Framework using Multitenancy Architecture in Cloud Computing

Varsha
Student
M.tech, CSE
Amity University, Haryana

Amit Wadhwa
Assistant Professor
Dept.of Computer Science
Amity University, Haryana

Swati Gupta
Assistant Professor
Dept.of Computer Science
Amity University, Haryana

ABSTRACT

As we all know Cloud computing is an emerging field in the world of computation and security of the data must be confined over the network. There are some security issues occurring while using services over the cloud and stress of our study is the multi-tenancy issue.

Many organizations nowadays are looking for improving security while sharing resources, application etc. on same hardware and same software by implementing multi-factor authentication i.e. authentication requiring more than one independent mechanism to prove one's identity like One-time passwords. We describe how cloud computing can address these issues. Our approach is based on a flexible framework for supporting authentication with multi tenancy architecture. For that, we proposed a framework using multitenant architecture for secure cloud computing environment that secure our data over the cloud and support multi-tenancy nature with the help of OTP.

Keywords

Cloud Computing, Security issues, Security model, Authentication, multi-tenancy.

1. INTRODUCTION

Cloud Computing provides shared resources and services via Internet. In last few years, usage of internet is increasing very rapidly which increases cost of hardware and software. So, the new technique known as cloud computing used to solve these problems by giving service when user demand over the internet and definitely it decreases the cost of hardware and software Services offered in cloud computing have various features like high scalability, reliability, flexibility and dynamic property[20].

Fig1. Cloud computing [22]

1.1 Services Models

Three types of cloud services and user can use any services which are mentioned below:

- Software as Service (SaS)
- Platform as service (PaS)
- Infrastructure as service (IaS)

Software as Service (SaS): It is also called a delivery model where the software and the data which is associated with is hosted over the cloud environment by third party and that third party is called cloud service provider, like your Gmail account, you use that application on someone else's system[20].

Platform as Service (PaS): In this, you can use Web-based tools to develop applications so they run on systems software which is provided by another company, like Google App Engine [20].

Infrastructure as Service (IaS): It provides services to the companies with computing resources including servers, networking, storage, and data centre space on a pay-per-use basis [20].

1.2. Deployment models

There are three Deployment Models and are described below:

- Public Model
- Private Model
- Hybrid Model

Public Model: This infrastructure is available to the general public. As the name suggests, public cloud is a model in which resources are generally available to everyone or anywhere [20].

Private Model: This model is developed for the private organizations like one house and an organization and they can use it for their own purpose. This kind of a service is not accessed by everyone[20].

Hybrid Model: Hybrid Clouds are combination of public and private cloud in a same network. This can be done if private cloud need some important services from the public cloud like Private cloud can store some information on their private cloud and we can use that information on public cloud[20].

In cloud computing, there are many issues but security is the major issue which we will discuss further.

2. PROBLEM STATEMENT

Our Research focus on the Security which is major concern in cloud computing and Security can be improved by using strong authentication. Authentication, on which Cloud computing greatly depends for security, provides the capability of using different means for ensuring authentication like OTP. The problem is to determine what kind of approaches should be used to multi tenant architecture that will provide the most efficient authentication, confidentiality and protection using perfect blend of different mechanisms.

The aim of this thesis work is to provide a framework which ensures two way protections in term of authenticity using OTP concept, confidentiality using SSS concept.

3. LITERATURE REVIEW

Arijit Ukil, Debasish Jana and Ajanta De Sarkar [2], in this paper, the problem of security in cloud computing has been analyzed. This paper gives security architecture and necessary support techniques for making our cloud computing infrastructure secured.

Rabi Prasad Padhy, Manas Ranjan Patra, and Suresh Chandra Satapathy [3], all the Security issues of cloud computing are highlighted in this paper. Because of the complexity which users found in the cloud, it will be difficult to achieve end-to-end security. New security techniques need to be developed and older security techniques needed to be changed or improved.

