International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-1 Issue-9 March-2013

Review of Information Authentication in Mobile Cloud over SaaS & PaaS Layers

Vineet Guha[1], Manish Shrivastava[2]

Abstract

The Revolution has begun; time has come when we no more have to worry about the size, format & storage of data at a single place. Cloud computing is a revolution which has made world of internet more like a place of dynamic storage & facilitator of new methodology, which generates tools for consumers in a very effective style of computations. Cloud Computing has made lots of changes not only in infrastructure side, but has also deeply impacted the software industry. Many Companies, Institutions are moving towards using Cloud computing technology, but with every new technology emerging in this Information technology world, with major issues holds with security models to implement & problem like how we can keep data secured & safe. Cloud Computing; do pose various new security concerns, which have not been well identified & worked on. When we talk about the security of data in Cloud computing the vendor's has to ensure assurance to get confidence of customer on the security issues. Institutions & organizations are planning to use cloud computing for certain level of confidential issues for their business applications though guaranteeing the security is difficult task for now. With most of companies & IT giants planning to incorporate usage of Mobile technology to enrich their existing services & with more & more advance smart phones available in market, we can think of certain ideas & solutions to use mobile devices as alert medium & help securing use of data & network in cloud environment to an extent? It can also help us to keep a watch on intruders & we can impose checks on illegal access to data & network. So we can think of using Mobile Technology with Cloud Networks. We in this paper, review certain security concerns in Cloud computing technology & also about certain ways to restrict & overcome such issues over SaaS & PaaS Layers using mobile technologies. In this paper we try to focus ourselves to find answers to all such questions & improvise the use of Mobile technology in complex but future cloud computing networks.

Vineet Guha, M.Tech Research scholar, LNCT, Bhopal, India.
Manish Shrivastava, Director (PG), LNCT, Bhopal, India.

Keywords

Cloud Computing, Mobile Cloud Computing, EBCDIC, Cloud Security.

1. Introduction

Information security is a major area of concern in all IT related domains. With increase in usage of internet & changing trend & future demand of using Cloud network for storing all the information & data for global access & availability. Cloud security is now a new area of research & development, Cloud computing security is an emerging sub-domain of computer & network security, dealing basically with information security, its heart. Cloud security also refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Cloud Computing has now became the future generation architecture of any IT organization. In contrast to traditional solutions, Cloud computing moves the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. In cloud computing, both data and software are not fully contained on the user's computer; Information Security concerns arising because both user data and program are at service provider's end. Clouds usually have single security architecture but emerging & changing demands & requirements of customers, we would need to find & work on more and more flexible & durable security solutions to fit such networks.

2. Literature Review

Cloud Computing – SaaS (software as a service) and PaaS (platform as a service) providers all trumpet the robustness of their systems, it is often claimed that claiming that security aspects in the cloud is better in most enterprises. But the simple fact is that every security system that has ever been breached was once thought infallible [3]. Google was forced to make an embarrassing apology in February, when its Gmail service went collapsed in Europe, while Salesforce.com is still stinging from a phishing attack

from 2007. While cloud service providers also face similar security issues, as other sorts of organizations, analysts do warn that the cloud is becoming particularly attractive to cyber attacks. Cloud service users need to be more attentive, understand the risk of data breaches in this all new environments. As with most SaaS (Software as a Service) offering, the applications offering are constantly being tweak and changed, a fact which raises more security issues for clients. Companies need to understand, whether software changes might really make change in its safety settings [1].

This idea of intergalactic computer network was introduced by J.C.R. Licklider, who was responsible for enabling the development of ARPANET (Advanced Research Projects Agency Network) in 1969.His vision was for everyone on the globe to be interconnected and accessing programs and data at any site, from anywhere. However, the time the internet only started to offer proper bandwidth in the nineties onwards, the development was Amazon Web Services in 2002, which provided a suite of cloud-based services including storage, computation and even human intelligence through the Amazon Mechanical Turk [2].

