that belongs to the key owner and may be used to get secret keys for different classes. More importantly, the extracted key may be an aggregate key that, while still being as small as a secret key for a single class, aggregates the decryption strength of several such keys, or any subset of ciphertext classes.

In our KAC schemes, the sizes of the ciphertext, public key, master secret key, and aggregate key are all fixed. Only a tiny portion of the public system parameter, which has a size linear in the number of ciphertext classes, is required each time, and it may be retrieved on demand from a large cloud storage facility.

The data owner creates a public/master-secret key pair using KeyGen and sets up the public system parameter using Setup. Anyone who chooses the ciphertext class that corresponds to the plaintext message to be encrypted may encrypt messages using the Encrypt command.

The owner of the data may use Extract to build an overall decryption key for a number of ciphertext classes using the master-secret. Delegates may get the produced keys safely (using secure email or secure devices). Last but not least, any user with an aggregate key may decode any ciphertext through decode given that the class of the ciphertext is present in the aggregate key.

User Behavior Profiling

By keeping an eye on how data is being accessed in the cloud and seeing odd tendencies, A well-known technique that may be used in this case to simulate how, when, and how often a user accesses their information on the Cloud is called user profiling. where use is constantly monitored to see whether unusual access to a user's data is taking place.

Applications for fraud detection often use this technique of behavior-based security. Such profiles would materially include substantial information, such as how many and how often papers are generally viewed. The connection of search behavior anomaly detection with trap-based decoy files should give greater proof of wrongdoing and so increase a detector's cleanness. I check for anomalous search behaviors that indicate deviations from the user baseline.

Decoy Technology

Technology used as a decoy is that which gives false information to an attacker or unauthorized user. Technologies used as decoys, such as honeypots or the producing. The system requests the meaningless data files to conduct an attack

on the attacker. By using this strategy, the original data is altered in an unanticipated way, making it hard to filter the data or document again.

The term "decoy" refers to the relative false information about the relevant data documents.

This method primarily maintains a few dummy data files in the customer's database as a component of his database. Since the fake files are in the same user's database, the attacker cannot distinguish between the real and fake documents. Since the hacker will keep attacking user data documents, there will be direct links to sites that employ fog computing.

Therefore, the attacker is receiving more fake papers than usual. As the attacker downloads the fake data, he becomes uncertain about whether data is the real target data. But since every document is a fake, the actual data is protected against dangerous insider attacks.

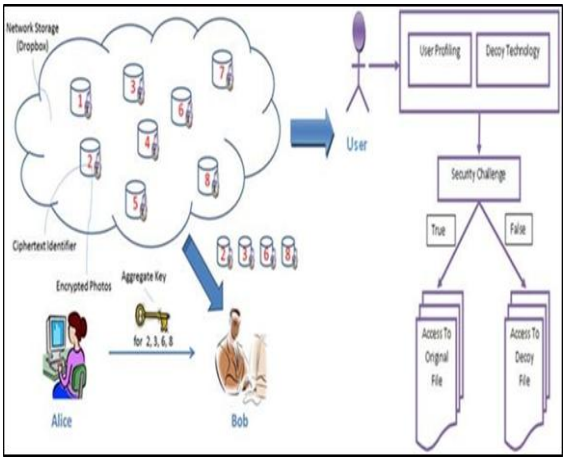

Figure 1: System Architecture

Conclusions

Combining ciphertext and the aggregate key encryption provides very secure attack prevention. Key distribution can be simply controlled and perfectly secure. The use of numerous keys for a single application is becoming increasingly common in access control and cryptography techniques. Compared to previous key assignment methods that can merely store data, the approach is more versatile.

References

[1] Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, Senior Member, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," IEEE Transaction on Parallel and Distributed System, Vol. 25, NO. 2, February 2014.

[2] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Middleman," Proc. IEEE 33rd "Inl t Conf. Distributed Computing Systems (ICDCS), 2013.

[3] Yong Cheng, Jiangchun Ren, Zhiying Wang, "Attributes Union in CP-ABE Algorithm for Large Universe Cryptographic Access Control," Second International Conference on Cloud and Green Computing,pp.180-186, Nov 2012.

[4] Ashish Agarwala, R Saravanan, "A Public Key Cryptosystem Based on Number Theory" Recent Advances in Computing and Software System (RACSS), pp. 238-241, April 2012.

[5] Fengli Zhang, Qinyi Li, Hu Xiong, "Efficient Revocable Key-Policy Attribute Based Encryption with Full Security," Eighth International Conference on Computational Intelligence and Security,pp. 477- 481,Nov 2012.

[6] P.Jyothi1, R.Anuradha2, Dr.Y.Vijayalata3, "Minimizing Internal Data Theft in Cloud Through Disinformation Attacks," International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.

[7] G.Jai Arul Jose, C.Sajeev, "Implementation of Data Security in Cloud Computing",International Journals of P2P Network Trends and Technology, Vol. 1, Issue 1, 2011.