International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com
ISSN No: 2456 - 6470 | Volume - 2 | Issue – 6 | Sep – Oct 2018

Securing Cloud Data with the Application of Image Processing

Bilal Hussain CH, Subayyal
Research Scholars, Department of Computer Science and Engineering,
University of Engineering & Technology, Lahore, Pakistan

ABSTRACT
Cloud computing is a new paradigm of shifting resources over the network so that the user can access the resources over the network. The resource mainly consists of Platform as a service, Software as service, and infrastructure as a service. Cloud computing is a basically internet based computing where the services are provided on pay as you go model. The consumers pay for the services they want and services are provided to them on cloud. Since cloud uses distributed resourcing scheme it is important to provide security in the cloud. And we also know that security is the main problem in cloud. It is mainly the loop hole in cloud which requires serious attention. In this paper we have described the scheme to implement security in cloud using finger print reader and GSM module. In this paper first we have discussed the security issues and security problem and we have enlighten the steps to increase the security in cloud. Our methodology mainly focuses on finger print scanner and GSM module.

Keyword: *Cloud Computing, Utility computing, Risk, Finger print scanner, GSM module*

INTRODUCTION
Cloud computing provides infrastructure, platform, and software as services, which delivered to consumers to the basis of pay as you go model. These services are respectively referred to in industry as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Clouds aim to power the next generation data centers by architecting them as a network of virtual services (hardware, database, user-interface, application logic) so that users are able to deploy and access applications globally and on demand at competitive costs depending on users QOS (Quality of Service) requirements. Developers with innovative ideas for new Internet services no longer require large capital outlays in hardware to deploy their service, or human expense to operate it. It offers significant benefit to IT companies by freeing them from the low level task of setting up basic hardware (servers) and software infrastructures, and thus enabling more focus on innovation and creating business value for their services.

Before the invention of cloud the users have to buy the infrastructure and software to carry out the daily basis work, which is very costly and not affordable for the common users and small enterprises. The cloud solved this major problem of purchasing and managing the whole system and infrastructure.

Despite of the facts the cloud has developed efficiently and advanced rapidly there is still a loop hole in the cloud. The security of the cloud is not as strong as it is considered.

Because the services are delivered over the network the chances of getting hacked and attacked are enormous. That's why we have to increase the security of the cloud. Several methodologies are provided to increase the security of the cloud. And we are going to propose one.

CLOUD COMPUTING ARCHITECTURE:-
The major providers of the cloud are providing their resources i.e. software as a service, infrastructure as a service and platform as a service to the customers and consumers over the internet. The major providers include Amazon, Google, yahoo, Microsoft.

The services provided by the cloud are mainly platform as a service software as a service and a infrastructure as a service.

The three main services are discussed below:-

Software as a service:-

In this type of service the cloud provides the users ability to use the software that basically owned by the cloud. There are many instances of the software and the end users and consumers uses the instance of the software.

The main example of the software as a service is salesforce.com

Platform as a service:-

In this type of the service the cloud provides the user's ability to program their own software. The cloud provides the users the software to carry out their instructions and execute them. In this type the consumer can make the program according to the software provided by the cloud.

For example some clouds give the users platform for the development of software only in C# or only in java or only in C or assembly. There are different platforms provided by different cloud companies.

Infrastructure as a service (IaaS):-

Infrastructure as a service provides the user ability to store and compute capabilities over the network. Different type of routers, switches hard drives, servers are pooled together and made available to the users so the users can use them on pay as you go services. This is the most expensive and difficult type of service that is provided to users by the cloud.

Cloud computing deployment:-

Cloud computing is basically divided into four types:-

Public cloud:-

In this type of cloud the services are pooled together and provided to the consumers as single virtualized services. They are delivered publically and on the common bases so there is no private portion for any one. This type of cloud is basically provided by the government or the big corporations and the companies so that employees or public use them.

Public cloud is usually implemented when:-

1. There are lot of people that need to access the cloud.
2. You need to testify and program application code.
3. You need incremental capacity.
4. You are doing big collaborative project.

They are typically larger than other type of clouds. And they can handle larger mob.

Private cloud:-

Provide a dedicated instance of these services for your exclusive use and, as a result, can be secured and accessed privately.

Private cloud is a cloud that is hold by a particular organization.

There are basically two flavors of this type of the cloud:

1: On premise private cloud:-
This type of cloud is maintained within a organization own facility. They are of best use when you require complete control over the configurability and security.

