International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

GPS Based Authentication Mechanism in Cloud Computing

Prince Jain[1] ,Umesh Kumar Pandey[2]

[1]Research Scholar MSIT, MATS University Raipur CG (India)

[2]Research Supervisor, MSIT, MATS University Raipur CG (India)

ABSTRACT

Cloud Computing is a concept of modern and smart computing world. People buy high configuration computer system for their use but a little amount of the total capacity is used by them. So, computing power and money both becomes waste. This results in producing very large amount of hardware waste due to frequent buying of new system. The solution of this problem is cloud computing. In cloud computing environment the client's whole data is on cloud server which is offered by cloud service provider (CSP). Cloud service provider offers facility of processing power, storage space, software etc. The whole data of user is on cloud server and accessed by user through login credentials. Cloud computing reduces the on-demand hardware and processing power requirement of these days. As the whole data of user is on server side and all the processing is done on cloud server, if any attacker gains login credentials s/he may misuse the data. This paper proposes a user authentication scheme which works using GPS coordinates and user device combination, if any attacker gains the login credentials and user device also, s/he will not be able to access the service provided to the user and is also restricted to login into the cloud system out of the specified region.

Keywords- Cloud computing, GPS Based Authentication, Security in cloud computing

I.INTRODUCTION

The main concept behind the cloud computing is that instead of installing many servers and buying new hardware for short term, or for a time period, user can get these requirement as a service. User has to pay only for the amount of service used by him or her. In cloud computing software is provided as service, and platform is also pro-vided as service. The user only has to pay according to his/her need, and after that, if user doesn't want to continue then user can discontinue the one or more services. Suppose any user requires a 50 octa core CPU, for any high-end project, for the project duration of 6 months, in this case, conventional user has to own hardware and install, in this case there will be two options for the user, either user will buy required hardware or bring on rental basis and maintain it by its own. But in cloud computing user is free from all these worries, the user only has to register on the cloud service providers site, and have to configure the hardware, software, and platform using GUI or CUI feature, provided as a service, according to need i.e. hourly, daily or monthly. Here two benefits for the user, first s/he does not have to bring hardware and configure and test it, for proper working. Second if some hardware or software is urgently required, it can be arranged quickly and easily through GUI provided by Cloud Ser-vice Provider. This paper considers that the user is accessing his/ her cloud account by registered devices only, and those devices having GPS inbuilt or external GPS attached to it, and a wearable device with them which is also having GPS inbuilt. User cloud account is restricted to the registered region

defined by the user, at the time of registration. Accessing the account from outside the registered region is permitted using OTP authentication mechanism.

II.RELATED WORK

Number of researches is done in the area of user authentication in cloud computing. Some of the work which is discussed below: -

Raina P and Patel B proposed ascendable and economical, user authentication, them, in their paper "Authentication Scheme in Cloud Computing Environment". In this theme, the user is verified before being given access to cloud account. "In recommended model, to substantiate the identity of a user, consuming primarily based authentication agent is employed and for unregistered devices, software package as a service application has been used, to keep free the server from authentication and cryptography from main servers, separate servers are used for various processes" [1].

Sain M., Kumar P, Choudhury A.J., Hyotaek L, and Jae-Lee H [2] in their paper proposes a strong user authentication framework for cloud computing, where user legitimacy is strongly verified before enter into the cloud. The proposed framework provides identity management, mutual authentication, session key establishment be-tween the users and the cloud server. A user can change his/her password, whenever demanded. Furthermore, security analysis realizes the feasibility of the proposed framework for cloud computing and achieves efficiency.

Hong N, Kim M, Jun M and Kang J [3], in their paper done, a study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environment is done. And in this paper, author propose a user authentication method using the JSON Web Token (JWT) and International Mobile Equipment Iden-tity (IMEI) in the smart home and solved the problem of unauthorized smart home device registration of hackers by the application of IMEI and JWT technology [3].

Lee W and Lee R [4], in their paper propose a user authentication scheme in which Implicit Sensor-based authentications of Smartphone Users is done, with the help of Smart watch. In this paper author proposes a novel authentication system, iAuth, for implicit, continuous authentication of the end-user based on his or her behavioral characteristics, by using the sensors built in the smart watch in this small training is also given to the system abut user behavior pattern for future authentication phones.

