ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (47-52), Month: April-June 2014, Available at: www.researchpublish.com

3-D (Dimensional) security in Cloud Computing

Ms. Gayatri Dhavale[1], Mr. Rajnish Kumar Baranwal[2], Mr. Kapil Nagare[3],
Mrs. S.N. zaware[4]

BE student (Computer Engineering), AISSMS'S Institute of Information Technology, Pune-01, India [1, 2, 3]
Head of Department (Computer Engineering), AISSMS'S Institute of Information Technology, Pune-01, India [4]

Abstract: **Cloud computing 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. Now there is third entity who is either company's (whose data is stored) employee or customer who want to access, they need to register first and then before every access to data, his/her identity is authenticated for authorization.**

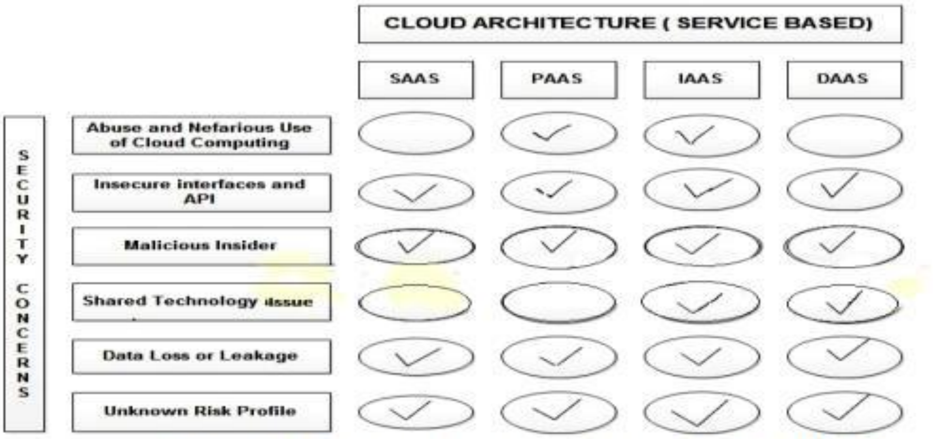
***Keywords*: Cloud security, Data protection, Cost Reduction, Data Storage, Confidentiality, Integrity, Availability.**

I. INTRODUCTION

Cloud computing is internet based technology which provides variety of services over internet such as software, hardware, data storage and infrastructure. Within the cloud computing systems environment, the virtual environment lets user's access computing power that exceeds that contained within their own physical worlds. Fundamentally, abundant security issues arises as it comprises many technologies including networks, virtualization [6], operating systems, resource scheduling, transaction management(when user query about some secure data), load balancing (preventing the cloud from crashing when the user demand increases),concurrency control(many users simultaneously requesting or accessing the same data on the cloud) and memory management. Data security doesn't only engross encrypting the data but also comprises on implementing and enforcing the appropriate policies for data sharing and as well as authenticating the user who required to access the data on cloud. It also encompasses scheduling data backup and safe storage of the backup media. Security is implicit within these capabilities, but more over elementary concerns exists that need attention. To beat these concerns, a security model must be developed which ensures CIA (confidentiality, integrity, and availability). With the competence provided by the cloud systems, as the number of users enhances, the probability of cybercrime increases. Cloud computing is becoming a tempting target for cybercrime. If not all cloud providers supply adequate security measures, then these clouds will become high-priority targets for cybercriminals. As cloud systems are inherited architecture so a single cyber attack offers opportunity to the attacker to influence a large number of sites through a single malicious activity. There are many security issues are arises for accessing these services in cloud. To remove these issues the 3D security system is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data on cloud. Categorization is depends on 3 important factors: Confidentiality, Integrity and Availability.

