SURVEY ON A LOCATION AND TIME BASED FUNCTION FOR SECURE ACCESS OF CLOUD SERVICES

Damini Prajapati[1] , Dishant Soni[2], Krunal Suthar[3]
[1]Research Scholar Sankalchand Patel College Of Engineering, Gujarat,India.
[2,3]Assistant Professor Sankalchand Patel College Of Engineering, Gujarat,India.

Abstract:Location-based cloud services (LBS) are highly popular, LBS are the services provided to the user according to their real-time and location. But as we know cloud computing has certain limitations, so does LBS pursue. Several techniques such as Anonymity, Obfuscation, and Multi-factor authentication are used for location and user identification privacy. So survey has to be made in this direction to identify problems and the better solution. We emphasis the Location-based applications and their security issues in computing.

Index terms: Location and time based cloud services, Authentication, Authorization, and Encryption Techniques.

I. INTRODUCTION

Cloud computing is one of the hottest core technical topics in the modern era. According to the National Institute of Standards and Technology (NIST) definition , "the cloud computing is a model for enabling convenient, resource pooling, ubiquitous, on-demand access which can be easily delivered with different types of service provider interaction" [1]. The cloud computing follows simple "pay as you go (PAYG) model, where you pay for the services you've used.Cloud computing implements virtualization technique is to provide resources efficiently to the end user.Cloud computing offers mainly three service delivery models; Infrastructure as a Service (IaaS), Platform as a Services (PaaS) and Software as a Service (SaaS). NIST defines four-development model of the cloud: public, private, hybrid and community.

Cloud service delivery models:

Cloud services are typically deployed based on the end-user (business) requirements. The primary services include the following:

Software as a Service (SaaS)

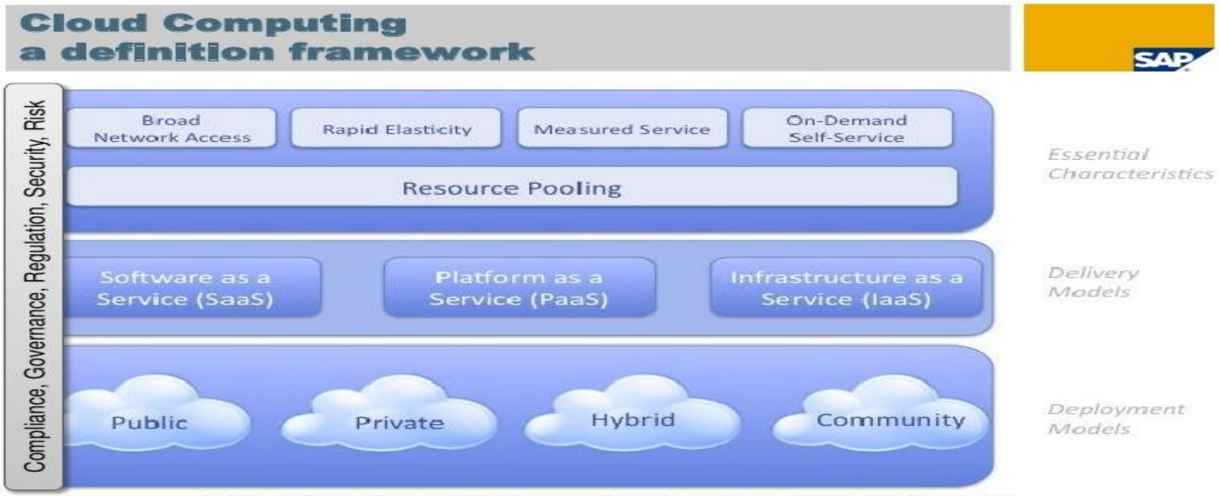
A software delivery method that provides access to software and its functions remotely as a Web-based service. Software as a Service allows organizations to access business functionality at a cost typically less than paying for licensed applications since SaaS pricing is based on a monthly fee [2].

Platform as a Service (PaaS)

A computing platform being delivered as a service. Here the platform is outsourced in place of a company or data center purchasing and managing their own hardware and software layers [2].

