ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Credential and Identity Access Management for Client Awareness in Mobile Cloud Computing Framework

[1]Silviya Nancy J, [2]D. Uma Nandhini, [2]D. Latha Tamilselvan

[1]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai - 602105, India*
[2]*Department of Information Technology, B.S.Abdur Rahman University, Chennai- 600048, India*

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Credentials Management, Identity and Access Management (IAM), Cloud Computing, Mobile Cloud Computing (MCC), Cloud Service Providers (CSPs), Cloud storage.

ABSTRACT

In the world of emerging technological revolution, Credentials and management of Identity (IAM) are the tasks that have become more crucial. With the advent of cloud computing, which is the currently been used as the reliable computing infrastructure, all the organizations and industries have leaped forward to provide the consumers and the clients with secure transactions and services. To govern and manage the security of an enterprise, the strategies of IAM set good opportunities with the assistance of credential management. This executive idea of user credentials also plays a vital role in Mobile Cloud Computing (MCC). The integration of Mobile and Cloud started with the proliferation of mobile devices' competence to handle resource intensive tasks. These complications moves the applications of mobile devices to cloud service providers (CSPs) for availing various services, "as-a-service". In spite of these up gradations, security for the users' personal data and credentials remains as a critical problem in cloud environment as well as in mobile cloud scenario. This mainstay of this research work is to mitigate the possible challenges and risks in IAM and credentials. This is to provide an adaptive security and identity confederation for the mobile cloud users by providing trusted model called Mobile Cloud Credential System (MCCS) with secured IAM and credentials ensured before accessing the service or applications from the cloud (storage).

To Cite This Article: Silviya Nancy J, D. Uma Nandhini, D. Latha Tamilselvan, Credential and Identity Access Management for Client Awareness in Mobile Cloud Computing Framework. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 624-630, 2015*

INTRODUCTION

The cloud computing has been advocated as powerful infrastructural tool for all the organizations and business concerns. The internet can otherwise be called as cloud, whose services are profoundly very popular in all the areas and aspects spread wide. It assures reliability by providing the users with the information whenever needed, which is been cached by the data center and can be retrieved by the client whenever necessary. Cloud Computing provides on-the-go service with on-demand payment for the usage. The remuneration of cloud computing is diverse, providing end-to-end services. This enables the clients to attain larger business agility. It has been initiated as a new swing in paradigm with the concepts and orientations of distributed computing. It guarantees boundless storage capability and computing strategies including wide network access with reliable services. Cloud being service-oriented architecture, it not only provides software, platform and infrastructure as-a-service, but also includes testing, learning, security, database and identity as-a-service and many more Umme Habiba (2014).

Cloud computing not only offers first-rate delivery and provisioning service to IT industries, but it also supports the new service runners of the business. The Figure 1 depicts and highlights the various service orientations of cloud. Cloud also employs certain complications in the view of security. Management of sensitive data on cloud is most critical concern. In addition to that, there is no secure provision provided for the credentials of users. There are also many challenges consisting of privacy demolishment, loss of integrity, transparency, etc.

Corresponding Author: Silviya Nancy, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Chennai, India.
Tel: +91 9487752343 E-mail: jsilviyanancy@gmail.com

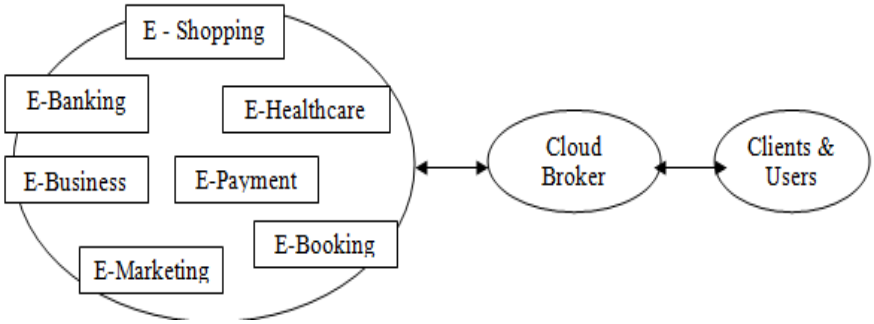

Fig. 1: Cloud computing services and infrastructure.

