ISSN: 2348-2079 Volume-10 Issue-3

International Journal of Intellectual Advancements and Research in Engineering Computations

SECURE AUTHENTICATION IN CLOUD BIG DATA WITH HIERARCHICAL ATTRIBUTE AUTHORIZATION STRUCTURE

[1*]M. KANAGA, [2]Dr. S. JAYANTHI, [3]S. SIVAGAMI

[1]PG Scholar, Department of C.S.E, Tagore Institute of Engineering and Technology, Attur, Tamilnadu, India
[2]Principal, Tagore Institute of Engineering and Technology, Attur, Tamilnadu, India
[3]Head of the Department, Department of C.S.E, Tagore Institute of Engineering and Technology, Attur, Tamilnadu, India

Corresponding Author: M. Kanaga
Email: kanagacse2022@gmail.com

ABSTRACT

Organizations must handle and store huge data in the cloud due to the rising demand for it. Since the cloud cannot be completely trusted and anyone can access it, the data therein may be exposed. In this work, i provide a hierarchical attribute authorization structure for a safe cloud large data authentication system. Our suggested method makes use of a tree-based signature to significantly boost the security of attribute authorisation. To suit the needs of big data, i improve the suggested authentication system to allow for multiple levels in the hierarchical attribute permission structure. Security study shows that our protocol can withstand forgery and replay attacks. Additionally, our protocol can safeguard the entities' privacy. I can show that, as compared to earlier studies, our technique has lower computational and communication overhead.

Keywords: Third Party Authority, Trusted Mechanism, Tree Based Mechanism

1. INTRODUCTION

Cloud computing is a complete new technology. It is the development of parallel computing, distributed computing grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). Cloud is a metaphor to describe web as a space where computing has been pre installed and exist as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared IT resources through the Internet. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interactions with service providers. Cloud computing can much improve the availability of IT resources and owns many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode; this would benefit and save the cost to buy the physical resources that may be vacant.

1.1 ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed in the cloud; concerns are beginning to grow about just how safe an environment is. Issues of cloud computing can summarize as follows:

A.Privacy

Cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data centers rather than stay in the same physical location, users may leak hidden information when they are accessed cloud computing services. Attackers can analyze the critical task depend on the computing task submitted by the users.

B. Reliability

The cloud servers also experience downtimes and slowdowns as our local server. C. Legal Issues Worries stick with safety measures and confidentiality of individual all the way through legislative levels.

D. Compliance

Numerous regulations pertain to the storage and use of data requires regular reporting and audit trails. In addition to the requirements to which customers are subject, the data

centers maintained by cloud providers may also be subject to compliance requirements.

E. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

Long- Term Viability

You should be sure that the data you put into the cloud will never become invalid even your cloud computing provider go broke or get acquired and swallowed up by a larger company.

1.2 SECURITY AND PRIVACY ISSUE

Cloud computing can provide infinite computing resources on demand due to its high scalability in nature, which eliminates the needs for Cloud service providers to plan far ahead on hardware provisioning. Many companies, such as Amazon, Google, Microsoft and so on, accelerate their paces in developing cloud computing systems and enhancing its services providing to a larger amount of users. this paper investigate's the security and privacy concerns of current cloud computing systems provided by an amount of companies. As cloud computing refers to both the applications delivered as services over the Internet and the infrastructures (i.e., the hardware and systems software in the data centers) that provide those services. Based on the investigation security and privacy concerns provided by companies nowadays are not adequate, and consequently result in a big obstacle for users to adapt into the cloud computing systems. Hence, more concerns on security issues, such as availability, confidentiality, data integrity, control, audit and so on, should be taken into account.