Infrastructure as a Service (IaaS)

A computer infrastructure, such as virtualization, being delivered as a service. IaaS is popular in the data center where software and servers are purchased as a fully outsourced service and usually billed on usage and how much of the resource is used [2].



Reference: "Rational Survivability Blog". Chris Hoff. http://www.rationalsurvivability.com/blog/?p=519

Fig.1Cloud computing framework.

Cloud Issues and challenges:

1. Security and Privacy

The main challenge to cloud computing is how it addresses the security and privacy concerns of businesses thinking of adopting it. [3]

2. Interoperability and Portability

Businesses should have the leverage of migrating in and out of the cloud and switching providers whenever they want, and there should be no lock-in period. Cloud computing services should have the capability to integrate smoothly with the on-premise IT. [3]

3. Reliability and Availability

Cloud providers still lack round-the-clock service; this results in frequent outages. It is important to monitor the service being provided using internal or third-party tools. It is vital to have plans to supervise usage, SLAs, performance, robustness, and business dependency of these services. [3]

4. Performance and Bandwidth Cost

Businesses can save money on hardware but they have to spend more for the bandwidth. This can be a low cost for smaller applications but can be significantly high for the data-intensive applications. Delivering intensive and complex data over the network requires sufficient bandwidth. Because of this, many businesses are waiting for a reduced cost before switching to the cloud. [3]

Why and what is Location based services?

Location based services (LBS) are **services** offered through a mobile phone and take into account the device's geographical **location**. LBS typically provide information or entertainment [4].

LBS is one of the solutions for security and privacy issue of cloud computing.

II. RELATED WORK

[Yan Zhu et al 2013] in [5]authors have recognized a problem with LBS fine-grained access control. In this paper, three different parties such as Mobile User, Trusted Third Party (TTP) and LBS Provider are in communicating with each other. They have introduced spatiotemporal predicate-based encryption (ST-PBE) fine-grained access control scheme for ensuring data policy, In which authors have used Attribute-based encryption (ABE) privilege constraint such that minimum guarantee that the user's information cannot be obtained by LBS Providers. Whenever the user requests to LBS Provider for desired data, S/he already have a certificate issued from TTP which has a private key and the certificate will anonymously authenticate the user, So that the LBS can receive user query in a secure way. The LBS Provider process the data according to location and sent the cipher text to the user and the user can only decrypt the data with the obtained private key from the certificate.

[Y.Lalshmi Prasanna et al 2014] in [6] authors have examined various LBS encryption techniques, which are:

i. The geo encryption techniques: The encryption techniques used before are based only on data but in this encryption, the data, has been encrypted according to the specific position, velocity, time (PVT). The PVT block defines the recipient's location and the data will be encrypted according to PVT.

ii. Location Dependent Encryption Algorithm (LDEA): In this encryption technique the author has introduced Toleration Distance (TD) which can be any distance around 10 or 20 meters that allow the data to be encrypted by XORing the session key to the Hashed data and regarding that bounded area so that an attacker could not gain exact location to decrypt the ciphertext.

iii. Self-Encryption: In this encryption technique the dataset is treated as a binary bit stream and the keystream is generated by extracting n bits in a pseudo-random manner based on user's unique PIN and a nonce and the remaining data stream is encrypted with this keystream. The advantage of this method is that the original data stream cannot be obtained from the ciphertext.

iv. Mobile User Location specific Encryption (MULE): This encryption technique is used for mobile user, when a User wants to access sensitive file, MULE contacts Trusted Location Device (TLD) which transmit key according to location and the user can decrypt the file and after decrypting the file if the user will move to another location than the data has been encrypted on its own and the user again have to request to TLD for key for that location.

[Marcos Portnoi et al 2016] in [7] the authors have introduce LOCATHE (Location- Enhanced Authenticated Key exchange), a generic protocol that provides multifactor and two tier authentication for two parties such as a user and a service for establishing secure session and mutually authenticate with additional factors. Service employ multi-authority CP-ABE, so that participating services and relying parties can control their own Attribute Based Encryption (ABE) secret key generation and update and access policies.