Mobile computing and communications has become that fastest growing phenomenon, where people not only use mobile devices for voice and message transactions, but also can be used for various wireless services Pankaja A.Hadole *et al*. (2014). The users employ the devices for different functions like capturing pictures and videos, accessing internet and many other complex applications like image editing and Photoshop, intensive document creation, etc. By the year 2000, the popularity of personal computers were reaching hype because of the reduced size and costs including internet flooding. As the years went by, the use of PCs were declined with the rise of smart phones which is portable with all required functionalities. To extend these mobile applicability and features, the cloud computing following the principle of services have embarked its new fame in mobile and smart device technology. This sudden outbreak is to support all the characteristics of smart mobile devices additionally with outstanding capabilities. With the gradual improvement, the battery size of the mobile devices is reduced to a minimum length and breadth due to which its competency outranges. Obviously, mobiles are restrained with storage and processing of intensive applications which cannot be processed effectively. The most prominent service offered by cloud to smart mobile technology is vast storage facility, where to a certain extent, the inefficiencies can be avoided. Mobile cloud computing (MCC) is the fastest and upcoming innovation with the incorporation of all the services of cloud.

With the evolution of smart devices in the world of mobile technology, it has taken over the rule of all the applications. Basically, 94% of the total population is using smart handheld devices for accessing the needs. This paved way for the marketers and developers to occupy the pace of generation with all types of amenities in the form of easily accessible applications. Its simplicity and the feature of portability have led to the rise in use of these devices, because it can be accessed anywhere and anytime seamlessly.

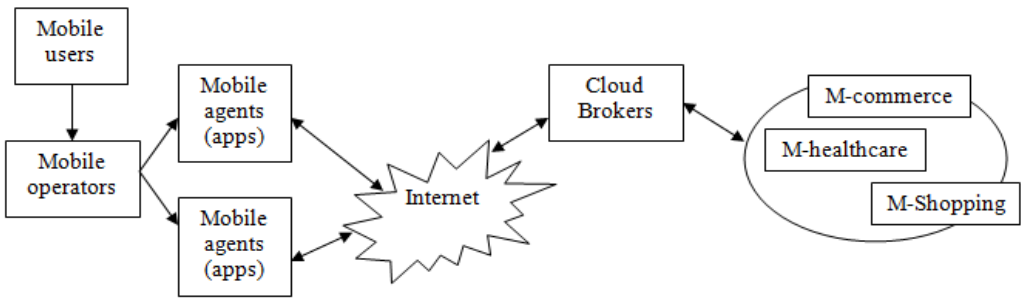

Fig. 2: Mobile cloud environment.

Appending to it, it also has wide broadband network availability which is very flexible to use all the services CAO Wanpeng and BI Wei (2014). The above figure 2, explains the working and flow of mobile cloud computing which defines the way in which the mobile users are linked to cloud through cloud brokers with the help of mobile agents (applications) and internet.

Issues in credential and identity management policies:

The backbone and basis for all the concerns is to manage the ability of controlling access rights and definitions to the users. There are varieties of trust systems and preventive technologies that are employed to protect the identity and access rights of the user. But the security for the credentials is not successfully achieved till today. To maintain the identity of an individual has become a tedious scenario in today's business world. Previously the

business organizations were trusted ones and it was an interoperated colleagues. But now, with the expansion of policies and levels all the organizations have started migrating towards the public sector for data and service maintenance.