Kashif Munir and Prof Dr. Sellapan Palaniappan [4], in this study, we reviewed the literature for security challenges in cloud computing and proposed a security model and framework to make cloud computing environment secure.

Ayesha Malik and Muhammad Mohsin Nazir [5] in this paper discussed various techniques which helps to protect the data, secure data such as:

Mirage Image Management System [6]: This system addresses the problems related to safe management of the virtual machine images that summarize each application of the cloud [5].

Client Based Privacy Manager [7]: This technique helps to reduce the loss of private data and threat of data leakage that processed in the cloud, as well as provides additional privacy related benefits [5].

Transparent Cloud Protection System (TCPS) [8]: This provides protection system for clouds designed at clearly monitoring the reliability of cloud components. TCPS is planned to protect the integrity of distributed computing by allowing the cloud to monitor infrastructure components [5].

Secure and Efficient Access to Outsourced Data [9]: This Provides secure and efficient access to Outsourced data is an important factor of cloud computing and form the foundation for information Management and other Operations [5].

Krešimir Popović, Željko Hocenski [10], in this paper, discussed security in cloud computing was in a manner that covers security issues and challenges, security principles and security management models.

Takeshi Takahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, and Shin'ichiro Matsuo [11], in this paper introduced technical layers and categories, with which it recognized and structured security challenges and approaches of multitenant cloud computing.

Nagarjuna, C.C kalyan srinivas, S.Sajida,lokesh.[12], in this paper the main issue with multi tenancy is that the clients use the same computer hardware to share and process information and the result is that tenants may share hardware on which their virtual machines or server runs, or they may share database tables.

Paras Babu Tiwari Shashidhar Ram Joshi [14], in this paper, when client manually authenticates in the portal site and tries to login into the following application then one time password is generated for that session and this password is used to authenticate the client into the applications.

Arvind D Meniya, Harikrishna B [15], This paper focuses on the concept of Single-Sign-On (SSO) across all the open cloud to use their computing resources in single or shared manner.

Miceli, Christopher [16]: A one-time password scheme based upon techniques developed for secret sharing techniques has been presented.

S.Jaya Nirmala 1, S.Mary Saira Bhanu 1, Ahtesham Akhtar Patel [17] in this paper the performance of two secret sharing algorithms is compared. The Shamir's secret sharing algorithm and Rabin's Information Dispersal Algorithm (IDA) are implemented in a private cloud setup using the Open Stack Cloud framework

S. Ramgovind, M. M. Eloff, E. Smith[19], in this paper we studied about the major challenges that avoid Cloud Computing from being adopted like security, costing model, Charging Model, Service Level Agreement (SLA)

Varsha, Amit Wadhwa, Swati gupta [20], in this paper, we investigate and carry out a small study and highlight all the issues of emerging over a cloud related with security of Cloud.

4. SECURITY ISSUES IN CLOUD COMPUTING

Based on the study, we found that there are many issues in cloud computing but security is the major issue which is associated with cloud computing.

- Misuse and reprehensible Use of Cloud Computing.
- Insecure API.
- Wicked Insiders.
- Shared Technology issues/multi-tenancy nature.
- Data Crash.
- Account, Service & Traffic Hijacking.
- Unidentified Risk report.

Misuse and reprehensible Use of Cloud Computing : Hackers, spammers and other criminals take advantage of the suitable registration, simple procedures and comparatively unspecified access to cloud services to launch various attacks like key cracking or password [4][20].

Insecure Application Programming Interfaces (API): Customers handle and interact with cloud services through interfaces or API's. Providers must ensure that security is integrated into their service models, while users must be aware of security risks [4] [20].

Wicked Insiders: Malicious insiders create a larger threat in cloud computing environment, since consumers do not have a clear sight of provider policies and procedures. Malicious insiders can gain unauthorized access into organization and their assets [4] [20].

Shared Technology issues/multi-tenancy nature: This is based on shared infrastructure, which is not designed to accommodate a multi-tenant architecture [4] [20].

