I.J. Education and Management Engineering, **2017, 3, 25-34**
Published Online May 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2017.03.03

Available online at http://www.mecs-press.net/ijeme

Role of Identity Management Systems in Cloud Computing Privacy

Kamyab Khajehei[a*]

[a] *Department of Computer, Islamic Azad University - Dashtestan Branch, Borazjan, Iran*

Abstract

These days cloud computing is a main concern for small and medium enterprises. The major concern for these enterprises is about security and privacy. This paper defines privacy and concept of identity management that may help to increase trust in the cloud environment privacy. Cloud computing brings us on-demand service by reduction of hardware costs, but it also suffers from reduction of security. Enterprises scruple to decide which provider is a proper cloud provider by understanding the different types of IDM. IDMs have a major role in applying privacy in various services in cloud computing. Thus, it is vital to have a vision about accessing resources in a secure manner. This paper focused on the SaaS (Software as a Service) and communication on cloud computing environment.

Index Terms: Cloud Computing, Identity Management, Cloud Computing Security, Cloud Computing Privacy.

1. Introduction

Cloud computing is an on-demand network services with pools of computing resources such as processing and storage. As shown in the Fig. 1, cloud computing most popular services is a SaaS (Software as a Service), PaaS (Platform as a Service). In cloud service instead of buying software license, enterprises can use SaaS. Instead of buying software and hardware in PaaS and instead of buying software and hardware and network infrastructure easily every small or medium enterprise can buy a service over Internet base cloud based on as pay-you go basis.

* Corresponding author. Tel.:+989390918551
E-mail address: k.khajehei@gmail.com

Fig.1. Cloud Model

Users can access to their services over Internet by entering their user name and password. This is front of cloud computing authentication and authorization. But, in back there are different services that help enterprises to keep their privacy over the Internet. Thus, keeping unwanted access away from enterprises precious data has a major role in cloud services [1]. Cloud computing Identity Management (IDM) provides information that contains user roles and permissions for access management. Access management is just responsible for applying these roles provided by IDM for preserving privacy in a cloud computing. In this paper, we first define privacy and identity management concepts. Also, in other sections, it reviews different schemes to understand IDM frameworks that helps technicians to decide which cloud vendor is meets their privacy policies.

This paper consists of three parts. Part one is about the definition of related IDM and privacy eras. Part two explains different models of IDMs based on the deployments which enterprises use these models. And the final and third part is a comparison of different protocol for exchanging data based on their pros and cons over cloud computing environments.

2. Privacy Definitions in cloud computing

There are different definitions when we talk about the privacy. Privacy defined as any individual or organization must decide when, how and how much of its information should be accessible to others [2]. Based on the definition enterprise administrator must decide how access what. On the other hand, cloud security mechanism must check the identities and prevent access of unauthorized user that trying to access these resources. The identity is a term of the usable unique characteristic of an entity [3]. It cloud be any kind of information that comes from an individual or an object in the cloud environment [2]. Thus, these characteristics based on their uniqueness are used for authentication purposes and known as identifiers.

3. Role of Identity Management systems in Privacy

Identity Management (IDM) has a direct effect on cloud computing privacy and security. In cloud security first thing you should concern about it is identity to put a border in a borderless environment like cloud computing environment. To maintain a massive amount of users in cloud environment separate and independent component needed. This component distinguishes unauthorized users from authorized users. In the next step, it draws a line that shows how much of the data that each user may or should access. It completely matches by definition of privacy. IDM works with help of identities over network to control every individual access to their resources. The tasks that IDM performs are: a) Establishing identities. b) Describe identities. c) Logging the activities. d) Destroy unused identities [4, 5].

The IDM is not just a simple password manager in a cloud environment, but it is also responsible for

maintaining user's data privacy over cloud environment [6]. IDM is maintaining user identity and avoiding illegal access to secure data over cloud environment and it is called as provisioning and de-provisioning [7]. To avoid illegal access for extract roles and access rights to the resources from data which is entered by administrators and enterprise authorities. Then, it delivers this information via communication protocols that will explain later. The next section defines and shows the different locations that identity manager component could place in.