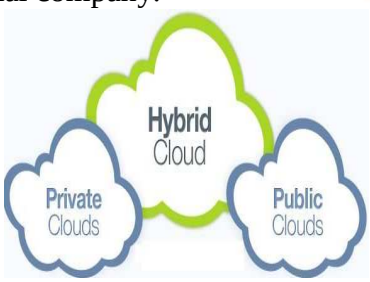
2: Externally hosted private cloud:-
This type of cloud is maintained within a organization but is maintained and setup third party.

Hybrid cloud:-

Hybrid cloud is a cloud that is a combination of public and private cloud. Both type of clouds are remain distinct but are bound together by offering the advantage of multiple deployment model.

When to use the hybrid cloud:

1. The company wants to use the SAAS service but there are security issues, then hybrid cloud is most suitable.
2. You want to provide the public cloud to users and the public while maintaining a private cloud for the internal company.



Characteristics of a cloud:-

There are several characteristics of a cloud. Some of them are given below:

➢ **Scalability and elasticity:-**

Clouds are more scalable and have more elasticity than conventional computing. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

- Availability and reliability:-

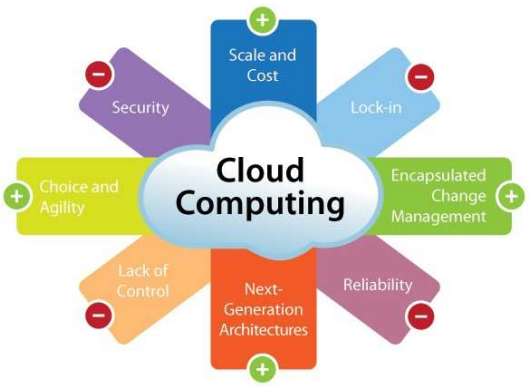
Cloud are readily available and more reliable than conventional computing in a way that they can accessed anywhere and anytime. Availability is the significant characteristics of a cloud.

➢ **Manageability and interoperability:-**

Manageability is also the main feature of the cloud. They are manageable in case some error occurs. And they are interoperable, so that the user can easily operate the cloud without having any problem.

➢ **Performance and optimization:-**

Clouds hold the pool of powerful devices that are responsible for providing the performance to the user. The cloud should also be optimized so that they are able to provide the resources to the user on runtime bases.



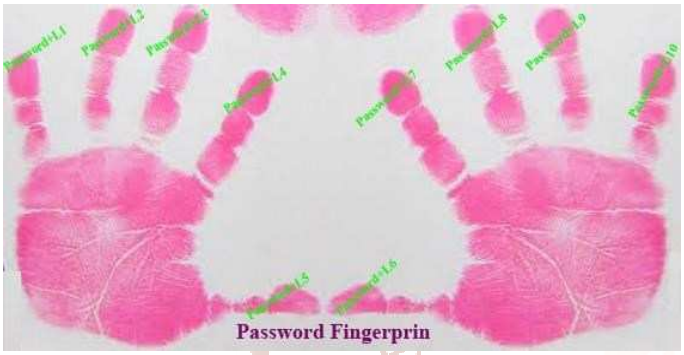
➢ **Portability and accessibility:-**

Clients and consumers should be able to use the cloud and access the cloud with only web browser and nothing else. They are easily accessible and cloud should be portable.

Our methodology:-

To enhance the security in the cloud we are using finger print scanner and a GSM module. The basic concept behind out methodology is that when the users access the cloud he or she is required to place the password. But as we know the password can be hacked, key logged and can be stolen. So we are using finger print of the user instead of the password. Instead of the password the user is asked to place the thumb on the device (finger print scanner) and the device scans the thumb of the user and then check with the database that either the user is authentic or not. If yes the user is authentic the system will send a password to the user cell phone using the GSM module. Then the user will enter the password received on the cell phone on the required field and then accesses the cloud.

Only the finger print scanner is sufficient but the GSM module is used to ensure the security of the cloud.



There are basically three phases of the process. We will discuss each phase briefly:-

