International Journal of Research in Engineering, Science and Management
Volume-2, Issue-1, January-2019
www.ijresm.com | ISSN (Online): 2581-5792

Two Way Authentication for Analytics as a Service in Cloud

Don Pezo Tshilombo[1], V. V. Gopala Rao[2]
[1]*Student, Department of Computer Science & engineering, Aditya engineering College, Surampalem, India*
[2]*Associate Professor, Department of Information Technology, Aditya engineering College, Surampalem, India*

***Abstract*: Every enterprise strives to be truly data driven with analytics embedded into every level of decision making. Analytics offer away of changing the abstraction of messy data management, complex predictive modeling and your decision making to a new level. Cloud technology understands this problem and provides a total platform from data acquisition, to transformation, modeling and analysis as a service. However, the risk assessment of any Network or Security systems has a high level of uncertainties because to number of load, several types of unknown attack; which requires a continuous security mechanism to be always maintain. As Data Analytics reveals both a strategic and tactical level to run a business, to avoid those information to be reveal to the opponent or concurrent Beyond the security measures maintain by the cloud provider, this paper defines a model for accruing authentication in two ways as security measure for analytic as a service by making used of password along with One Time Password integrated to authentication through ticket; which reinforce security through mutual authentication by making a corporation to be able to provide relevant and reliable information.**

***Keywords*: Security, Authentication, Data analytics, cloud**

1. Introduction

In today's very complex business world, organizations must find innovative ways to differentiate themselves from competitors by becoming more secure, collaborative, virtual, accurate, synchronous, adaptive and agile. They need to be able to rapidly respond to market needs and changes. Many organizations noticed that data they own and how they use it can make them different than others. That's why having efficient and effective decision making processes with right data that is transformed to be meaningful information with data-driven discoveries are becoming mainstream processes for companies to run smarter, more agile and efficient businesses[1]. Security issues in cloud big data are also of particular concern[2].As saying by" holding information it is a sign of power"; With the development of cloud computing and its services nothing is indifferent to the opponents, day by day they are still looking and developing several techniques and methods to grant, disclose and misuse the information[3]. Data analytics as a service in cloud, its allows processing of examining data sets in order to draw conclusions about the information they contain, increasingly with the aid of specialized systems and software. To make relevant that information, many mechanisms must be deployed to secure access as well as storage. Reason for that an authentication Service must be implemented to control access. However several Cloud Service Provider do so, in manner that user should provide credential information before accessing to any services provided. Moreover, providing user identification and password there is less probability to guarantee confidentiality and integrity. As the big data in the cloud is under many security threats, such as data leakage, illegal access and so on [2]. That is why this project focus on access to analytics service in cloud by developing a reliable and dynamic authentication mechanism, in two way by using what the customer has and what he knows. User id and password follows by one time password with choice delivery approach. The remainder of the paper is organized as follows. Section 2 discusses the related work; Section 3 presents the system model. We then propose the two way based authentication mechanism and implementation in Sections 4. And evaluation result in section 5 and conclusion is given in Section 6.

2. Prio and related work

Security issues of data in cloud are also of particular concern for many numbers of enterprises wanting to adopt a cloud-based analytics that is hosted outside their own Demilitarized Zone (DMZ) because the cost of security failure could quickly exceed the benefits of cloud computing [4]. That is why in the cloud big data security assurance community, governments and industry, researcher have realized the importance of strong authentication and consider it as a basic security requirement. Several access control and protocols schemes have been proposed, which mainly focus on the attribute-based encryption to design the schemes [5]. As for analytics as a service provides in cloud, to assure the function of the authentication service from customer and cloud is authentic; many projects and researches relative to security of analytics in cloud have been proposed.

A. Analytics as a delivery model in cloud

Big data and Cloud, two of the trends that are defining the Enterprise Computing which is prominent and highly visible, show a lot of potential for a new era of combined applications. Cloud service delivery models are highly flexible and enable IT

to assess the best approach to each business user's request. This project has defined a cloud-based analytical model which can make BI affordable by enabling Analytics as a Service. AaaS delivers clients with analytics on demand and provides various tools for data analytics and it can be configured by the user to efficiently process and analyze huge quantities of heterogeneous data; and access through two credential user Id and password. The result presented the opportunities to enable big data analytics in cloud environment, which makes BI affordable for all organizations [6].

