I.J. Wireless and Microwave Technologies, **2018, 4, 54-65**
Published Online July 2018 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2018.04.04

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

Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management)

Kamyab Khajehei [a*]

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

Received: 30 March 2018; Accepted: 04 June 2018; Published: 08 July 2018

Abstract

In these days all businesses trying to use global applications on cloud computing infrastructure to reduce their costs and also decentralize their application. This movement also causes more security risks over the unbounded cloud environment. Therefore, accessing enterprise information for an unwanted user will be more than other environments.

Thus, the proposed Identity Management System (IDMS) tries to preserve security in communication between clients and server over cloud computing. The proposed method suggested token based Identity Management and also enhanced privacy by adding one. Dual Certificate Manager (DCM) block is a replacement for a combination of symmetric and asymmetric cryptography, which is commonly used for SSL/TLS protocol to immune data transmission, uses asymmetric cryptography in both participants.

Furthermore, for more privacy and invulnerability DCM uses Elliptic Curve Cryptography (ECC) as asymmetric cryptography algorithm.

Index Terms: Cloud Computing, Identity Management, Cloud Computing Security, Cloud Computing Privacy, Internet of Things (IoT).

1. Introduction

There is no doubt about that the cloud computing is the future of the computational power of the enterprises. Thus, the security of these data [1] to enhance information privacy is one of the major challenges for enterprises [2]. There are different platforms are known for cloud computing. These platforms are 1) public cloud, 2) private cloud and 3) hybrid cloud.

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

In all of these platforms accessing unauthorized user is a huge problem. The main problem is not that anyone tries to control your platform, but, it is about stealing your data by eavesdropping your communications [3].

As shown in Fig. 1, there are different service models in the cloud. These models are 1) Infrastructure as a Service (IaaS) 2) Platform as a Service (PaaS) 3) Software as a Service (SaaS). In each service model correlation between cloud service provider (CSP) and users at different levels are obvious.

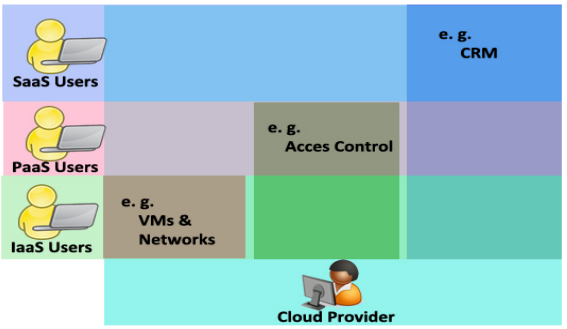

Fig.1. Cloud Stack View

In these days different services are introduced in cloud computing, but, as shown in Fig. 2, all services are based on the main three services. Thus, if discussing about a service, it can include all the services that available in cloud computing.

Fig.2. Cloud Service Model

As discussed before, maintaining authorized users and distinguishes action for an authorized and unauthorized user is the main goal of the IDMSs. Therefore, keeping unauthorized user away to get access to information is defining the level of privacy in cloud computing [4].

This paper consists of four parts. Part one defines privacy and other necessary subjects. Part two reviews various user authorizing methods. Part three reviews various classifications of identity management. And in the last part, paper discuss proposed IDMS.

2. Privacy Definitions in cloud computing

In cloud computing environment, based on the structure of hardware and software components, every individual user instance are living beside the others instances. Therefore, the definitions are differs from other environments. In this section, we define some terminologies which are important in cloud computing and they are useful for our concept. The major words are: privacy, identity and personally identifiable information.

2.1. Privacy:

Information that belongs to any individual and that person will decide when and amount of this information should be accessible to others [5].

2.2. Identity:

Identity is a term of the usable unique characteristic of an entity. It cloud be any kind of information that comes from an individual or object in a cloud environment [5].

Thus, these characteristics based on their uniqueness are used for authentication purposes and known as identifiers.

2.3. Identity:

Personally Identifiable Information (PII) also known as Sensitive Personal Information (SPI) which used in privacy law and information security, is information that can be used to identify its self to others. This information can identify, contact or locate a single person, or identify an individual in the context [6, 7].

With the help of identities and identifiers, cloud environment can decide whether an individual is an authorized user or not. Whole these definitions and operations define privacy in cloud computing.