B.Jondhale N, K.Kadam S, B. Shinde S, N. Dumbare A[5] in their paper proposes a Security in Cloud Computing Using Geo-Encryption Authentication and Time Based Data Access. The term "geo-encryption" or "location-based encryption" refer to a security algorithm that limits the access or decryption of information content to specified locations and/or times.

Moghaddam F, Rouzbeh S, Varnosfaderani S [6], proposes a Scalable and Efficient User Authentication Scheme for Cloud Computing Environments. In their paper a client-based user authentication agent has been introduced to confirm identity of the user in client-side and a cloud-based software-as-a-service application has is also used to confirm the process of authentication for unregistered devices and further, there are two separate servers for storing authentication and cryptography resources from main servers to decrease the dependency of

user authentication and encryption processes from main server. Cryptography agent was also introduced to encrypt resources before storing on cloud servers and a theoretical analysis is also done.

III. PROPOSED MODEL

1. Architecture Overview: Proposed architecture model has following component for its functioning

Wearable device: The proposed authentication scheme considers two-device authentication. One is user machine and another is wearable device. Wearable device will be connected with the user device, by Bluetooth and sends its location coordinates and IMEI (International Mobile Equipment Identity) number to the user machine.

User machine: This device is the main device by which user will access the cloud services and access their data from cloud server, here it is compulsory that, user machine must have a GPS sensor inbuilt or external GPS device attached to it, so that it gets GPS coordinates. User machine can be laptop, desk-top, mobile phone, and tablet. Now a day's all mobile phone and tablet have inbuilt GPS and all latest laptop also have location sensor inbuilt in them.

Authentication server: Authentication server is another server not owned by the cloud service provider. This server is only used for authentication of the user device, to access his/her cloud account and for encryption purpose only. By this server, cloud service provider's database administrator, also does not have any user credentials and cannot be able misuse the data if s/he wants.

Satellite: Satellite only provides location coordinates to the GPS chip inbuilt in the user machine or attached externally.

2. Working process

In proposed authentication method there are two phases, first is user machine registration and second continues checking of valid user machine.

2.1 User machine registration

User registers his/her machine and provide credentials like id, password some security questions and their answer, center points and radius of GPS coordinates.

Centre point can be set using GUI feature and also from IDE, provided by the system, like Google map, shows the circle around the current location, and user also have to set the pairing wearable device, which user will use every time when using the system.

This wearable device at the time of registration is paired with the user device, from which user will access his/her account. And the wearable device is paired and its IMEI is saved into the data base.

During time of registration when user registers his/her device, s/he have to give his/her personal mobile number, in which the OTP will be send for the first time, and through this OTP, the device id and the credentials will be stored in the data base, in the authentication server, now this OTP will be not required every time at the time of login process.

2.2 Continue Checking of valid user

In this phase when user log into the system, and start accessing cloud services, the system internally checks for both the device pairing and their location, in every fixed interval of time, and sending these information to the authentication server for verification.

2.3 Detail Working

First scenario when user log into the system, it asks for the wearable device paring, if not paired, ask for pairing first, after that get the geographical location coordinates of both the devices and IMEI number of wearable device automatically, if paired. And if any one device is in the given geographical region and all the credentials is correctly given, it will be verified by the authentication server through authentication SaaS, and user will log into the Cloud account, after every fixed interval, credentials like GPS coordinates and wearable device pairing with blue tooth, and IMEI of paired wearable device is checked, and if any one of the parameter is not satisfied authentication SaaS will Stop, and break the connection and ask for parameters required.

Second scenario when both the devices are out of the registered region, the authentication server will send OTP request to the registered mobile number. When the user tries to login to the system and with that OTP user will be allowed to set the temporary geographical region, date & time for accessing the account from current region, after that the system will ask for pairing the wearable device. After pairing from Bluetooth both the devices, SaaS will verify for the temporary credentials provided by the user. After that user can access the account for the given time period from current device location.

The detailed working model is shown in the figure 1.

