INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SITE USER AUTHENTICATION/AUTHORIZATION MECHANISMS IN CLOUD SAAS APPLICATIONS

C.V. Satyanarayana [1], Dr. P. Suryanarayana Babu [2]

[1] Research Scholar, Rayalaseema University, Kurnool
[2] Research Supervisor, Department of Computer Science, Rayalaseema University, Kurnool

Abstract: -Cloud computing is the novel computing paradigm which is capable to manage/ host scalable enterprise applications, services and user sensitive information. Users of enterprise are quite different based on their business, which can access the cloud resources via various communication channels (Portals, Communities, Social Networks, Mobile Networks, etc.). Protecting / accessing enterprise application data (Application data, code, services) is challenging research issue whe3n the user access over the multiple medium. We analyzed existing identity management mechanism merits and demerits. Legacy mechanism offers weak credentials and insufficient for validate various users over the cloud. Maintain data/ application secrecy is complex without proper user identity mechanism in place. Based on the previous mechanism review we identify cloud based secure user authentication required. In this paper we are proposing a new self-Reference/Host-Id key based user identity mechanism to Authenticate / authorize the users over the multiple on-premises applications as Single Sign On.

Introduction:

Cloud computing is a new technology which allows the users to manage, store and process data on a cloud servers located remotely vis internet instead of using on-premises servers. The remote cloud server has large capability in terms of high storage area, instant recovery / backup and able to flow/move the data from one application to another. Cloud has three deployment models, namely Public, Private & Hybrid. Hybrid cloud captures around 75% of which involves both public and private collaboration. Cloud offers three services called SAAS (Example: Dropbox, salesforce.com), PAAS (Example: Windows Azure, Force.com and Google App engine), IAAS (Example Amazon web services). Usually SAAS is accessed by end users to access/ create custom applications, PAAS is used by developers to build novel SAAS Applications and where as IAAS is accessed by Identity provider's / system architects. Cloud computing have many number of research issues out of which security is one of the primary concern. Cloud offers multi-tenant architecture, validating a tenant is the basic security concern. The process of authenticating and authorizing of the user is well defined in NIST [1].

Literature of the work:

Authentication is a validation of user before logging to any system, which is a mandatory functional task. To authenticate the user, previous researcher worked hard to identify and analyze the user permissions. In this paper we studied and discussed various user validation methods in detail. Multi Factor Authentication [2][3] followed Fuzzy Hashing Encryption Algorithm /Fuzzy Vault. Secret Splitting Data [4][5] used CAM Tool for Bio-metric based authentication approach. Three Part Key Distribution Protocol, Analysis Tool [6],[7] assess data security in smart cards. K means clustering Algorithm [8] followed "Key stroke Analysis" to authenticate external users. Single Sign On[9][10], Graphical Authentication[11], OTP Protocol[12], Second Pass word Algorithm[13], Mouse Behavior Pattern Mining Method[14], Visual Crypto-Pass window Graphical-Pass no[15], Ethnographic methods[16], Remote access scenario, detecting device type controlled environment[17], Huwag Pattern [18], Selection Algorithm[19], Privacy preserving authentication protocol[20], Key Insertion Algorithm, Tree Encryption Algorithm[21], Novel Mutual Authentication Protocol [22], Kerberos Protocol[23], Consolidated authentication model[24], Voiceprint biometric authentication[25], Face Recognition System (FRS) on Cloud Computing for User Authentication[26], ALP: An Authentication and Leak Prediction Model for Cloud Computing Privacy by [27] are other security approaches attempt to identify/recognize the various applications, which have their unique limitations and are not addressed for novel or next generation cloud applications. The Limitations of the existing work is:

1. In previous techniques authentication score is compared with threshold, it is limited to know best authentication results.
2. Two factor authentication techniques do not address context-aware users (Mobile users).
3. User credentials maintained with local machine(on-premises) may cause security breach.
4. Voice, Bio-Metric, Face-Recognition, ALP have overheads and do not address novel attacks.
5. Not scalable, allows only certain threshold of users to authenticate.

Reference / Host ID key approach:

As part of continually augmenting technologies used across the organization's, enterprise needs to migrate the On-Premise Single Sign- on to Cloud based Centrify / OKTA with Registration and Login process to be implemented on Force.com Sites users over the multiple applications. Current cloud based enterprise facing many difficulties and few important things are as follows:

- Due to the on premise Single sign on resources with the servers residing in the US, the APAC users generally face performance issues with the Registration process.
- There are many moving parts involved in terms of the number of on premise and cloud based resources for making the Login and Registration process work.
- Huge license cost for IBM Tivoli Suite of Management products which includes Tivoli Identity Manager Tivoli Access Manager, Tivoli Federated Identity Manager

In the current study of research, research environment have multiple scalable application which are not related to each other. Our objective is to authenticate or validate the user and able to connect over the multiple applications with single user system credentials. For the proposed system we have identified various goals/objectives and some of them are:

- Leverage the cost advantages provided by utilizing the cloud based SSO.
- Accelerate the on boarding of new users and improve productivity by allowing end users to rapidly register, reset and synchronize their passwords on cloud based platform.
- Address performance issues and improve the stability of the system to provide a seamless experience to the end user's life-cycle of accessing various Cadence applications.

