IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-6 E-ISSN: 2347-2693

BYOD with Multi-Factor Authentication

Surabhi Shukla[1*] and Neelam Joshi[2]

[1*,2] *Computer Science (MPCT), RGPV, India*
surabhishukla1206@gmail.com, neelam.khemariya@gmail.com

www.ijcseonline.org

Received: Jun /02/2015 Revised: Jun/10/2015 Accepted: Jun/22/2015 Published: Jun/30/ 2015

Abstract - Data is currency in today's world. Security teams are now tasked with protecting the brand and intellectual property through the protection of the second-most important asset of a company: data (the first one being people). There are two approaches here. The first is to label – or classify – information so users know if they can place it in the cloud or not. The second is to look at how IT provision can be changed to make security less burdensome. As tablets and smartphones become the primary work computing device, offering easy access to the cloud, users will be less tolerant of VPN, multiple logins etc. Smaller organizations typically rely on services such as iCloud. For these businesses, it would make sense to implement additional security measures provided such as two-factor authentication. In this paper I have highlighted the options which can be useful in the two-factor authentication.

Keywords – SLA. QoS, RBAC, IDM, OTP.

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three delivery models, and four deployments models.

Service level agreements (SLAs) are used to define the necessary Quality of Service (QoS) for an application or user in an IT system. SLAs originally were defined as a contractual document between IT resource providers and consumers that involved cost analysis and pricing, along with financial incentives or penalties.

II. IDENTITY AND ACCESS MANAGEMENT

The following controls apply to the cloud provider's identity and access manages provider's identity and access management systems (those under their control).

Authentication & authorization is the base pillar here. User entity is very important here. File download/upload is OK but have to manage the path where file wants to save itself.

A. Authorization

- Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations (read/write/delete)?
- How are the accounts with the highest level of privilege authenticated and managed?
- How are the most critical decisions (e.g., simultaneous de-provisioning of large resource blocks) authorized (single or dual, and by which roles within the organization)?
- Are any high-privilege roles allocated to the same person? Does this allocation break the segregation of duties or least privilege rules?
- Do you Role-Based Access Control (RBAC)? Is the principle of least privilege followed?
- What changes, if any, are made to administrator privileges and roles to allow for extraordinary access in the event of an emergency?
- Is there an 'administrator' role for the customer?

B. Authentication

- What forms of authentication are used for operations requiring high-assurance? This may include login to management interfaces, key creation, access to multiple-user accounts, firewall configuration, remote access, etc.
- Is two-factor authentication used to manage critical components within the infrastructure, such as firewalls, etc.?

C. Identity and access management systems offered to the cloud customer

- Does the system allow for a federated IDM (identity management) infrastructure which is interoperable both for high assurance (OTP

systems, where required) and low assurance (e.g. Username and password)?
- Is the cloud provider interoperable with third party identity providers?
- Is there the ability to incorporate single-sign-on?
- Does the client credential system allow for the separation of roles and responsibilities and for multiple domains?
- How do you manage access to customer system images - and ensure that the authentication and cryptographic keys aren't contained within in them?
- Do you support a federated mechanism for authentication?
- How does the cloud provider identify itself to the customer (i.e. is their mutual authentication)?
- When the customer sends API commands?
- When the customer logs into the management interface?

III. MULTIFACTOR AUTHENTICATION

Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Typical MFA scenarios include:
- Swiping a card and entering a PIN.
- Logging into a website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the requester's phone or email address.
- Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to a network.
- Swiping a card, scanning a fingerprint and answering a security question.
- Attaching a USB hardware token to a desktop that generates a one-time passcode and using the one-time passcode to log into a VPN client.

The three most common categories are often described as something you know (the knowledge factor), something you have (the possession factor) and something you are (the inherence factor).

A. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics to describe the latter class of biometrics.

B. Knowledge-based authentication (KBA) is an authentication scheme in which the user is asked to answer at least one "secret" question. KBA is often used as a component in Multi-Factor Authentication (MFA) and for self-service password retrieval.

A good KBA question should meet these four criteria:
1. The question should be appropriate for a large segment of the population.
2. The answer should be something that is easily remembered.
3. The question should only have one correct answer.
4. The answer should not be easy to guess or discover through research.

KBA questions can be static or dynamic. Both static and dynamic schemes rely on the assumption that if someone knows the correct answers to the KBA questions, their identity has been confirmed.

C. A **one-time password** (**OTP**) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to *something a person has* (such as a small key ring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as *something a person knows*.

Multifactor authentication is effective to validate humans but less so for IoT (Identity of Things) because many methods- biometric verification, for ex. are not relevant. It's necessary to find other means of securely authenticating IoT identities.

IV. PLANNING

Planning is the main part here. We have to decide that how these techniques can help us to manage data. Managing data is a hard task but the actual hard task is to maintain its

security and confidentiality. At both the end points we can use high level of encryption techniques, strong and effective firewalls etc. when the data is travelling in the network, the data traffic, and security of data is responsibility of the provider. But main question arises here that how to maintain the data file secure on the BYOD.

90% IT companies are turning toward the concept of BYOD. BYOD stands for "Bring Your Own Device". This concept is gaining more attention on the cloud network. Cloud has the flexibility to access data from anywhere/anytime. Observing this facility of cloud to access data at any location, any time, cheap cost etc. the IT firms decided to give its employee a right to do their work on their own convenient device; this is what we call as 'Bring Your Own Device'. When the data is highly confidential than only companies machine should be used else regular task can be performed on their own device which can be according to their convenience.