Data Crash: Comprised data may include; deleted or altered data without making a backup; unlinking a record from a larger environment; loss of an encoding key; and illegal access of sensitive data [4] [20].

Account, Service & Traffic hijacking: Account or service hijacking is usually carried out with stolen credentials. Such attacks include phishing, fraud and exploitation of software vulnerabilities. Attackers can access critical areas of cloud computing services like confidentiality, integrity and availability of services [4] [20].

Unidentified Risk Report: Cloud services means that organizations are less involved with software and hardware, so organizations should not be aware with these issues such as internal security, security compliance, auditing and logging may be overlooked [4] [20].

We will discuss Multi-tenancy issue which we found a major concern in cloud computing.

5. SECURITY MODEL

User can be certificated by the 3rd party certificate authority that can issued token for service by End User Service Portal. After joining service portal, user can buy and use cloud services which are provided by single service provider. End User Service Portal which is composed access control, security policy, Key management, service configuration, auditing management, and virtual environments provides secure access control using Virtual Private Network (VPN) and cloud service managing and configuration [4].

We found a problem that is SSO Problem which we face when user wants to use the services which user gets from service Provider.

Single Sign On: Sso is basically a session authentication method that permits a user to enter one name and password in order to access various applications or services.

To resolve this problem we have to check user name and password and checking user name and password is not sufficient, we have to use an authentication procedure for network

To Provide Authentication we have to use authentication technique i.e. One time filling.

One Time Filling: We use one-time filling that is a long chain of random letters. These letters are combined with the plaintext message to create the cipher text. To decipher the message, a individual must have a copy of the one-time filling to reverse the procedure and this is done with the help of a Vigenere table. A one-time filling should be used only once (hence the name) and then destroyed. This is the first and only encryption algorithm that has been proven to be unbreakable.

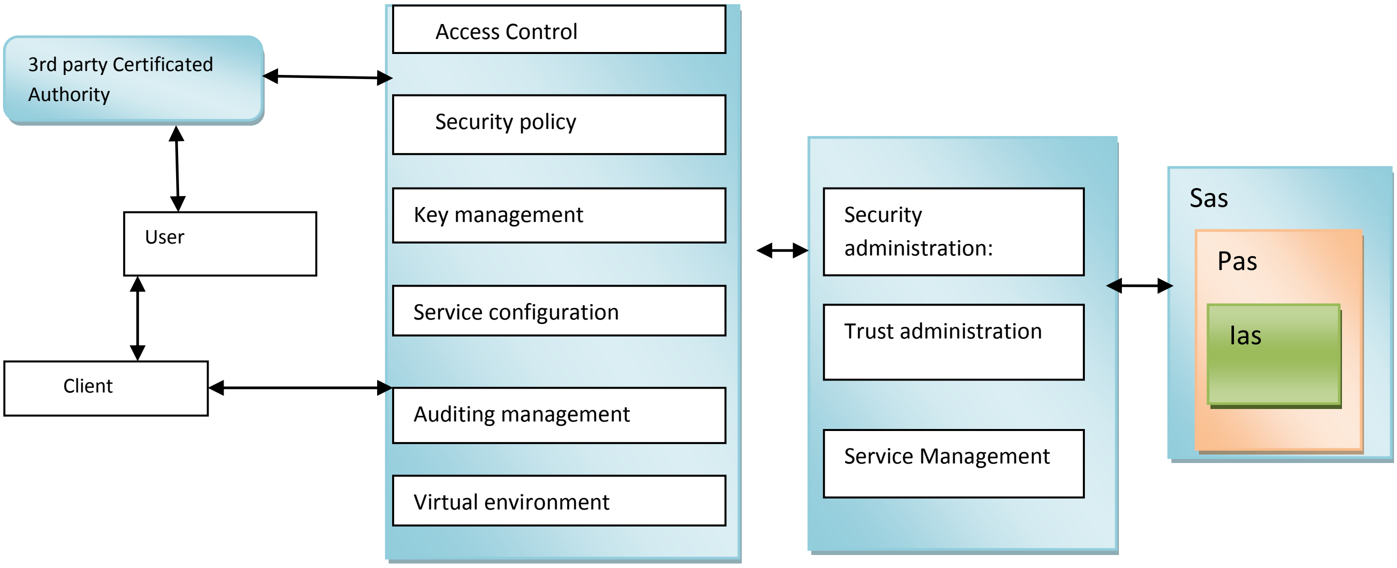

Fig 2.Security model [4]