[Ruchika Gupta, Udai Pratap Rao 2017] in [8] authors has found a problem with Trusted Third Party because all the data queried are available at the central node which results the central node susceptible to privacy attack so the authors have introduced CAST (CAching with TRust) model in which the authors have mentioned that the data needed by other users are available in the cache memory of Mobile devices so that the data is available on various devices and the mobile user can access that data by establishing P2P (Peer to Peer) connection with other Mobile devices. This formation of devices is based on the interests of users and the authors also provided Fulfillment count (FC), Exchange count (EC), Raised flag count (RFC) for identifying the malicious users and providers in the P2P connection.

[Hanunah Othman et al 2010] in [9] authors found the problem with privacy enhancement with user's personal data, and for that, they have used Privacy Enhanced Technologies (PETs). With that, the authors also have proposed a group signature scheme known as Direct Anonymous Attestation (DAA) to anonymously identify users. In this, they have integrated DAA, LBS and Trusted Platform Module (TPM). DAA Issuer is a third party that provides the blind signature to TPM prover, then prover generates DAA signature and verified it with the verifier (LBS) that whether the client is registered and authorized and thus the communication going on in a secure way.

[Hao Zang et al 2013] in [10] authors have found Serious privacy concerns for cautious users are present in LBS, So the authors have proposed solution that leverages a mobile cloud computing paradigm, in which each mobile device is replicated with a system-level clone via a peer-to-peer (P2P) protocol in a proximate cloud environment. So that there is no theft of single point failure, load balancing and overhead reduction, which also protect the location and value privacy of the individual user in presence of malicious user.

III. CONCLUSION

In recent era, different security issues are faced by cloud computing environment, there are various types of threats regarding data privacy, user identification, data breaches, system vulnerabilities and so on. And that tends the cloud provider to implement various cryptographic techniques and authentication techniques and thus by doing rigorous survey we come up with idea to explore Location-based services as one of the good solutions, but we found that LBS has limitations such as user identification, data transfer, location revelation and access control and that drives us to make survey regarding the security issues regarding LBS and the solutions are enough strong to complement LBS.

REFERENCES

[1] Saurabh Singh, Young-Sik Jeong, Jong Hyuk Park “A Survey on Cloud Computing Security:Issues, Threats, and Solutions”.https://doi.org/10.1016/j.jnca.2016.09.002

[2] Beal, Vangie. “Cloud Computing.” What Is Cloud Computing? Webopedia Definition, www.webopedia.com/TERM/C/cloud_computing.html.

[3] CloudTweaks. “Top Five Challenges Of Cloud Computing.” CloudTweaks, 17 Apr. 2017, cloudtweaks.com/2012/08/top-five-challenges-of-cloud-computing/.

[4] www.google.co.in/search?q=location%2Bbased%2Bservices%2Bdefinition&oq=locati&aqs=chrome.2.69i57j0j35i39l2j0l2.7247j0j8&sourceid=chrome&ie=UTF-8.

[5] Yan Zhu, Di Ma, Dijiang Huang, Changjun Hu. “Enabling Secure Location-based Services inMobile
Cloud Computing” 27-32.IEEE-2014.

[6] Y. Lakshmi Prasanna, Prof. E. Madhusudhan Reddy “A generalized study on Encryption Techniques for Location based Services.” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul –Aug. 2014), PP 19-26www.iosrjournals.org.

[7] Marcos Portnoi, Chien-chung shen, “Location Enhanced Authenticated Key Exchange.” 2016 international conference of computing, networking and communications(ICNC), Workshop on Computing, Networking andcommunications(CNC).

[8] Ruchika Gupta and Udai Pratap Rao “Achieving Location Privacy through CAST in location based services.”239-249, JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL. 19, NO. 3, JUNE 2017

[9] HanunahOthman,HabibahHashim,lamalul-lail AbManan“Aconceptualframework providingDirect
Anonymous Attestation(DAA) protocol in trusted location basedservices”IEEE.

[10] Hao Zhang, Yonggang Wen, Nenghai Yu and Xinwen Zhang‡ Privacy-Preserving Computation for Location-based Information Survey via Mobile Cloud Computing”2013 2nd IEEE/CIC International Conference on Communications in China(ICCC) Future and Mobile Interment(FMI).