Now in this case BYOD plays an important role. Employee can perform task on the personal machine but how can a machine justify that the user is correct or not. So security should be high enough. In this case single authentication is not sufficient according to survey. We have to use multi factor authentication. Different type of authentication are described here, in which biometric is strong enough; but can't be used in general life.

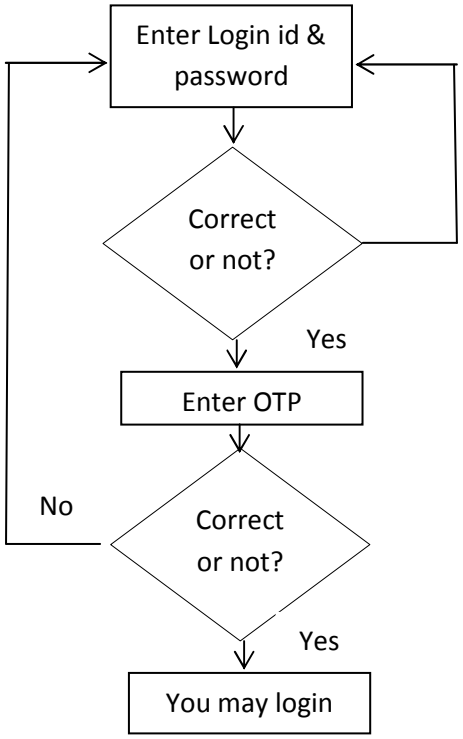
Knowledge Based authentication (KBA), is also found in two types; static and dynamic. In static the question you choose will remain same for all the time. So in case a person knows you very well can access your account and can make the appropriate changes which can be negative for you. Dynamic has its own disadvantages, it will regenerates the question again and again this will finally cause confusion and irritation for user. That how many answers should the person remembers to log-in to his account. So this is also not so efficient idea for authentication.

After this, Biometric Authentication is also there to support us for the sake of user's identity. It's a better option, but in many cases the general people doesn't afford to have a biometric device. This kind of authentication is used in generally in high profile equipment's because it needs heavy maintenance too.

So finally here comes the concept of OTP. OTP is a general form which can be easily accessible and supportable by almost every device. Till date it is found to be convenient too. That's why this concept is acceptable in each area. OTP generates random number, alpha numeric code etc. to make the process more secure.

V. ELABORATION

The following figure can easily make you understand that what I am trying to do, so that only authenticated user can access the data; Fig(a.).Figure is just depicted below to show the authentication process.



The responsibility of giving authentication to a client is task of Third Party Auditor. In case of file transformation from client side to server the TPA assures that whether the user is correct or not. It will ask for the login Id & password from the user. In case the login id & password mismatches then process will stop here only. If these are matched then the multi factor authentication concept starts working. Our concept of OTP will start working from now onwards. The OTP will be sent to an individual mobile no./email id from where a user can check it out and enter the OTP.in case it founds to be correct then the transformation of files can be done.

This on whole depends on SLA with TPA. SLA defines that what type of service it will provide to the user with the help of Third Party Auditor. The entire question asked above in the Identity-Access Management can be answered now.

VI. CONCLUSION

Cloud represents one of the biggest challenges of the era – it is a technology that makes it easy to move data around and even contract a service without the knowing of the IT, security or compliance department. Another dimension is technology – there are ways to make sure even using public cloud services, data leaves the enterprise encrypted, with the

right security measures.The right policies will educate users on which technology is safe to use, which is not safe to use, and the appropriate behavior for maximum data security.Security teams can now use the triad of people-process-technology to make sure cloud services are used in the right way, maximizing the benefits of technology and the ease of use of a universe of services available for the enterprise, without losing perspective of the most important things: protecting the brand, defending the people and saving intellectual property. Improve the work in the area of TPA and encrypting file transformation among the network safely.

VII. REFERENCES

[1] www.wikipedia.com
[2] www.techgig.com
[3] www.webopedia.com
[4] "Security and Privacy Challenges in Cloud Computing Environments"; IEEE security & privacy **nov/dec 2010**.
[5] "Information Assurance Framework";**2010**
[6] Lee and Sill ;"A Design Space for dynamic service level agreements in Openstack"; *Journal of Cloud Computing: Advances, Systems and Applications* **2014, 3:17**
[7] Kuyoro S. O., Ibikunle F., Awodele O.**;**"Cloud Computing Security Issues and Challenges";International Journal of Computer Networks (IJCN), **Volume (3) : Issue (5) : 2011**.
[8] Surabhi Shukla and Dharamjeet Singh;"Cloud's Software-Security as a Service(S-SaaS) via Biometrics"; IJCSE, **Volume (2): Issue (3):2014**.
[9] Surabhi Shukla;"Public Cloud Security Challenges and Solutions"; IJSER, **Volume (3): Issue (4): April 2015**.
[10] Clarke, N. L., and Furnell S. M. 2007. Advanced userauthentication for mobile devices. Computers & security **26, no. 2: 109-119**.
[11] Pursani, M. P. J., and Ramteke, P. L. 2013. Mobile Cloud Computing. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 2, **no. 4: pp-1512**.
[12] D. Zissis, D. Lekkas / Future Generation Computer Systems **28 (2012) 583–592**

AUTHORS PROFILE

Surabhi Shukla holds a B.E. in Computer Science, from RGPV and is currently pursuing M.E. in Computer Science at the same university RGPV. She has been involved with Infosysworld, as a business analyst for 1 year. Her interest area is Cloud Computing and database security. She is trying harder to secure database in cloud.

Prof. Neelam Joshi is working as Assistant Professor in CS dept. at MPCT from 2007. She did her Bachelor degree in CS from RGPV, Bhopal and did her M.Tech in Software Engineering from RTU,Kota.She was awarded by hon'ble CM when topped in M.Tech.