International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-3 Issue-11 September-2013

Watchdog Technology to impose Information Authentication in Mobile Cloud over SaaS & PaaS Layers

Vineet Guha[1], Rajeev Kumar Shrivastava[2], Manish Shrivastava[3]

Abstract

Cloud computing is a revolution which has made this world of internet more like a place of storage & facilitator of new mechanism to deliver products from producer to consumer in a very different and efficient style of computing. Cloud Computing has made lots of changes not only in infrastructure side, but has also deeply impacted the software industry. More & more people are moving towards using this computing tech, But with every new thing emerging in this IT computing world, major concerns stands with security models to implement & how we can keep data secured & safe. This unique attribute, however, poses many new security challenges which have not been well understood yet. When we talk about the security of data in Cloud Computing the vendor has to ensure assurance to convince the customer on the security issues. Organizations are using cloud computing for confidential issues for their business applications though guaranteeing the security is difficult. With more & more people diverting towards high usage of Mobile technology. With more & more advance smart phones in market, do we have a way to interrelate & use Mobile Technology to alert & secure use of data & network in Cloud? How we can watch out the illegal intruders & how we can impose checks on illegal access to data & network. In this article we try to focus ourselves to find answers to all such questions & improvise the use of Mobile technology along with encryption methods in complex but future cloud computing domain.

Keywords

Cloud Computing, Mobile Cloud Computing, TEA, Cloud Security, EBCDIC

1. Introduction

Information security is a major area of concern in IT. With more and more usage of Internet & changing trend & future demand of using Cloud network for storing all the information & data for global access. Cloud security has become a major area of research & development, Cloud Computing security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It is the major concern of studies now days due to its popularity & future, It 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 centers, 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; Data Security concerns arising because both user data and program are residing in Provider Premises. Clouds typically have single security architecture but have many customers with different demands & requirements. Looking at all the perspectives with customer demands & emerging technology advancements we would need to find & work on more and more flexible & durable security solutions to fit such a network [5].

2. Literature Review

Cloud Computing – SaaS (software as a service) and PaaS (platform as a service) providers all trumpet the robustness of their systems, often claiming that security in the cloud is tighter than in most enterprises. But the simple fact is that every security system that has ever been breached was once thought infallible [1]. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment [2]. As with most SaaS offerings, the applications offering are constantly being tweaked and revised, a fact which raises more security issues for customers.

2.1 Latest Threats in Cloud Computing.

In [3], Responsibility Ambiguity: Cloud service users consume delivered 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, (mostly management APIs and PaaS services are one of the easiest attack vector). Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, 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: 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 [3].

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: 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. The strength of cloud computing in information risk management is the ability to manage risk more effectively from a centralize point [10].

2.2 Security Technique

In [6], 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. RSA- is one of the 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].

2.3 Mobile cloud computing

It is the combination of cloud computing and mobile networks to bring benefits for mobile users, network operators, as well as cloud providers. Cloud computing exists when tasks and data are kept on the Internet rather than on individual devices, providing on-demand access. Nearly every mobile should have a suitable browser. This means developers will have a much wider market and they can bypass the restrictions created by mobile operating systems. Mobile cloud computing gives new company chances for mobile network providers [7].

2.4 Framework

Cloud computing systems actually can be considered as a collection of different services, thus the framework of cloud computing is divided into three layers, which are infrastructure layer, platform layer, and application layer [1].

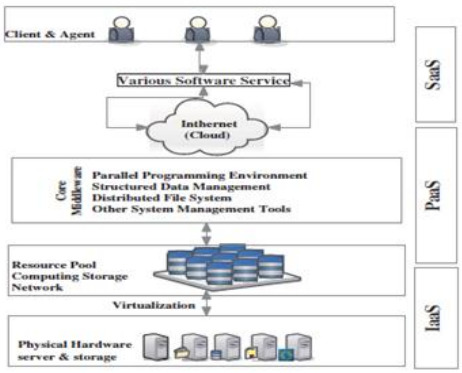

Fig. 2.1: The Framework of Cloud Computing [2].

The Framework of Cloud Computing

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 [2].
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 [2].
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 [2].

So our current challenge & problem domain involves securing Cloud Computing data as well as its channel information in Platform & Application layers.

3. Proposed Design

We can have couple of network entities on SaaS & PaaS layers that 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.