4. Classification of Identity Managements Base on the Deployment

Combination of locations in a cloud application server and identity management server defines different strategy. Based on the assets we have in a cloud, each of these strategies can be implemented. Following Figures shows main player component location and some of component not shown here [8].

4.1. Independent IDM

Independent Identity Manager (IDM) also introduced as Isolated IDM [4, 9] single server is responsible for managing all users and controls them. As shown in Fig. 2, independent IDM is the simplest scheme of implementing privacy and security and also it is common in cloud software design in small and medium enterprises [10, 11]. Fig. 6 is showing that how all parties can communicate to each other.

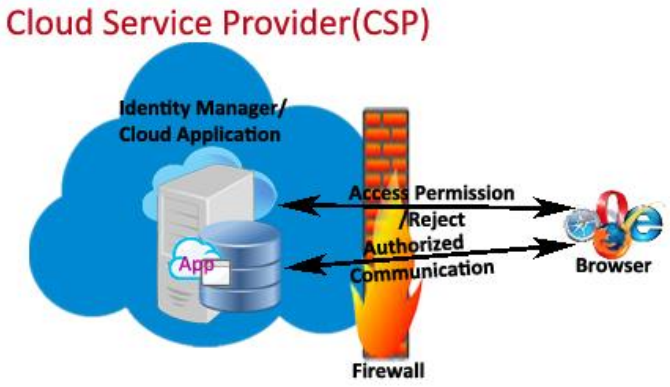

Fig.2. Independent IDM Workflow

4.2. User-Centric IDM

User-centric design built on user needs [12]. Users used their digital identities to use cloud application in different places on various devices such as smart phones and tablets [13]. Users just need to logon once and all needed cloud applications will be accessible for that user [14]. Figure3 shows how different component can be located in a cloud environment.

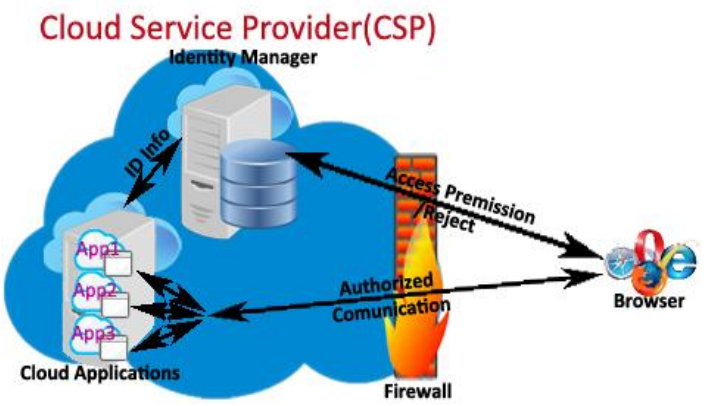

Fig.3. User-Centric IDM Workflow

4.3. Federation IDM

This model, as we can see in Fig. 4, is more like the user centric model, but instead of related group of users, there is federation of users [15, 9]. Different parties which are contains their own users, consolidate different, but related identity managers. It is suitable for medium or small size enterprises that consolidate resources and reducing their costs or sharing their information. But the major problem is heterogeneity of different identity management [16] and also interoperability of different clouds [17].

