Authentication Techniques in Cloud and Mobile Cloud Computing

Mahamudul Hasan[1], Md. Hasnat Riaz[1], Md. Auhidur Rahman[2]
[1]Department of Computer Science and Telecommunication Engineering
[2]Institute of Information Technology, Noakhali Science & Technology University, Bangladesh.

Abstract
A major challenge in cloud and mobile cloud computing is to ensure security and privacy of user's personal information (e.g., financial data, health record, location information) from malicious attacks. It is important for a cloud service provider (CSP) to establish trust and gain confidence by providing proper security and privacy to the clients. Authentication is important for establishing accountability and authorization of the users while allocating cloud resources. Researchers have proposed several techniques, such as token-based, image and biometric based, to make the authentication process more efficient, secure and user friendly. In this paper, we discuss different authentication techniques proposed for both cloud and mobile cloud computing environments. We categorize the algorithms based on its input, i.e. the credentials required for validating users. However, we emphasize that the classification is not precise, as it is difficult to classify the authentication algorithms relying on more than one user credentials (multi-factor authentication). To understand the complexity and delay of an authentication process, we focus on the number of entities involved in an authentication process and the number of handshakes taking place between them. We also compare the authentication algorithms on the basis of design principles and popular security attacks.

Index Terms
Could Computing, Mobile Cloud computing, Authentication, Confidentiality, Integrity.

1. Introduction

With the increasing number of cloud based applications, one of the major concerns of cloud computing (CC) and mobile cloud computing (MCC) is to provide data security to its users. It includes confidentiality, integrity, availability and accountability of the data [**1**]. Security is particularly important for applications transmitting personal information and performing financial transactions [**2**]. In MCC, as the data transactions between cloud and mobile devices are over unreliable wireless medium, the issue of data security becomes even more challenging. In this paper, we focus on one particular aspect of security dealing with the accountability on CC and MCC, which is obtained by authentication of the users.

Authentication is a process of verifying the identity of an individual or an object such as a mobile device. It requires the user or object to furnish its credentials which is compared with the ones already present in the database [**3**] [**4**]. This is important for providing security and privacy to the users [**5**], particularly for applications transmitting sensitive and personal data to the cloud. Some of the challenges of authentication include complexity in providing user credentials, number of handshakes required for verification and delay. In MCC, the task of authentication becomes more complex, as the communication between the cloud and mobile device takes place over various wireless networks (Wi-Fi, 3G, 4G). Authentication delay is important in MCC for the real time applications such as online movie watching, online game playing [**6**].

In this paper, we discussed the authentication techniques for both CC and MCC. Similar types of approaches also done by the researches to make a comprehensive study on authentication. But in most of the cases they have cover only either the authentication techniques in CC or MCC. Suppose in [**7**] authors presents a state-of-the-art of MCC authentication and in [**8**] authors reviewed some of the authentication method of CC only. In [**9**] authors only review a very few approaches based on biometric mechanisms for only the cloud computing and [**10**] explained the algorithm which is based on text and token, but they totally ignore the biometric approaches. To the best of our knowledge this paper in the first approach where we cover the authentication techniques for both the CC and MCC.

We classify these techniques according to the user inputs such as text-based [**11**] [**12**] [**13**] [**14**] [**15**] [**16**] [**17**] [**18**], device-based [**19**] [**20**] [**21**] [**22**] [**23**], image and biometric based [**24**] [**25**] [**26**] [**27**] [**28**], third party authentication [**5**], [**6**], [**29**], and hybrid authentication [**30**] [**31**] [**32**]. The choice of an authentication technique depends upon the level of security we need to enforce for a particular application. Moreover, we also need to consider the available resources for implementing such technique, as the resources of a mobile device, i.e., computational power, bandwidth, are not same compared to a desktop computer. Thus, in order to understand the complexity and delay required in an authentication process, we consider the entities involved in the authentication process, the user credentials required and the numbers of handshakes between the cloud and user devices. Some authentication process requires 4-way handshaking [**12**], [**15**], [**16**], [**19**],

Manuscript received November 5, 2017
Manuscript revised November 20, 2017

[**26**], [**31**], while others require 2-way handshaking [**12**] [**16**]. The trade-off is between the security and the complexity of these techniques.

Finally, to understand the effectiveness of the authentication techniques, we discuss their performance under different types of attacks, such as sniffer attack, DoS attack, dictionary attack. We also discuss the basic characteristics of the authentication techniques based on its functional entities.

Rest of the paper is organized as follows. In section-II & III, introduces the authentication model and discuss different authentication techniques based on user input and handshakes. In section -IV we present the attacks and design paradigms of authentication algorithms and finally we conclude our discussion in section-V.

2. Architecture of authentication in cc and mcc

Authentication is the process of determining the identity of a user, device or a server by verifying its credentials. It is essential for maintaining security of a system. After verification, a set of privileges can be granted to the valid users or services can be rejected for malicious entities. Authentication is a mandatory process and is usually the first step required for accessing a service, such as online financial transaction through debit/credit cards or for accessing email accounts, online purchases, online ticketing, online learning, online gaming. The protocols used for authentication are generally designed by considering the constraints and requirements of the system. For example, authentication protocol of a communication networks (like GSM, 3G), is different from that used for verifying email accounts. In CC and MCC, authentication plays a major role in providing security and establishing trust in the system. Due to unavailability of an authentication standard for CC and MCC, the responsibility of authentication relies on the CSP.