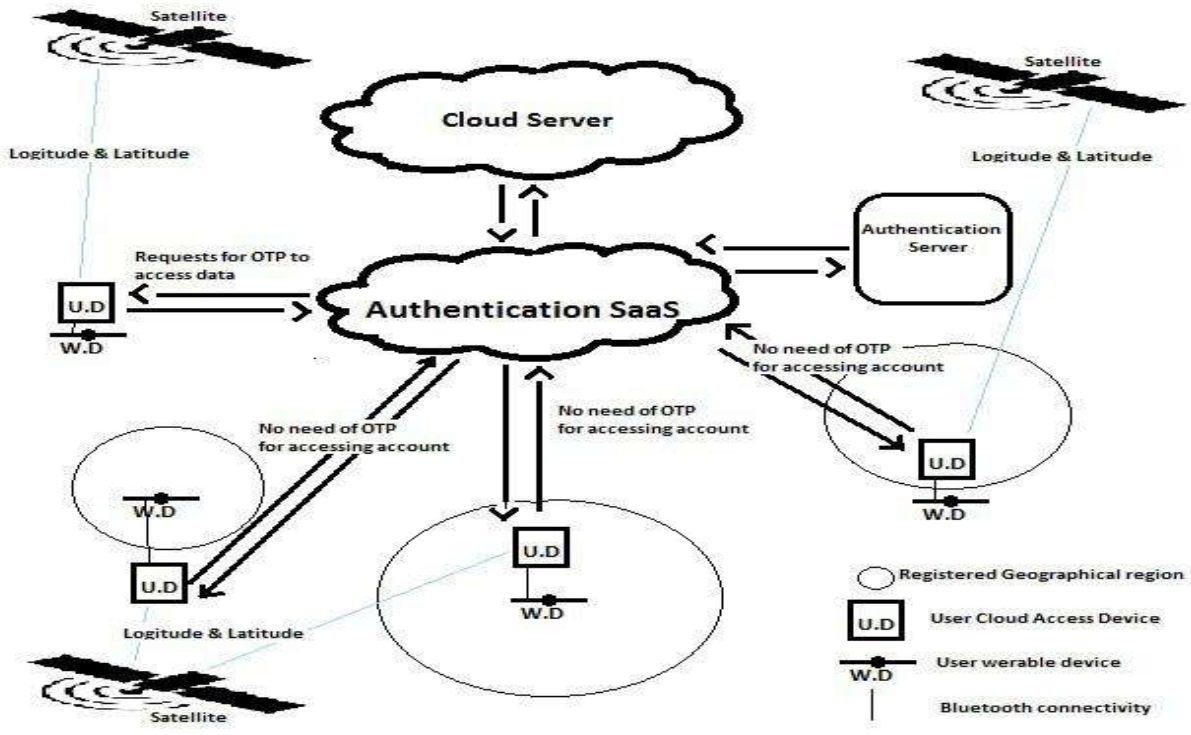

Fig. 1: Detailed diagram of proposed authentication process

IV. AUTHENTICATION METHODS USED FOR CLOUD

In Geo-Encryption Authentication and Time-Based Data Access method the location and time is used for authentication of data access, but if that data is required at another time then there will be restriction in accessing the account. Authentication credentials are stored in the cloud thus the anyone become able to get access to the user account and all the data stored in the database in encrypted form.

In "Implicit Sensor-based Authentication of Smartphone Users with Smart watch", [4] technique a training has to be given to the system, of user behavior. New user has to compulsory provide the training. Anyone whose behavioral training is not given to the system, will not be able to access the services, in spite of if account holder wants that the other user accesses the account.

In "Biometric Identification and Authentication Providence using Fingerprint for Cloud Data Access" [7], method fingerprint is used for authentication, but now a day's fingerprint replica of rubber is available on demand, in very cheap rates and people are using it also, for giving fake attendance so this method of authentication cannot be assumed as trusted method.

In the present time OTP is used for user authentication. OTP is one-time password for user authentication using mobile phones. User has to get every time one-time password and valid only for single time with a time limit. if it is entered wrong or expires, then user is not able to access the data services. The drawback of OTP system is that it is received very late at peak hours, network weak location etc. and most of the time it expires and user makes request again and again for OTP which increase the overhead on OTP generation server.

V. PROPOSED MODEL BENEFIT

In proposed model of authentication, user have to provide login credentials manually and credential of user machine and wearable device are send automatically using programed method. It is necessary that both devices i.e. user machine and wearable device are paired to each other and in defined geographical registered area. The paired feature of user machine and wearable devices reduces the OTP requirement in the registered region. Second advantage of the proposed model is that if the user is not in the registered region, then OTP is requested. So, a user is able to access the cloud service out of registered region also.