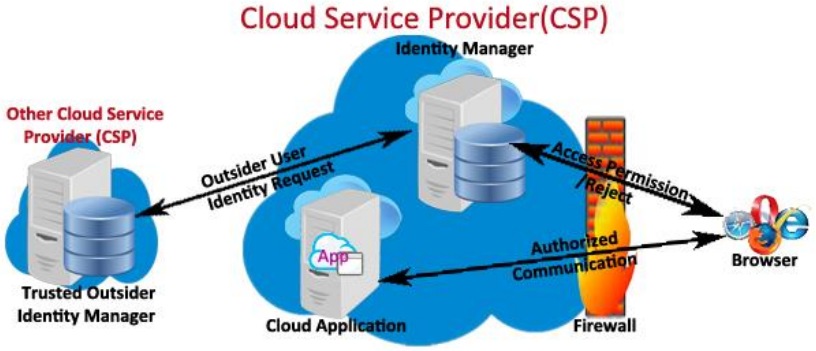

Fig.4. Federation IDM Workflow

4.4. Anonymous IDM

Anonymous identity management also acts like user-centric IDMs with one difference and it is unknown user. This model designed for users which do not trust any CSP. They may use this type of IDM in a cloud environment. This model ensures anonymity of each Entity and keeps data anonymous from anyone else in a cloud environment [18]. There is one approach in anonymous IDM which known as Entity-Centric Approach. The entity-centric is designed based on the Active Bundle (AB) scheme [19] and VMs are considered to enforce privacy and security policies [20]. An active bundle also known as IDM Wallet included identity data, disclosure policy, disclosure history, negotiation policy and virtual machine [20].

5. User Authentication and Authorization Data Exchange Protocols

When a user authenticated, it means the user can access to the resources, necessary information will provide by IDM and two parties need to exchange their data across the cloud environment. In traditional application, usually, session and cookie will be created to keep authorization information. But in the cloud environment for security reasons (attacks like hijacking sessions) cannot be used. Also, because there is a lot of communication between participants and resources one concept needed, which known as Single Sign-On or SSO. SSO is a way that each user must authenticate once and no needed extra authentication process for the rest of the communication. In contrast, a traditional cloud authentication and authorization token is used for replacement of sessions and cookies. Therefore, specific protocols and frameworks are designed. Most common protocols of this group are SAML (Security Assertion Markup Language), OAuth2 and JWT (Json Web Token).

5.1. Session IDs/ Cookies

Simplest authentication and authorization process can be implemented by designers. The major advantages of using sessions and cookies are simplicity and easy to manage. But, in a cloud computing environment which is you cannot be sure how is will be present on VMs next to you, it will be very vulnerable. In this environment your privacy will be on the edge and fragile and session can compromise. Another drawback is identity and role information should send every time for each request.

5.2. SAML (Security Assertion Markup Language) authentication Protocol

After authentication process, one of the tokens may generate for authorized communication is SAML [21, 14]. SAML structure is significantly, XML base. The structure of SAML is shown in Fig. 5. As shown in Fig. 5, SAML transport is based on the HTTP protocol and SOAP [14]. The main part which is known as Assertion provides authentication information each client. By generating this token client will convert to authorize user and can access to the cloud resources. Another tip about the SAML is about its architecture, which is the client-server architecture base. Thus, it has its own SAML request and response structure. Also SAML has its own digital signature to ensure the appropriate party.

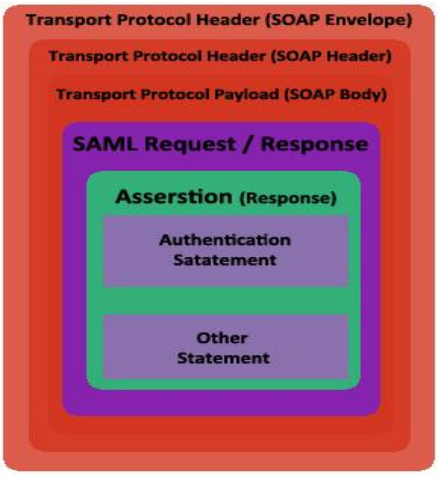

Fig.5. SAML Structure

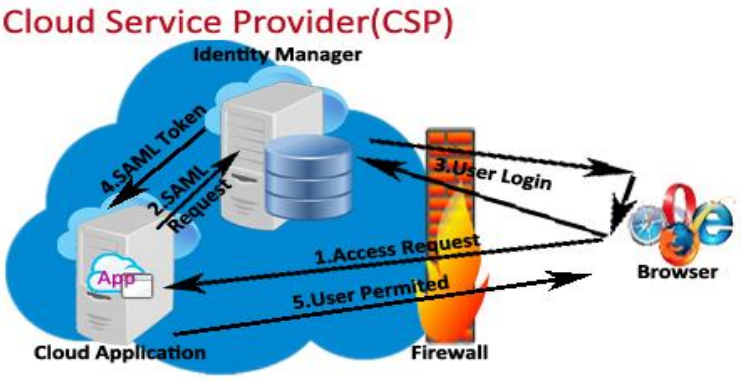

Fig.6. SAML Flow

The workflow of the SAML is shown in Fig. 6. For instance, if one user wants to log in a website these actions will happen:

