RESEARCH ARTICLE OPEN ACCESS

Data Security in Mobile Cloud Computing Using TOTP Generated By HMAC-SHA1 Algorithm

D. Divya Priya [1], A. Mahalakshmi [2]
Assistant Professor [2]
CMR Institute of Technology Hyderabad
India

ABSTRACT
Mobile Cloud computing is a collection of easily usable and accessible transitive resources dynamically allocated. It is a model for accessing data that is ready for gathering / retrieving data from a pool of shared resources. In mobile cloud computing data storing and data processing can be done in the outside world. Mobile cloud applications can save the mobile resources power and storage capacity and also bringing cloud data to be accessible easily and efficiently. To secure mobile data i.e. accessing everything from anywhere i.e. when identity are in move we can access data using many devices and access critical, business data overtime. We can secure the data by using username and password. An additional method for authenticating the data is HMAC-SHA1 algorithm.
Keywords:- Mobile Cloud Computing, HMAC-SHA1algorithm, security issues , architecture, challenges.

I. INTRODUCTION

1.1Cloud Computing

Cloud computations are transforming the way of transform data making IT more efficient and cost factors. Cloud computing is the transferring of data and computing the queries and storing them which are given to end-users. Cloud security is really important .It is the use of latest technologies and security techniques to protect our data application and infrastructure associated with cloud computing. To overcome on threats we can upgrade technology of techniques. Choosing of public, private or hybrid.

1) Private: To store the highly confidential files in cloud platform. We have dedicated servers on our premises.
2) Public: Files that is not important. We can easily hosting the websites. The cost is very effective.
3) Hybrid: Private files stored on our own premises.

Cloud security is combination of arts and science. It is a science because we have to come up with new ways of securing our application. It is a art because authentication should be defined with users experience in mind.

Trouble shooting a threat in cloud:

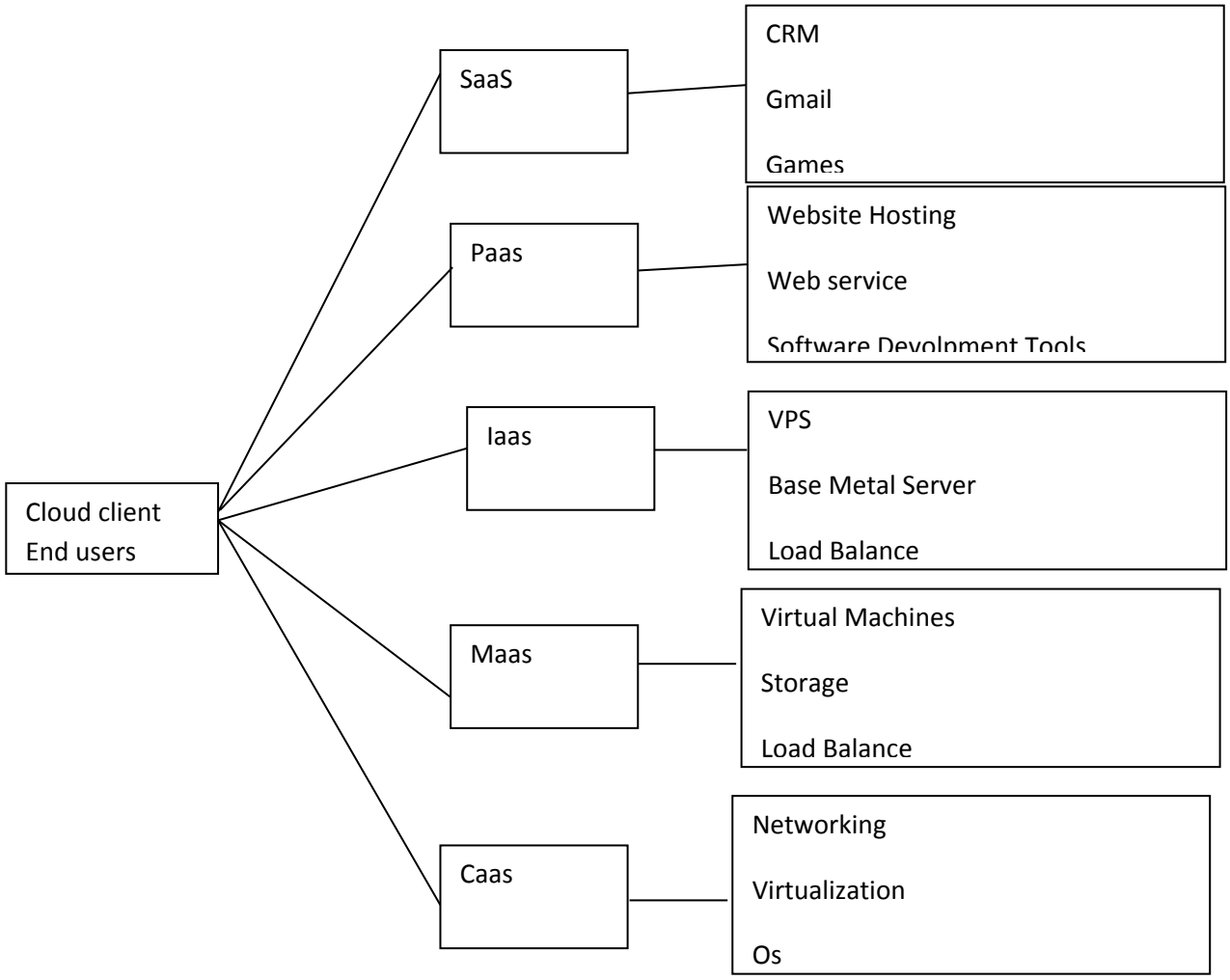
Monitoring data: Cloud security by experts.