In a traditional authentication technique, users need to enter multiple keys for accessing a service from a system, e.g., username/password or PIN, which is verified by the system using its database. The process is repeated by the user for accessing a different service or when the session expires due to user mobility or network failure. Currently, most CSPs use traditional authentication for providing their services [**3**]. However, the authentication process incurs significant delay as the keys are entered manually (sometimes using mobile devices). Thus, the traditional authentication technique is not efficient for accessing on-demand services from multiple CSPs. This is more significant for MCC, as switching between various cloud-based services or changing network condition requires re-initiation the authentication process, incurring significant overhead on the mobile devices.

As the resources in a cloud environment are shared and accessed by several users in the network, it increases the system vulnerability to both internal and external attacks. Thus, new authentication model, such as biometric or device based authentication [**25**], [**27**], is required for providing better security to the users. Moreover, for the applications offloading computational or storage requirements to the cloud, seamless authentication model is required for accessing uninterrupted services from different CSPs. The authentication model of CC and MCC can be different, as the two platforms differ significantly in terms of technology. In MCC, for example, biometric information can be used for fast authentication; but in CC, same may be difficult due to the hardware limitations. In addition, the authentication model for MCC must be lightweight, considering the resource limitations of the mobile devices [**15**].

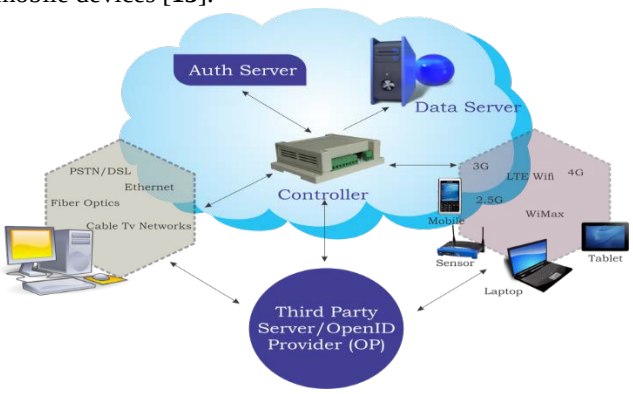


Figure 1: Architecture of CC and MCC

Figure-1 shows the general authentication architecture for CC and MCC. A request for authentication or for any service from a user is handled by a cloud entity, which we refer as cloud controller. A cloud controller provides an interface for the user for interaction with the cloud. On receiving an authentication request, the controller forwards it to an authentication server that stores the information of all users and their privileges in a database. The identity of the requester is verified by the authentication server and based on the result access to the cloud can be granted or denied. After successful authentication, the user can access the services of the cloud through the controller.

Another mode of authentication in CC and MCC is called the third party authentication, shown in the figure 1. Since a cloud user can access various on demand services form different CSPs using multiple devices and networks, an efficient authentication model is important for providing security and smooth services. To this end, researchers have proposed the third party authentication technique, in which the authentication requirements from different applications are handled by a third party server on users behalf. In a third party authentication, users send their

authentication request to the third party authentication server. The server then sends the required authentication information (e.g. username/password) to the cloud controller, which is verified by the authentication server in the cloud. Finally, the controller sends an accept or deny response back to the user via the third party server. The third party authentication technique is more effective for MCC applications, as it is improving the battery life time of the devices by reducing the computational and communication overheads [**5**], [**6**]. However, for successful implementation of this technique, the trustworthiness of the third party authenticator is essential for both the user and CSP.

The authentication techniques in CC can be classified based on the type of credentials that users enter for authentication with the system [**33**]. The credentials can be textual, graphical, bio-metric, device-based or a combination of all. The underlay complexity of the authentication algorithm depends primarily on the input from the theme of this paper and discusses various authentication techniques for CC and MCC. At the beginning we define some common terms of authentication and in table-I we define users and the level of security the system demands for its services. The essential features of an authentication
algorithm include simplicity of the process, security of the personal information passed through the network and the delay
in processing the authentication request. Another mode of classifying the authentication techniques is based on the number of messages exchanged between user and the cloud in the authentication process. It is also known as handshaking between the two entities. The parameter is important for understanding the architecture of an algorithm and is directly related with the communication delay.

In this section, we focus on the main the notations used in this paper. After that classify the authentication techniques based on user inputs and the number of handshakes.

3. Authentication in cc and mcc

A. Authentication Techniques in CC

1) **Text Based**: This is one of the popular authentication schemes for accessing traditional and cloud-based services. In this scheme, a user enters text information or keys through a keyboard for its identification. It can be a username and password shared between a client and server. The security of a username and password based authentication depends on the strength of password. For improving security, the password should be unpredictable, long combination of all characters and unique for each system. Although authentication using username and password can be used for a cloud environment. But as discussed above it is not efficient for accessing on-demand services, particularly through mobile devices. Moreover, in most cases, username and password can be compromised using modern attacks like dictionary, eavesdropping, man-in-the middle, replay attacks [**15**].

Researchers have proposed various modifications to overcome such limitations [**12**], [**13**], [**14**], [**16**], [**17**], as discussed below.

In authentication techniques the use of smart card is very familiar. In [**12**] authors proposed an authentication algorithm which is based on smart card. Mutual authentication has been provided in this authentication algorithm and 4-way handshaking is needed to complete the whole authentication process, which is shown in figure 2. Before sending the authentication request to the cloud, a local server checks the validity of the user by using its ID, PW and smart card information. If the user is valid an authentication request (M1) is sent to the cloud. After that cloud generates an OTP (K) and computes (M2) hash function using (M1, K) and send M2 to the user. The user verifies the authenticity of the cloud by computing hash function (B') on M2. On successful verification, it proceeds to the next phase to authenticate itself and send M3 containing hash value using ID, (B') and time stamp. In the last phase, cloud verifies the identity of the user and sends the message M4 to valid user containing a hash function of a session key (Sk). Finally user gets the conformation reply, which is verified by comparing the session key.