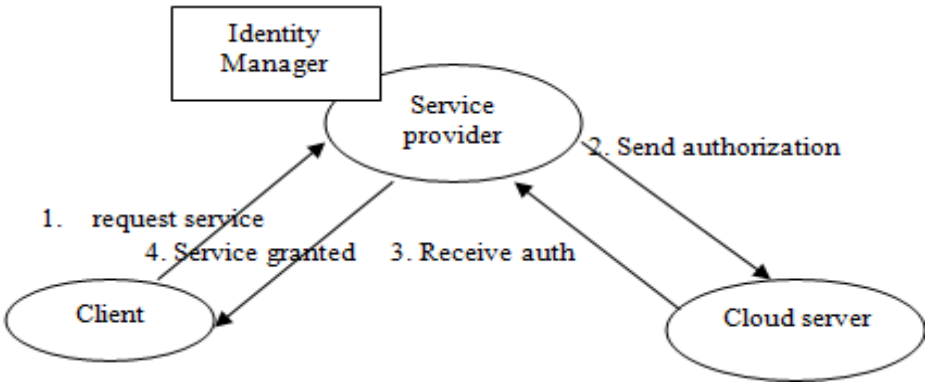

Fig. 3: Distinctive identity access management module.

In case of this distributed cloud environment, the collected data is scattered at different regions servers by the cloud service providers. There is no security and privacy for the users' data. Increasing theft and hacking have created chaos in stealing the identity entities of every individual user like username, password, security questions and other personal details. The figure 3 portrays the typical IAM module which is still being used even today. Here the service provider itself maintains the client details.

The following research presentation discusses about the related works, issues and risks in identity access management including need and scope for credential management policies, with the next section describes the strategies of credential management.

Literature review:

The related work focuses on different aspects of identity management and the pitfalls in variety of architectures and literatures. IAM is one of the most notable security issue in cloud computing. Each and every activity in the internet users interact with the service providers, in that case they would provide with digital identities for every access. The service providers (SP) would store and manage those credential details. Likewise, the SP would have lot of identities maintained for providing fast service to the customers. This is where the violation of privacy and stealing of data of occurs.

Identity access management:

Birrell and Fred B. Schneider (2013) claims that in last decade, the development of new policies for securing identity is increasing, at the same time the risk is also going high. Many other schemes came up with solutions like identity provider, certificate authenticator, maintaining authorization logs, etc. Here only the SPs will authenticate the consumers and there is no point to detect whether the credentials are been hacked or not and used by other illegal users. Some of the prevailing secure IAM methodologies are single sign-on, associate identity, and anonymous credential assessments.

Ardi BENUSI (2014) spoke about the secure transaction data from of cloud to cloud by preserving the identity management. It is proposed as there are some of the solutions provided to the identity management problems with the help of various dynamic security protocols like SAML and SICM.

Credential management:

Detlef H¨uhnlein (1998) proposes a simple credential management scheme for Simple Public Key Mechanism (SPKM). In case if the user ant to make use of more than one connection, there is a possibility of identity stealing is possible. To overcome the problem of identity misuse, Secure Single Sign Login (SSSL) was introduced with symmetric keys. In this junction, it is enough that if the user has logged in once with single password. There will not be a need for caching of secret passwords everytime.

ITU-T recommended X.509 were the certificates that were normally used. These certificates were used for authorizing the party in trusted way. It usually focuses on managing the identity and manages the credentials in a very secure way by explicitly informing the users with all the details such as revocation, management strategies, etc. It is mentioned with several common attributes. The real critic in this is user has to identify his own certificate and corrections.

Ninghui *et al* (2001), presents their views on trust management of the identity and credentials with a role-based trust language and set theory semantics. This work reveals the work on the fact that, when the user identities are stored in different credential cache or manager, the authors proposes a chain discovery algorithm for retrieving details from the credential manager with queries. In addition to that the authors also speak about the storage system which is also useful in efficiently searching for the identities.

Jatinder Singh *et al* (2008) focuses on the security credentials of health-care management data. The authors have presented the OASIS, a role based access model, which discloses the data in a very fine and secured manner. It also explains about the importance of health-care emergency and management and also enlightens about the privileges of the person's record. The Open Architecture for Secure Internetworking Services provides each and every roles with access based rules for storing and retrieving the data. A note on context- awareness and its security incorporating the access control policies.