• **MCNSP:** Mobile Cloud Network Service Provider is an Organization / Company, which provides Cloud related Services, Resources and Database etc to User. They are capable of managing the client resources & operating Cloud information processing & managing Networks. These could be a set or sub sets of Software to manage cloud & would reside on our expected SaaS & PaaS Layers. 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 cases where users need to have its information secured it has to perform some security check & validations to prove its authenticity. 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 need to ensure that users have valid tools & technique to continuously monitor, validate its information over its Cloud environment. Understanding & assuming that user is connected to the Cloud Network Service provider through some secured & reliable channel with proper authentication methods 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 which may not be feasible every time in case the data/ information size grow in due course of time, This will also help us to remove a major overhead of encryption of information at the database or infrastructure level. To achieve the objective of security and dependability or 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). Restricting the illegal intruders to enter the cloud network for accessing the information & continuous monitoring of system (d) The system & software should be simple & easy to use & should be capable to using the minimal 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 Provider it actually authenticates the key along with the network from which the request has been made this validation is called as a "Digital Validation" 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 algorithm as shown below [10] is used.

Procedure for Token Generation & encryption
Algo. and code.
Procedure for Token Generation & encryption Algo.

Choose parameters Vx, Kx Array values
Function GenerateTokenValue as long Pointer v, long Pointer k
Begin Procedure
Set default values for variable yx=vx[0],zx=vx[1], sumx=0,
Generate deltacodex =< Random Alphanumeric Code>, taking n=32; this is for a 32 Bit encryption.

Start Loop n > 0
Begin
Do Sum of value sumx = deltacodex + sumx
Regenerate next Pass value using logic
yx = Yx+ ((zx<<4) + kx[0]) expo (zx + sumx) expo ((zx>>5)+kx[1])
Zx = Zx+ ((yx<<4) + kx[2]) expo (yx + sumx) expo ((yx>>5)+kx[3])
Reduce N by 1
End
Generate main key Yx and validation key Zx
Assign Value in Array vx[0]=yx ; vx[1]=zx

Repeat the Procedure as vx[0] & vx[1] as input values these will work as key for validation, Authentication & authentication.
Store all the keys at the Cloud Server Side. This will be used to authenticate user.
End procedure

Algorithm InformationEncryptionAlgo
Begin
Create two Constructors with the same name of the class Name. Like here

InformationEncryptionAlgo
new InformationEncryptionAlgo ()

Function Informationencrypt
Get the length of string to be encrypted.
bx[] = str.length()
Set a variable to with the Encrypted message will be stored (in Binary unit)
Encryptedoutput [] = str.length()
Bx = str.getBytes()
Loop till i<str.length()
Encryptedoutput[i] = (byte) ((byte) bx[i] (byte) 16)
End Loop
return ((Encryptedoutput)

End Algorithm

Algorithm for Decryption of the String
Algorithm InformationDecrypt
Identify the length of the Encrypted code
byte bx[] = str.length()
set this length to the array
DecryptedOutput[] = str.length()
bx=str.getBytes()
Loop till I < str.length
DecryptOutput [i] = (byte) ((byte) b[i]+ (byte)16)
Increment i with 1
End Loop
return ((DecryptedOutput)
End Algorithm

4. Results & Analysis

Tokens & related signature keys are generated of MCNS side which actually restricts invalid intruders to read files or login to system. Illegal intruder is being given information that you are not authorized to read the information. All we can set is some junk data so as intruder can never make out that he was not show the right information from the Cloud server. Third Colum shows an Encrypted key generated for the user to access its data which is actually validated at the server side before he is allowed to access or review his information

Fig 4.1: Key stored in DB with reference to User.

Fig 4.2: internally information is being reviewed for illegal intruder accessing the information

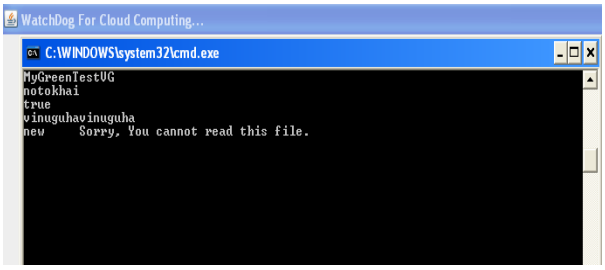

Fig 4.3: Encrypted information kept on the server side

Fig 4.4: Encrypted user information on the Server side

With this proposed system, it's an effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' information in the cloud. We rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. Whenever data corruption has been detected during the storage correctness verification, our scheme can ensure the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s).

1. Compared to many of its predecessors, which only provide binary results about the storage state across the distributed servers, the challenge-response protocol in our work further provides the localization of error.
2. For best results it is being identified that encryption codex value our algorithm should be multiplied by 2m (m is a set of bits to be encrypted like 2, 4, 8, 16 etc. sumx is set to be deltacodex * n (n stands here for number of loops in the algorithm). Call the functions is arbitrary: Decryption (Encryption (P)) = Encryption (Decryption (P)).
3. Below is sample result generated for encryption that was done to generate the key value & encrypt user information. Remember we need to pass "Sample Key" & "User Value" given by user as Vx & Kx

Below is Sample example result set generated by the algorithm.