B. Analytics cloud security, privacy, and architecture

The Analytics Cloud Services include a variety of configurable security controls that allow customers to tailor the security of the Analytics Cloud Services for their own use. There are operated in accordance with the following procedures to enhance security:

- User passwords are stored using a one-way salted hash.
- User access log entries will be maintained, containing date, time, User ID, URL executed or entity ID operated on, operation performed (created, updated, deleted) and source IP address.
- *User Authentication:* Access to Analytics Cloud Services requires authentication via one of the supported mechanisms, including user ID/password, SAML (Security Assertion Mark-up Language) based Federation, Social Login, or Delegated Authentication as determined and controlled by the customer. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state. For marketing and research, many of the businesses use big data, but may not have the fundamental assets particularly from a security perspective. If a security breach occurs to big data, it would result in even more serious legal repercussions and reputational damage than at present [7].

C. An enterprise architect's to big data

In Security Architecture, the Big Data ecosystem must be secure. Oracle's comprehensive data security approach ensures the right people, internal or external, get access to the appropriate data and information at right time and place, within the right channel. Defense in-depth security prevents and safeguards against malicious attacks and protects organizational information assets by securing and encrypting data while it is in-motion or at rest. It also enables organizations to separate roles and responsibilities and protect sensitive data without compromising privileged user access, such as DBAs administration. Furthermore, it extends monitoring, auditing and compliance reporting across traditional data management to big data systems. Apache Hadoop projects enable data at rest and network encryption capabilities. Below is the logical architecture for the big data security approach [8].

The spectrum of data security capabilities are:

- Trend, Privileged user access and administration
- Data encryption pt) and redaction
- Data masking and sub setting
- Separation of roles and responsibilities
- Transport security & API security (Database Firewall)

3. Security challenges

A. Security threats in cloud

Security threats related to the authentication process are discussed below. These threats are discussed with respect to internet and cloud scenarios and include security risks related to the remote authentication process.

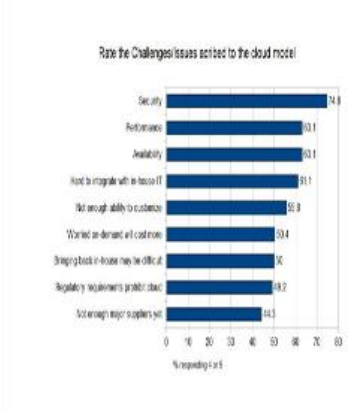

Fig. 1. Rate the challenge issue to the rate model

B. Conduct risk assessment

Risk assessment is the first step of information security process. It lays ground for upcoming security related decisions and also plays a decisive role in technology selection. Risk assessment is a part of the risk management. Risk management is performed to minimize the effect of risk and achieve higher security standards. The four components of risk management model are shown in figure below. Following is a brief description of all four components with main focus on risk assessment.

$$Risk = Likelihood \quad Impact$$

C. Password - edge of breaking down

Password authentication is the most commonly used single-factor authentication mechanism. We can agree that a password authentication mechanism and argue that passwords are at the edge of breaking down, especially in the cloud environments. A password is a secret shared between the claimant and the verifier. A claimant is one who claims to know the secret and the verifier is one who confirms or denies this claim. A password is bound to a unique user name and is known only to the claimant, apart from the verifier. The correct user name and password is provided to the verifier to access the secured resources [9]. Although password authentication is widely

adopted because of its ease of use, the fact is, it is not the best authentication mechanism. Password authentication is vulnerable to brute-force attacks. Brute-force attacks can be divided into online and offline attacks. As the name suggests, different password combinations are tried online during the online brute-force attack. On the other hand, during an offline brute-force attack, the attacker gets access to the encrypted authentication key. He can then try different combinations at his leisure to discover the key. The password authentication is vulnerable to both brute-force attacks. Recent security implementations and guidelines force the users to choose random passwords [10].The idea behind these guidelines is that randomness increases the password strength [11]. Strong passwords are those with higher randomness involved. The users are asked to use numerals along with capital and lower-case letters in the passwords to increase its randomness. They are encouraged to use long passwords with eight or more characters. Although most of the organizations force users to choose strong passwords, the fact is, the computational capability is also rising with the passage of time. Less time is required these days to crack a password with high speed computers. The Figure below shows the relation between entropy and password length with respect to different password choosing techniques. The passwords can be chosen randomly, using abbreviations, using phone numbers or using a combination of all these. For any given password length, a randomly chosen password has the highest entropy. It shows that the entropy of a password and the ease of memorizing it are competing characteristics and system generated passwords have high entropy values. At the same time, they are hard to memorize and more prone to be written down by users.

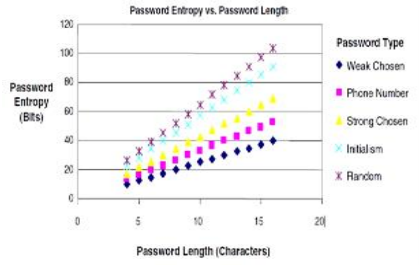

Fig. 2. Password entropy vs password length

We can realize that passwords do not provide further room for strong authentication and any attempt to use passwords only to strengthen the security can result in collapse of the whole process.

