3 Dimensional Security in Cloud Computing

D. A. Kulkarni, Sayali Dadas & Aniket Kakade

Department of Computer, P.V.G's C.O.E.T, Pune, India
E-mail : dineshakulkarni@yahoo.com, sayali.dadas@gmail.com, aniketvkakade@gmail.com

***Abstract* – Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. So it is emerging field because of its performance, high availability, least cost and many others. Besides this companies are binding there business from cloud computing because the fear of data leakage. Due lack of proper security control policy and weakness in safeguard which lead to many vulnerability in cloud computing.**

This paper has been written to focus on the problem of data leakage and proposes a framework works in two phases. First phase which is known as Data classification is done by client before storing the data. During this phase the data is to be categorized on the basis of CIA (Confidentiality, Integrity, and Availability). The client who wants to send the data for storage needs to give the value of C (confidentiality), I (integrity), A (Availability). The value of C is based on level of secrecy at each junction of data processing and prevents unauthorized disclosure, value of I based on how much assurance of accuracy is provided, reliability of information and unauthorized modification is required, and value of A is based on how frequently it is accessible. With the help of proposed formula, the priority rating is calculated. Accordingly data having the higher rating is considered to be critical and 3D security is recommended on that data.

After completion of first phase the data which is received by cloud provider for storage, uses 3Dimentional technique for accessibility. The sensitive proved data will send for storage to cloud provider. According to the concept of 3D user who wants to access the data need to be authenticated, to avoid impersonation and data leakage. Authentication is done by using 2 factor password and OTP. OTP is send to user via message.

Keywords – Cloud security, Data protection, Cost Reduction, Data Storage, Confidentiality, Integrity, and Availability.

I. INTRODUCTION

A. Motivations and background

Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. In contrast to traditional 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. Since it is new, so it require new security issues and face new challenges as well [1]. In last few years it is grown up from just being a concept to a major part of IT industry. Cloud computing widely accepted as the adoption of virtualization, SOA and utility computing, it generally works on three type of architecture and these are: SAAS, PAAS, IAAS. There are different issue and challenges with each cloud computing technology. The various security concerns and upcoming challenges are addressed in [2], [4], and also reviewed in terms of standards such as PCI-DSS, ITIL, and ISO- 27001/27002. Until now there is no such standard is available regarding service or operational functioning, and it's security is a major concern. There are also the architectural security issues which are changing according to various architectural designs functioning over cloud computing [3]. Various surveys are in the market depicting the current scenarios such as the leading US research firm Gartner released a report "Assessing the security risk of cloud computing" in June 2008, this report raises the concern about risk in data storage, data recovery, data privacy, and data integrity [5]. Cloud computing providing services in layered medium, so there must be some SLA (Service Level Agreement) or service management, must be applied over the layers, which eventually increase the confidence of the user. Data security over the cloud also

a major concern and various methodologies are proposed [6], also privacy preserving auditing for the data storage security in cloud computing [7], raising the concern over the privacy related issues in data storage [8], such that no critical information can be intercepted as recently a case happened with Wikileaks, over the security of the data. \Apart from data security, security management, and security risk management frameworks are also proposed [9], [10] addressing risk associated with cloud computing, and activities are planned in such a way ensuring that information is available and protected by applying Deming model or PDCA to curb the risk related to cloud computing security. Cloud computing works in layers as applying policies on these layers provide better security approach to manage the security concerns [11].

Cloud computing has given a new horizon to the data Hosting and deploying services. The most important thing of cloud computing is that it enables customers a new way to increase capacity and add capability to their machines on the go. Proposed framework is complying with data protection and privacy legislation of most of the nations, like in India section 43A of the Information Technology (amendment) Act 2008 .In U.K data protection act 1998 . In the Canada personal information protection and electronic documents act.

B. Model and Problem

Now a day cloud computing make everything flexible and easier but there is another aspect that is what about security? Is cloud computing in current scenario is providing confidentiality, integrity and being regulated by compliance like Data Protection Act. Through cloud computing the resource are centralized, so the exposure factor proportionally increase which results in risk. So it is necessary to put a countermeasure to mitigate the potential risk. According to the survey , some company says that due to cloud computing it become easier for bad guys to focus their effort and breach hundred of thousand of record.[1] There is no security rating system in place for cloud computing, so business users can't rely on third party security mechanism. Risk factor with cloud computing are high because level of security provided by cloud provider are not same.

