ISSN 2278 – 3091
International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 5 , No.1 Pages : 27 - 29 (2016)
Special Issue of ICCEIT 2016 - Held on February 16, 2016 in The Solitaire Hotel, Bangalore, India
http://warse.org/IJATCSE/static/pdf/Issue/icceit2016sp07.pdf

Endorsement for Web-based and Cloud Solutions

Sk Rubel[1], Sri Rashmi C.N.[2]
Dept. of MCA, Acharya Institute of Technology[1,]
Dept. of Computer Applications, Dayananda Sagar College of Arts, Science and Commerce, India.[2]
skrubel93@gmail.com, rashmi.chakravarthy@gmail.com

Abstract*:* As solutions have migrated to the Web and evolved to serve the entire enterprise, users often now include contractors, external business partners and even customers or clients. Your solutions today may, in fact, deliver services for different users, who require access to different types of functionalities and data. Users are now accessing services over the Internet − and perhaps through the Cloud − on different devices and from different locations, including home. It is quite obvious that there are now many more gateways to the information and functionalities in your solutions that must be secured.

Key words: Cloud Authentication, Security.

CLOUD AUTHENTICATION

Identity management and security is one of the major issues that is faced today in web based and cloud based applications. Cloud applications playing the vital role today in all the corporate issues also brings in problems which include security, application security, identity management, authentication and access control. Strong user authentication is the major requirement as on today for cloud computing to restrict illegal access of cloud server [1][2][5]

Authentication is process of confirming the identification of a user when he/she logs on or access a resource like a database file. Cloud uses various authentication mechanisms to verify ones identity. Few of the authentication types include password authentication, smartcard authentication and biometric authentication of which password authentication is the most insecure one.

Password authentication is the most popular authentication where in when a user logs on to the network, assigned username and password are entered and checked against the database where all the authorized users and passwords are stored. The drawbacks of this authentication are that the password should always be "strong" which should be a combination of alphabets, numeric and special symbols which cannot be easily guessed. Secondly, password authentication is vulnerable to the password cracker which may use a simple brute force attack. Thirdly, all the passwords must be encrypted.

Smart card authentication is stronger over password authentication wherein they use cryptography based authentication. Smart cards contain chips which are used to store public and private keys which are used to identify a person. It is as much same as an ATM card which is required to be physically slide through a reader and enter the personal identification number (PIN).

Biometric authentication is much stronger authentication technique than the above mentioned two types. It is based on the concept of "Every individual having unique biological characteristics". For example, fingerprints, voice, retinal and iris patterns are unique for every individual. Though it requires expensive equipment for the input, this method efficiently proves the identification of a person without any falsification.

This paper explains the use of web key fingerprint biometric based authentication solution that provides more flexibility and security.

While all the business applications are making a paradigm shift from traditional software models to internet cloud which gained a momentum. Life before cloud computing was complex in terms of security, storage, resources, man power and cost.

The SOA, service oriented architecture which was before cloud computing urges "services thinking" approach to business problems. Cloud gives the better solution by simply replacing or reconfiguring the technology. Cloud computing has evolved through number of phases which includes utility and grid computing, application service provision (ASP), and software as a service (SaaS)[17][18]

Though all the business organizations are quickly shifting to cloud computing, there are also many organizations and users who are not efficiently utilizing cloud services.

When surveyed few users about why not using cloud services efficiently one of the user's raised the questions on limitations of space on cloud, user friendliness and security of data.

Users expect similar services like SaaS in cloud computing which is a difficult task. Many of the users while agree to the fact that data sharing is easier and provides efficient access control also expressed their concerns on privacy and efficiency of data.

APPLICATIONS OF CLOUD AUTHENTICATION

When users logon to access data and application remotely, organizations have to implement access controls for corporate resources. Organizations are having difficulty in managing and implementing the access policies. Authentication mechanisms overcome these problems by extending a secure access to the cloud. To implement secure access controls cloud applications uses authentication as a service.

All sectors are migrating to cloud computing because IT costs can be cut, it reduces capital expenses, and is a viable

ISSN 2278 – 3091
International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 5 , No.1 Pages : 27 - 29 (2016)
Special Issue of ICCEIT 2016 - Held on February 16, 2016 in The Solitaire Hotel, Bangalore, India
http://warse.org/IJATCSE/static/pdf/Issue/icceit2016sp07.pdf

option to modernize legacy systems and they need more secure systems. In this regard, authentication serves a vital function by securing access to corporate networks, software-as-a-service and cloud applications, protecting the identities of users, and ensuring that a user is who he claims to be. Cloud authentication ensures that the users are who they claim to be by requiring them to identify themselves with a combination of password, smartcard and biometrics.

DRAWBACKS OF CLOUD AUTHENTICATION

Though cloud authentication mechanisms provide and promise to secure the data, this also has its drawbacks. In cloud based applications, it's a nightmare to manage the users remotely.