Table 1: Notations used in the paper

Notations	**Definition**
U_i	User U or U_i
AS	Trusted authentication Server
M_i	Message M or M_i
PW	Password
ID	User identity Information
TA	Trusted Authority
P	Private Key
Q	Public Key
H	Hash function
S_k	Session Key
N	Nonce
||	Concatenation Operation

For improving security, authors in [**16**] suggest authentication of both user and the device. User's authentication is performed by checking the username and password. For device authentication users need to install an application called client based user authentication (CBUA) to get the access code for the registered device. The paper also proposes two methods for accessing cloud services using unauthorized devices. (a) Personal phone/e-mail for retrieving the access code and (b) By comparing

the location of authorized and unauthorized devices. The proposed algorithm uses a 4-way handshaking for authenticating user and device (figure-2). The first two handshakes verifies the device and the last two is used for user verification.

2) Token Based: Electronic IDs (eID) are unique for every user and it can be used for unique identification and authentication. [**14**] describes a "secure identity across borders linked (STORK)" framework for secure cloud authentication using eIDs. The proposed framework is designed to authenticate users of eighteen European Union (EU) nations using their eIDs in a cost effective and secure manner. STORK is a SAML based protocol. It provides SSO between different clouds. Once a user is authenticated with a cloud provider via STORK, it needs not re-authenticate on other clouds for accessing services. STORK performs seamless authentication for the user on all collaborating cloud service providers. Chiang et. al [**17**] discuss a framework for accessing multiple cloud services using the idea of single sign-on (SSO) over a hybrid cloud platform. It is based on OpenID and O'Auth for authentication, authorization and file synchronization. The OpenID platform supports SSO and using O'Auth, a user can get access to a third party service, as discussed above. For designing a hybrid cloud environment, authors consider Google Apps and Hadoop as the public and private cloud, respectively.

[**11**] proposes an algorithm for sharing cloud storage space among multiple users. Two phase mutual authentication takes place between the users trying to access shared resource and also between the user and the cloud. In the proposed algorithm, users get their identity (i.e private or public key) from a trusted authentication component (TA) present in the cloud. The identity of a user acts as a token, while accessing the shared resource. For mutual authentication between two users, say U1 trying to access the storage space owned by U2, first U1 sends a request message to U2 containing various information, including a hash value computed on the public key of U2 and the private key of U1. U2 recalculates and compares the result with the received hash value to authenticate U1. Using same procedure, U1 also authenticates U2. A token is shared by U2 to grant permission to U1 to access the storage space. Another mutual authentication takes place between U1 and the TA. On completing the authentication processes, U1 can use the token to access the shared space.

3) Device Based: The device based approaches are primarily used for implicit authentication. In the following, we focus on the proposed algorithms that rely on device information for user identification [**20**], [**34**] [**35**], [**36**], [**37**], [**38**].

In [**38**], authors propose an authentication architecture by combining both explicit and implicit authentication factors to gain access to different cloud services. Explicit authentication can be performed using username-password, swiping card, SMS or by voice, depending on the sensitivity of the cloud service. For implicit authentication, the algorithm collects various information from the user mobile device, such as messaging behaviour, browsing history, call history, typing motion and typing patterns. The algorithm uses meta-learner, which is a machine learning engine, to assign relevant weights to the above factors by comparing with the training data set already present in the database. Finally, authentication score is computed as a weighted sum and compared with the sensitivity level of the service that a user wants to access. More authentications (either explicit or implicit) can be performed if current authentication score is less than that sensitivity of the service. The Proposed algorithm lessens the user's work burden of authentication by upto 29%.

Human behaviours are based on habits. For example, a person's route to office, the time spent in the office or his/her activities in the weekend [47]. Such human behaviours do not change very frequently and it can be used to uniquely identify a person. In [47], authors discuss an implicit authentication algorithm by collecting independent features from the user's mobile device, which includes the location information of the user, browsing history, phone calls, SMS. Then, the algorithm extract features from these data, performs clustering and finally generates an authentication score using machine learning algorithm, showing the probability that the device is with a legitimate user.

GPS (Global Positioning System) is being widely used in cloud computing environment to locate an authentic user. In GPS-Directed mobile cloud GPS applications are taking services from cloud at the back end. Authentication in GPSdirected mobile cloud has been firmly described in [24]. In GPS-directed mobile cloud seamless authentication have been done between the devices and cloud through wireless networks. In the proposed algorithm cloud provides the data which are needed for authentication and GPS provides the real geographic locations and timing of that data. In the proposed algorithm vertical-horizontal design have been used for authentication which is a cross layer design. Vulnerabilities and possible threats are well explained in the paper.