In [10] it's being described about **Mobile cloud computing** is the combination of cloud computing and mobile networks (see Fig 1) to bring benefits for mobile users, network operators, as well as cloud providers. Cloud computing exists when data and task both are kept on the Internet instead on individual mobile devices or client system, providing methods for on-demand services. Applications are executed on a remote system and then results or information is sent to the user. Because of the advanced development in mobile browsers work of Apple, Google, Microsoft and Research in Motion etc are appreciated, nearly every mobile have a suitable browser. This means developers will have a much wider market and they can bypass the restrictions created by mobile systems. Mobile cloud computing gives new company chances for mobile network providers.

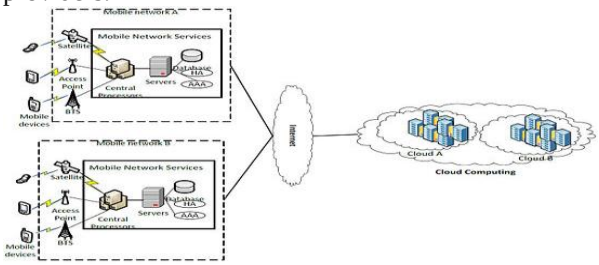

Fig. 1: Mobile Cloud Network [10].

Cloud Framework

Cloud computing systems can be considered as a set of different services, the framework of cloud computing is divided into three layers, they are infrastructure layer, platform layer, and application layer (see Fig. 2) [3].

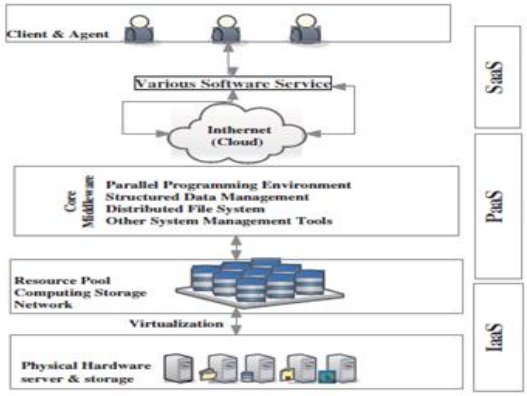

Fig 2: The Framework of Cloud Computing [3].

a) Infrastructure layer: It includes resources of computing and storage. In the bottom layer of the framework, physical devices and hardware, such as servers and storages are virtualized as a resource pool to provide computing storage and network services users, in order to install operation system (OS) and operate software application. Thus it is denoted as Infrastructure as a Service (IaaS). Typically services in this layer such as Elastic Computing Cloud of Amazon [3].

b) Platform layer: this layer is considered as a core layer in the cloud computing system, which includes the environment of parallel programming design, distributed storage and management system for structured mass data, distributed file system for mass data, and other system management tools for cloud computing. Program developers are the major clients of the platform layer. All platform resources such as program testing, running and maintaining are provided by the platform directly but not to end users. Thus, this type of services in a platform layer is called Platform as a Service (PaaS). The typical services are Google App Engine and Azure from Microsoft [3].

c) Application layer: this layer provides some simple software and applications, as well as costumer interfaces to end users. Thus we name this type of services in the application [3].

Latest Threats in Cloud Computing.

In [4], Responsibility Ambiguity: Cloud service users devour deliver resources through service models; the

customer-built IT system thus relies on the services. The lack of a clear definition of responsibility among cloud service users and Providers may evoke conceptual conflicts. Moreover, any contractual inconsistency of provided services could induce anomaly, or incidents. However the problem of which entity is the data controller which on is the data processor stays open at an international scale (even if the international aspect is reduced to a minimal third party outside of the specific region like EU).

Unsecure Cloud Service User Access: As most of the resource deliveries are through remote connection, non-protected APIs, (a mostly management APIs and PaaS service is one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks [4].

Unsecure Administration API: The administration middleware standing between the cloud infrastructure and the cloud service user may be not sure with insufficient attention devoted to sanitation of cloud service user inputs and authentication. Non-protected APIs, mostly administration APIs becomes a target of choice for attackers. This is not specific to cloud environment. However, the service-oriented approach makes APIs a basic building block for a cloud infrastructure. Their protection becomes a main concern of the cloud security [4].