System Architecture: Figure.1. Illustrates the overall system architecture for medium and above level enterprise applications as per modern business. The user can access multiple applications over the system seamlessly by having common reference key / Host id .Host id is unique for individual tenant and encrypted with HMAC 128 bit.

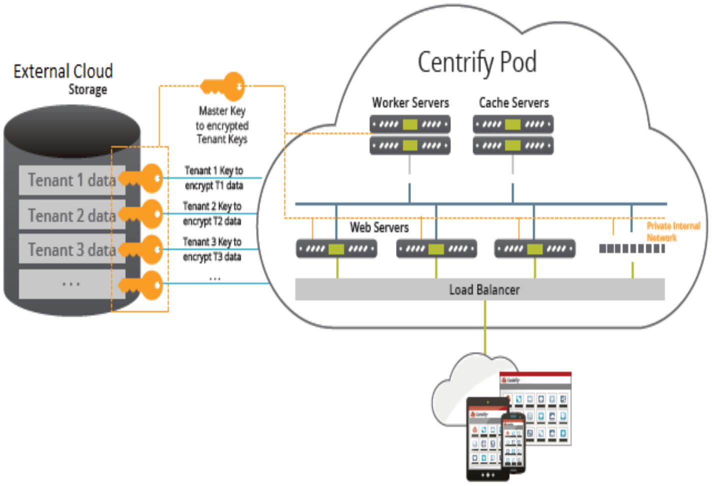

Figure.1.Scalable enterprise architecture

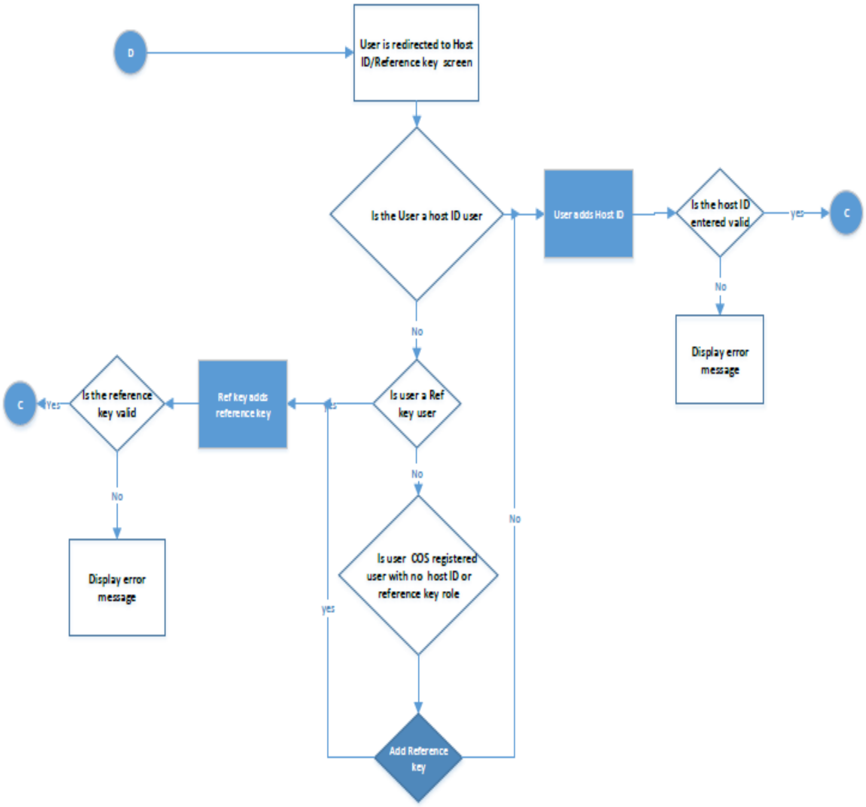
D
User is redirected to Host ID/Reference key screen
Is the User a host ID user
User adds Host ID
Is the host ID entered valid
yes
C
No
Display error message
No
Is user a Ref key user
Yes
Ref key adds reference key
Is the reference key valid
Yes
C
No
Display error message
No
Is user COS registered user with no host ID or reference key role
yes
No
Add Reference key