1st phase:-

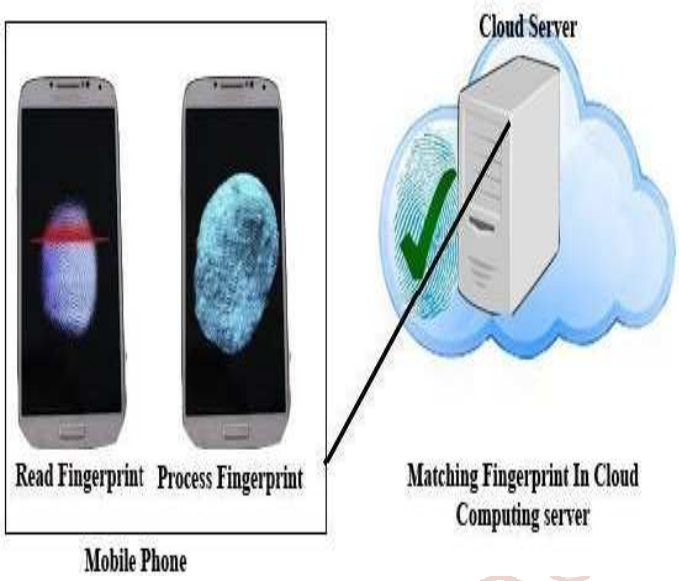
This is the first phase. In this phase the finger print is recorded by the finger print scanner. The user is prompted to place the finger on the device so that the device can get the image of the finger. The image is then saved in to the database if it's not there.

2nd phase:-

In this phase the image of the finger received from the device is checked with the image placed in the database. Basically it matches the both images and find similarity between them. If the image passes the test then the process is passed to the third phase. If not the message will be prompted that the user is not authentic.

3rd phase:-

In the third phase the, system will send a message to the user cell phone that is basically a code for accessing the system. The user has to enter the given code on the required field to use or enter the cloud. In this phase our GSM module is used.



CONCLUSION:-

We have used finger print scanner and GSM module to enhance and ameliorate the security of the cloud. We have devised a system of finger print detection in which system and cloud will be accessed using the scheme we have devised. First the user places the finger on the device, the device then scans the finger print and checks with the database that the given print either exists in database or not. If the print exists in the database the system will send the user a code to enter the cloud. The user is then asked to place the code on the required field. If the code matches then user will be given permission to enter the cloud.

Future work:-

In future some other techniques can be devised using our methodology as a paragon.

Some techniques can be

- Iris detection
- Face detection

Some other modules can also be integrated with our proposed model to enhance the security in cloud.

REFERENCES

1. Buyya R, Chee Shin Y, Venugopal S, Broberg J, Brandic I. Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems; 2009; 25(6):599–616.
2. Armbrust M, Fox A, Griffith R, Joseph A D, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M. A View of Cloud Computing. Communications of the ACM; 2010; 53(4):50–58.
3. Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. Journal of Network and computer Applications; 2011; 4(1):1–11.
4. Takabi H, Joshi J B D, Ahn G. Security and privacy challenges in cloud computing environments. IEEE Security & Privacy; 2010; 8(6):24–31.
5. Sangroya A, Kumar S, Dhok J, Varma V. Towards analyzing data security risks in cloud computing environments. Communications in Computer and Information Science; 2010; 54:255–265.
6. Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing, 2009. http://www.ibm.com/developerswork/websphere/zones /hipods/ library.html.
7. Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011. http://www.productionscale.com/home/2011/8/7/t he-nist-definition-ofcloudcomputingdraft.html #axz z1X0xKZRuf.
8. Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing (v2.1). Decemeber, 2009.
9. Pearson, S. and Azzedine Benameur, “Privacy, Security and Trust Issues Arising from Cloud Computing” in 2010 IEEE Second International Conference Cloud Computing Technology and Science (Cloud Com), Nov 30-Dec 3,2010, page(s): 693-702.
10. Jinzhu Kong, “A Practical Approach to Improve the Data Privacy of Virtual Machines” 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), June 29 -July 1, 2010, pp. 936-941.
11. Esteves, R. M. and Chunming Rong, “Social Impact of Privacy in Cloud Computing” in 2010 IEEE Second International Conference on Cloud Computing Technology and Science (Cloud Com), Nov. 30-Dec. 3 ,2010, pp. 593-596
12. Cloud Computing: Web-Based Applications That Change the Way You Work and Collaborate Online Michael Miller
13. Cloud Application Architectures: Building Applications and Infrastructure in the Cloud (Theory in Practice) by George Reese.

14. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice) by Tim Mathe

15. Dot Cloud: The 21st Century Business Platform Built on Cloud Computing Peter Fingar

16. Ramanujam, S., Gupta, A., Khan, L., & Seida, S (2009). R2D: Extracting relational structure from RDF stores. In Proceedings of the ACM/IEEE International Conference on Web Intelligence, Milan, Italy

17. Smith, S., & Weingart, S. (1999). Building a high performance, programmable secure coprocessor [Special Issue on Computer Network Security] Computer Networks, 31, 831–860. doi:10.1016 S1389-1286(98)00019-X

18. Teswanich, W., & Chittayasothorn, S. (2007). ATransformation of RDF Documents and Schemasc to Relational Databases. IEEE Pacific Rim Conferences on Communications, Computers, and Signal Processing, 38-41.