User Input Key: Vx [0]= "123456"
Vx[1] = "12345678"
Loop 1
Key Code Identified [Kx] = 0x0000
Resultant Encryption is: 0x9e3779d9 dae8b32f,
Encoded Information = 0x9e3779d9dae8b32f
Loop 2:
Key Code Identified [Kx] = 0x1000
Encoded Modifies to data = 0x60a9d239b3681922
Encoded Information = 0x60b9d23ad3681904
Loop 3:
Key Code Identified [Kx] = 0x2000
Encoded Modified data = 0xa22fe2693d005643
Encoded Information = 0xa22df4723b0077ec
Loop 4:
Key Code Identified [Kx] = 0x3000
Encoded Modified data = 0xb199be65390bd63
Encoded Information = 0xb177cd75361e7b2
Loop 5:
Key Code Identified [Kx] = 0x4000
Encoded Modified data = 0xa57900b9761f765a
Encoded Information = 0xe0348261bf0475cb
Key Code Identified [Kx] = 0x5000
Loop 6:
Encoded Modified data = 0x4b9b76adc87de75b
Encoded Information = 0x78d912d85da8e081

4. It is being identified that while working on the low bits like 2, 4 & less number of loops. The results were poor & the encryption key that was being generated was repetitive & less effective. This is one of the major issues with TEA algorithm used.
5. But unlike most prior works for ensuring remote data integrity, the new scheme supports secure and efficient dynamic operations on data sets, including: update, delete and append. To brief, looking at the results & time involved in encryption & decryption process, it clearly shows that the user information is registered well encrypted & is fairly unusable & for any intruder trying to access the cloud data. Secondly whenever user is registered to a cloud service provider it generates a key for the user which is then used for handshaking b/w client machine & Cloud Network service provider to retrieval of data real time. The total effective time to access data using this encryption & key validation is much more less than the total time consumed in Encryption & decryption of data at IaaS layer itself.

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 effort majorly in encrypting the data at the lowest layer of any Architecture to ensure that illegal usage of information is protected, this does not look feasible always looking at the large chunk of information available over internetwork & using technology like Cloud which heavily uses the wireless technology & has many limitations of speed & severe concerns about illegal access over internet & availability of resources as of now. We have to think further more on the higher side to create an environment like application layer (SaaS & PaaS) which has an ability to be less venerable to any kind of network attack &

only allows proper person to access its proper data in authorized format. Similarly with increase in use of Mobile technologies which has 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 or critical information from the Cloud Network alerts are being triggered etc. Involvement of Mobile Technology along with Cloud can certainly help us to deal with security issues to an extent keeping in mind the limitations of mobile tech as of now.

References

[1] Han Qi & Abdullah Gani, "Research on Mobile Cloud Computing: Review,Trend and Perspectives", IEEE, Digital Information and Communication Technology and it's Applications (DICTAP), Second International Conference 16 May 2012.

[2] David Binning, "Top five cloud computing security issues", [Online] Available: http://www.computerweekly.com/news/2240089111/Top-five-cloud-computing-security-issues, APR 2009.

[3] Kangchan Lee, "Security Threats in Cloud Computing Environments1", International Journal of Security and Its Applications,Vol. 6, No. 4, October, 2012.

[4] Anthony Bisong and Syed (Shawon) M. Rahman, "An Overview of the Security Concerns In Enterprise Cloud Computing", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.1, January 2011.

[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] 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.

[7] 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.

[8] 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.

[9] Traian Andrei, "Cloud Computing Challenges and Related Security Issues", Cloud Computing Challenges and Related Security Issues. A Survey Paper,April 30, 2009.

[10] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing” proceeding of International workshop on Quality of service 2009”, pp.1-9.

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.

Prof. Rajeev Shrivastava is currently working as an Assistant Professor in Department of Information Technology, LNCT, Bhopal.

Dr. Manish Shrivastava had started his carrier with Software companies and worked for SIS (P) Ltd. and TCS at PMU, after completing his graduation in Computer Technology from UIT, RGPV (Technical University) (formerly Govt. Engineering College), Bhopal, India in 1993. He left software industry in 1998 & switched to academics and has been working with reputed private engineering colleges since last fourteen years. He did M.Tech. & PhD from MANIT, Bhopal, India in Digital Communications & Optical Communications respectively. He has software development, teaching and research experience of more than 18 years. Presently he is working as Director, PG Education & Research Center, LNCT, and Bhopal, India.