Shared Environment: Cloud resources are virtualized, different cloud service users (possibly competitors) share the same infrastructure. One key concern is related to architecture compartmentalization, resource isolation, and data segregation. Any unauthorized and violent access to cloud service user's sensitive data may compromise both the integrity and confidentiality [4].

Flooding Attacks: The fourth issue is Flooding Attack. Attacker attacks the cloud system openly. The most significant feature of cloud system is to make available of vigorously scalable recourses. Cloud system repeatedly increase its size when there is further requests from clients, cloud system initialize new service request in order to maintain client requirements. Flooding attack is basically distributing a great amount of non-sense requests to a certain service. Once the attacker throw a great amount of requests, by providing more recourses cloud system will attempt to work against the requests, ultimately system consume all recourses and not capable to supply service to normal requests from user. Then attacker attacks the service server. DOS attacks cost extra fees to the consumer for usage of recourses. In an unexpected situation the owner of the service has to compensate additional money. Counter measure for this attack is it's not easy to stop Dos Attacks. To stop from attacking the server, Intrusion detection system will filter the malicious requests, installing firewall. Occasionally intrusion detection system provides fake alerts and could mislead administrator [6].

In [5], where Research has shown that it is possible for attackers to precisely map where a target's data is physically located within the "cloud" and use various tricks to gather intelligence. Another vulnerability to an attack is the use of denial-of-service attack and it has been found out that if an attacker is on the same cloud servers as his victim, a conventional denial-of service attack can be initiated by amping up his resource usage all at once[4].

Service level agreements [SLA]

Analysis done in [5], which details us about SLA, i.e. service level transfer between a service user and provider a SLA is been issued. A SLA [service level agreement] is a document which defines the relationship between two parties: the provider and the recipient. This is clearly an extremely important item of documentation for both parties [5]. If used properly it should: • Identify and define the customer's needs • Provide a framework for understanding • Simplify complex issues • Reduce areas of conflict • Encourage dialog in the event of disputes • Eliminate unrealistic expectations specifically it should explain a wide range of issues. Amongst these are usually the following:

1) Services to be delivered performance, Tracking and reporting problem management legal compliance and resolution of disputes customer duties and responsibilities security IPR and confidential information termination. The SLA is the Legal agreement between provider and client. The provider can gain the trust on his client is only through SLA [5].

2) These SLA are been used to fulfill the issues of the service user based upon the rules present in it but they would not go for any legal action if the not met

that present in agreement, they don't really help the customers fulfilling their losses. The SLA is fully not a good security consideration [5].

Service Level Objectives (SLO)

In [6] we got to understand SLO defines a characteristic of a service in precise, measurable terms. Here are some samples SLOs:

The system should never have more than 10 pending requests.

Throughput for a request should be less than 3 seconds.

Data streaming for a read request should begin within 2 seconds.

At least five instances of a VM should be available 99.99999% of the time, with at least one instance available in each of a provider's three data centers. Obviously different Service Level Objectives will apply to different use cases, applications and types of data. SLOs can also include an urgency rating to indicate the relative importance of different SLOs. A consumer could use an urgency rating to indicate that availability is more important than response time if the cloud provider cannot deliver both SLOs [8].

Different roles also affect the SLOs that apply. For example, consider an application written by a cloud consumer, hosted by a cloud provider and accessed by an end user. If the application and its data are hosted by the same cloud provider, chances are the application can access that data without leaving the provider's data center. The cloud consumer will expect very fast response times whenever the application accesses its data. On the other hand, the consumer will have lower expectations of response times whenever an end user accesses the application across the Web [6].

Secure Architecture Models

Open Security Architecture (OSA) provides free frameworks that are easily integrated in applications, for the security architecture community. Its patterns are based on schematics that show the information traffic flow for a particular implementation as well as policies implemented at each step for security reasons. The following description of a proposed cloud computing architecture, should help the reader envision the components of cloud computing architectures along with descriptions of elements that make it secure. The important entities involved in the data flow are end users, developers, system architect, 3rd party auditors and the cloud itself. The following summary looks at their attributions and mechanisms available for them [7].