Figure.1. Hosted /Reference Key based Approach

```
HMAC Crypto Class for AES256 algorithm:-
Blob cryptoKey = Crypto.generateAesKey(256);
Blob data = Blob.valueOf('Test data to encrypted');
Blob encryptedData = Crypto.encryptWithManagedIV('AES256', cryptoKey, data);
Blob decryptedData = Crypto.decryptWithManagedIV('AES256', cryptoKey, encryptedData);
String decryptedDataString = decryptedData.toString();
```

Test Bed results: we tested the proposed approach with multiple on-premises and cloud based SAAS applications and experienced novel results over the existed user authentication approaches. The proposed work adapted HMAC based encryption mechanism secure tenants data over the cloud systems. Fig.3. describes the applications scalability over the 24 hours clock time and Fig.4. Explains the time versus the number of user's access.

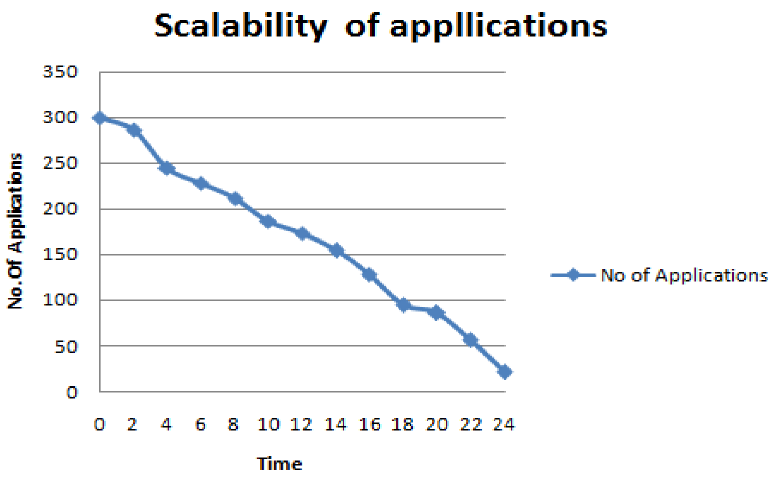

Figure.3. Time versus No. applications accessed over the cloud

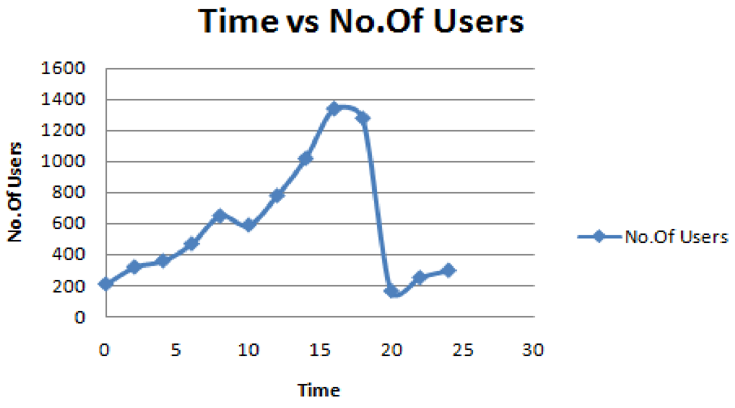

Figure.4. Time versus No. Users accessed over the cloud

Conclusion:

The paper witnesses the evolution of user authentication mechanism. In this paper we studied and analyzed various previous mechanisms *pros* and *cons*. It shows the development from the usage of hardware tokens to multi modal biometrics to authenticate the client. Research is still in progress finding new methods and schemes to authenticate the user in order to challenge the security threats faced by the Cloud. User Authentication with oAuth2.0, HMAC based security is an emerging solution which provides granular level of security from user perspective. In the paper we identified the gaps in the existed work and proposed novel HMAC based self referential/Host id key based authentication of multiple tenants over the cloud. This new proposed approaches enhance the cloud security in terms of user authentication and data security over the cloud.

REFERENCES:

[1] NIST Computer Security Handbook, http://csrc.nist.gov/publications/nistpubs/800-12/.

[2] A.Wenyi Liu, SelcukUluagac, and Raheem Beyah, “MACA: A Privacy-Preserving Multi-factor Cloud Authentication System Utilizing Big Data,”in IEEE INFOCOM Workshop on Security and Privacy in Big data 2014, pp.518-523.

[3] Z. Shen, L. Li, F. Yan, X. Wu, 2010. Cloud Computing System Based on Trusted Computing Platform. International Conference on Intelligent Computation Technology and Automation (ICICTA). 2010, vol 1, pp 942-945.

[4] Hua-Hong Zhu, Qian-Hua He, Hua-Hong Zhu, Hong Tang, Wei-Hua Cao, 2011. IEEE international Conference on Cloud and Service Computing on Voiceprint-Biometric Template Design and Authentication Based on Cloud Computing Security.