6. PROPOSED WORK: MULTI-TENANCY

Multi-tenancy is a major concern in cloud computing. Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server.[20]

Multi-Tenancy in Cloud Computing occurs when multiple consumers share the same application, running on the same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server[20].

Framework for multi-tenancy cloud architecture

1. Multi-tenancy at the datacenter layer can be a service provider renting datacenter space, and supplying servers, routers, etc, that supports multiple customer software requests [18]

2. Multi-tenancy at the infrastructure layer can be achieved through software stacks, where one stack belongs to a particular customer. Compared to datacenter-layer multi-tenancy, this infrastructure layer multi-tenancy saves costs because these stacks are deployed in accordance with actual customer accounts [18].

3. Implementation of Multitenancy at the cloud application service layer requires architectural implementations at both the software layer and the infrastructure layer. Modifications are required to existing multi-instance software architectures, with a variety of multi-tenant patterns being used throughout the application layer [18].

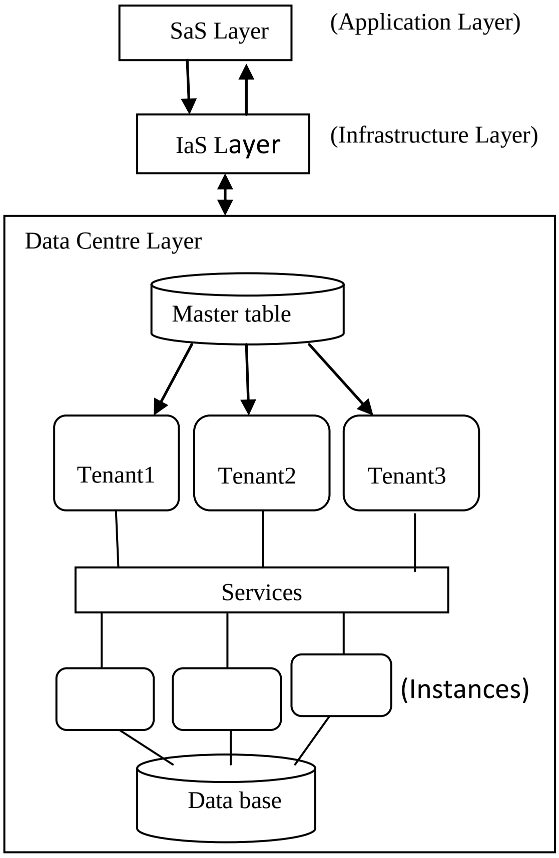

Figure 4 Framework for multi-tenancy cloud architecture

We should provide authentication to our architecture so before applying authentication technique we should know what is authentication.

Algorithm 1:
It is named as User Validation Algorithm. Purpose of this algorithm is to check user is valid or not and if user is valid Sharer share services with the valid user.

Step-1: Sharer sends request to users for sharing services.

Step-2: Sharer applied OTP Technique to check user is valid or not

Step-3: Sharer sends OTP to every registered user who requested for the service

Figure 5 User Validation Algorithm

Algorithm 2:
It is named as Sharer Share Service Algorithm. Purpose of this algorithm is to share the services among valid users.

Step-1: Sharer wants to share services with users and send key to users.

Step-2: Sharer breaks the main key into unique parts

Unique parts ← Key

Step-3: Sharer distribute its own unique part to each user from the key

K=U1, U2---UN

Figure 6 Sharer Share Service Algorithm

Algorithm 3:
It is named as Collection Key Algorithm. Its Purpose is to share the services among valid users after collecting all the keys.