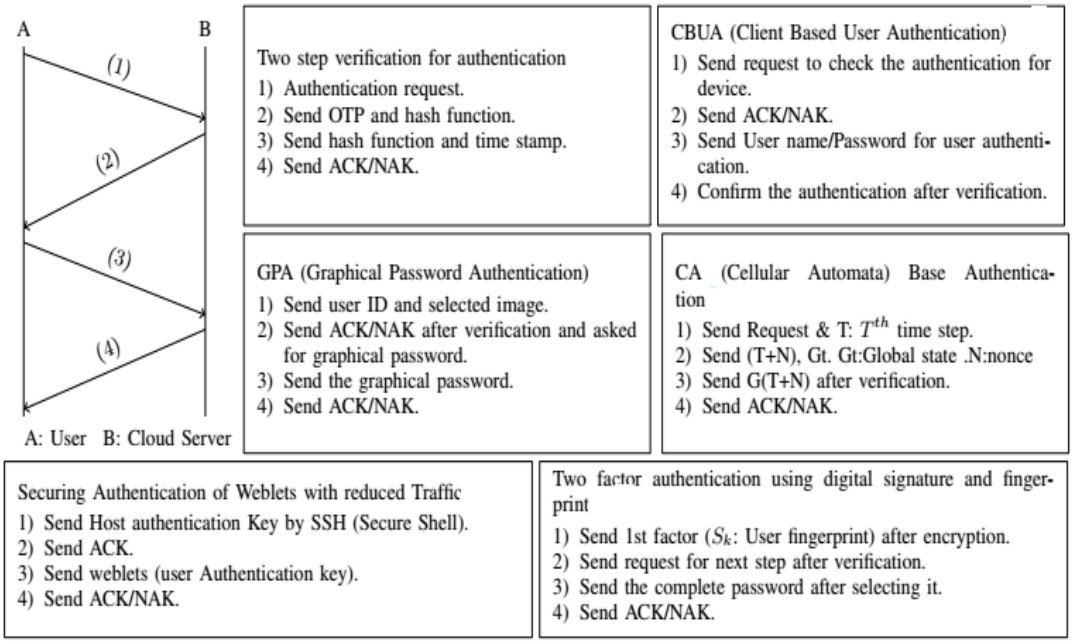


Figure 2: Authentication using 4-way handshake in CC

In [**20**] authors propose a secure cloud based RFID authentication algorithm for protecting the privacy of RFID tags and readers against untrusted database keeps in the cloud. The algorithm operates in two phases. In the registration phase, RFID reader writes its identifier R and initializes a session identifier S into the tag. Moreover, the reader saves an encrypted record H(R||T||S);E(R||T||S) in a database, where T is the tag identifier. In the authentication phase, first, the reader needs to retrieve T and S from the database. For this, the tag generates a hash function H(R||T||S) and sends it to the reader. The reader uses H(R||T||S) as index and reads the corresponding E(R||T||S) from the database, decrypts and obtains T and S. Subsequently, mutual authentication takes place between tag and the reader. To authenticate the tag, reader sends a pseudorandom number Nr as a challenge message. The tag sends back a hash function H(R||T||Nr) as a response, which is verified by the reader. Similarly, a challenge message is generated by the tag for authenticating the reader.

4) Image and Biometric Based: As mentioned before, traditional alphanumeric authentication system suffers from several limitations, including difficulty in remembering long string for password and typing password in a small mobile phone. As a result such techniques are vulnerable to many security threats, such as dictionary attack [**24**], surfing attack, spyware attack and social engineering attack [**26**]. To overcome these challenges, researchers have proposed graphical or image based password authentication as an alternative to the traditional approach. It is easy to remember pictures compare to a string of characters, such as people's face, places visited, animals or flowers. Moreover, graphical passwords can be easily selected or drawn on the touch screen of a mobile device. [**24**], [**26**], [**39**] are the recent works on image based authentication, as discussed below.

In [**24**] authors proposes a graphical password based authentication for the cloud computing environment. In the login phase, 4-way handshakes are needed between the client device and the cloud environment (figure-2). User first presented with a set of images from a library for selection. The selected image along with user ID is sent to the authentication server in the cloud for verification. On successful verification the user is asked to enter the graphical password, which is a path traced over the selected image. The graphical password is verified by the authentication server. The selected image and graphical password should match the information provided during the registration phase. On successful verification, user can access the cloud services. [**26**] discusses similar authentication technique using graphical password.

[**39**] presents an image based two factor authentication algorithm. The three main components for this algorithm are trusted third party (TTP), service provider (SP) and user. TTP generates shared key (sh) using edge detection on an image (img) and by reading the corresponding gray-scale pixel values. In the setting phase, the user applies MD5 hash function on its username and password and forwards the result to the TTP. The TPP, again forwards these information along with the img and sh to the cloud as a public key and also forwards a secret key to the user, consisting of sh, img and a product of two large prime

numbers. The authentication phase, requires 3-way handshake between the SP and user. To begin with, the user sends the first factor for authentication to the SP, containing a random number and hash values of username and password. On successful verification, the SP generates a random number by choosing pixel of the image pi 2 img at location (x,y). Then, SP sends pi and (x,y) to the user as a challenge message. The user verifies the pixel value pi at img(x,y). On success, the user generates the second factor by using edge detection on img and encrypting the result with key Ki = sh _ pi. Finally, the user sends the encrypted message (E') to SP. Then the SP computes the key in a similar way, performs encryption and compares the result with E' to authenticate the user.

Biometric information of a person, i.e. finger print, face recognition, iris, can be used for authentication. This is more secure, difficult to lose, faked or duplicated, and also it cannot
be pirated [**25**]. Although biometric sensors are not readily available in current mobile phones, but in future the scenario may change as the demand and necessity increase. None the less, the biometric authentication is gaining popularity, particularly for dealing with bank transactions [**40**]. Researcher are investigating options to integrate biometric authentication and cloud computing, to improve security for accessing cloud services [**27**], [**41**].