1) A user opens its web browser and goes to a website.
2) The website does not authenticate the user by itself. The Website will generate a SAML authentication request and signs it, then user will redirect to the IDM to authenticate.
3) If the request is a valid request by checking the digital signature, the login form for entering username and password will provide for user to enter its username and password.
4) If user logged in, IDM generates a SAML token that includes all necessary identity information and permissions for user and then redirect user again to the wanted website.
5) Website easily can extract the identity information and also user permissions from SAML token and user authentication will be completed.

5.3. OAuth2 authorization Framework

OAuth2 which is used for applying privacy over cloud computing [22] basely is similar to SAML. In this framework the 'Auth' word does not stand for authentication, it is stands for authorization. As mentioned in the previous section, unlike SAML, OAuth2 not directly consist of digital signature. Instead of that OAuth2 uses grants method which has given permission for users to access its information. OAuth2 is simpler that SAML, but this simplicity brings some disadvantages like incompatibility for all servers. Another issue of OAuth2 tokens is the security issue and it must be protected. Also, it has a limitation for token lifetime and it must refresh in short periods of time. Fig. 7 is showing workflow of the OAuth2.

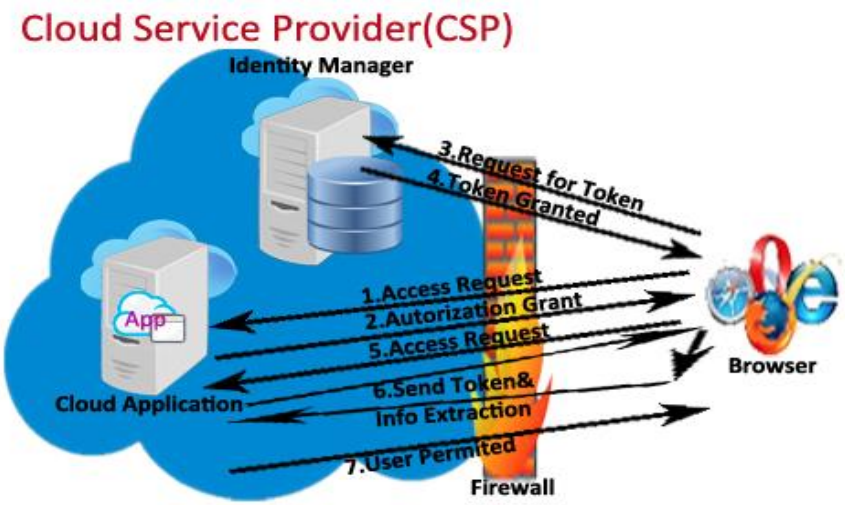

Fig.7. OAuth Flow

The sequence of workflow will be like this:

1) A user opens its web browser and goes to a website.
2) The website server receives the request, but it cannot handle authorization by itself. It redirects to the IDM. Login form will be provided and IDM generates a grant for the user's browser. The client redirects to the website server along with provided grant. Then, server sends grant to the client browser.
3) With this grant, client can clarify itself for IDM. Client sends a grant and also a request for a valid access token.
4) IDM generates access token and send it to the client browser.
5) Client which now is the owner of the valid access token sends this information to the website server.
6) But server must validate the token. So, it sends a token to the IDM to validate it. If the token is valid, IDM will provide necessary user information and send it to the server.
7) At the last, server informs the client that your request is valid and you can use resources.

Here also we can use an HTTP protocol for communications, but in a simpler manner. Thus, easily we can use the provided information in URLs.

