International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-028 PAGE NO: 146-149

A Serial Based Encryption for Enhanced Access Control in Cloud Computing

M.SUGANYA
PG IN COMPUTER SCIENCE AND ENGINEERNG
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM,DINDIGUL DT),INDIA
suganya.mku12@gmail.com

H.PRABHA

ASSISTANT PROFESSOR IN COMPUTER SCIENCE AND ENGINEERNG
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM,DINDIGUL (DT),INDIA

Abstract— ***Cloud storage allows us to enjoy the on demand cloud application without any hardware implementation. Cloud provides the service a required by the cloud user in a rental basis. Even though the cloud issues the cloud application without any physical implementation results in a security risk since the cloud data can be accessed by everyone.When requested data from the user is retrieved from CSP, Organization needs to secure their data & CSP. Access to CSP should be flexible so that it can adapt the different conditions easily. To maintain data integrity on CSP, Attribute based encryption (ABE) with KP-ABE and CP-ABE can be used with access control implementation for cloud computing. But these schemes also lack of scalability and flexibility*** **.Cloud computing is an advanced emerging technology. In this world the storage of data is a big headache for all. Cloud computing is an efficient solution for the easiest and fastest storage and retrieval of data.**

INTRODUCTION

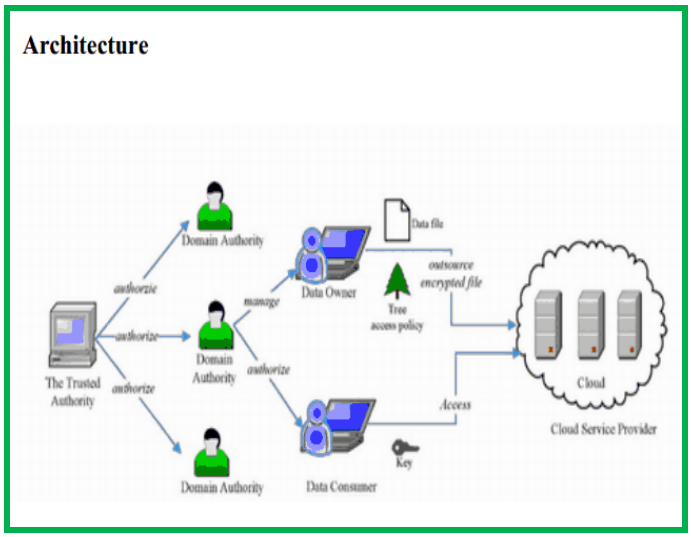
On the need of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption scheme with a fine-grained access control to encrypt outsourced data. Hierarchical Attribute Based Encryption, as one of the most promising encryption systems in this field, allows the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. The hierarchical Attribute Set-Based Encryption (HASBE) scheme is for accessing control in cloud computing and extended the cipher text policy attribute set based encryption. Hierarchical Attribute Based Encryption security for data's based on public key and master key with the help of Domain Authority Check. paragraphs must be

Published by SK Research Group of Companies (SKRGC).

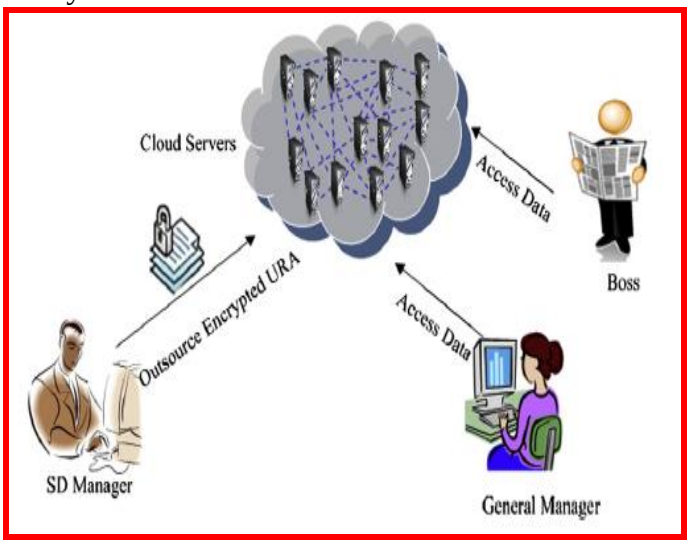
International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-028 PAGE NO: 146-149

indented. Emerging computing paradigm, enables users to remotely store their data in a cloud, so as to enjoy services on-demand. Migrating data from the user side to the cloud offers great convenience to users, since they can access data in the cloud anytime and anywhere, using any device, without caring about the capital investment to deploy the hardware infrastructures.

I. Architecture



Company A pays a CSP for sharing corporate data in cloud servers. Suppose the sales department(SD), the research and development department (RDD), and the finance department (FD) are collaborating in Project X. The SD manager wants to store an encrypted user requirement analysis (URA) in the cloud, so that only the personnel that have certain certificates can access the document. This cloud computing has a lot of advantages especially in ubiquitous services where everybody can access computer services through internet. With cloud computing, you can develop a device which contains a small display, processor and RAM. There is no need of other hardwares such as secondary memory. It will reduce the size of our new technology devices. Also it reduces the expences of our system.