In proposed model devices are registered and that device is registered to geographical region, so attacker/hacker must have both the devices and must be in the registered region with all the user credentials to access the account. This reduces the probability of hacking the data stored in the cloud region.

VI. CONCLUSION

After studying various research papers, it is observed that now a day's geographical location, time based, OTP, biometric method etc. are used for authentication of cloud user. Every authentication mechanism has some limitation on access. In proposed authentication technique secure and scalable authentication is applied. It is usually seen that most of the people uses their devices in some particular geographical region or the set of geographical regions respectively [8], so bounding the device to the region and binding the user account and cloud services with device is also very helpful. The hackers or the person who wants to steal the user

information, or want to access the user account without permission, will not be allowed unless and until s/he have all the credentials and in the registered geographic region with the registered devices paired. The proposed authentication model will help to make authentication process more secure, reliable. Also reduces the requirement of OTP based authentication dependency and faster login into the cloud environment.

REFERENCES

[1.] Palak Raina and Bhavik Patel, Authentication Scheme in Cloud Computing Environment, International Journal of Advanced Research in Computer Science , Volume 8, No. 3, March – April 2017.

[2.] M. Sain ,P. Kumar, A.J. Choudhury, L. Hyotaek, and H. Jae-Lee, A Strong User Authenti-cation Framework for Cloud Computing, in Proc. IEEE Asia-Pacific Services Computing Conference (APSCC), Jeju Island, South Korea, 2011, pp.110-115.

[3.] Namsu Hong, Mansik Kim, Moon-Seog Jun and Jungho Kang, A Study on a JWT-Based User Authentication and API Assessment Scheme Using IMEI in a Smart Home Environ-ment, http://creativecommons.org/licenses/by/4.0/.

[4.] Wei-Han Lee, and Ruby Lee, Implicit Sensor-based Authentication of Smartphone Users with Smartwatch, arXiv:1703.03523v1 [cs.CR] 10 Mar 2017, http://dx.doi.org/10.1145/2948618.2948627.

[5.] Nilesh B.Jondhale, Sonal.K.Kadam, Shweta B. Shinde, Amol N. Dumbare, Security in Cloud Computing: Using Geo-Encryption Authentication and Time Based Data Access, International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 10, October 2014.

[6.] Faraz Fatemi Moghaddam, Sohrab Rouzbeh, Shirin Dabbaghi Varnosfaderani, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", https://www.researchgate.net/publication/264197050.

[7.] A.Amali Mary Bastina1, N.Rama, "Biometric Identification and Authentication Provi-dence using Fingerprint for Cloud Data Access", Vol. 7, No. 1, February 2017, pp. 408~416, ISSN: 2088-8708, DOI: 10.11591/ijece.v7i1.pp408-416.

[8.] Senaka Buthpitiya, Ying Zhang, Anind K. Dey, and Martin Griss, "n-Gram Geo-trace Modeling", Carnegie Mellon University, 5000 Forbes Avenue, Pittsburgh, PA 15213, USA.

[9.] L. Hong and A. Jain. Integrating faces and fingerprints for personal identification. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 1998.

[10.] M. Qi, Y. Lu, J. Li, X. Li, and J. Kong. User-specific iris authentication based on feature selection. In Computer Science and Software Engineering, International Conference on, 2008.

[11.] Lamia Youseff, Maria Butrico, Dilma Da Silva,"Toward a Unified Ontology of Cloud Computing", Grid Computing Environments Workshop, 2008.GCE '08.

[12.] Rajkumar Buyya, Chee Shin Yeo, and Srikumar Venugopal, Market-Oriented Cloud Com-puting: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities, The 10th IEEE International Conference on High Performance Computing and Communica-tions.

[13.] Mayank Sahni, DETECTING AND AUTOMATED REPORTING OF CHANGE IN IMEI NUMBER, International Journal of Advancements in Research & Technology, Volume 3, Issue 5, May-2014.

[14.] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taint-Droid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In OSDI, 2010.

[15.] ANDROID PRIVACY by Te-En Wei, Albert B. Jeng, Hahn-Ming Lee, Chih-How Chen andChin-Wei-Tien.(https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6359654&pageNumber% 3D137050)