1.2.1 Cloud Security

Security remains the biggest barrier preventing companies from entering into the cloud. Security is a continuous consideration in IT-related projects. Unlike many other traits in technological contexts, security is notoriously hard to quantify or even compare qualitatively. For this reason, security evaluation of cloud offerings will mostly hinge on company reputation and, eventually, real-world track records – but even real world track records are difficult to compare between companies, because security breaches may not be publicly disclosed unless compelled by regulation. Like SLAs, companies might specify contractual compensation for certain kinds of provider negligence leading to security failures, but such provisions may be worth very little since security failures are not as easily observable as service availability failures. Businesses using cloud services want to ensure that their data is secure from both external attackers as well as internal snoopers (employees of the cloud provider). Although data theft and snooping is mitigated by properly encrypting data to be stored within the cloud, encryption cannot prevent denial-of-service attacks such as data deletion or corruption. Some early research users of Amazon S3 suggest, "users should employ some kind of data authentication technology to assure themselves that data returned by S3 is the same as the data that was stored there. Technology such as an HMAC or a digital signature would protect users from both accidental data modification by Amazon and from malicious modification by third parties who managed to crack a password or intercept a password reset email message". Service integrity is another security issue: businesses want to ensure their running services are not subject to denial-of-service attacks or hijacked. The latter can be very insidious, as a third party might (for example) gain control of a business's e-commerce site and besmirch its reputation. This situation is the digital equivalent of identity theft. Isolation is a related concern – cloud providers serve many customers and they all share common hardware and infrastructure. Although resource virtualization prevents customers from having to explicitly coordinate resource sharing, the cloud provider must ensure that multiple customers do not interfere with each other, maliciously or otherwise.

1.2.2 Security on Demand

Cloud services are applications running somewhere in the cloud computing infrastructures through internal network or Internet. Cloud computing allows providers to develop, deploy and run applications that can easily grow in capacity (scalability), work rapidly (performance), and never (or at least rarely) fail (reliability), without any concerns on the properties and the locations of the underlying infrastructures.

Availability

The goal of availability for cloud computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. As its web-native nature, cloud computing system enables its users to access the system (e.g., applications, services) from anywhere. This is true for all the cloud computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). Required to be accessed at any time, the cloud computing system should be severing all the time for all the users (say it is scalable for any number of users). Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the cloud system or applications hosted on it.

2) Confidentiality

It means keeping users' data secret in the cloud systems. There are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, which are extensively adopted by the cloud computing vendors.

3) Data integrity

In the cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data are the base for providing cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task.

4) Control

In the cloud system means to regulate the use of the system, including the applications, its infrastructure and the data.

5) Audit

It means to watch what happened in the cloud system. Auditability could be added as an additional layer in the virtualized operation system (or virtualized application environment) hosted on the virtual machine to provide facilities watching what happened in the system. It is much more secure than that is built into the applications or into the software themselves, since it is able watch the entire access duration.

1.3 Techniques to secure data in cloud

Authentication and Identity:

Authentication of users and even of communicating systems is performed by various methods, but the most common is cryptography [8]. Authentication of users takes place in various ways like in the form of passwords that is known individually, in the form of a security token, or in the form a measurable quantity like fingerprint. One problem with using traditional identity approaches in a cloud environment is faced when the enterprise uses multiple cloud service providers (CSPs) [8]. In such a use case, synchronizing identity information with the enterprise is not scalable. Other problems arise with traditional identity approaches when migrating infrastructure toward a cloud-based solution.