D. Authentication

The possible approach of authenticating someone falls into three categories. These categories are based on the factors of authentication used during the authentication process. There are three factors of authentication, as explained below.

- *Proof of Knowledge Factor:* Something a person knows falls into this fact. A secret is shared between the user and the information security system. The shared secret is used as an authentication token. Some examples of the secret are password, PIN, personal question or a picture. The shared secret can be revealed to an attacker in case of a security breach.
- *Proof of Possession Factor:* Something a person has is used as an authentication token during the authentication process. The possession factor can be software or hardware token. Some examples are smart cards, USB tokens and one-time password generators. The authentication token can be stolen or copied by an attacker in case of a security breach.
- *Proof of Characteristics Factor:* Authentication tokens belonging to this factor are based on something a person is. Each person has certain characteristics, which distinguish him from others. Biometrics like fingerprints, iris and retina patterns can be used as authentication tokens as shown below.

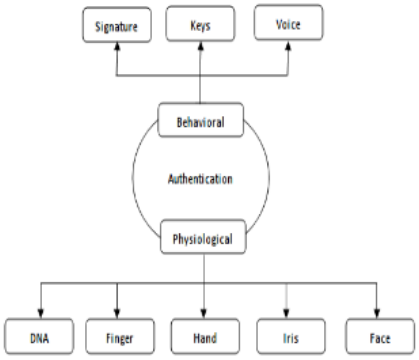

Fig. 3. Authentication

The number of factors used can directly defined as:

- One Factor Authentication
- Two Factor Authentications.

Multi-factor authentication mandates use of more than one factor of authentication. Two or more than two factors are used together during authentication. The security level provided by multi-factor authentication is supposed to be equal or higher than two-factor authentication.

4. Proposal approach

The security in cloud, especially for analytics heavily depends on a strong authentication mechanism. Which establishing confidence in the user identity, electronically presented to an information system, by defining a two way mutual authentication.

A. Two way authentication model

Two way authentications is an approach to assert the identity of an entity using two factors of authentication as well as a mutual authentication. It must be used together for successful authenticate by issuing a ticket that has the client credential, and then the client can use it for accessing to analytics as a service

web.

This approach uses:

- *Ticket-Granting Service:* This service issues tickets for connection to computers in its own domain. When clients want access to a computer, they contact the ticket-granting service in the target computer's domain, present a TGT, and ask for a ticket to the computer. The ticket can be reused until it expires, but the first access to any computer always requires a trip to the ticket-granting service in the target computer's account domain.

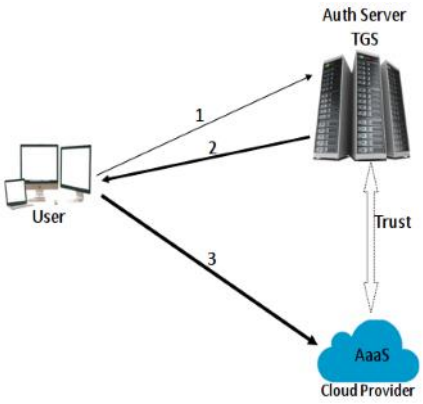

Fig. 4. System model

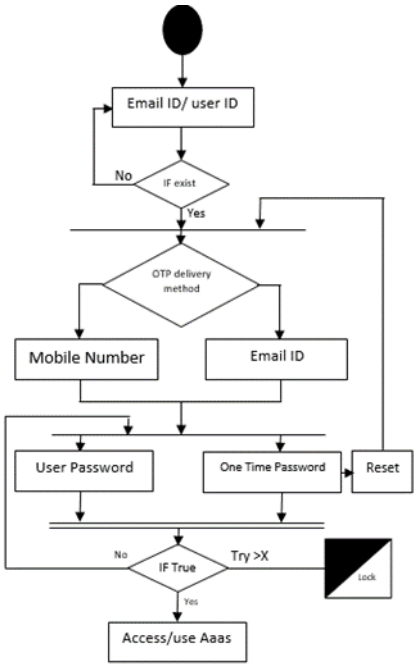

Fig. 5. Activity diagram

- *Password based authentication:* The protocol is still the most extended mechanism for online authentication. This is understandable, given that the only requirement is for everyone to remember their username and password, instead of the inconvenience of having to carry a digital certificate, USB token, intelligent card, specialized hardware or software, etc.
- *One time password:* This protocol provides a mechanism for logging on to a network or service using a unique pin which can only be used once, as the name suggests. This prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time. Typically the user's logon name stays the same, and the one-time password changes with each logon. One-time passwords are a form of so-called strong authentication, providing much better protection to *on-line bank accounts*, corporate networks and other systems containing sensitive data

B. Operating principle

The implementation of this proposal model for authentication mechanism follows exactly the description present through activity diagram. Resumes as follows: For accessing or using the analytics as a service, the user is called to provide the Email Identification via the authentication interface, and also specify which mode of he would like to receive the one time password; he may proceed further if only if his user identification existed. Then the verification interface will load where He has to submit both pair of credentials, password and one time password. If there are matching, only there access will be grant to the user; otherwise it will be re invited to province those information once again. However if the number of attempt exceed the threshold defined via X, that particular account will be suspended for a time T according to the security policies. Beyond that the user can reset his onetime password in case of failure during reception.