5.4. JWT authentication Protocol

Unlike SAML and OAuth2, JSON Web Token (JWT) [23] does not need complex structure because it is a token. Simply it consists of three parts: a) Header which is about itself b) Claims or Payload which is about user sensitive information and c) Digital signature which is separated by dot (.). Provided information will be encoded with base64encode. More important is JWT even can use as grant in OAuth2.

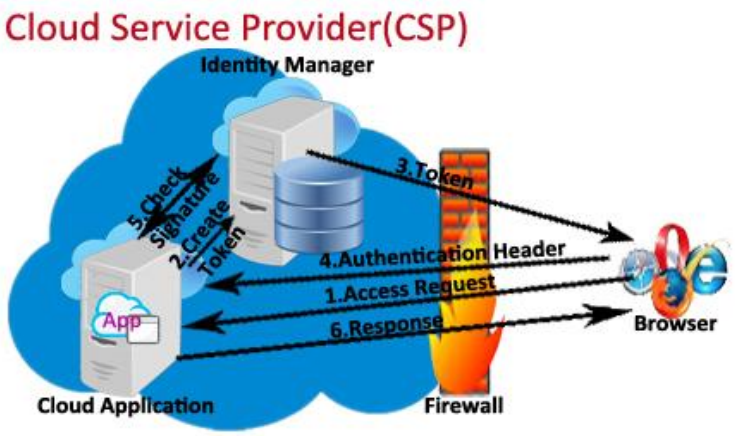

Fig.8. JWT Flow

Sequence JWT workflow shown in Fig. 8. It will be like this:

1) Server provides a login form for a website.
2) Browser posts the username and password for login.
3) Server generates a JWT token and sends token to browser.
4) Browser sends a JWT for communication.
5) Server checks the JWT signature for validate client.
6) Server response to the client.

5.5. SSL/TLS Protocol and X.509 certificates

As discussed previously all protocols and frameworks which are based on token only can provide authentication and authorization. A main problem which still presents in communication privacy is attacks like man-in-the-middle. To secure communication between two parties still SSL/TLS security protocol which is based on the issuing digital certificates are needed. A digital certificate is used to create a secure communication via Internet. Actually, certificates are an important part of SSL or TLS protocols. The protocols provide a secure environment to pass different token between different participants.

6. Conclusion

In traditional hosted web application maybe a session/cookie model is suitable for keeping user data privacy, but in a cloud computing environment this model are absolutely vulnerable. To increase privacy in cloud token base approach is necessary. In token base model identity managers has a major role for data privacy [24]. Depend on needs there are different frameworks that can implement that can be useful. But on any conditions users need to find a trusty cloud service provider that can maintain the sensitive information.

References

[1] N. F. M. Kubach, “Identity Management and Cloud Computing in the Automotive Industry: First Empirical Results from a Quantitative Survey”, In Gesellschaft für Informatik eV (GI) publishes this

series in order to make available to a broad public recent findings in informatics (ie computer science and informa-tion systems), to document conferences that are organized in co-operation with GI and to publish the annual GI Award dissertation, 2015.

[2] K. Gunjan & G. Sahoo & R.K. Tiwari, "Identity Management in Cloud Computing –A Review", International Journal of Engineering Research & Technology, Vol. 1, No 4, 2012.

[3] A. Benusi, "An Identity Management Survey on Cloud Computing", International Journal of Computing and Optimization, Vol. 1, No. 2, 2014, p. 63-71.

[4] U. Habiba1 & R. Masood & M. A. Shibli & Muaz A Niazi, "Cloud identity management security issues & solutions: a taxonomy", Vol. 2, No. 1, 2014, p. 1.

[5] P. Angin & B. Bhargava & R. Ranchal & N. Singh & M. Linderman & L. B. Othmane & L. Lilien, "An entity-centric approach for privacy and identity management in cloud computing", In Reliable Distributed Systems, 2010 29th IEEE Symposium, 2010, p. 177-183.

[6] T.A. Johansen & I. Jorstad & D. Van Thanh, "Identity management in mobile ubiquitous environments", The Third International Conference on Internet Monitoring and Protection, 2008, p. 178-183.