The outcome of this definition shows that there is no straight borderline to define out border or in border information. Thus, it is really hard to distinguish sensitive information in the cloud.

Disclosure during communication, this becomes even more important where the sensitive data might be held by a Cloud Service Provider (CSP) [8].

3. Identity Management systems

Identity Management (IDM) has a major role in cloud computing privacy and security. In cloud privacy, a concern should be about identities which draw a border in a borderless environment like cloud computing environment. Your identity in the virtual world could be an email address or unique ID that shows who you are [9]. The duty of identity manager is maintaining and securing these identities and distinguishes authorized and unauthorized users.

IDM doing a different action which consists of [10]: a) Establishing identities. b) Describe identities. c) Logging the activities. d) Destroy unused identities.

There is a massive difference between IDM and simple cloud application password manager. Here IDM responsible for user privacy and user data integrity [11]. The process of maintaining and securing user's identity in cloud environment also called as provisioning and de-provisioning [12].

4. User Authentication and Authorization Data Exchange Protocols

After IDM grant authorization for users, then IDM provides the necessary data and it should exchange between two parties across the cloud environment. Instead of using simple sessions for secure communication, frameworks such as SAML [13] and OAuth2 are the most common frameworks which are works by generating token [14, 15] instead of a session and setting a cookie.

4.1. Session/Cookie-based Authentication and Authorization

The main advantages of using session/cookie base web implementation are easy to implement and also it is easy managing session lifetime.

But, besides these advantages, disadvantages are more. Implementing a simple cookie-based authentication in cloud environment which virtualizes a computer network, puts privacy at a various risk.

The problem over cloud environment is the VMs over cloud act like physical computers over the single local network domain. Different kinds of attacks could be harmful to this environment.

Base on the structure of infrastructure of cloud computing that shown in Fig. 3, all communications will pass through a hypervisor and these hypervisors are unsecured channels for sensitive data communications [3].

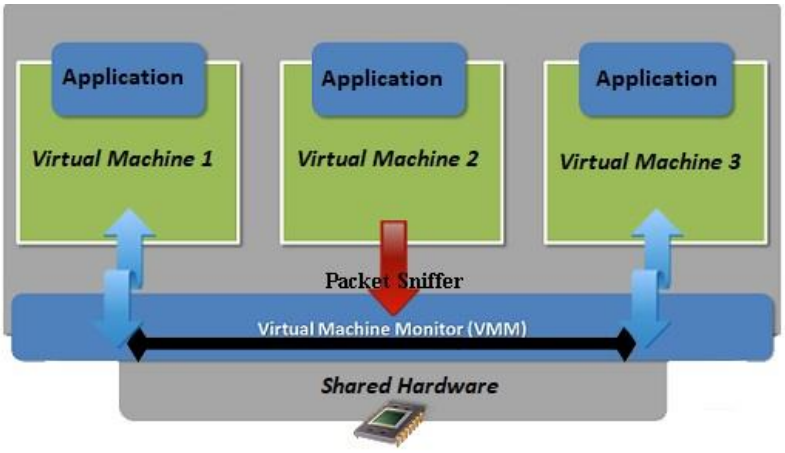

Fig.3. Sniffing Packets for Session Hijacking

Thus, if session/cookie uses in designing applications for cloud computing, it is possible to attack VMs by active attacks like hijacking active sessions or even Cross-Site Request Forgery (CSRF) attacks and it is in contrast of cloud information privacy. In next sections, some of these protocols will discuss to find the proper one for this environment to enhance privacy.

4.2. SAML (Security Assertion Markup Language)

Using global applications in environments like cloud forcing the user to communicate with different systems or in this case different VMs. It is an advantage that user access another system without trying to for each VM. This routine is known as Single Sign-On or SSO. To meet this goal one of the token-based frameworks which help us known as Security Assertion Markup Language (SAML) [16]. SAML is an XML based standard that uses for the exchange of user authentication and authorization across VM domains in a secure manner. When a user wants to login into a web application, a SAML token will generate and a user can get access to the web application and other resources. SAML token contains user PII alongside with roles and user level that create a platform for access management to apply in cloud infrastructure.