[5] Rohitash Kumar Banyal, Pragya Jain, Vijendra Kumar Jain, “Multi factor authentication framework for cloud computing”, in Fifth international conference on computational intelligence, modeling and simulation 2013, pp.105-110.

[6] Daniel Mouly: Strong User Authentication, Information Systems Security, 11:2, 2002, pp.47-53.

[7] Viktor Taneski, Marjan Hericko and Bostjan Brumen,”Password Security-No Change In 35 Years?”, in MIPRO, May 2014, pp.1360-1365.

[8] TapalinaBhattasali, Khalid Saeed, “Two Factor Remote Authentication in Healthcare”, in International conference on advances in computing, communications and informatics,2014, pp.380-386.

[9] Dinesha H A, 2012. Multi-level Authentication Technique for Accessing Cloud Services. International Conference on Computing, Communication and Applications (ICCCA), IEEE, 22-24 February 2012, pp 1-4.

[10] Liliana F. B. Soares, Diogo A. B. Fernandes, Mario M. Freire and Pedro R. M. Inacio, “Secure User Authentication in Cloud Computing Management Interfaces”, 2013, pp.78-79.

[11] Maslin Masrom, FarnazTowhidi and Arash Habibi Lashkari, “ Pure and Cued Recall-Based Graphical User Authentication ”, 2009, pp.40-45.

[12] Arcangelo Castiglione, Alfredo De Santis and Francesco palmieri, ” An efficient and transparent one time authentication protocol with non interactive key scheduling and update ”, IEEE 28th International Conference on Advanced Information Networking and Applications, 2014, pp.351-358.

[13] Faraz Fatemi Moghaddam, Nasrin Khanezaei and Sina Manavi,”UAA: User Authentication Agent for Managing User Identifies in Cloud Computing Environments”, IEEE 5th Control and System Graduate Research Colloquium, August 2014, pp.208-212.

[14] C. Shen, Z. Cai, and X. Guan, “Continuous authentication for mouse dynamics: A pattern-growth approach,” in 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2012, pp. 1-12.

[15] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, “the quest to replace passwords: a framework for comparative evaluation of web authentication schemes”, in proc. of the IEEE symposium on security and privacy, 2012, pp.553–567.

[16] C. Paul, E. Morse, A. Zhang, Y.-Y. Choong, and M. Theofanos, “a field study of user behavior and perceptions in smart card authentication”, in Human-Computer Interaction INTERACT, ser. Lecture Notes in Computer Science Springer, vol. 6949, 2011, pp.1–17.

[17] Z. Jorgensen and T. Yu, “on mouse dynamics as a behavioral biometric for authentication”, in proc. of the 6th ACM symposium on information, computer and communications security, 2011, pp.476–482.\

[18] M. Kumar, “new remote user authentication scheme using smart cards”, consumer electronics, IEEE Transactions on, vol. 50, 2004, pp.597–600.

[19] Shraddha, M.Gurav, et al,” Graphical Password Authentication”, in International conference on Electronic Systems, Signal Processing and computing technologies, 2014, pp.479-483.

[20] Hong Liu, et al.,” Shared authority based privacy-preserving authentication protocol in cloud computing “, in IEEE Transactions on Parallel and Distributed Systems, 2013, pp.1-11.

[21] Mercy Gnana Rani, et al, “Key insertion and splay tree encryption algorithm for secure data outsourci ng in cloud”, in world congress on Computing and Communication Technologies, 2014, pp.92-96.

[22] Nimmy K. et al, “Novel mutual authentication protocol for cloud computing using secret sharing and steganography”, 2014, pp.101- 106.

[23] Navneet Singh et al., “An efficient approach for software protection in cloud computing”, in Fourth International Conference on Communication Systems and Network Technologies, 2014, pp.550-554.

[24] J. Kim and S. Hong, 2011. One-Source Multi-Use System having Function of Consolidated User Authentication, YES-ICUC, 2011.

[25] L. B. Jivanadham, A.K.M. Muzahid ul Islam, Yoshiaki Katayam, Cloud Cognitive Authenticator (CCA) A Public Cloud Computing Authentication Mechanism, 2013, IEEE.

[26] Wang, P., Ku, C. C., & Wang, T. C., 2011.A New Fingerprint Authentication Scheme Based on Secret-Splitting for Enhanced Cloud Security. www.intechweb.org.

[27] Tereza Cristina Melo de BritoCarvalho, Charles Christian Miers, Mats Näslundand Abu Shohel Ahmed, 2013. A framework for authentication and authorization credentials in cloud computing. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.