Migration of the data is the major drawback as it's difficult to synchronize login and authentication data between external clouds and the internal systems.

Customer's privacy is another drawback as customer information is stored on the cloud as per the service providers request [10][12]

Lack of transparency in the cloud makes the customer to regularly monitor their private information

The usage of multiple cloud services is another drawback as user has to store his authentication details in multiple clouds which would lead to a security issue. The redundant actions may also exploit the authentication mechanism

Usage of various authentication mechanisms may have less impact on SAAS, PAAS, and IAAS which also is a present challenge

Security issues in cloud computing has played a major role in slowing down its acceptance.[3][4]

AUTHENTICATION FRAMEWORK

In general, authentication framework will have the client devices, data aggregators, and authentication engine, and authentication consumers as the participants. An activity is initiated by the client device and pushes to the data aggregator. Data aggregator accepts a query that is generated by the authentication engine for individual device reports. It also collects the data from third parties; the service is requested by the client device from the authentication consumer and also authenticates itself through the authentication engine; the authentication engine collects data from data aggregators and may also request data directly from client devices; at the time of authentication the authentication engine authenticates itself through the authentication engine.[6][8][11]

Figure 1 below represents Authentication frame work

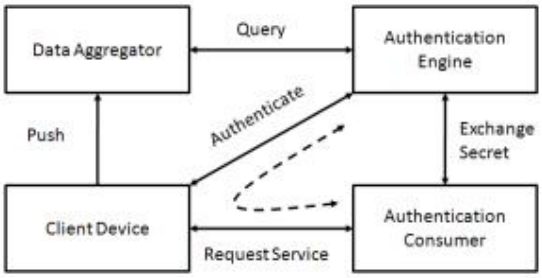

Fig 1: Authentication framework

The decisions for authentication are based on collected data and authentication policies that are provided by authentication consumers which are based on end user requests. Then the authentication consumer comes up with the authentication result based on the client's request.

Based on the above general architecture this paper explains the authentication framework based on the bio key's exclusive biometric algorithm called as Vector Segment Algorithm. As every registered user expects an accurate identification, the web key manages and assures the accuracy and is capable of capturing more data than any other biometric with a very less false acceptance rate (FAR) standard which is less than one in ten thousand.

The major problem that an organization faces during deployment is overcome by web key which provides a set of flexible services, tools for administration and API connectivity. The architecture of web key includes client browser plug-in, application server plug-in and web-key authentication server.

Client Browser Plug-in retrieves the image from the reader and reads it through the user interface provided on the user device, creates a template and secures the device.

Application Server Plug-in manages communications between the web key authentication server and the client devices which are attached

All the back-end functions like enrolling and authenticating users, matching VST are tasked by Web-key authentication server which can be geographically located anywhere.

While the context questions about the limitation then this Service Oriented Architecture of a Web key comes up with an extensive solution and says that it is capable of storing millions of fingerprints and also is efficient in handling unlimited number of simultaneous authentication requests. And when security comes into picture, then the application server plug-in can be placed on any number of servers and at any number of locations.[13][20][21]

WEB-KEY − ACCURATE, FLEXIBLE RISK-BASED AUTHENTICATION

WEB-key offers a fingerprint biometric-based advanced authentication solution that provides more security and flexibility than passwords. If you choose, fingerprint-based authentication as a replacement for passwords entirely, then

ISSN 2278 – 3091
International Journal of Advanced Trends in Computer Science and Engineering (IJATCSE), Vol. 5 , No.1 Pages : 27 - 29 (2016)
Special Issue of ICCEIT 2016 - Held on February 16, 2016 in The Solitaire Hotel, Bangalore, India
http://warse.org/IJATCSE/static/pdf/Issue/icceit2016sp07.pdf

with WEB-key we can have the single method of authenticating all users at log-in time. Passwords are easy to forget; eliminating them entirely reduces user frustration, down time and calls to the help desk. It also saves user time, which makes your solution more convenient to use.[16]

HOW IT WORKS

There are two phases that are included when users interact with web key. One is initial enrolment phase and the other is the authentication phase [14] [19]

At the enrolment phase, with in the biometric SDK which is provided the finger print is obtained by the registered user which is digitized and encrypted and is converted into a mathematical template with the features of the fingerprint. More than forty levels of image enhancement is used by the bio key's patented technology which creates a template and reduces the false acceptance or rejection response during authentication. And this enrolment template cannot be reversed by any intruder with false intentions once the template is stored in the web key authentication server.

During the Authentication phase, whenever the register user logs on or whenever requests for a resource finger print scan is processed by providing the user instructions in an understandable manner. Above Forty plus finger print readers are compatible with the web key server, which is used in capturing the fingerprint. This also includes the embedded readers that are available with the laptops and notebooks. [15].

The fingerprint data is extracted from the scan and reference template is built. This template is matched against the user's enrolment template. Over 1,200 data points are compared by the patented algorithm which matches with the template with in a second's time. The web key then reports the authentication to the solution application server upon positive match result and the access is provided to the user.