The problem is the tokens that can be stored in the browser cache or cookie form containing some of user private data. Retrieving user sensitive data from these standalone tokens could be easy [14]. The solution will discuss in continue.

Eventually, to have a trust between two parties, we also need assistance of the certificates which issues trusted communication. This extra trust blocks may have an overload of our communication environment.

4.3. OAuth2

OAuth2 uses for authentication, which is useful for applying privacy over cloud [17]. Essentially, OAuth2 is similar to SAML. As mentioned in the previous section, unlike SAML, OAuth2 not directly consist of a digital signature. This mechanism will offer only authorization and the 'Auth' word not stands for authentication.

This lack of digital signature can reduce privacy over the cloud, but as mentioned before, for secure communication still SSL/TLS protocol is still strongly useful. The digital signature and public key cryptography that builds SSL/TLS protocol have responsibility for these deficiencies. But, in contrast to SAML, the combination of OAuth2 and SSL/TLS will provide a simple and strong mechanism for implementing cloud privacy.

On the other hand, OAuth2 has strong points like a small amount of coding for implementation and it is easy to maintain. Thus, it reduces costs for providers. These strengths make it powerful for both private and public cloud.

4.4. JWT

All we need in communication between global application and client browser is to use some token to use for the authorization process. Unlike SAML and OAuth2, JSON Web Token (JWT) does not need complex structure to carry our sensitive data or PII [19]. Simply it consists of three parts: a) Header which is about itself b) Payload which is about user sensitive information and c) Digital signature and the provided information will encode with base64encode.

This structure essentially can pass through the URL and it is much faster than other token generators discussed before.

Regards to that JWT brings us authentication and authorization together, but still, the communication in the cloud environment may not be safe for passing token [18]. In JWT instead of storing data on the server it needs only passing around and it is easy for the client side to manage. Because it is easily could read by users, still, SSL/TLS is required to secure the communication.

Base on previous disadvantage, it should be included for each HTTP request system may need. Another issue is about the size of JWT token and it must be not larger that session ID.

However, there are lots of advantages that make JWT suitable for the cloud. One is being fast and independence from cookies which is an easy risk in the cloud. It can protect users from Cross-Site Request Forgery (CSRF) attack. All of these advantages make it also suitable for mobile cloud global applications [20].

4.5. SSL/TLS Protocol and X.509 Certificates

As mentioned before, most communications are based on the HTTP request/response. Therefore, for security reasons, two parties use HTTPS. The SSL/TLS protocol provides a secure environment to pass tokens between different participant base on HTTP protocol. Digital certificates are an important part of the SSL/TLS protocol. They are used to carry information for creation of a secure communication via the Internet.

The mentioned protocol also works with the asymmetric cryptography algorithm. Thus, a certificate also contains information that provides by Public Key Infrastructure (PKI) [21]. Each certificate has verity critical information such as certificate serial number, digital signature algorithm, the validity period (not before or not after) and public key information (public key algorithm or public key) [22].

5. Proposed Identity Management System

As we mentioned before, application which are using cloud based environment, are more vulnerable on direct attacks. Because most direct attacks are attacking their neighbors in the very same networks and the cloud computing instances are originally lives on the same network area. Based on our knowledge about type of the cloud computing network, we proposed system that focused on trusting no one on their environment.

The proposed system mainly focused on secure communication two authorized certificated participants using smaller token, robust cryptography.

Basically, it has four different characteristics:

A) JWT token for soft and easily communicate.
B) TLS version 1.2 for the securing communication channel.
C) Elliptic Curve Cryptography (ECC) as asymmetric cryptography algorithm and digital signatures.
D) Separate unique digital certificate for all participants.

The proposed block, based on these characteristic named as Dual Certificate Manager (DCM). This block in one aspect, it is like a Public Key Infrastructure (PKI) [21] and in another aspect, it is similar to CA. The difference is DCM responsible for both duties in an environment.

As shown in Fig. 4, DCM act as a Certificate Authority (CA) creates a certificate for the server and also sends a request for client certificates. It means it creates private and public key for the server for one side, and for the public key for another side.

In this IDM beside user PII, a certificate related to each client also stores. Also, its role as a PKI [23], it is generating a private and public key for related certificates.