5. Evaluation and new direction

The strength of the proposed model on authentication is evaluated by analyzing based on different security threats, risks and negatively impact on the system such as:

- Duplication and Token theft which is related to the loss of a physical token and is possible if the attacker has physical access to the authentication token. Even though he has access to one token, access to service will not be granted because the authentication process requires two valid token. And the second is generated randomly; therefore the probability for taking control is very less.
- Session hijacking is resisted by not allowing an intruder to participate in the session. A session identifier (session ID) is agreed upon by the client and server before the session starts. In SCCM two-factor authentication system, the client and server agree upon the session ID during the TLS handshake. The session ID is encrypted using the asymmetric encryption keys before transmission. An attacker cannot decrypt the session ID, as he has no access to the private keys of

the client and server.

The session identifier is a short living and highly random value and guessing it using brute force techniques is not a feasible task. This authentication process also provides strong resistance to fishing and man-in-the-middle attack if it does not allow the user to reveal its secrets to an attacker, disguised as the verifier. Making used of data analytics in the cloud can provide several advantages, for that maintains some security policies and mechanism become a primordial. Some other direction can be taken such as

- Synchronous delivery method for two way authentication: to keep track of any access by notify to user a different technique.
- Optimize to authentication access time to analytic: By applying it to analytics as a service, we can be able to get more costumers, increase the profit per customer, enhance its operation, and perform cost reduction.

6. Conclusion

This paper provides insight in different aspects of information security to analytics as a service in cloud. By notifying we are not only in age of data but also in age of concurrence, in which to hold the right information of other it is a sign of power, because we can make decision based on those information to grow or take advantage on other. To enhance the security of the information, we have defined an approach for mutual authentication .using ticket encryption and one time password. Each credential defined a different level of securing the system and insight get though analytics as a service provider will lead to a better decision and development of the corporation.

References

[1] Arun.J, Mohamed Hazaruthin.M., M.Karthik, “Analytics as a Service Delivery Model for the Cloud”, IEEE International Conference on Engineering and Technology (ICETECH), Coimbatore, TN, India, 2015.
[2] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “Verifiable computation over large database with incremental updates,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015.
[3] F. Mouton, M. Malan, L. Leenen and H.S. Venter, “Social Engineer Attack Framework,” IEEE Conference on Information Security for South Africa, pp. 1 – 9,2014.
[4] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, “Protection of big data privacy,” IEEE Access, vol. 4, pp. 1821–1834, 2016.
[5] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute sets: A practically motivated enhancement to attribute based encryption,” in European Symposium on Research in Computer Security, pp. 587–604, 2009.
[6] M. Moorthy, R. Baby, S. Senthamaraiselvi,” An Analysis for Big Data and its Technologies”, International Journal of Computer Science Engineering and Technology (IJCSET), Volume: 4, Issue 12,412-418, Dec 2014.
[7] Jian Shen, Dengzhi Liu, Qi Liu, Xinming Sun and Yan Zhang, “Secure Authentication in cloud Big Data with Hierarchical Attribute Authorization Structure”, IEEE journal, 2016.
[8] Mrudula Sarvabhatla and Chandra Sekhar Vorugunti, “A Robust Mutual Authentication Scheme for Data Security in Cloud Architecture”, Future Information Security Workshop, COMSNETS, 2015.
[9] A. M. Axel Buecker. Protecting Data Assets by Deploying a Multi-Factor Authentication Solution with End-to-End Encryption. IBM, 2013.
[10] Shao Ying Zhu, Richard Hill, Marcello Trovati; “Guide to Security Assurance for Cloud Computing; Computer Communications and Networks; Edition Springer; 2016.
[11] Marcos D., N. Calherious, Silvia Bianchi, Marco A.S. Netto, Rajkumar Buyya, “Big data computing and cloud: Trends and future direction”, Journal of parallel and distributed computing, Elsevier, May 2014.
[12] Salesforce.com, inc.;” Analytics Cloud Security, Privacy and Architecture Documentation”; 2015.
[13] Rhoton, J, Cloud Computing Explained. 2. Edition, Kent: Recursive Limited, 2011.