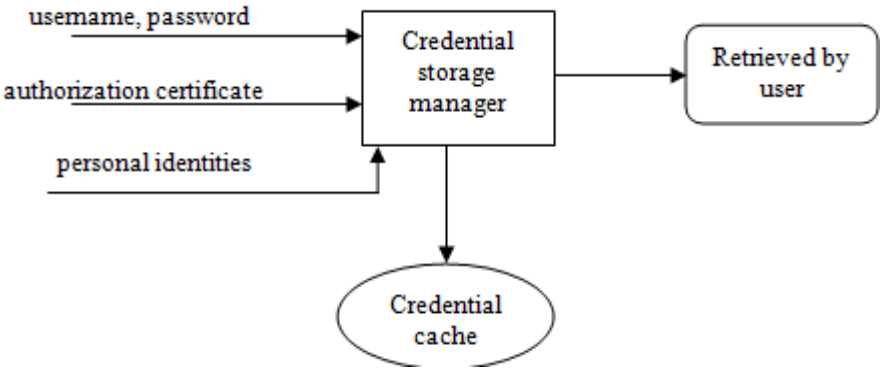

Fig. 4: Featured credential management system.

Mobile cloud environment:

In the research article of Pankaj S Kadam and Manoj V Bramhe (2015) the presenters draws about the various security issues and identity crisis in mobile cloud computing. It is portrayed that, when the users are accessing the cloud services with handheld devices, the login credentials as well as the data are not in secure safe. There is the possibility of unknown access during transaction or in the storage space itself. To mitigate these obstacles, the researchers' advice context aware security services like obtaining the actual user information for maintenance to prevent data loss.

Sheetal S *et al* (2014) discusses on dynamic storage of credentials. The article openly advocates on the transparent problems of mobile cloud users and safety issues of the digital and smart data. This paper also integrates a light weight algorithm for identities to secure efficiently.

Jana, D. Bandyopadhyay, D. (2013) triggers about various security parameters for mobile cloud users. The authors have interrogated about the robustness of security-as-a-service. Adding up to the above mentioned aspects, they have also entitled about different challenges and risks of IAM in mobile cloud environment and have made an analysis on security models.

Credential management system for mobile cloud platform:

Mobile cloud computing (MCC) means, processing of rich applications in cloud with mobile devices. The rise in this emerging technology is due to increase in smart phone users and quite a lot of people prefer using smart phones to computers, whereas the less resourced devices are not able to accommodate all the functional requirements of the user. To bridge this gap, cloud computing offered many services of processing intensive tasks from the mobile devices. It also provides storage and avoids battery wastage. Since, the MCC is in its infant stage, there is some notable security and privacy issues are addressed and faced by the community users. It is obviously known that there are many general security flaws, but this research paper mainly adheres to the security threats of user personal identities and the designing a proper credential management system for the mobile cloud environment community. Let us take for an instance, an example of uploading a document/video/image to the cloud storage through an application (mobile agent) in the following design phase.

System design proposal of Mobile Cloud Credential System (MCCS):

The design of the system is mainly for protecting the identities and the digital signatures of the mobile cloud users.