II. SECURITY ISSUES IN CLOUD

The cloud security and privacy is a big concern now a day. Security, privacy and secure storage of data are two barriers which are preventing the organizations and users from adopting the cloud computing. Emphasis must be given on security, privacy and stability on the cloud based technologies and computing to make them admirable among the corporate multitenant environment. Malicious and Abusive attacks are proliferating cloud security. The data leakage and security attacks can because by insufficient authentication, authorization, and audit (AAA) controls, inconsistent use of encryption. and software keys, operational failures, persistence and reminisce challenges: disposal challenges, risk of association, jurisdiction and political issues, data center reliability, and disaster recovery. Some of the risks in cloud computing are well known in traditional computing models.



CLOUD ARCHITECTURE (SERVICE BASED)

SECURITY CONCERNS	SAAS	PAAS	IAAS	DAAS
Abuse and Nefarious Use of Cloud Computing	○	✓	✓	○
Insecure interfaces and API	✓	✓	✓	✓
Malicious Insider	✓	✓	✓	✓
Shared Technology issue	○	○	✓	✓
Data Loss or Leakage	✓	✓	✓	✓
Unknown Risk Profile	✓	✓	✓	✓

Figure 1. Security concerns in Various Clouds Architecture

These risks include, for example, malicious insiders, insecure user authentication (such as usage of weak passwords), malicious code running on the cloud, vulnerabilities of the shared resources leading to information leakage, or account hijacking by phishing methods, unknown risk profile, data loss(no stability in data storage on cloud). Many of these risks can be handled using conventional security practices.

III. PROPOSED SYSTEM

The 3D security system is provided with powerful and more secure authentication techniques. This system is responsible to categories the files or confidential data. It is a multi-level authentication system. The system makes the confidential data secure using highly secure graphical passwords. It removes the time complexity issue. User accesses the cloud services. User is going to upload a file on the cloud. There are 3 protection rings. The inner most ring is most secure. The file categorization is done using Revised- CIA algorithm. The R-CIA divides the files into ring 1, ring 2 and ring 3. Biometric Password is used for ring1. Two way SMS Authorization password is used for ring2. Graphical password is used for ring3. At the time of downloading, this password should be match. If it is matched, then the authentication is successful. The user can access the cloud services.

IV. 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 2 allotted to D[k]th data.

IF S [K] = = 8||9||10 then R[k] =1 /* ring 1 allotted to D[k]th data.

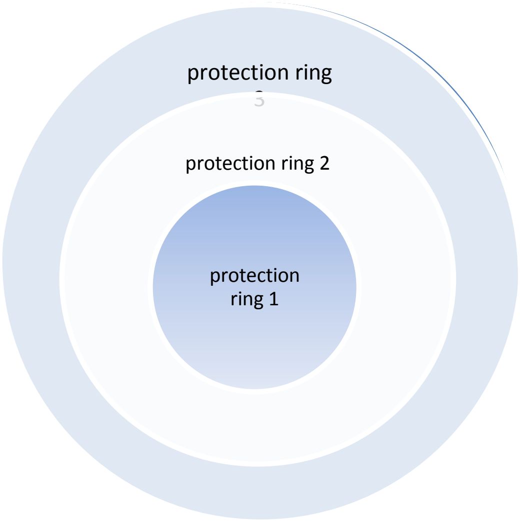


Figure 2. Protection rings

In above algorithm the first job of the user is to categorize it on the basis of 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 Cr criticality 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 require more security technique to ensure confidentiality.

V. GENERAL FRAMEWORK

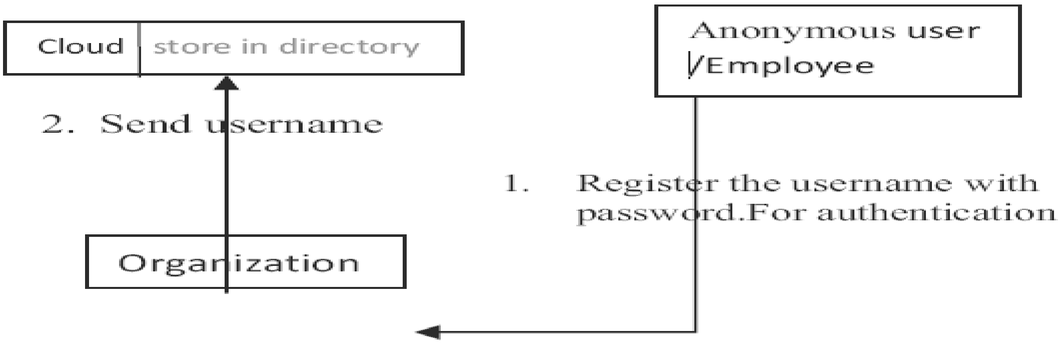


Figure 3. Frame work

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 ring 2 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 user name to cloud provider.