Security Techniques & Algorithms

In [8], Sai & Khaja describes about the past researches & work done in Hierarchical Identity Based Encryption System where the user identities are well organized in the hierarchy basis and at each level in the hierarchy the node can assign various access rights to its subordinates. New users can enter the system and acquire the access policies without any changes to the already existing system. Thus by modeling the cloud system using the HIBE model can enhance the data security of the cloud. We can assume the hierarchy as shown in the figure 2. The root has the subordinates and they further have their subordinates and the access rights are issued to them by its higher level nodes. 4 HIBE - BASED DATA SECURITY Identity based encryption was first developed by Shamir later on constructed by Boneh, Franklin and Cocks. Using dual system encryption Waters provided another efficient IBE system with less public parameters. Hierarchical Identity based Encryption was first proposed by Horwitz and Lynn and constructed by Gentry and Silverberg.

Security Algorithms

RSA- is an algorithm for public-key cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. User data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [9].

MD5- (Message-Digest algorithm 5), a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks. The message is padded so that its length is divisible by 512 [9].

AES- In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper. Its algorithm is as follows: 1. Key Expansion 2. Initial Round 3. Add Round Key 4. Rounds 5. Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table. 6. Shift Rows—a transposition step where each row of the state is shifted cyclically a certain number of steps. 7. Mix Columns—a mixing operation which operates on the columns of the state,

combining the four bytes in each column 8. Add Round Key—each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule. 9. Final Round (no Mix Columns) 10. Sub Bytes 11. Shift Rows 12. Add Round Key Encryption- converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text [9].

3. Problem Domain

Our current challenge & problem domain involves securing Cloud Computing data & its access methodology. This is our need, where we require looking out a way, that an illegal intruder do not has access to any confidential & secure information. Identifying how can we ensure that SaaS & PaaS layers have few more levels of safety measures that would help to further secure data & its access on global platform. We work to choose certain algorithm & design a system in this review paper, which can be light on network giving less overhead of encryption & decryption time space & does a nice job in encrypting information over the public channel of communication TCP, UDP under client server networks.

4. Proposed Design

We can have couple of network entities on SaaS & PaaS layers stated as below:

• Cloud Service User: This is an individual or set of people or a Company which uses / need or requested for the Cloud services from a Cloud Network Service Provider. Now this user can be on any Mobile Device like phone or tablet.

• MCNSP: Mobile Cloud Network Service Provider is an Organization / Company, which provides Cloud related Services, Resources and Database etc to User. It is capable in supervising the client systems & operating Cloud information processing & managing Networks. These can be set or sub sets of system to manage cloud & would reside on our expected SaaS & PaaS Layers shown Framework (Fig. 2)

In our cloud data storage, a user submits/stores his desired information through MCNSP into a set of cloud networked server (IaaS Layer), which are running in a distributed manner. For application purposes, the user has to interact with the cloud network server via MCNSP to access or retrieve his information back on his local system. In certain conditions, when users need to have its information protected, it has to go through certain defense methodology & validations to prove its legitimacy. This have to be done on SaaS layer or PaaS layer to ensure that we get rid of heavy encryption of data at IaaS layer which could leads to a slow and time consuming effort to retrieve the correct information back. This means that we may have to ensure that users have valid tools & methods to continuously monitor, validate its information over its Cloud environment. These could be its mobile devices as well, understanding & assuming that user is connected to the Cloud Network Service provider through some secured & reliable tunnel with legitimate authentication ways like SSL or else. So the overall idea here is to authenticate the user & its access level & privileges on the application layer itself rather than encrypting data at lower levels, every time this may not be a feasible case & in case the data/ information size grow in due course of time, So it would help us to remove a major overhead of encryption of information at the database or infrastructure (IaaS) layers.

To achieve the objective of security and dependability for cloud data storage over SaaS & PaaS layers, we have certain objectives for our security validation & authentication: (a) Error Corrections & detection on Application layer: Identify the network status, whenever we identify that information has been damaged. (b) Availability of features like modification, correction removal of information from the Cloud network on user request. (c). Restrict the illicit intruder to go through the cloud network for accessing the information & incessant monitoring of system (d) The system & software should be simple & easy to use & should be competent to using the nominal resources. (e) Use of Mobile Tech: Possibility of getting some alerts & basic information to the normal end users.