II. DESIGNED ALGORITHM

Algorithm

1. *Input*: Data, protection ring, D[] array of n integer size. Array C,I, A, S,R of n integer size.
2. *Output*: categorized data for corresponding ring.
3. For i ← 1 to n

   3.1. C [i] = Value of Confidentiality.

   3.2. I [i] = Value of Integrity.

   3.3. A [i] =Value of Availability.

   3.4. Calculate

   S [i] = (C[i] + (1/A[i])*10)/2
4. for j ← 1 to 10

   For k ←1 to n

   IF S [K] = = 1||2||3 then

   R[k] =3 /* ring 3 allotted to D[k]th data.

   IF S [K] = = 4||5||6 then

   R[k] =2 /* ring 3 allotted to D[k]th data.

   IF S [K] = = 8||9||10 then

   R[k] =1 /* ring 3 allotted to D[k]th data.

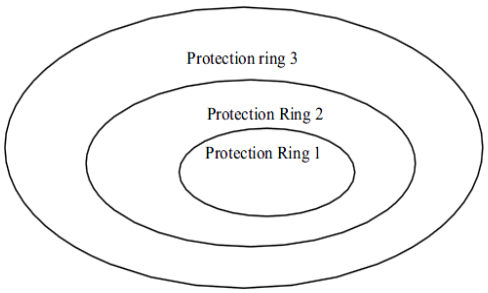


Fig. 1

In the above algorithm first data is classified user giving values for confidentiality, integrity and availability. Here D [] represents data, now the user have to give the value of C – confidentiality I – integrity and A –availability. After Appling proposed formula the value of Crcriticality raring is calculated. Now allocation of data on the basis of Cr is done in protection ring. This suggests that internal protection ring is very critical and it

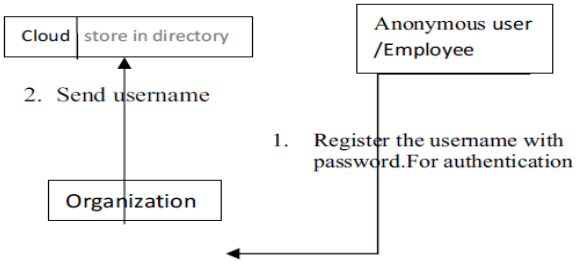


Fig. 2

After classification of data in above step, three entity is considered, first one is cloud provider itself, second is organization whose data resides at cloud and last one is employee or anonymous user who request for access of cloud data.

Now the above figure gives overview of first step of second phase, in which if a user (either employee or anonymous) want to access the data if it belongs to protection ring2 then user have to register itself (if he is already registered need not require further registration), if the data belongs to ring 1 it require strong authentication, if the data belongs to ring 3 then it is public need not require any authentication.Now suppose the user registered itself for accessing data,organization will provide username and password for authentication. At the same time organization sends the username to cloud provider.

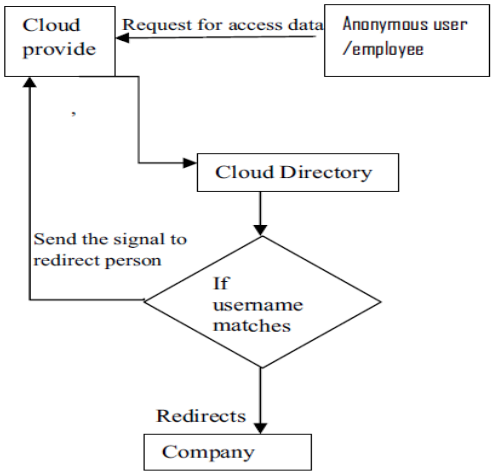


Fig. 3

Now when user sends request along with username to access the data to cloud provider, the cloud provider first check in which ring requested data belong. If authentication is required, it first check the username in its own directory for existence, if the username does not exist it ask the user to register itself. If the username matches it redirect the request to company for authentication.