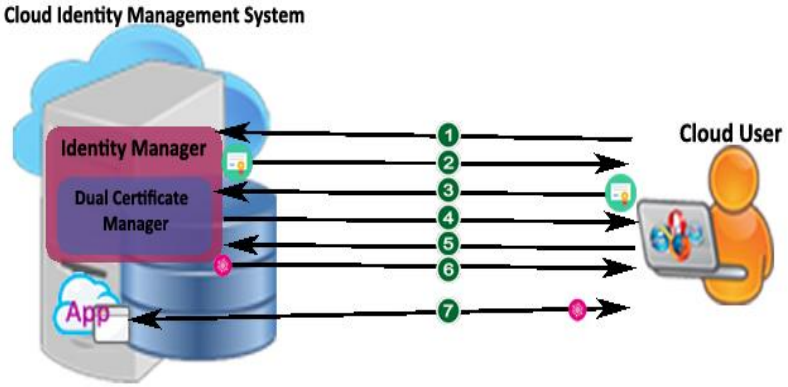

Fig.4. Proposed Identity Management System

The sequence of actions shown in Fig. 4:

1) Cloud user (browser) tries to cloud application, then it redirects to the IDM-DCM to verify access request along with a request for a certificate.
2) IDM-DCM sends a server certificate with a private and public key to the cloud user along with a request for client certificates.
3) Now cloud user (Browser) has a server-side certificate. Therefore, it checks the signature and base on a selected cryptographic algorithm which is ECC recommended here, creates its own certificate, then encrypts the certificate with server public key and sends it to the IDM-DCM.
4) IDM-DCM decrypts certificate information checks the signature and PII which are stored in IDM, then if exists, stores the certificate information besides a user PII and send roles. The sequence of one to three also used for dual authentication and also used for handshaking process.
5) Now handshake process completed and the user sends the token request for communication.
6) IDM-DCM creates the token which is here JWT token and sends it to the cloud user in a secure manner.
7) Cloud user has a token and also it can encrypt all data for the application, then it can communicate with the application in secure channels.

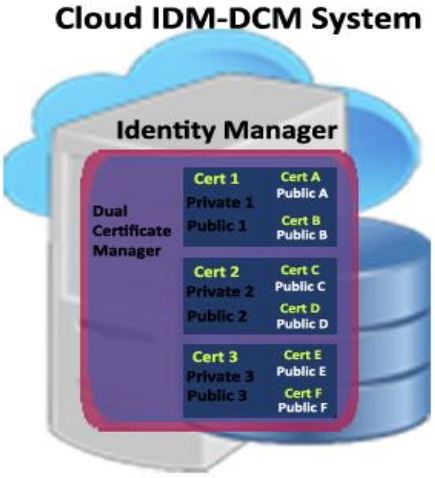

Fig.5. IDM-DCM with Grouping Certificates

DCM also can divide the whole environment into different domains with one private and public key and also maintain client public keys as shown in Fig. 5. By grouping the users for global applications in cloud computing in case of any successful attack on a signature of key pairs only part of the system will fall and rest of the users will be safe.

6. Proposed Design Base on the Deployment Classification

In this section we separated our proposed system into two major parts. In part one, we defines main common components in our proposed identity management system. In part two, based on which type of deployment you are working with in your cloud environment, we define and explain other related components. In explanation figures we shows each and every steps and we sequenced them by numbers for following sequence.

6.1. Main Components

6.1.1. User Browser

This component is important for us because the token created by server and certificates will store in the browser cache.

6.1.2. Proxy server

A proxy server or web proxy can use for receiving HTTP post and extract token and also make URL which contains a token that can redirect to other servers. This server is important because IDM can retrieve necessary information from a URL that created by this server and prepare the user to log in.

6.1.3. DCM (Dual Certificate Manager)

Based on the proposed design major part of this design is DCM. Secure communication between users and cloud application needed public key cryptography. For such a reason SSL/TLS protocol required.

In the cloud, the major problem and attacks will be on cryptographic pair keys like POODLE or DROWN attacks. Thus, one of the solutions to attacks on SSL/TLS is restricted a risk area and applying expiration period. For these reasons proposed DCM use grouping strategy. Each group has its own private key and different client's public keys. With grouping strategy, even private key also has its own expiration date.