Initially user is when registered to the Cloud Network Service provider we generate a authentication code (this is an Encrypted code) that is available only to user, we can say it second password, but this is not like a normal passkey & it's called as an validation key for the validating the user & its network, User is allowed to keep its information publicly accessible to all or either secured & restricted i.e. accessible only by providing legal key. Once this key is provided to the source service provider, it actually authenticates the key along with the network from where the request has been made, this validation is called as a "Digital Confirmation" if such information is authenticated & user is authorized he is able to see & download & make changes to it, the information else

invalided & information is thrown to the user. Simple but effective encryption & decryption algorithms stated below can be used.

Choose parameters P, Q Array values
Function GenerateaTokenValue as long --> v,
long --> k
Start procedure
Set unsigned long pz=p[0],qx=p[1],
Set Total =0
Code =< Random Alphanumeric Code>, n=32
We have considered n= 32 for 32 bit encryption; it can be modified to 16 or 8.
Do till n-->0
Begin Loop
Assign Total = code + Total ;
Yz = Yz+ ((zx << 8)+ qx[0]) ^ (zx + Total) ^ ((zx>>9) + kx[1]) ;
zx = zx + ((yx<<8)+qx[2]) ^ (yz+Total) ^ ((yx>>9)+qx[3]) ;
End Loop
These finally generates main key Yz and validation key Zx. P[0]=yx ; p[1]=zx
End procedure
Store all these keys at the Cloud networks Server Side. They will help us authenticate user & retrieve its desired information from Cloud Network when accessed from any client environment.

5. Conclusion

With increasing in usage of various methodologies for keeping & validating the information we need to look forward into various ways to access & restrict availability of information to proper environment & persons. There is always been an attempt in encrypting the data at the lowest layer of any architecture, this is to ensure that illegal usage of information is confined, this does not look realistic always, looking at the large chunk of information available over internetwork & when using technology like Cloud, which heavily uses the wireless technology & has many limitations of speed bandwidth & also severe concerns about illegal access over internet & availability of resources as of now. We have to think further more on the higher side to understand & design a data & channel security algorithm or adding security layer in environment like on application layer (SaaS & PaaS), which has an ability to be less venerable to any kind of network attack in Cloud & only allows proper person to access its proper data in authorized format. To achieve this we have mobile Cloud methods, with increase in use of Mobile technologies, which poses limited resources but are capable in playing an critical role in security of information in various forms like in case an intruder tries to access personal information.

References

[1] Webpage "Top five cloud computing security issues",[Online] www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues/.
[2] Arif Mohamed, "History of Cloud Computing" [Online] http://www.computerweekly.com/feature/A-history-of-cloud-computing.
[3] Han Qi & Abdullah Gani, "Research on Mobile Cloud Computing: Review,Trend and Perspectives", IEEE, Digital Information and Communication Technology and it's Applications (DICTAP), 16 May 2012.
[4] Kangchan Lee, "Security Threats in Cloud Computing Environments1", International Journal of Security and Its Applications,Vol. 6, No. 4, October, 2012.
[5] Anurag Porwal and Rohit Maheshwari and B.L.Pal and Gaurav Kakhani,"An Approach for Secure Data Transmission in Private Cloud", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-1, March 2012.
[6] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases A white paper produced by the Cloud Computing Use Case Discussion Group", Version 4.0, 2nd July 2010.
[7] Traian Andrei, "Cloud Computing Challenges and Related Security Issues", Cloud Computing Challenges and Related Security Issues. A Survey Paper, April 30, 2009.
[8] Sai Krishna Parsha and Mohd.Khaja Pasha,"Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE)",International Journal of Scientific & Engineering Research Volume 3, Issue 5, May-2012,ISSN 2229-5518.
[9] Suresh & Prasad, "Security Issues and Security Algorithms in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012 ISSN: 2277 128X.
[10] Wikipedia "Mobile cloud computing" [Online] http://en.wikipedia.org/wiki/Mobile_cloud_computing.

Vineet Guha completed his Bachelor of Engineer (Computer Science & Engineering) from RGPV University; Bhopal, India in 2002, currently is pursuing M.Tech in Information Technology from LNCT, Bhopal, India.