ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 5, Issue 4, April 2018

Data Privacy in Cloud

[1] Sree Aswini.J, [2] Kavitha Juliet

[1] M.Tech, 4th Sem Dept of Computer Science &Engineering RYMEC college, Ballari, India

[2] Assistant Professor, Dept of Computer Science and Engineering, RYMEC college, Ballari, India

Abstract: **- Cloud Computing provides the services to the users for storing the data moved into the cloud securely. Small and medium organisations are nowadays giving least importance to the IT infrastructure and instead moving their data and information to the cloud. To provide secure access to the data moved into the cloud by Data privacy in cloud. This approach uses the cryptographic ways to encrypt the data which is being stored into the cloud by the owners of the data. The data is secure because the access to the data is being given by the owner any of other users to decrypt the data. Without the owner permitting the access to the data, any other user cannot access the data. So, by using the Data privacy in cloud approach, data uploaded to the cloud is much more secure.**

Keywords **:- Cryptography, Role-based access control, Data-centric solution, Proxy re-encryption, Private key generator.**

I. INTRODUCTION

Cloud computing is in demand nowadays due to it’s advantageous characteristics. People nowadays are very much dependent on the cloud as the information can be accessed from multiple devices, being hands free over storage devices such as pen drive,hard disk etc. Important documents are being stored on the cloud by the users as it is very much easy to be searched. Cloud Computing is receiving much importance from the organisations, academic and industrial communities. The organisations are focusing less on the IT infrastructure and giving much importance to the cloud storage due to its flexibility and accessibility. Cloud Computing is mainly designed for providing the services to the users. The services provided by the cloud to the user are memory, processor, storage and bandwidth are visualised. The technologies included in the cloud computing are service oriented architecture, web 2.0, virtualisation and more. By above mentioned qualities and facilities Cloud Computing provides the efficient services to the small and medium organisations by reducing the cost in purchasing and maintaining the infrastructure. Even though Cloud computing has many security issues, the organisation needs cloud for their abundant resources. This paper defines the implementation of the data security with the help of four modules, they are: i) Proxy Re-encryption and Identity based encryption. ii)Authorization Model with Enriched Rolebased Expressiveness. iii)self-Protected authorisation Model for Data -centric security. iv)Data-Centric solution for Data protection in the cloud.

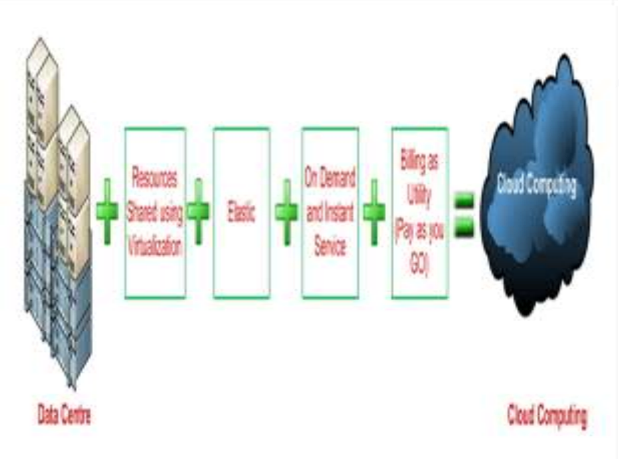

Resources Shared using Virtualization
Elastic
On Demand and Instant Service
Billing as Utility (Pay as you GO)
Cloud Computing
Data Centre
Cloud Computing

Fig. 1: Schematic definition of cloud computing [1]

Cryptography is used in Data privacy in cloud when the data is moved to the cloud. Authorization model is being protected by the advanced cryptographic techniques to avoid unauthorised access to the data. This solution is being based on the Proxy Re-Encryption(PRE). A PRE scheme enables an entity called proxy to re-encrypt data from one key to another that cannot be decrypted. As the management of security and access control would be complex,in distributed systems like cloud computing. Authorization models help in the regulation of security and deal with the complexity. Administrators are aid with the task of enabling the specification of high level access control rules are interpreted to the system. The most supported authorisation scheme is Role-Based access Control(RBAC).

The authorisation model decides the privileges that are provided to the subjects. Access request is being cross-checked by the cloud service provider to ensure that the request is being permitted or not. Data-Centric solution for the data security in cloud is done when the data is being moved to the cloud a self-protected package will be produced by the data owner. This package contains authorisation rules, encrypted data objects and corresponding re-encryption keys.

II. LITERATURE SURVEY

Cloud computing changed the world around us. Now people are moving their data to the cloud since data is getting bigger and needs to be accessible from many devices. Therefore, storing the data on the cloud becomes a norm. However, there are many issues that counter data stored in the cloud starting from virtual machine which is the mean to share resources in cloud and ending on cloud storage itself issues. In this paper, we present those issues that are preventing people from adopting the cloud and give a survey on solutions that have been done to minimize risks of these issues. For example, the data stored in the cloud needs to be confidential, preserving integrity and available. Moreover, sharing the data stored in the cloud among many users is still an issue since the cloud service provider is untrustworthy to manage authentication and authorization. In this paper, we list issues related to data stored in cloud storage and solutions to those issues which differ from other papers which focus on cloud as general[1].