Gaining visibility: Tools to look in to that data.

Managing Access: A list of users who have accessed we can eliminate the user.

Cloud Service Models:

Cloud computing is a model for enabling the data seems to appear everywhere at the sometime conveniently, on-demand network access to a shared collection of configurable computing resources (e.g., networks, servers, storage, applications, and services)it is for service provider which requires less effort.



Mobile Cloud Computing:

Mobile cloud computing is a smart way to reduce cost of IT services provide anywhere and anytime. In MCC data can be encrypted and stored for future retrieval. MCC is used to access data securely anywhere and anytime without carrying the computer. Mobile computing can be divided into three categories:

i)mobile hardware

ii)mobile software.

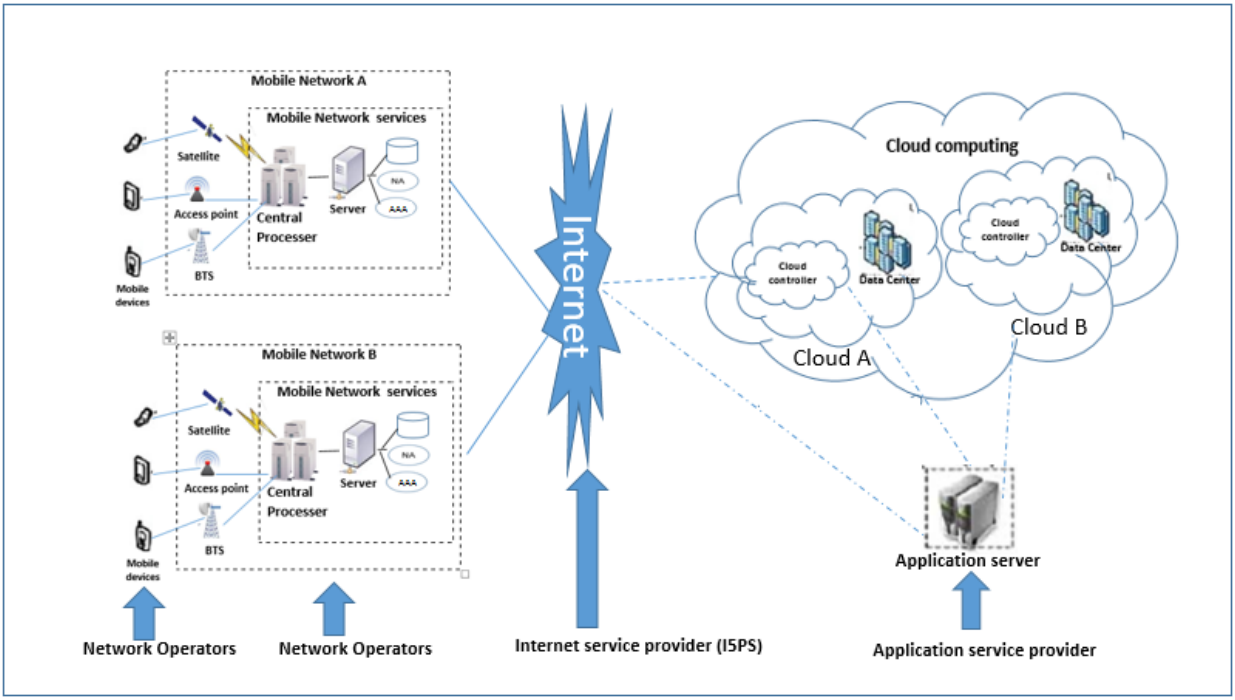
iii)mobile communication.