Step-1: Collect all the unique parts from users

K=U1, U2---UN

Step-2: Join all the unique parts of the key to get main key

U1+U2+-----UN=K

Step-3: User sends the main key K to sharer.

Step-4: If Sharer gets the correct key K,

Then, user uses the Services

Else, show message invalid key

Figure 7 Collection Key Algorithm

Authentication: In the perspective of computer systems, authentication is a process that ensures and confirms a user's identity and here we applied authentication to protect our data from unauthorized user.

1. We can apply Authentication to protect our data form hackers so we used Shamir's Sharing Secret Encryption Algorithm.

a) According to Shamir's Sharing Secret Algorithm, Secret key is breaking into parts and send it to many users. When we have to recreate that code, we need to join all the parts and after that all users can access that data.

b) Before using the Algorithm, we have to discuss why we use this authentication and where we should use that.

2. As you read earlier, Multi-tenancy occurs when various consumers using the same cloud to share the information and data or runs on a single server. Here, we can share some services with the clients or users.

a) We have a Sharer who wants to share his services among Users but before using the services sharer checks the user is valid or not using OTP Technique that is One Time Password.

b) If user is not valid then it can't use the services and if user is valid then we use Shamir's Sharing Secret Authentication Technique and we applied this Authentication technique before users use the services.

c) We break out the Secret Key into some unique Parts and send it to the users and when they have to access the code they have to join all keys to reconstruct the code and after that they uses the service.

We face a problem in this, if sharer wants that only one user can use that service among all, then how can he do that because secret key is distributed among all users and without joining all the keys they can't access the data.

So here, we can't apply SSS technique. In this situation, sharer can divide the key into parts and he sends half key on the registered mobile number with and half key is send on email id and when user join both the keys and then user can access the service.

We face one more condition here, how an unregistered user can use the service?

1. If the user is not registered for using the services and he wants to use the service so first of all, he sends a request message to sharer that he gives him permission to use the services.

2. If sharer permits the request, then unregistered user can only use a part of the service instead of using the full service.

3. If user wants to use the full service without registration, then he used the service, but he should pay for it.

4. If user wants to register and then he uses the service, then user has to send request to sharer.

5. If sharer Declines, it's up to the user that he wants to use that service by purchasing it or not.

6. If sharer gives him permission, then the user can register himself and pay something to register herself.

There are three conditions:

a) If User pays without registration, then he can use only that service and he can pay next time for using next service.

b) If User Pay full amount during registration then he can use services anytime and anywhere.

c) If User can't pay full amount during registration then he can use services for some time.

7. User uses the services after registering herself and sharer check that user is authenticate or not at the time of registration using OTP.

7. FUTURE WORK

We suggest that future research should be directed towards the Multitenancy which provides more confidentiality to the user and make the data very secure.

8. CONCLUSION

Cloud computing is an immense prospect both for the businesses and the attackers – both parties be able to have their own reward from cloud computing but we found that there are various challenges in cloud computing and security is the main issue is and we discussed multi-tenancy issue and design a framework for multi-tenancy issue and provide authenticity to users data. Basically, we provide a framework which ensures two way protections in term of authenticity using OTP concept, confidentiality using SSS concept.

9. REFERENCES

[1] "Security Guidance for Critical Areas of Focus in Cloud computing", April 2009, presented by Cloud Security Alliance (CSA).

[2] Arijit Ukil, Debasish Jana and Ajanta De Sarkar" A SECURITY FRAMEWORK IN CLOUD COMPUTING INFRASTRUCTURE "International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013 DOI: 10.5121/ijnsa.2013.5502 11.

[3] Rabi Prasad Padhy, Manas Ranjan Patra and Suresh Chandra Satapathy ," Cloud Computing: Security Issues and Research Challenges", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS) Vol. 1, No. 2, December 2011.

[4] Kashif Munir and Prof Dr. Sellapan Palaniappan," FRAMEWORK FOR SECURE CLOUD COMPUTING ", International Journal on Cloud Computing: Services and Architecture (IJCCSA), Vol.3, No.2, April 2013.