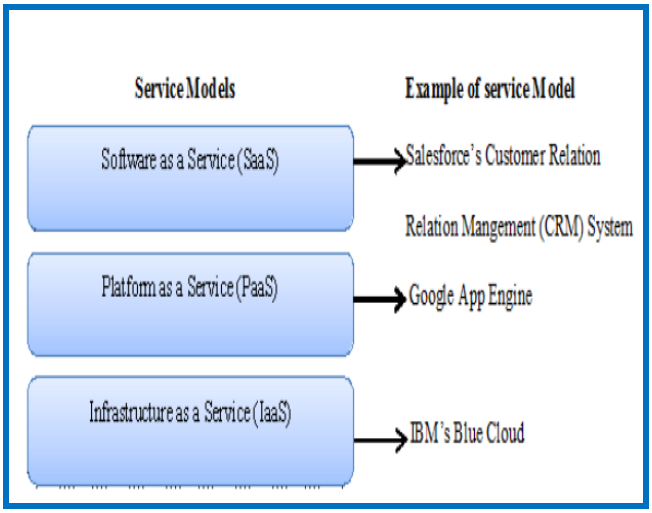
Cloud computing incorporates virtualization, on-demand deployment, Internet delivery of services, and open source software [1].
The following figure shows the cloud computing model.

a) SaaS- To use the provider's applications running on a cloud infrastructure and accessible from various client devices through a thin client interface such as a Web browser.

b) PaaS- To deploy onto the cloud infrastructure consumer-created applications using programming languages and tools supported by the provider (java, python, .Net)

c) IaaS- To provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-028 PAGE NO: 146-149



The trusted authority acts as the root of trust and authorizes the top-level domain authorities. A domain authority is trusted by its subordinate domain authorities or users that it administrates, but may try to get the private keys of users outside its domain. Users may try to access data files either within or outside the scope of their access privileges, so malicious users may collude with each other to get sensitive files beyond their privileges. The trusted authority is responsible for generating and distributing system parameters and root master keys as well as authorizing the top-level domain authorities. A domain authority is responsible for delegating keys to subordinate domain authorities at the next level or users in its domain. Each user in the system is assigned a key structure which specifies the attributes associated with the user's decryption key.

(1) High performance. In the cloud-computing environment, users may access data anytime and anywhere using any device. When a user wants to access data using a thin client with limited bandwidth, CPU, and memory capabilities, the CP-ABE scheme should be of high performance. That is, the communication costs and computation costs introduced by the CP-ABE scheme should be low enough, so that the user can successfully retrieve data from the cloud, and then decrypt it using the thin client.

(2) Full delegation. In a large-scale enterprise with many employees, each employee needs to request secret keys from the attribute authority (AA), when he joins the enterprise. If all these employees require their secret keys from one AA, there will be a performance bottleneck on the AA. To reduce the workload on the AA, some CP-ABE schemes provide key delegation between users, which enables a user to generate attribute secret keys containing a subset of his own attribute secret keys for other users. However, a full delegation mechanism, which can embody the hierarchical structure in the enterprises, is more applicable to the environment of enterprises outsourcing data in a cloud. Full delegation means key delegation between AAs, where each AA independently makes decisions on the structure and semantics of its attributes.

(3) Scalable revocation. In the case of a large-scale enterprise with a high turnover rate, a scalable revocation scheme is a must. That is, the enterprise can revoke data access rights from users once they are no longer its employees. A user whose permission is revoked will still retain the keys issued earlier, and thus can still decrypt data in the cloud. The traditional revocation scheme usually requires the AAs to periodically re-encrypt data, and re-generate new secret keys to remaining authorized users. This approach will cause heavy workload don the AAs. A more scalable approach is to take advantage of the abundant resources in a cloud by allowing the AAs to delegate the CSP to re-encrypt data and re-generate keys to users, under

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 2, No 5, 2013. ISSN: 2348-6600
Reference ID: IJCS-028 PAGE NO: 146-149

the environment that the CSP knows nothing about the data and keys.

Conclusions

Cloud computing is a model where user access computing resources and applications being delivered in the internet cloud remotely. A cloud service provider is an entity in cloud computing which take data from the users so that data will be stored & utilized for a variety of applications including various areas like business. An organization needs not only to secure their data & Cloud service provider but also it should provide flexible access to CSP so that it can adapt the different conditions easily. It is a highly efficient model for provide access control in cloud computing. It is in a hierarchical structure and it using a clock for providing decryption key based on time. This model ensure both security and access control in cloud computing. The HASBE scheme contains hierarchical structure of system user in which ASBE encryption algorithm is implemented. HASBE not only supports compound attribute set but also provides flexibility in attribute combination.

ACKNOWLEDGMENT

I am greatly indebted to my parents and department faculties for their great encouragement and co-operation in all aspects to develop this paper.

I wish to thank everyone who helped us directly or indirectly for the successful completion of this paper.

REFERENCES

1) Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers Guojun Wanga,*, Qin Liu a,b, Jie Wub, Minyi Guo c
2) Scalable Access Control in Cloud Computing Using Hierarchical Attribute Set Based Encryption (HASBE). **A.Vishnukumar, G.Muruga Boopathi, S.Sabareessh. International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.**
3) **Access control in cloud computing, Bibin K Onankunju,** International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013 ISSN 2250-3153.
4) Hierarchical CP-ASBE Scheme in Cloud Computing for fine-Grained Access Control with Scalability and Flexibility **V. S. Dhumal Prof. D. N. Rewadkar , Volume 3, Issue 11, November 2013 ISSN: 2277 128X.**
5) A Serial Based Encryption for Enhanced Access Control in Cloud Computing **N.Pandeeswari, P.Ganesh Kumar, P.C.Rubini. International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.**

Published by SK Research Group of Companies (SKRGC).