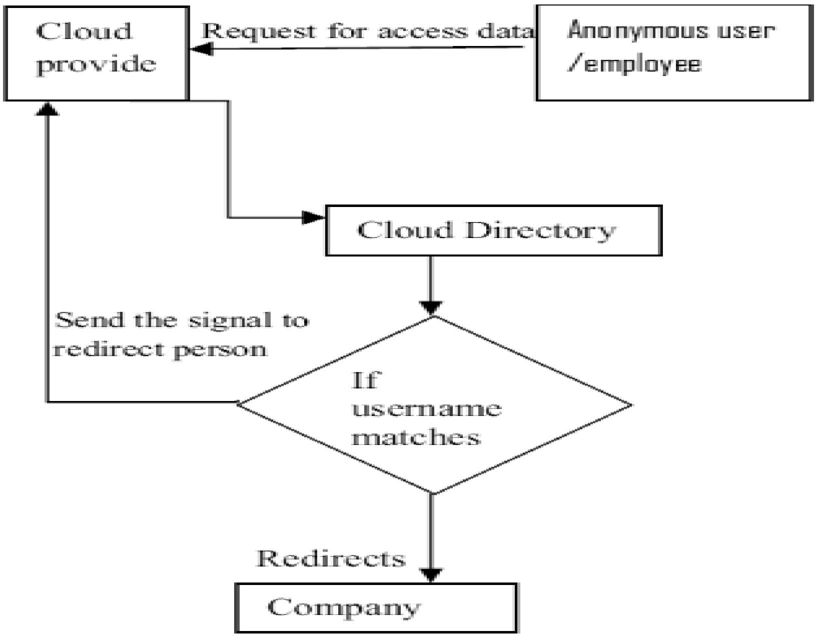


Figure 4

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 checks 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.

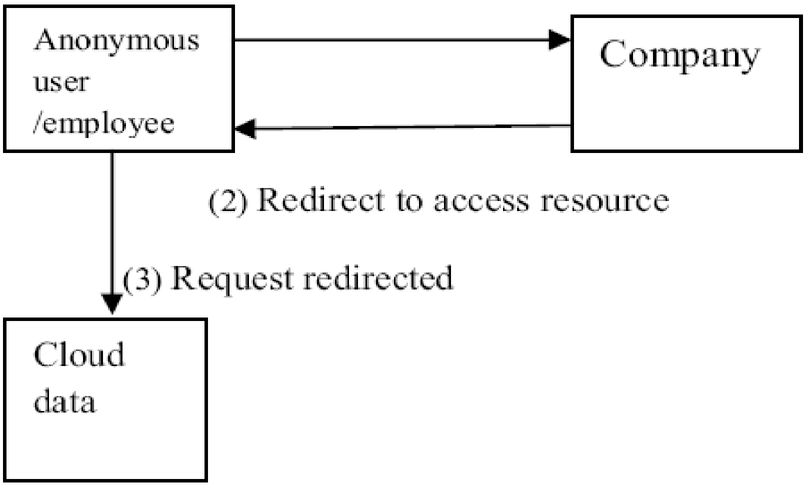
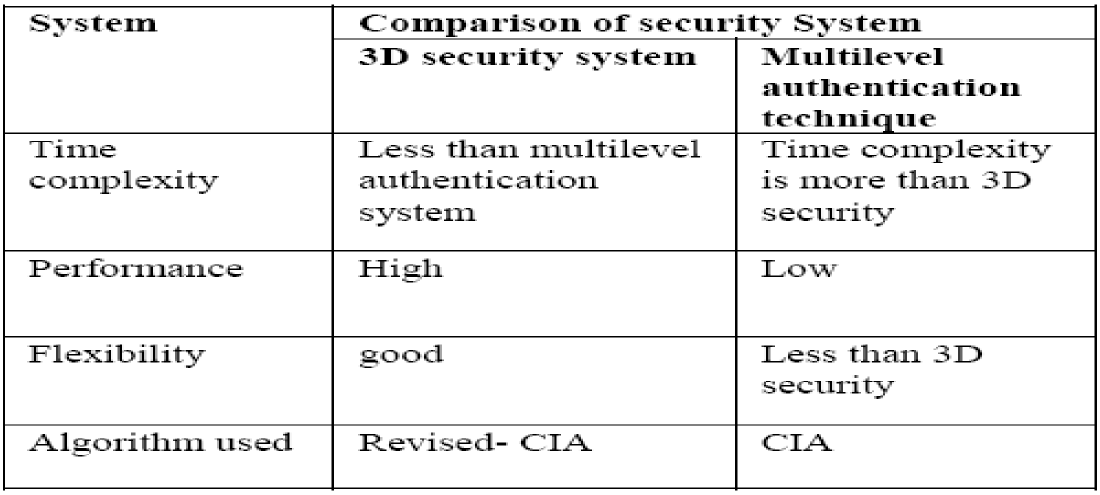