6.1.4. Identity Management

The role of IDM is to store and manage Personally Identifiable Information (PII) of users for cloud computing access.

6.1.5. Cloud Application

The global application, which is located on Virtual Machines (VMs) that serves cloud users.

6.2. Independent IDM

An independent IDMs scheme which is known as Isolated IDM [24, 25] is a scheme with a single server. IDM and application both are residents in the same server. Independent IDM is the simplest scheme for implementing privacy and security and common cloud software design in small and medium enterprises [26, 27]. This type of IDM does not use and trust any third-party to manage their user's identities.

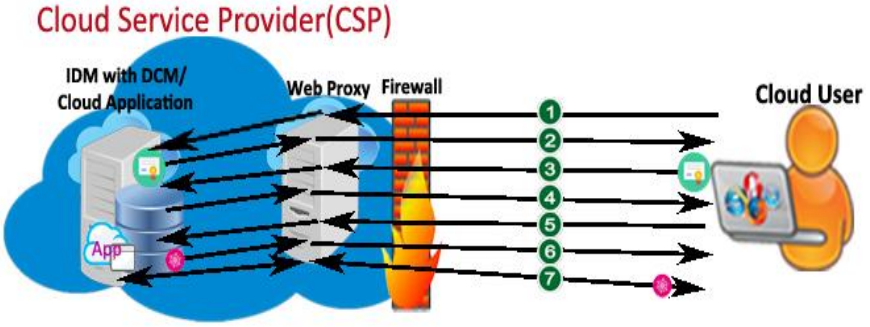

Fig.6. Independent IDM with DCM

As illustrated in Fig. 6 the sequence of actions are:

1) The user sends a request for an application server certificate.
2) IDM-DCM sends the certificate and also request for client certificates.
3) User encrypts its certificate with server public key and sends it to the server.
4) IDM-DCM encrypts finish message with user public key and sends it to the user for authentication and handshaking.
5) Users authorized and can send a request for the token.
6) IDM-DCM generates a token base on the user roles and responsibilities, then sends it to the user.
7) Application and cloud user now can communicate in full secure manner.

6.3. User-Centric IDM

Essentially, a user-centric scheme is based on the user needs to interact with a different application over cloud [28]. In this scheme, applications need to be compatible with users, not vice versa. The user needs to login once and all needed cloud applications will be accessible to that user [29].

User digital identities and user roles are very important here. Users need to use cloud applications in different places on various devices such as smartphones and tablets [30] and one of the main solutions is a user-centric scheme. This scheme involves the third-party for managing PII and certificates.

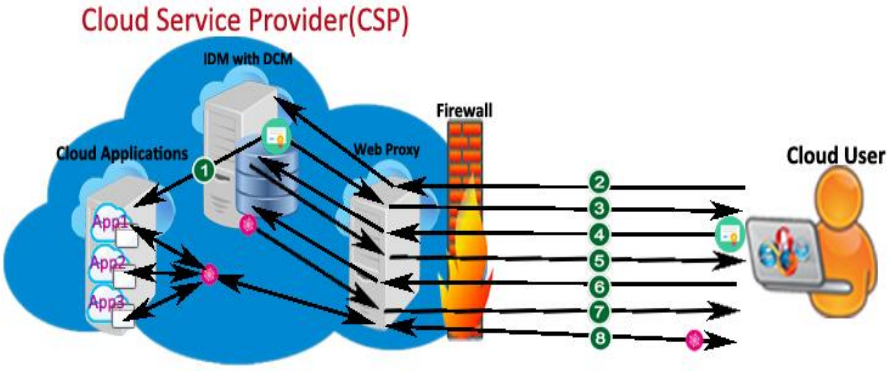

Fig.7. User-Centric IDM with DCM

As illustrated in Fig. 7, sequences of actions are:

1) IDM-DCM generates a key pair and certificate for an application server and sends it to an application server which is paired by DCM before. In case of grouping technique, different certificates need to be generated.
2) The user sends a request for an application server certificate.
3) IDM-DCM sends the certificate along with a request for client certificates.
4) User encrypts its certificate with server public key and sends it to IDM-DCM.
5) IDM-DCM encrypts finish message with user public key and sends it to the user for dual authentication and handshaking process.
6) The user sends the request for token and IDM-DCM extract roles and access level generate a token.
7) IDM-DCM sends a generated token.
8) Full secure communication between all applications and cloud user based on the generated token.