In [**27**] the authors proposed a cognitive authentication scheme called cloud cognitive authenticator (CCA) which uses cognitive biometrics as an authentication parameter. Cognitive biometrics have the capability of recording both the sentimental and cognitive status of an user. CCA is the combination of biometrics, advanced encryption standard (AES) and zero knowledge protocol (ZKP), providing rigid security with very less power and storage capacity. CCA operates in four steps. Firstly, it reads the electrodermal response (EDR) of the skin conductance of the user, which is checked to determine the mental state of the user. On successful verification, CCA proceeds to the second step, where an encrypted user-id is generated by merging the EDR reading, IP address, device details and current timestamp. Thirdly, the user-id is transmitted to the cloud for decryption. Finally, connection with the hypervisor is established by employing ZKP protocol.

5) Hybrid: A combination of two or more of the above approaches can be used for authentication. We classify them as hybrid authentication technique. These approaches fall under the realm of multi-factor authentications (MFA), such as combining text and biometric authentications [**31**] or by combining device information with biometrics [**16**]. MFA creates multiple layer of defence against malicious attacks. An unauthorized person must compromise or break all layers/factors to access a system. MFA provides more security and robustness to the authentication algorithms. Researchers have also designed and studied several hybrid authentication techniques for CC and MCC. Most of the algorithms discussed in the device-based section use MFA and belongs to this category [**20**], [**34**], [**42**]. However, we notice that device's information is not essential for designing a hybrid authentication algorithm. In this section, we discuss hybrid authentication algorithms that rely on multiple factors for user authentication [**16**], [**31**].

Yassin et.al. in [**31**] discussed a two factor authentication using username/password and fingerprint as biometric information of the users. Three components of this algorithm are user, data owner (DW) and the service provider (SP). In this, for the first factor (username and password) Schnorr digital signature is used so that DW cannot impersonate users to login. It also extracts three features form the user's fingerprint (pattern, points and shape) to enhance the security for user authentication. There are four phases of this algorithm. In the setup and registration phase, user sends its identity (fingerprint (Fpi), username Uni = H(Uni), password Pwi = H(Pwi)) to DW. Using this, DW generates public system parameters (PK) and a secret key (SK) and forwards to SP and user, respectively. User encrypts SK using private key, which is hash value computed on password and a shared key between user and SP, and stores it in a storage devices for future use. Encryption protects the secret key (SK), even if the storage device is lost. Information in SK is used in the login and authentication phase. A 4-way handshake takes place between user and SP in the login phase, as shown in figure-2.

In [**16**], authors propose an agent-based model 'access control and user authentication (ACUA)' using one client-based and four cloud-based agents. The client-based user authentication (CBUA) agent is an application installed in the user's registered device. ACUA sends an access code to CBUA and registers the device using its MAC ID. The login phase uses 4-way handshake between CBUA and ACUA, as shown in figure-2. CBUA initiates the process by sending a login request to the cloud user authentication (CUA) agent. CUA checks the access code and sends back a accept/reject message to CBUA. On receiving an accept message, CBUA sends user's login information (i.e., username and password) to CUA. Finally, CUA sends back the ACK/NACK to the CBUA for authentication. Moreover, in the proposed algorithm, authors investigate two tools for accessing cloud services though unregistered devices, namely user authorization code (UAC) and region detection. In UAC, the CUA agent generates and sends an authorization code though user's email, which is used during the authentication process. In the region detection mode, location of the user (i.e., registered device location) is compared with the location of the un-authorized devices, before accepting the authentication request.

B. Authentication in Mobile Cloud Computing

As discussed in section-II, authentication in MCC is different from CC. Communication in MCC occur over an insecure wireless network, which demands more security against malicious attacks. Other challenges in designing an authentication algorithm for MCC include mobility of the users, heterogeneity of the wireless networks and resource limitations of the mobile devices (processing speed, storage, energy and bandwidth). Thus, the authentication algorithm for MCC needs to be adaptive to various changes in the network and needs to be light-weight and energy-efficient. Moreover, the authentication process in MCC should reduce user interaction by using sensors, camera, microphone that are available in the mobile devices. Some research works on this topic [**42**], [**43**], [**44**], [**45**], [**46**], [**47**], [**48**], [**49**], [**50**], [**51**] are discussed below. We begin our discussion by introducing three frameworks [**5**], [**6**], [**29**], [**52**] for authenticating mobile users in MCC. These framework consider a separate entity for handling the authentication request on behalf of the user with an aim to reduce the authentication overhead of the MCC. Details of these algorithms are discussed below.

[**52**] propose an architecture for authentication and single sign-on (SSO) for an operator centric mobile cloud environment, where the mobile operator hosts a cloud environment for its users. In this framework, user concurrently gets authenticated with cloud at the time it connects with the serving mobile network. The proposed algorithm, EC-AKA3 (Ensured Confidentiality Authentication and Key Agreement Protocol), is designed on the basics of LTE AKA (Long Term Evolution) and is an extension of EC-AKA2 [**53**]. In EC-AKA3, the authentication is moved from the application layer to the LTE NAS (Non-Access Stratum) layer. Figure-3, shows the authentication procedure and the messages passed between different entities in EC-AKA3. First, the user equipment (UE), intending service from the service network's cloud (SNC), sends a NAS attach request to the service network's mobility management entity (MME) containing identity (IMSI number), that can only be verified by the home subscriber server (HSS). MME forwards the message to HSS along with the serving network's Id (SNID) and HSS responds to MME with a user's identity certificate. A mutual authentication takes place between MME and UE. On success, MME generate a proxy certificate for future use and acts as an identity provider (IdP) for SSO. MME uses the proxy certificate to authenticate UE, and after which the UE can access services from the cloud.