[7] A. Gopalakrishnan, "Cloud Computing Identity Management", SETLabs Briefings, Vol. 7, No. 7, 2009, p. 45-55.

[8] S. Khatua & A. Ghosh & N. Mukherjee, "Application-centric Cloud management", Computer Systems and Applications, 9th IEEE/ACS International Conference, 2011, p. 9-15

[9] K. Ashanpreet & R. Singh, "Identity Management in Cloud Computing: Issues, Incidents and Solutions", International Journal of Scientific & Engineering Research, Vol. 6, No. 3, 2015, p. 999-1004.

[10] W. A. Alrodhan & Chris J. Mitchell, "Enhancing user authentication in claim-based identity management", In CTS, 2010, pp. 75-83.

[11] C. Yuan & L. Yang, "A survey of identity management technology", Information Theory and Information Security, 2010 IEEE international conference, 2010, p. 287-293.

[12] A. Černezel & M. Heričko, "A user-centric approach for developing mobile applications", 7th International Conference on Knowledge Management in Organizations: Service and Cloud Computing, 2013, p. 455-465.

[13] X. Yang & L. Liu, "Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing", IGI Global, 2013, p. 172-173.

[14] A. M. Lonea & H. Tianfield & D. E. Popescu, "Identity management for cloud computing", New concepts and applications in soft computing, 2013, p. 175-199.

[15] H. Y. Huang & B. Wang & X. X. Liu & J. M. Xu, "Identity federation broker for service cloud", Proceedings of the 2010 International Conference on Service Sciences, ICSS '10, Washington, DC, USA, 2010, p. 115-120.

[16] A. Celesti & F. Tusa & M. Villari & A. Puliafito, "Security and cloud computing: Intercloud identity management infrastructure", Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 19th IEEE International Workshop on, 2010, p. 263-265.

[17] S. Dowell & A. Barreto & J. B. Michael & M. T. Shing, "Cloud to cloud interoperability", System of Systems Engineering (SoSE), 6th International Conference, 2011, p. 258-263.

[18] E. McCallister & T. Grance & K. A. Kent, "Guide to protecting the confidentiality of personally identifiable information", US Department of Commerce, National Institute of Standards and Technology, Diane Publishing, 2010.

[19] L. Ben-Othmane & L. Lilien, "Protecting Privacy in Sensitive Data Dissemination with Active Bundles", Proc. 7th Annual Conference on Privacy, Security & Trust (PST 2009), Saint John, New Brunswick, Canada, 2009, p. 202-213.

[20] P. Angin & B. Bhargava & R. Ranchal & N. Singh & M. Linderman & L.B. Othmane & L. Lilien, "An entity-centric approach for privacy and identity management in cloud computing", Reliable Distributed Systems, 29th IEEE Symposium, 2010, p. 177-183.

[21] S. Ferdous & R. Poet, "Managing dynamic identity federations using security assertion markup",

Journal of theoretical and applied electronic commerce research, Vol. 10, No. 2, 2015, p. 53-76.
[22] C. Wise & C. Friedrich & S. Nepal & S. Chen & R. O. Sinnott, "Cloud Docs: Secure Scalable Document Sharing on Public Clouds", IEEE 8th International Conference on Cloud Computing, 2015, p. 532-539.
[23] M. Jones & J. Bradley & N. Sakimura, "Json web token (jwt)",. No. RFC 7519. 2015.
[24] D. Nuñez & I. Agudo & J. Lopez, "Privacy-Preserving Identity Management as a Service", Accountability and Security in the Cloud, 2015, p. 114-125.

Authors' Profiles

Kamyab khajehei has completed his M.Sc. in Computer Science from Osmania University, Hyderabad, India. Presently, he is teaching in Islamic Azad University, Dashtestan Branch, Borazjan, Iran. His main research interest include Cloud Computing, Green Cloud and Big Data.

How to cite this paper: Kamyab Khajehei,"Role of Identity Management Systems in Cloud Computing Privacy", International Journal of Education and Management Engineering(IJEME), Vol.7, No.3, pp. 25-34, 2017.DOI: 10.5815/ijeme.2017.03.03