2. SYSTEM ANALYSIS

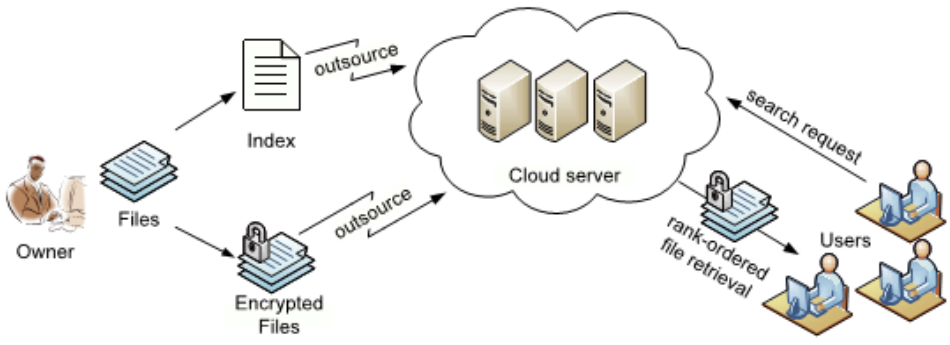
2.1 EXISTING SYSTEM

In researchers exploit multiple authorities to manage and distribute attributes. Yang et al. proposed the data access control scheme for multi-authority in cloud storage, which can support attributes revocation and provide both forward security and backward security. Ruj et al. in proposed the decentralized access control scheme, which can provide anonymous authentication for users while resisting replay attacks and supporting data creation, data modification, reading data stored and user revocation. Besides, Ruj et al.'s scheme is decentralized, which is different from other centralized access control schemes. In, Yang et al. proposed a scheme that supports efficient access control with dynamic policy updating. Because the previous encrypted data and old access policies can be used to achieve dynamic operations, it can prevent the transmission of new encrypted data, which saves much computation resource for data owners. The decryption of the CP-ABE based access control scheme is not efficient and flexible, so most of access control schemes are not suitable for the cloud to realize the distributed access control. In security communities, the technology of the lowest density maximum distance separable (LD-MDS) can greatly improve the efficiency of the decryption. Note that Huang et al. in exploited LDMDS to design a fully distributed, scalable and effective data access control scheme. Almost of cloud data access control schemes focus on the data privacy and access control, but the privilege control and identity privacy are ignored. In order to make up for this deficiency, Jung et al. In presented a semi anonymous privilege control scheme, which can not only protect the data privacy, but also ensure that a user's identity will not be compromised.

2.2 PROPOSED SYSTEM

In this section, our protocol is presented in detail. The protocol in the structure of two levels is firstly presented, which is designed for a common structure of the hierarchical attribute authorization. In order to meet usage requirements in real-world big data applications, the protocol is then extended to support multiple levels of the hierarchical structure . The Two-Level Structure, In the two-level attribute authorization structure, the TRA is in the first level and users are in the second level. That means the TRA can distribute attributes to users directly hence, in our authentication protocol, the TRA needs to authenticate the arbitrary user who wants to obtain attributes from the TRA. In the signature scheme, the user encrypts his/her data to construct a signature and sends the signature to another user. After the receiver receives the signature, he/she can verify the signature's validity. Actually, the verification processes of the signature can provide the identity authentication. Through checking the validity of received security parameters, the verify can determine whether the sender is the authorized client or not. In this paper, with the aid of the tree-based signature, design the protocol to authenticate users or DAs. In the two-level structure of the hierarchical attribute authorization, the TRA needs to authenticate all its child users. Here, user j denotes the child of the TRA. Our protocol is consisted of three phases: KeyGen, SigGen and Verify.

3.ARCHITECTURE DIAGRAM



4. IMPLEMENTATIONMODULES

4.1 Cloud Group Construction

This module, allocates Identity numbers to each and every user while registering into our group. I can collect information regarding the users present in the group. i can also send and receive files from the user in our group or individual. An individual or group entity, which owns its data stored in the cloud for online data storage and computing. Different users may be affiliated with a common organization, and are assigned with independent authorities on certain data fields.

4. 2 Duplication Identification

In this module, the design of an attribute-based storage system supporting secure deduplication of encrypted data in the cloud, in which the cloud will not store a file more than

once even though it may receive multiple copies of the same file encrypted under different access policies. If same file is uploaded to cloud from different user file will be eliminated and it protects from wastage of storage. Attribute based encryption algorithm is used to encrypt user data which will provide a hash value that is unique for each and every file. If same file is uploaded again by the user it will identified efficiently through the parameters like name, size, type and content within the file.

4.3. Attribute Authority

The AA issues every user a decryption key associated with his/her set of attributes. The cloud consists of a public cloud which is in charge of data storage and a private cloud which performs certain computation such as tag checking. When sending a file storage request, each data provider firstly creates a tag T and a label L associated with the data, and then encrypt the data under an access structure over a set of attributes.

4.4 File Decryption

At the user side, each user can download an item, and decrypt the cipher text with the attribute-based private key generated by the AA if this user's attribute set satisfies the access structure. Based on access policy, user requested key through AA is received by verifying its access policy by data provider. Then data provider will transmit the key to respective user and particular user will decrypt the downloaded file using secret key. Here, the search from user side was performed based on content based search. The keyword entered by user will be taken as query and search the content not alone based on file name it will also search based on keyword that are available within the content of the file.