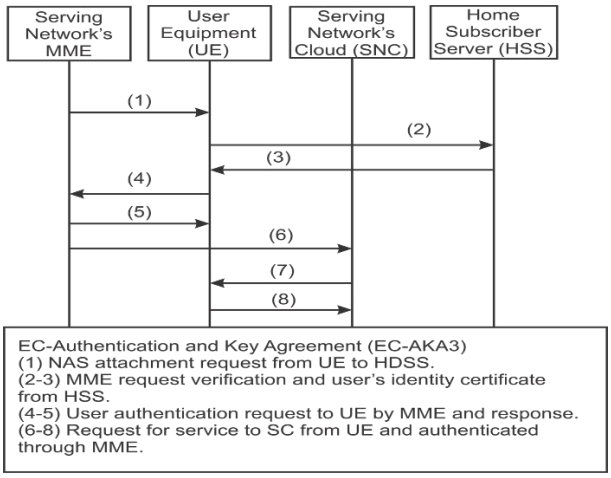
MiLAMob [**6**], is a SaaS authentication framework for handling authentication request on behalf of the mobile users in MCC. The framework can adopt any open standard authentication approach to identify the user, such as OAuth 2.0 used by social networking services (Facebook, Google+, and Twitter) and can use the access token to authenticate the user with an IaaS cloud provider (Amazon S3, Dropbox, MEGA). A key component of MiLAMob, see figure-3, is a middleware that connects mobile users, social networking clouds, and IaaS clouds. To access service from an IaaS cloud, a mobile user first sends a request to the MiLAMob middleware using its URL. The middleware, using OAuth 2.0 redirects the request to a social networking for authentication. If the authentication is successful, the middleware receives an access token (as discussed before). The middleware retrieves the user's IaaS security credentials from its repository and sends a login request to the IaaS cloud over HTTPS protocol. On success, the middleware retrieves and delivers the requested object to the user.

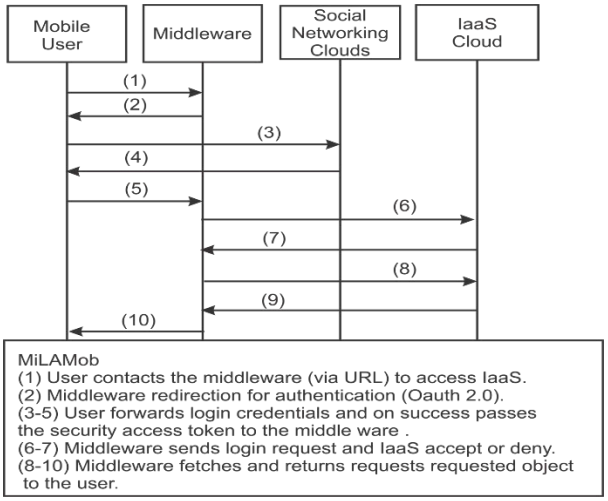
Implicit authentication can be used for validating mobile users in MCC. As mentioned above, advantage of implicit authentication is that it reduces user interaction and can be performed seamlessly in the background to improve QoS for the user. TrustCube or Trust3 [**29**], is a framework that uses implicit authentication to validate mobile users in MCC. It supports fine-grained and user-specific polices to make the authentication process flexible and secure. Four components of this framework are client device (CD), data aggregator (DA), authentication engine (AE) and authentication consumer (AC), and figure-3. An agent in a CD periodically sends user's behavioral information, such as phone calls, SMS, browsing history, location and network information to the DA. The AE generates an authentication score by collecting data from the DA or CD and comparing the recent and past behavioral pattern of the user. The AC (i.e. a web server) can set or modify policies by informing the AE. Before serving a client, as shown in figure-3, the AC authenticates the client through AE. The AE retrieves the policy, collects data from the CD and/or

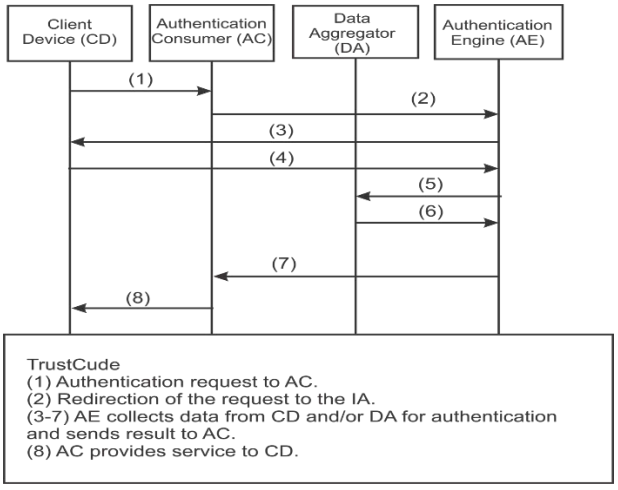
DA and generates an authentication score and sends the result back to the AC. If the authentication score is less than a threshold value, more authentications can be performed. On successful verification, the AC provides service to the CD.