Figure 5

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

VI. COMPARATIVE ANALYSIS



System	Comparison of security System	
	3D security system	Multilevel authentication technique
Time complexity	Less than multilevel authentication system	Time complexity is more than 3D security
Performance	High	Low
Flexibility	good	Less than 3D security
Algorithm used	Revised- CIA	CIA

Figure 6. Comparison of Security System

VII. 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.

VIII. CONCLUSION

To provide Cloud services to the intended customer, it is a better option to use 3D Security system rather than multi-level authentication technique**.** This technique helps in generating the password in many levels of organization so that the strict authentication and authorization is possible. The security level of cloud environment is much stronger by using multi-level security system. Depending on rings, levels of multilevel security system increases for secure access of cloud services. This system is able for thwarting Shoulder attack, Tempest attack, and Brute-force attack, dictionary attacks and many more which are present at client side, with the use of strong techniques in the Graphical password.

ACKNOWLEDGMENT

Acknowledgement is not a mere formality as, it is the general notation. It is the only way through which express our deep and profound gratitude to the people who directly or indirectly contribute to our work. It's not until you undertake a Project like this one that you realize how much you must rely upon others help. I highly obliged and respond to express my admiration to the best conscious to convey respect towards **Mrs. S. N. Zaware (H.O.D. Computer engineering)** for valuable contribution towards completion of our project. I thank all the Staff members & lab Assistants of Computer Department who have helped me directly or indirectly in making this work a success.

REFERENCES

[1] Surabhi Anand, Priya Jain, Nitin and Ravi Rastogi,"Security Analysis and Implementation of 3-Level Security System Using Image Based Authentication" the 14th IEEE International Conference on Modeling and Simulation, Oregon, USA, 2012.

[2] 3 Dimensional Security in Cloud Computing Parikshit Prasad, Badrinath Ojha, Rajeev Ranjan shahi, Ratan Lal *Abhishek Vaish, *Utkarsh Goel Indian Institute of Information Technology, Allahabad U.P India.

[3] Kuyoro S. O. ,Ibikunle F. and Awodele O." Cloud Computing Security Issues and Challenges", International Journal of Computer Networks (IJCN), Volume (3):Issue (5):2011.

[4] Dinesha H A Agrawal V K, "Multi-level Authentication Technique for Accessing Cloud Services", Computing, Communication and Applications (ICCCA), 2012 International Conference on Feb 2012.

[5] Cloud Computing security issues and challenges Kresimir Popovic, etal, 2010.

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