5. CONCLUSION

I offer a safe authentication method for hierarchical attribute permission n structures that is based on trees and inspired by signatures. Our approach is applicable to hierarchical attribute authorization with multiple levels as well as the typical scenario of a two-level structure. Our protocol has the property of privacy preservation and is resistant to forgery and replay attacks, according to the security study. With regard to performance analysis, i contrast our methodology with the HASBE. Based on the findings of simulations, our method has a lower computational and communication overhead, indicating that it will likely have a successful future in safe authentication for cloud huge data.

6. FUTURE WORK

In further research, we intend to focus on making the CP-ABE algorithm simpler and more efficient along with making it even more suitable for access control in a cloud environment.

7. REFERENCES

1. United N. World urbanization prospect. United Nations; 2014 [online]. Available from: http://dl.acm.org/citation.cfm?id=308574.308676.
2. Hossain MS. Cloud-supported cyber-physical localizationframework for patients monitoring. IEEE Syst J. March 2017;11(1):118-27. doi: 10.1109/JSYST.2015.2470644.
3. Hossain MS, Muhammad G, Abdul W, Song B, Gupta B. 'Cloud-assisted secure video transmission and sharing frameworkfor smart cities,' Elsevier, Future Generation Computer SystemsJournal; April 2017.
4. Liao J, Stankovic L, Stankovic V. Detecting household activitypatterns from smart meter data. In: Intelligent environments (IE) International Conference on. Vol. 6; 2014. p. 71-8.
5. Yassine A, Nazari Shirehjini AAN, Shirmohammadi S. Smartmeters big data: Game theoretic model for fair data sharing inderegulated smart grids. IEEE Access. 2015;3:2743-54. doi: 10.1109/ACCESS.2015.2504503.
6. Yassine A, Shirmohammadi S. Measuring users' privacypayoff using intelligent agents. IEEE Int Conferenceon Comp Intell Meas Syst andApplications, May 2009. 2009:169-74.
7. A business privacy model for virtual communities. IndersciencePublishers Int J of web based communities,vol. 2009;5.
8. Chen YC, Hung HC, Chiang BY, Peng SY, Chen PJ. Incrementally mining usage correlations among appliances insmart homes. In: Network-Based Information Systems (NBiS), 201518th International Conference on. Vol. 9; 2015. p. 273-9.
9. Jack K, William K. The UK-DALE dataset, domesticappliance-level electricity demand and whole-house demand from five UK homes. Sci Data. 2015;2, no. 150007.
10. Clement J, Ploennigs J, Kabitzsch K. Detecting activities of daily living with smart meters. Germany: Springer. Vol. 11. p. 143-60 [online]; 2014,ch. Advance Technology and Societal Change,. Available from: https://link.springer.com/chapter/10.1007/978-3-642-37988-8 10.
11. Ni Q, Garca Hernando AB, de la Cruz IP. Theelderlys independent living in smart homes: A characterizationof activities and sensing infrastructure survey to facilitateservices development. Vol. 15(5). p. 312-11 362,2015 [online], P. 11. Sensors. Available from: http://www.mdpi.com/1424-8220/15/5/11312Fig.
12. Chalmers C, Hurst W, Mackay M, Fergus P. Smart meterprofiling for health applications. Int Joint Conferenceon Neural Netw (IJCNN), July 2015. 2015:1-7.
13. Hossain MS. A patient's state recognition system for health careusing speech and facial expression. Springer J Medsyst. December 2016;40(12):1-272:8, P. 272.
14. Hossain MS, Muhammad G. Cloud-assisted industrial internetof things (iot)-enabled framework for health monitoring. Elsevier Comput Netw. June 2016;101:192-202.
15. Pouladzadeh P, Kuhad P, Peddi SVB, Yassine A, Shirmohammadi S. Mobile cloud based food calorie measurement," in2014 IEEE International Conference on Multimedia and Expo Workshops(ICMEW), July 2014, pp. 1-6.