FLOW OF WORK FOR CLOUD AUTHENTICATION

Figure 2 below represents data flow diagram for cloud authentication.

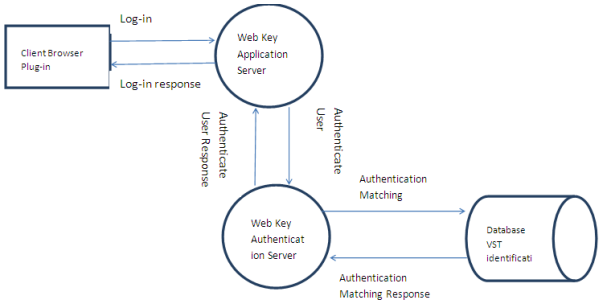

Fig 2: Basic DFD for cloud authentication

CONCLUSION

Cloud Authentication is the new challenge in the field of cloud computing which also creates different opportunities in the field of research. Increasing demand to access services and data also increases the demand for different and new authentication mechanisms. The deployment of data in the corporate sector among different business resources asserts the demand for understanding the context of cloud authentication. As privacy is a major concern in any of the business organizations user authentication becomes more intrusive. This paper explains the most efficient authentication mechanism among all the other mechanisms while also making it a challenge for further research on the same. [7][9]

REFERENCES

[1] Armbrust M, Fox A, Griffith R, Joseph A, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, and Zaharia M. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report No. UCB/EECS-2009-28. Electrical Engineering and Computer Sciences. University of California at Berkeley. USA. 2009
[2] Avetisyan A, Campbell R, Gupta I, Heath M, Ko S, Ganger G, Kozuch M, O'Hallaron D, Kunze M, Kwan T, Lai K, Lyons M, Milojicic D, Lee HY, Soh YC, Ming NK, Luke JY, Namgoong H. Open Cirrus: A Global Cloud Computing Testbed. IEEE Computer, Vol 43, No 4, pp. 42–50, 2010.
[3] Baun C und Kunze M. Infrastrukturen fu¨r Clouds mit Eucalyptus selbst aufbauen. iX 4/2009. S.128–130. Heise Zeitschriften Verlag
[4] Baun C, Kunze M und Ludwig T. Servervirtualisierung. Informatik-Spektrum 3/2009. S.197–205
[5] Bengel G, Baun C, Kunze M und Stucky K-U. Masterkurs Parallele und Verteilte Systeme. Grundlagen und Programmierung von Multicoreprozessoren, Multiprozessoren, Cluster und Grid. Vieweg und Teubner, Wiesbaden. 2008.
[6] Klems M, Nimis J, and Tai S. Do Clouds Compute? A Framework for Estimating the Value of Cloud Computing. Proc. 7th Workshop of e-Business (WeB 2008). Springer LNBIP
[7] Lai K, Rasmusson L, Adar E, Sorkin S, Zhang L, and Huberman BA. Tycoon: an Implementation of a Distributed Market-Based Resource Allocation System. Multiagent and Grid Systems. 2005
[8] Lenk A, Sandholm T, Klems M, Nimis J, and Tai S. What's inside the Cloud? An Architectural Map of the Cloud Landscape. ICSE 2009 Workshop on Software Engineering Challenges of Cloud Computing. 2009
[9] Menzel M, Sch€onherr M, Nimis J, and Tai S. (MC2)2: A Generic Decision-Making Framework and its Application to Cloud Computing. Proc. International Conference on Cloud Computing and Virtualization. 2010
[10] Nurmi D,Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, and Zagorodnov D. The Eucalyptus Open-source Cloud-computing System. October 2008
[11] Nurmi D,Wolski R, Grzegorczyk C, Obertelli G, Soman S, Youseff L, and Zagorodnov D. Eucalyptus: A Technical Report on an Elastic Utility Computing Architecture Linking Your Programs to Useful Systems. August 2008
[12] McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, and Turner J. OpenFlow: Enabling Innovation in College Networks. 2008
[13] Sch€afer A. Die Kraft der sch€opferischen Zerst€orung. Campus. 2008
[14] http://www.naa.gov.au/records-management/agency/secure-and-store/rm-and-the-cloud/
[15] http://www.finance.gov.au/sites/default/files/community_cloud_governance_better_practice_guide.pdf
[16] http://www.finance.gov.au/blog/2013/06/12/aps-mobile-roadmap/
[17] http://www.finance.gov.au/big-data/
[18] Streitberger W, Ruppel A. Cloud Computing Sicherheit - Schutzziele. Taxonomie. Marktu¨bersicht, FhG SIT Sept. 2009
[19] Varia J. Cloud Architectures, White Paper, Amazon. 2009
[20] Wang L. Virtual environments for Grid computing. Universit€atsverlag Karlsruhe. 2009
[21] White T. Hadoop – The Definite Guide. O'Reilly Verlag. 2009