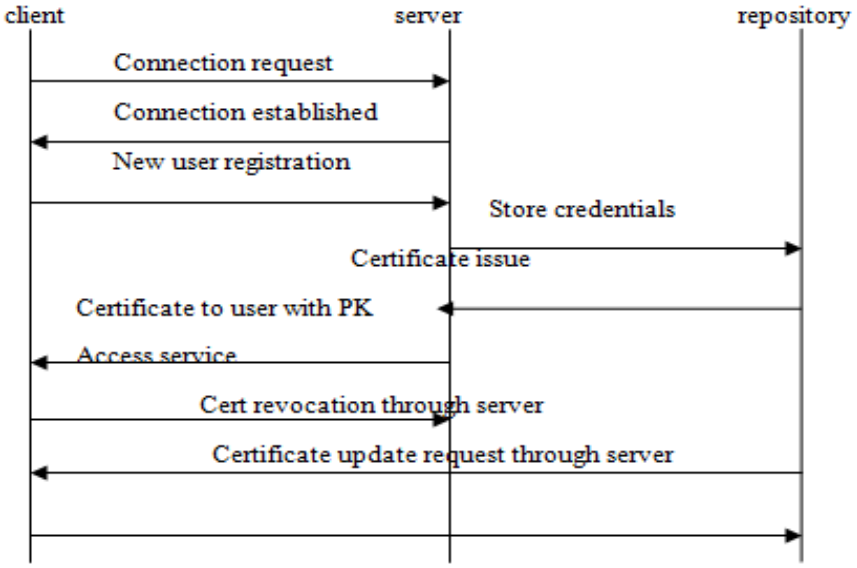

Fig. 5: Sequential workflow of Mobile Cloud Credential System (MCCS).

The credentials can be obtained in many types. One of its types is physical identity like passport, identity cards, and licenses, professional and other certificates. The other criterion is software credentials named as digital signatures.

MCCS is based on the model of client-server architecture. In this design the user (client) can save all the credentials in an online private storage backup and can retrieve it whenever necessary. MCCS uses a proxy certificate to store and revoke the identity credentials ranging different lifetimes.

This proposal is to mainly support the mobile cloud users. Due to the advancing characteristics of handheld devices and low cost cloud services, users tend to use mobile cloud services for better and easy handling of all the tasks.

The system design proceeds as follows,

Connection establishment and account registration:

The mobile client establishes the connection with the cloud server with the help of usual protocol TCP handshake. When the secure connection is established with the putty or SSH client, successful linkage is been made. Having linked with the server, the users can request for registering them as an authorized user. On initiation of this request the server would respond with mandatory personal credential attributes for getting the details of the user which is termed as account creation.

Translating into understandable credentials:

In the same as mentioned previously, *n* number of users can register for availing the service. To differentiate, store and to correctly identify the credentials a common interface is used. It can be defined in the form of user-defined extensible markup language (XML). The criterion is given below for instance with few attributes

Table 1: Credential storage.

<user> <username> uuuu </username> <password> **** </password> <name> abc </name> <age> 30 </age> <company> xyz</company> <gender> male </gender> <mobile no> +91 9999999999 </mobile no> <address> jjsfdsjskvndv </address> <payment mode> card </payment mode> <lifetime> 5 years </lifetime> </user>

Certificate issue by authority:

With the above mentioned attributes, the credentials are stored in the repository. The user will be offered with the certificate revocation and renewal status frequently to avoid unknown access and hackers.

Table 2: Certificate

New user Type of service: storage Status: active Date of creation: xx/yy/zz Identifier name: aaaa ------- ------- ------- History: --------- Validity period: xx/yy/zz

Policies for access control:

The server would enforce certain access control policies for using the account. Each and every time when the user login for the service, the details are retrieved from the repository by importing with the private keys provided for further access. The private key must be connected with SSH or putty for further access. With the aim of providing additional security, the registered user's mobile number and location aware status will be checked.

Uploading of files in the server:

Once the authentication is done, the user can upload the files in the server and retrieve it whenever necessary. The sample screen shots are shown below in the figure 6 and 7.

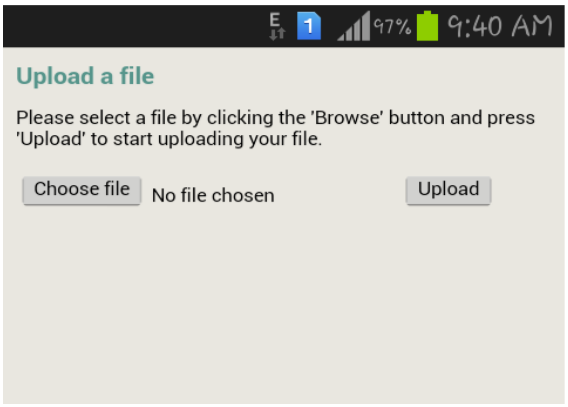

Fig. 6: Upload page.