In mobile cloud computing data storing and data processing can be done in the outside world. . Mobile cloud applications can save the mobile resources power and storage capacity and also bringing cloud data to be

accessible easily and efficiently . By securing the mobile data many customers are encouraged to place their data on the cloud.

Mobile cloud computing architecture:

Mobile phones are connected to satellites and different access points which are connected and central process of our system servers. Both mobile nodes A and B are similar connected to a internet or ISP.These ISP connect the mobile network to cloud controlled which controls data centers cloud A &cloud B.Now the analysis of impact of mc on various services shows how the mobile computing changed each service as mobile computing. It has become an container developed as hardware, software and network.



Applications:

- Mobile cloud computing in e-commerce.
- Mobile cloud computing in Healthcare
- Mobile cloud computing in e-learning
- Mobile cloud computing in Gaming
- Mobile cloud computing in security system
- Mobile cloud computing in Face recognition.

Multifactor Authentication Factors:

1)USB Tokens

2)Mobile applications: It is an application already available on mobile platforms like IOS,android .With then applications when we entered username and password we have to provide second factor.

push notification: we can get codes.

One-Time Passwords

3)Phone call: Phone call through a landline and mobile phone that will take as through some steps and gets proved identity.

4)Text messages: Similar to push notification but this time push notification through message.

5) Biometrics

6) Http request and response attributes

7) Hardware and software challenge/response

8) PKI certificate.

II. PREPARATION OF YOUR PAPER

[1][2][3]It presents three generations of mobile cloud service infrastructures by comparing their key features and limitations. Moreover, the paper discusses the issues, challenges, and needs in mobile cloud computing for future research.[4] components should support security applications such as message integrity, authentication, and time stamping are done by using the hmac algorithm. [5][6] The HMAC based protocol with signcryption can prevent the attacks and gives the guarantee for authentication and integrity.[7] [8]Introduced the application level security solution, secure web authentication protocol is a multifactor authentication protocol. Protocol is extended as a Two Way Authentication to support mutual authentication and also suggested that same solution can also be implemented to secure B2B communication with very small modification to the protocol. Proposed system is secure against internet based attacks. It is also secure in case of lost or theft of mobiles devices. The protocol can be implemented within limited resources of a Java MIDP device, without any modi-fication to the existing communication protocols or wireless network infrastructure.

III. EXISISTING SYSTEM

In previous systems tokens can be generated by using and batch of codes and pictures .In picture based techniques the user is guided to select a picture from a set of different pictures which are generated by a program. Then the user is authenticated by selecting /identifying those pictures again. The drawback of this is the server has to save the images in the form of plain text.

IV. PROPOSED SYSTEM

Multifactor Authentication USING HMAC TIMESTAMP OTP:

To secure mobile data i.e. accessing everything from anywhere i.e. when identity are in move we can access data using many devices and access critical, business data overtime. We can secure the data by using username and password. An additional method for authenticating the data is multifactor authentication.