[5] Ayesha Malik, Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment: A Review", Journal of Emerging Trends in Computing and Information Sciences ©2009-2012 CIS Journal. All

rights reserved, VOL. 3, NO. 3, March 2012 ISSN 2079-8407

[6] Jinpeng Wei, Xiaolan Zhang, Glenn Ammons, VasanthBala and PengNing, “Managing security of virtual machine images in a cloud environment”, November 2009, Proceedings of the 2009 ACM workshop on Cloud computing security pages 91-96.

[7] Miranda Mow bray and Siani Pearson, “A Client- Based Privacy Manager for Cloud computing”, June 2009, Proceedings of the Fourth International ICST Conference on communication system software and Middleware.

[8] Flavio Lombardi and Roberto Di Pietro, “Transparent Security for Cloud”, March 2010, Proceedings of the 2010 ACM Symposium on Applied Computing, pages 414-415. Objectives of this paper is to study the major security issues arising in cloud environment.

[9] WeichaoWang, Zhiwei Li, Rodney Owens and Bharat Bhargava, “Secure and Efficient Access to Outsourced Data”, December 2009, Proceedings of the ACM workshop on Cloud computing security, pages 55-65.

[10] Krešimir Popović, Željko Hocenski,”Cloud computing security issues and challenges”, MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[11] Takeshi Takahashi, Gregory Blancy, Youki Kadobayashiy, Doudou Fally, Hiroaki Hazeyamay, Shin’ichiro Matsuo,”Enabling Secure Multitenancy in Cloud Computing: Challenges and Approaches“.

[12] Nagarjuna,C.C kalyan srinivas,S.Sajida,Lokesh” SECURITY TECHNIQUES FOR MULTITENANCY APPLICATIONS IN CLOUD”, C.C. Kalyan Srinivas *et al*, International Journal of Computer Science and Mobile Computing Vol.2 Issue. 8, August- 2013, pg. 248-251.

[13] Image: Architectural Multi-Tenancy: http://devcentral.f5.com/weblogs/images/devcentral_f5_com/weblogs/macvittie/WindowsLiveWriter/ArchitecturalMultitenancy_46C0/image1.png.

[14] Paras Babu Tiwari Shashidhar Ram Joshi ,”Single Sign-on with One Time Password”

[15] Arvind D Meniya, Harkishan B Jethva ,”Single-Sign-On(SSO)across open cloud computing federation” International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 1,Jan-Feb 2012, pp.891-895 891

[16] Miceli, Christopher, "One Time Password Scheme Via Secret Sharing Techniques" (2011). University of New Orleans Theses and Dissertations. Paper 1330.

[17] S.Jaya Nirmala 1, S.Mary Saira Bhanu 1, Ahtesham Akhtar Patel,” A COMPARATIVE STUDY OF THE SECRET SHARING ALGORITHMS FOR SECURE DATA IN THE CLOUD”,International Journal on Cloud Computing: Services and Architecture(IJCCSA),Vol.2, No.4, August 2012

[18] J. Petersson. Best practices for cloud computing multi-tenancy.

[19] S. Ramgovind, M. M. Eloff, E. Smith. “The Management of Security in Cloud Computing” In PROC 2010 IEEE International Conference on Cloud Computing 2010.

[20] Varsha, Amit Wadhwa, Swati gupta,” Study of Security Issues in Cloud Computing”, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.6, June- 2015, pg. 230-234

[21] One-time Pad. Available online: http://users.telenet.be/d.rijmenants/en/onetimepad.htm

[22] Image: Introduction to cloud comptung: https://www.google.co.in/search?q=cloud+computing+architecture&biw=1360&bih=623&source=lnms&tbm=isch&sa=X&ei=oCeaVfvAGZKfugSz7a3wDg&ved=0CAYQ_AUoAQ&dpr=1#tbm=isch&q=cloud+computing+&imgrc=kSsq_wpQ-t9KWM%3A