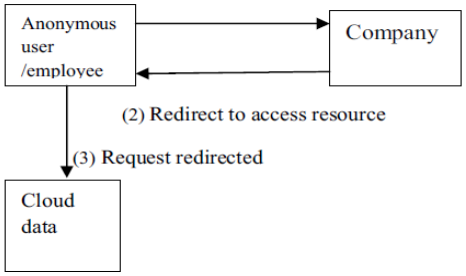
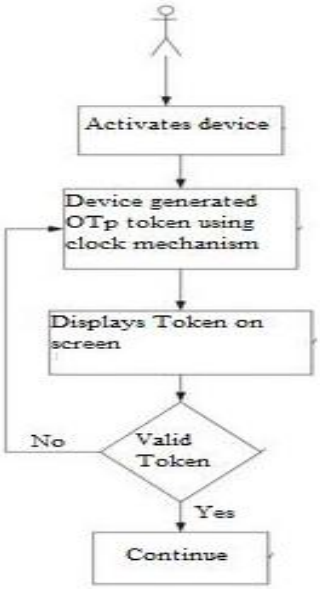
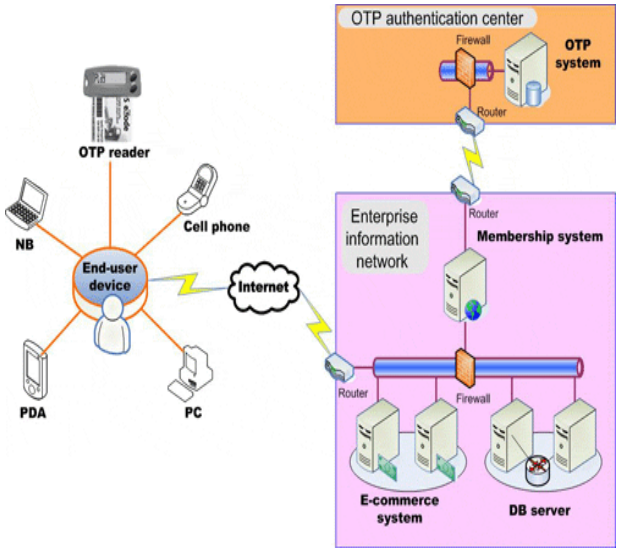


Fig. 4

Now the user sends password for authentication, and after authentication it redirect the request to cloud provider to access resource.

To access data from inner ring OTP(one time password) is used. User can send request for temporary password o access data. The password generated is valid for only 24 hour. User can request only once in 24hours for temporary password.





IIII. ANALYSIS

After applying algorithm for categorize the data on the basis of sensitivity. Now ring rule and conflict of interest is applied in the ring to make more robust security system.

Ring rule:

1. The user granted to access upper ring are not allowed to access lower ring i.e. no R/W in lower ring.
2. The user granted to access ring is allowed to access upper ring.

Applying conflict of interest:

It is an incompatibility between aim.

1. Data belongs to conflict of interest cannot be viewed by same user.

Subject S can read object O if and only if either condition holds:

1. There is an O_ such that S has accessed O_ and CD(O_) = CD(O) _ This implies that S has read something in O's dataset
2. For all O_ _ O, O_ _ PR(S) _ COI(O_) _ COI(O) _ This implies that S has not read any objects in O's conflict of interest class.

After applying above the user are required to register itself.

And whenever the user access the data he / she have to give username if it matches then it redirected to company for authentication. Now here the user is required to give password for corresponding password. If the user get validated, it redirect to cloud to access resource.

IV. CONCLUSION

This technique provides a new way to authenticate in 3 Dimensional approaches. It provides availability of data by overcoming many existing problem like denial of services, data leakage. As additional it also provides more flexibility and capability to meet the new demand of today's complex and diverse network.

V. REFERENCES

[1] On technical security issues in cloud computing , Meiko Jensen etal,2009

[2] Cloud computing security issues and challenges, Balachandran reddy et al, 2009

[3] Security & Architectural Issues for the national Security cloud computing, Anya Kim etal, 2010

[4] Cloud Computing security issues and challenges Kresimir Popovic, et al, 2010

[5] Heiser j Nicolett M. Assessing the security risk of cloud computing http://www.gartner.com/displaydocument? Id=685308, 2008

[6] Ensuring Data Storage security in cloud computing, Cong Wang, etal,2010

[7] Privacy reserving, Cong wang etal, 2010

[8] Data security in the world of cloud computing, John harauz, etal,2010

[9] Cloud computing security management, Sameera Abdulrahman etal,2009

[10] Information security risk management framework for cloud computing environments, Xuan Zhang etal, 2010

[11] A layered security approach for cloud computing infrastructure,Mehnet Yeldiz etal, 2010

[12] http://www.cioedge.com/content/state-cloud-computing-security

◈◈◈