6.4. Federation IDM

A federation scheme more like the user-centric scheme, but instead of the related group of users, there is a multilateral federation of a group of users [31]. In case of different enterprises need user others application in single private or public cloud or even a hybrid multi-cloud, this scheme is a solution [32]. IDM in different locations uses their own users and also consolidate other party users in its IDM to access one application. This scheme is useful for medium or small enterprises that can use this model to consolidate resources and eventually to share their costs and information.

The main consideration in the federation scheme is a heterogeneity problem [33]. For consolidation different parties, different IDMs can communicate to each other via SAML (Security Assertion Markup Language) to communicate to each other [13]. This scheme also involves third-party [34] as a broker in a consolidation process in addition to other responsibilities.

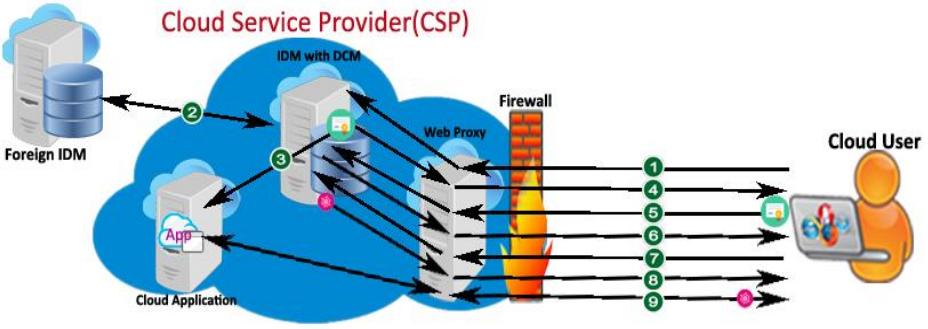

Fig.8. Federation IDM with DCM

As illustrated in Fig. 8, sequences of actions are:

1) The user sends a request for an application server certificate.
2) IDM-DCM cannot find user PII in its own data, then it takes it from foreign IDM which is paired with DCM before.
3) IDM-DCM generates a key pair and certificate for an application server and sends it to the application server which is paired by DCM before.
4) IDM-DCM sends the certificate along with a request for client certificates.
5) The user encrypts its certificate with server public key and sends it to IDM-DCM.
6) IDM-DCM encrypts finish message with user public key and sends finish message to the user for dual authentication and handshaking process.
7) The user sends the request for token and IDM-DCM extract roles and access level generates a token.
8) IDM-DCM sends a generated token.
9) Full secure communication between all applications and cloud user based on the generated token.

7. Conclusions

The main concern about cloud environment is a privacy and security of their data. Security always matters for enterprises and has a critical role in their existence. On the other hand, in recent years, attackers also have a better understanding of the cloud. Thus, it is important for us to increase a security level and techniques to avoid data vulnerability in the cloud environment. This paper proposes DCM technique for authenticating and authorizing users helps us to avoid attacks on privacy and accessing unauthorized users to individual and company sensitive information. In this technique, we propose token based terminology for tracking and easy data access.

Besides, we propose grouping technique that separates and break down into separate different users. By this action, we are downsizing the domain of the attacks. If any successful attack affects and determines key values of the one or more users in one area, even for a small amount of time, other areas in other groups will be safe.

The grouping technique very useful, especially in the concept of IoT. In the IoT, there is a large amount of small users are available. This concept still young and they are very vulnerable as we saw in recent years. Thus, separating and grouping IOT users can vital for some companies.

Also proposes an ECC algorithm for a cryptographic process based on the key length and strength of algorithm that not easy to break it. One of the major reasons that most of the designers are not using this cryptosystem is more computation mostly in the initialization process. In a cloud computing environment, we have a lot of computing resources, therefore this problem is not matter here. And for reduction of token passing process purposes, proposes JWT for token structure. The combination of these actions and certificates provides a secure environment in a cloud computing environment.