As discussed earlier, zero knowledge proof (ZKP) is a technique that can be used to hide the identity of a prover and a verifier in an authentication process. SeDiCi 2.0 [**5**], is a ZKP based authentication protocol for MCC. It relies on a trusted third party (TTP) to provide mutual authentication between consumers and service providers without revealing their password. The authentication process of SeDiCi 2.0 is shown in figure-3. First, the client sends a request for a service (or a webpage), for which an authentication is needed. The service generates a unique number, i.e. Auth ID, for the current session and sends it to the client. For authentication, client sends the service's URI and Auth ID to the authentication service

(AS). The AS verifies the given URI and if successful, inserts the Auth ID in the URI and sends the authentication decision to the client. The client provides the login details (as URI) to the service and the service verifies the same from the AS. Finally, the service returns the authentication result to the client.







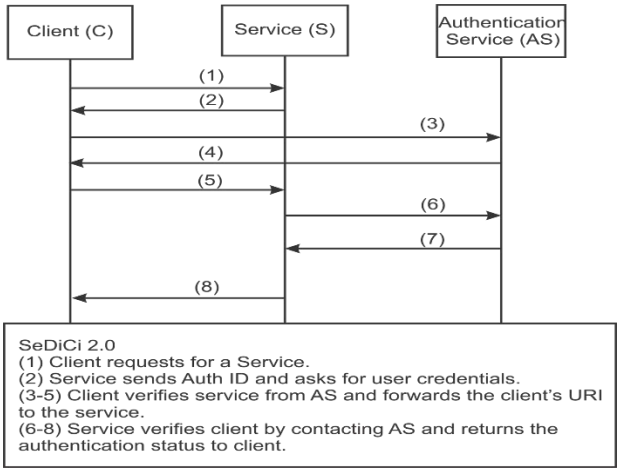


Figure.3: Authentication Handshakes in MCC.

Keystroke dynamics is another behavioural biometric information that can be used for user authentication [**54**] [**55**] [**56**] [**57**] [**58**]. This scheme analyze the pattern of users interaction with the keyboard by collecting various information for the device such as typing pressure, latency between two successive keystrokes, key holding time. As mobile devices are equipped with lot of sensors (like pressure sensors [**59**], accelerometer and gyroscope [**60**]), this authentication procedure is more applicable for mobile cloud computing environment. In [**58**] authors proposed an authentication algorithm based on the keystroke dynamics. The behavioural information used in this algorithm are the inter-key keystroke duration, key holding time and finger pressure. For experimental purpose, authors consider a notebook touch pad, which is similar to a mobile touch screen. Finally the collected data is analyzed using KNN classification algorithm. Based on which, authenticity of a user can be determined. [**54**] analyzes the keystroke sound measured through a microphone to apprehend user's behavioral information and uses it for authentication.

Authors in [**41**] propose a framework considering hand writing as a biometric information for authenticating users. In this, users enter their handwritten password on the touch screen of a smart phones which is analyzed on opensourse Apache Hadoop [**61**] cloud platform for authentication. Major steps in the algorithm include preprocessing, feature extraction and classification. In pre-processing, operations are performed on the raw image to enhance image rendering and to prepare it for segmentation. The next step extracts and analyzes two types of features of the input characters, using pixel density and segmentation, for training and verification purposes. Three techniques are used for classifying featured data, i.e. artificial neural network (ANN), K-nearest Neighbour(KNN) and euclidean distance. Parallel combination is used to combine the three classifying

techniques. After classification, final decision on the authenticity of the user is made based on a majority or weighted sum. In majority voting, each classifier's decision is treated as a vote and total numbers of vote is checked with a threshold value. For weighted voting each classifier is assigned with a weighted co-efficient according to its accuracy.

Table 2: Security Comparison table

	Text [12] [15]		Image [24] [27]		Device [30]	Hybrid [31]
Sniffer attack		✓	✓			✓
Impersonation attack	✓		✓		✓	✓
Replay attack	✓	✓	✓		✓	✓
DoS attack	✓		✓			
Modification attack	✓		✓		✓	
Man-in-the middle attack	✓		✓	✓	✓	✓
Forward & Backward attack		✓	✓			
Offline attack						
Dictionary attack					✓	✓
Insider attack	✓					
Phishing attack	✓			✓	✓	

Rassan et al. in [**49**], proposes an authentication algorithm for MCC using biometric information of the users. In the registration phase of this algorithm, user captures the fingertip (biometric) information using the camera of a mobile device and then send it to the cloud. In cloud, image processing techniques, such as preprocessing, core-point detection and feature extraction are used on the image and the features are stored in a database for future user verification. For login, user follows the same procedure to send the fingertip image to the cloud. The features are extracted in the cloud and is compared with the one stored in the database. If the two match successfully, the user is accepted or otherwise denied access to the cloud. A 2-way handshake takes place in this algorithm.

[**47**] considers the use of message digest for authentication in MCC. A message digest is a fixed size hash value returned by the corresponding hash function. Two message digests are used in [**47**] – MDuser digest for user's policy and MDcloud for the cloud policy information. In the registration phase, user sends a registration request to the cloud server by including userID, hash password and other information such as credit card, device information. On receiving the request, the cloud server computes two message digests; prepares a message containing MDuser, MDcloud, its public key PKpub cloud and a database pointer (CF). Finally, the cloud server encrypts the whole message using Tk = userID_hashfpasswordg, as the key and sends it to the user. In the login phase, mutual authentication takes place between cloud server and the user. First, the cloud authenticates the mobile and then the mobile authenticates cloud according to the data stored in the registration phase and finally they authenticate each other.