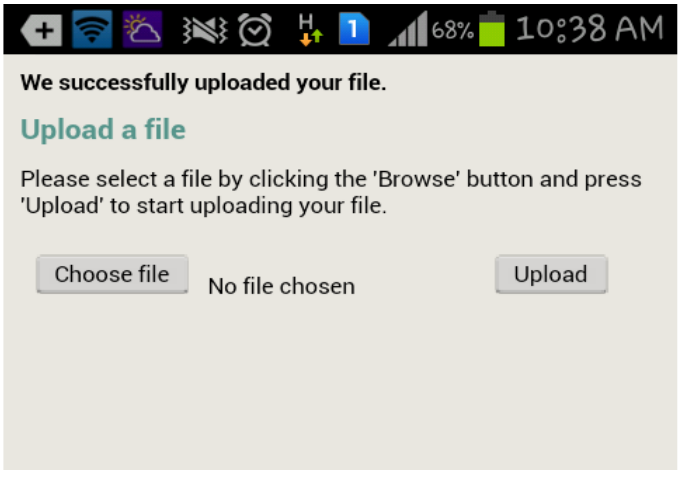

Fig. 7: Successful upload page.

Conclusion:

We proposed and presented a framework for Mobile Cloud Credential System (MCCS). This is chiefly for employing a secure transaction channel for the mobile users accessing the cloud services. This model also enlightens about the advantages and ease of using the mobile cloud environment for any complex services in a secured way.

REFERENCES

Ardi BENUSI, 2014. An Identity Management Survey on Cloud Computing, Int. Journal of Computing and Optimization, 1(2): 63–71.

Birrell and B. Fred Schneider, 2013. Federated Identity Management Systems: A Privacy-Based Characterization Eleanor, Copublished by the IEEE Computer and Reliability Societies, pp: 1540-7993.

CAO Wanpeng, BI Wei, 2014. Adaptive and Dynamic Mobile Phone Data Encryption Method, China communications.

Credentials Sheetal, S. Dharwadkar, M. Rashmi Jogdand, 2014. A User Identity Management Protocol Using Efficient Dynamic Credentials, International Journal of Scientific Engineering and Research (IJSER), ISSN (Online): 2347-3878, Volume 2 Issue 6.

Detlef H¨uhnlein, 1998. Credential Management and Secure Single Login for SPKM.

ITU-T recommendation X.509 | ISO/IEC 9594-8: "Information technology – open systems interconnection – the directory: public-key and attribute certificate frameworks".

Jana, D., D. Bandyopadhyay, 2013. Management of identity and credentials in mobile cloud environment, International Conference on Advanced Computer Science and Information Systems (ICACSIS).

Jatinder Singh David, M., Eyers Jean Bacon, 2008. Credential Management in Event-Driven Healthcare Systems, ACM.

Ninghui, Li., H. William Winsborough, C. John Mitchell, 2001. Distributed Credential Chain Discovery in Trust Management, An extended abstract of a preliminary version of this paper appeared in Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS-8), pp: 156–165, ACM Press.

Pankaj S Kadam, V. Manoj Bramhe, 2015. Survey on Secured Data Storage using Identity Management for Mobile Cloud Computing Environment, International Journal of Computer, Information Technology & Bioinformatics (IJCITB), ISSN: 2278-7593, Volume-2, Issue-3.

Pankaja Hadole, A., Jayant Rohankar, Priyanka Ambatkar, 2014. Development of Secure Mobile Cloud Computing Using Improved Identity Management Protocol, International Journal on recent and Innovation Trends in Computing and Communication, 3(3): 645–650.

Umme Habiba**,** Rahat Masood**,** Muhammad Awais Shibli and A. Muaz Niazi, 2014. Cloud identity management security issues & solutions: a taxonomy, Springer Complex Adaptive Systems Modeling.