References

[1] PankajDeep Kaur, Awal Adesh Monga,"Managing Big Data: A Step towards Huge Data Security", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.6, No.2, pp.10-20, 2016.

[2] M Ali & S.U. Khan & A.V. Vasilakos, "Security in cloud computing: Opportunities and challenges" Information Sciences, No. 305, 2015, p. 357-383.

[3] K.Khajehei, "Secure Communication in Cloud by Using ECC Algorithm", International Journal of Engineering Research and Technology, Vol. 3, No, 1, 2014.

[4] 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 information systems), to document conferences that are organized in co-operation with GI and to publish the annual GI Award dissertation, 2015.

[5] 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.

[6] 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.

[7] R. Gellman, "Fair information practices: A basic history", Available at SSRN 2415020, 2015.

[8] Ritu, Sukhchandan Randhawa, Sushma Jain,"Trust Models in Cloud Computing: A Review", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.4, pp.14-27, 2017.

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

[10] 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.

[11] 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.

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

[13] Pieczul, O. S., McGloin, M. A., Zurko, M. E., Kern, D. S., & Hepburn, B. A. U.S. Patent No. 9,699,168. Washington, DC: U.S. Patent and Trademark Office. 2017.

[14] D. Nuñez & I. Agudo & J. Lopez, "Privacy-Preserving Identity Management as a Service", Accountability and Security in the Cloud, 2015, p. 114-125.

[15] Wetter, A. E., Frei, A., Tsang, P. M., & Rouskov, Y. U.S. Patent No. 9,699,180. Washington, DC: U.S. Patent and Trademark Office. 2017.

[16] 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.

[17] 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.

[18] Naik, N., & Jenkins, P. Securing digital identities in the cloud by selecting an apposite Federated Identity Management from SAML, OAuth and OpenID Connect. In Research Challenges in Information Science (RCIS), 2017 11th International Conference on IEEE. May, 2017. p. 163-174.

[19] M. Jones & J. Bradley & N. Sakimura, "JSON web token (jwt)", No. RFC 7519. 2015.

[20] P Thanapal, K Marimuthu, S Rajkumar, R Niranchana," Smarter Way to Access Multiple Mobile Cloud Applications without Interoperability Issues", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.7, No.5, pp. 32-39, 2017.

[21] J. Li & J. Li & X. Chen & C. Jia & Wenjing Lou, "Identity-based encryption with outsourced revocation in cloud computing", Ieee Transactions on Computers, Vol. 64, No. 2, 2015, p. 425-437.
[22] Kim, S. M., Han, J., Ha, J., Kim, T., & Han, D. Enhancing Security and Privacy of Tor's Ecosystem by Using Trusted Execution Environments. In NSDI. March 2017. p. 145-161.
[23] Tania Gaur, Divya sharma,"A Secure and Efficient Client-Side Encryption Scheme in Cloud Computing", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.6, No.1, pp.23-33, 2016.
[24] 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.
[25] 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.
[26] W. A. Alrodhan & Chris J. Mitchell, "Enhancing user authentication in claim-based identity management", In CTS, 2010, p. 75-83.
[27] C. Yuan & L. Yang, "A survey of identity management technology", Information Theory and Information Security, 2010 IEEE international conference, 2010, p. 287-293.
[28] 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.
[29] A. M. Lonea & H. Tianfield & D. E. Popescu, "Identity management for cloud computing", New concepts and applications in soft computing, 2013, p. 175-199.
[30] X. Yang & L. Liu, "Principles, Methodologies, and Service-Oriented Approaches for Cloud Computing", IGI Global, 2013, p. 172-173.
[31] 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.
[32] 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.
[33] 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.
[34] 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.

Authors' Profiles

Kamyab khajehei received the Master degree in Computer Science in 2013 and Bachelor degree in Computer Engineering in 2001. Presently, he is teaching in Islamic Azad University, Dashtestan Branch. His main research interest includes Cloud Computing, Green Cloud and Fog Computing.

How to cite this paper: Kamyab Khajehei, " Preserving Privacy in Cloud Identity Management Systems Using DCM (Dual Certificate Management)", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.4, pp. 54-65, 2018.DOI: 10.5815/ijwmt.2018.04.04