Providing an additional level of authentication by using TOTP HMAC algorithm we can predict unauthorized access for cloud apps and resources . It can be used in addition to username and password. Trusted by thousands of enterprises to authenticate employee,customer,partner and security options.

In our proposed system otp is generated by depending on the HMAC algorithm.OTP is one of the most popular technique of two factor algorithm.Authentication provided by this is secure and stronger.the user gets the OTP to their email or phone by entering the user succeds from the login page

Algorithm: FOR HMAC OTP GENERATION

- *Assume that there are two variables let L=* secret key
- *D* =counter
- *Hashmobauth*(*L*,*D*) = SecureHashAlg1(*L* ⊕ 0x5c5c… ‖ SecureHashAlg1 (*L* ⊕ 0x3636… ‖ *D*)) with ⊕ as XOR, ‖ as concatenation, for more details see HashMoileAuthenticationCode (D is the timestamp)
- *Truncate*()which selects 4 bytes as OTP from the result of the

HashMobileAuthenticationCode in a defined manner

Then **HOTP**(*L*,*D*) is mathematically defined by

HOTP(*L*,*D*) = *Truncate*(*HMAC*(*L*,*D*)) & 0x7FFFFFFF

The mask 0x7FFFFFFF sets the result's most significant bit to zero. This avoids problems if the result is interpreted as a signed number as some processors do.For HOTP to be useful for an individual to input to a system, the result must be converted into a HOTP value, a 6–8 digits number that is implementation dependent.

HOTP-Value = **HOTP**(L,D) mod 10^d, where *d* is the required number of digits

And here we are adding the timestamp for our otp generation using hmac

We define TOTP as TOTP = HOTP(L, D), where D is an numeric value which represents the number of time slots between the initial counter.

TOTP HMAC algorithm flow:

- Request webpage.
- Obtain login page from provider.
- Request security token.
- Validate credentials with identity proider.
- Obtain second factor mechanism from provider.
- Presnt to client.
- Client submits required second factor details and submit to provider.
- Send a security token.
- Create security token and send page.

V. CONCLUSION

TOTP generation using HMAC algorithm we are combining a hash with a secret key for a particular time slot and generates OTP.It verify data integrity and authenticity .it is used in all network encryption protocols .You can take this implementation further, by generating QR codes for mobile devices to scan, making it as trivial as installing a mobile application, scanning the code, and using the tokens as needed.

REFERENCES

[1] Zohreh Sanaei, Saeid Abolfazli, Abdullah Gani, Muhammad Shiraz, "SAMI: Service-Based Arbitrated Multi-Tier Infrastructure for Mobile Cloud Computing", IEEE MobiCC'12 conference, MobiCC 2012:IEEE Workshop on Mobile Cloud Computing, Beijing, China.

[2] Dijiang Huang, "Mobile Cloud Computing", IEEE COMSOC MMTC E-Letter, April, 2011.

[3] Z. Sanaei, S. Abolfazli, A. Gani, and R. H. Khokhar, "Tripod of requirements in horizontal heterogeneous mobile cloud computing, " Proceedings of the 1st International Conference on Computing, Information Systems, and Communications, 2012.

[4] Benjamin Arazi, Senior member,IEEE,"Message Authenticaiton in Computationally Constrained Environments",IEEE Trans. Mobile Computing ,Vol.8 ,No.7 July 2009.

[5] Smith- Mstr Thesis, Dig " ittal signcryption " ,thesis presented on Combinatorics and Optimization Waterloo,Ontario ,Canada,2005.

[6] National Institute of Standards and Technology, "The Keyed-Hash Message Authentication Code (HMAC)," FIPS PUB 198, Information Technology Laboratory, 2002.

[7] White paper: Enhanced Online Banking Security, Zero Touch Multi-Factor Authentication, November2006, http://www.entrust.com/resources/download .cfm/22600/EfraudWhitePaper.pdf.

[8] S. Kungpisdan, B. Srinivasan and P.D. Le: (2004), A Secure Account-Based Mobile Payment Protocol, Proceedings of the International Conference on Information Technology: Coding and Computing, IEEE CS press, Las Vegas USA, volume 1, pp. 35-39. April 2004.