It is well-known that cloud computing has many potential advantages and many enterprise applications and data are migrating to public or hybrid cloud. But regarding some business-critical applications, the organizations, especially large enterprises, still wouldn’t move them to cloud. The market size the cloud computing shared is still far behind the one expected. From the consumers’ perspective, cloud computing security concerns, especially data security and privacy protection issues, remain the primary inhibitor for adoption of cloud computing services. This paper provides a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then this paper discusses some current solutions. Finally, this paper describes future research work about data security and privacy protection issues in cloud[2].

Cloud computing is a new computational paradigm that offers an innovative business model for organizations to adopt IT without upfront investment. Despite the potential gains achieved from the cloud computing, the model security is still questionable which impacts the cloud model adoption. The security problem becomes more complicated under the cloud model as new dimensions have entered into the problem scope related to the model architecture, multi-tenancy, elasticity, and layers dependency stack. In this paper we introduce a detailed analysis of the cloud security problem. We investigated the problem from the cloud architecture perspective, the cloud offered characteristics perspective, the cloud stakeholders’ perspective, and the cloud service delivery models perspective. Based on this analysis we derive a detailed specification of the cloud security problem and key features that should be covered by any proposed security solution[3].

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. In contrast to tradi- tional solutions, where the IT services are under proper physical, logical and personnel controls, Cloud Computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users’ data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks[4].

The Cloud Computing concept offers dynamically scalable resources provisioned as a service over the Internet. Economic benefits are the main driver for the Cloud, since it promises the reduction of capital expenditure (CapEx) and operational expenditure (OpEx). In order for this to become reality, however, there are still some challenges to be solved. Amongst these are security and trust issues, since the user’s data has to be released to the Cloud and thus leaves the protection- sphere of the data owner. Most of the discussions on this topics are mainly driven by arguments related to organisational means. This paper focusses on techni- cal security issues arising from the usage of Cloud services and especially by the underlying technologies used to build these cross-domain Internet-connected collaborations[5].

III. IMPLEMENTATION

Now, the actual important part of the paper Data privacy in clouds is being reached where the theoretical design of the concept is being turned out into a working system. This is the stage where the successful new system is being achieved which will be given to the user, with confidence that the new system will work effectively than the existing system. This stage of the concept includes careful planning, investigation of the existing system and the constraints on implementation.

A. Proxy Re-Encryption and Identity-based Encryption

In these methods of encryption cryptography is being used to protect the data when moved to the cloud. The authorisation model uses advanced cryptographic techniques in order to avoid the disclosing of data with CSP when not authorised. Proxy Re-Encryption (PRE) is the solution. The cryptographic scheme is the PRE scheme which enables an entity called proxy to re-encrypt data from one key to another without allowing to decrypt it.
The following set of features are needed by proxy Re-Encryption scheme used for the proposal in this paper:
*Unidirectionality: A unidirectional scheme allows the production of a re-encryption key $rk\alpha \longrightarrow_{\beta}$ without allowing re-encryption from β to α.
*Non-interactivity: A non-interactive scheme allows a user uαto construct a re-encryption key $rk\alpha \longrightarrow_{\beta}$ without allowing uβ or any other entity to participate.
*Multi-use: Amulti-use scheme allows the proxy to participate multiple re-encryption operations on a single cipher text .i.e to re-encrypt from uα to uβ, from uβ to cγ and so on.
The following set of functions are provided by IBPRE. It contains the cryptographic primitives:

$$\text{setup}\ (p,k) \longrightarrow (p, msk) \quad (1)$$
$$\text{keygen}\ (p, msk, id) \longrightarrow sk\alpha \quad (2)$$
$$\text{encrypt}\ (p, id\_,m) \longrightarrow c_{\alpha} \quad (3)$$
$$\text{rkgen}\ (p, sk\alpha, id\alpha, id_{\beta}) \longrightarrow rk\alpha \longrightarrow_{\beta} \quad (4)$$
$$\text{reencrypt}\ (p, rk\alpha \longrightarrow_{\beta}, c\alpha) \longrightarrow c_{\beta} \quad (5)$$
$$\text{decrypt}\ (p, sk\alpha, c\alpha) \longrightarrow m \quad (6)$$

B. Authorization Model with Enriched Role based Expressiveness

The regulation of security and access control could be a tougher and error prone task in distributed systems such as cloud computing. The complexity of cloud computing is being sealed by authorisation models with the help of regulation and management of security. The administrators are being employed with the task of enabling the specification of high level access control rules that are automatically interpreted by system. The authorisation scheme supported by most of the authorisation solutions in Role-Based Access control(RBAC).

The authorisation model can be further derived to hierarchical RBAC(hRBAC). Hierarchical RBAC defines the role hierarchies. The hierarchies allow the privilege inheritance between the roles, i.e by making a child role to inherit all the privileges given to the parent roles in the hierarchy. The role management is being simplified by adding role hierarchy to RBAC.

C. Self-Protected authorisation model for Dta-centric security

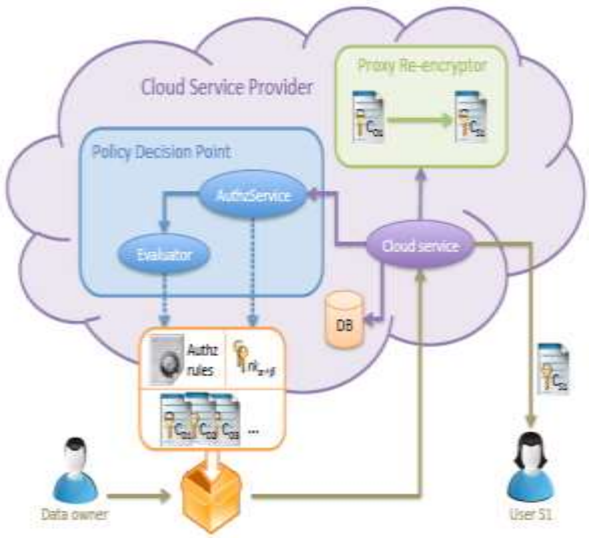
The privileges granted to subject are determined by the authorisation model. Access request will be evaluated by the cloud service provider weather the request to be permitted or not. The data can be potentially accessed by the CSP for its own benefit, if the data is not being protected cryptographically. CSP has to be trusted by the data owner to evaluate the model and enforce the authorisation decision. CSP can override the authorisation rules if it is not protected cryptographically and can give the data access to third party.

i)Protection and authorisation model: The data has to be protected by encrypting to avoid the unauthorised access is known as data-centric access is known as data-centric security. Then, the access control mechanism must regulate who are suppose to decrypt the data and get access to its contents.

ii)Representation and Evaluation: The information is being to construct the path and even in the re-encryption chain. As ontology is a direct representation of the sets and relationships of the secured authorisation model, reasoner derivations are directly mapped to original arts and relations.

D. Data-centric solution for data protection in the cloud

An architecture is being proposed for the development within a CSPs. This architecture considers different elements that needs to be deployed in order to give an overview of how the access to protected data is done in this approach.



when a data is being moved to the cloud, a self-protected package is being generated by the data owner. the package contains: authorisation rules , encrypted data objects and the corresponding re-encryption keys. Data object are being encrypted before moving the data to the cloud in order to prevent the CSP to access them. This can be done by the data owners with the help encrypt() function. Data has to be encrypted using the identity of the object being uploaded o1. Instead of the direct encryption, a digital envelope approach could be used to secure data objects. Authorization rules are being defined by the data owner and is directly mapped into the authorisation model. It’s done by considering the corresponding elements in the binary relations. The following are the conditions which has to hold good to protect the data in the cloud with Data privacy in cloud :

*The CSP should not be able to access the MSK

*The CSP should not be able to access secret keys of authorisation element.

*If a PKG is used, it should be ensued that it will not collude with CSP. labels are often a source of confusion. Try to use words rather than symbols. As an example, write the quantity “Magnetization,” or “Magnetization M,” not just “M.

V. CONCLUSION

Data privacy in cloud provides the security for the data moved into the cloud. Data-centric authorisation solution has been proposed for the protection of data being uploaded into the cloud. Dat privacy in cloud helps in the regulating authorisation of the data moved into the cloud with role-based expressiveness including role and object hierarchies . access control rules are restricted to the CSP being this not only unable to access the data, and even unable to release it to unauthorised parties with the help all the approaches and techniques Data Privacy in cloud provides security to the data moved into the cloud.

REFERENCES

[1] Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current SolutionsSultan Aldossary* Department of Computer Sciences and cypersecurityFlorida Institute of Technology Melbourne, Florida 32901*Prince Sattam Bin Abdulaziz University

[2] Deyan Chen, Hong Zhao,Data Security and Privacy Protection Issues in Cloud Computing.2012 International Conference on Computer Science and Electronics Enginee

[3] Meiko Jensen, Jörg Schwenk, Nils Gruschka and Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing," in IEEE ICCC, Bangalore 2009, pp. 109- 116.

[4] Mohamed Al Morsy, John Grundy, Ingo Müller, “An Analysis of The Cloud Computing Security Problem,” in Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia, 30th Nov 2010.

[5] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, "Ensuring Data Storage Security in Cloud Computing," in Proceedings of the 17th International Workshop on Quality of Service.2009:1-9.