Table 3: Design principles of authentication algorithm

	[24]	[12]	[20]	[19]	[5]
No Secure Channel	✓			✓	
Mutual Authentication	✓		✓		✓
Message Encryption	✓				
Privacy	✓				
Message Integrity	✓		✓	✓	
Two-factor Authentication	✓	✓			✓
Secret Value Updating	✓				

4. Comparison tables

It is important to analyze the security threats or vulnerabilities of a system to counter all possible attacks. Hackers use different types of attacks to get unauthorized access to the system, steal user's identity for committing fraud. Attacks can be broadly classified in two different categories, namely structured and unstructured attacks. The structured attacks are performed by highly motivated and technically sound attackers, while unstructured attackers are individuals with little experience and use weak tools like password crackers to attack a system. The CC and MCC environment are also vulnerable to various external and internal attacks [**43**], [**62**]. The external attacks in CC and MCC, are carried out by outsiders having no access to the internal system, while the internal attacks are performed by authorized personal of the system.

Attacks can be passive (traffic analysis, data capturing) or active (forge log in, DOS, Message modification). Authentication algorithms should be capable of handling these all attacks.

There are many research works focusing on the security issues on cloud and mobile cloud computing [**62**], [**63**], [**64**]. In this section, we provide a comparative analysis of the authentication algorithms to understand their resistance against different malicious attacks, such as Man-in-the middle attack, DOS attack, Dictionary and phishing attacks, as shown in table-II. For this, we consider algorithms from each category, i.e., text based [**12**], [**15**], [**24**], image or biometric based [**19**], [**27**], device based [**30**] and hybrid [**31**] authentication techniques.

Common attacks on an authentication process are dictionary, man-in-the middle, impersonation and replay attack. As most traditional authentications are text based, attackers may try the dictionary attack by systematically trying all common passwords, like family name, birthday or child's name, etc. The success probability of a dictionary attack can be minimized by making the password unpredictable by using long combination of alpha-numeric and special characters (both in uppercase,

lowercase) and by using unique password for each system. In man-in-the middle attack, the attacker secretly listens to the conversation between two parties and tries to alter the messages exchanged between them. Most authentication algorithms discussed above handle this problem [**15**], [**19**], [**24**] by using the concept of out-of-band secure channel, hashing and by encrypting/decrypting messages. Impersonation and replay attack can be resisted by using random values or OTP as second factor authentication. In some cases IMEI number of devices is used as it cannot be altered by a third party.

In table-III, we show the design principles of different authentication algorithms. The design of an authentication algorithm depends on various factors, including security demands of applications, communication media through which user credentials are transmitted and the type of user credentials needed for authentication. A secure channel and message encryption techniques [**24**] are generally used to meet the demands of sensitive applications, like banking and commerce. Message integrity is an important design consideration [**19**], [**20**], [**24**], which can be maintained by using various cryptographic technique, such as Hashing. Mutual authentication [**5**], [**20**], [**24**] and multi-factor authentication [**5**], [**12**] are also considered to furnish a rigid and secure system for the users.

5. Conclusion

In this paper, we investigate the proposed and widely used authentication techniques for cloud and mobile cloud computing. We classify the authentication algorithms according to the user credentials as text-based, token-based, image and biometric based device-based and hybrid-based approaches. The text-based authentication is the most popular technique for verifying user's identity and it relies on user credentials, like username/password or OTP. The image or biometric based algorithms use fingerprint, eris, ECG, EED or blood pressure for user identification. The device-based techniques mainly perform implicit authentication by collecting behavioral information from the users mobile device, such as messaging behavior, browsing history, call history, typing motion and typing patterns. To understand the complexity and delay of the algorithms, we consider the number of entities, the user credentials required and the numbers of handshakes involved in an authentication process. Finally, we analyze the performance of the authentication algorithms under different attacks and provide their comparative functional analysis.

References

[1] Zhifeng Xiao and Yang Xiao, "Security and privacy in cloud computing," Communications Surveys \& Tutorials, IEEE, vol. 15, no. 2, pp. 843-859, 2013.

[2] M. Alizadeh and W.H. Hassan, "Challenges and opportunities of Mobile Cloud Computing," in Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, 2013, pp. 660-666.

[3] M. Sarvabhatla and C.S. Vorugunti, "A robust mutual authentication scheme for data security in cloud architecture," in Communication Systems and Networks (COMSNETS), 2015 7th International Conference on, Jan 2015, pp. 1-6.

[4] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384-394, Feb 2014.

[5] S. Grzonkowski, P.M. Corcoran, and T. Coughlin, "Security analysis of authentication protocols for next-generation mobile and CE cloud services," in Consumer Electronics - Berlin (ICCE-Berlin), 2011 IEEE International Conference on, 2011, pp. 83-87.

[6] R.K. Lomotey and R. Deters, "SaaS Authentication Middleware for Mobile Consumers of IaaS Cloud," in Services (SERVICES), 2013 IEEE Ninth World Congress on, 2013, pp. 448-455.

[7] Mojtaba Alizadeh, Saeid Abolfazli, Mazdak Zamani, Sabariah Baharun, and Kouichi Sakurai, "Authentication in Mobile Cloud Computing," J. Netw. Comput. Appl., vol. 61, no. C, pp. 59-80, #feb# 2016. [Online]. http://dx.doi.org/10.1016/j.jnca.2015.10.005

[8] Mahnoush Babaeizadeh, Majid Bakhtiari, and Alwuhayd Muteb Mohammed, "Authentication methods in cloud computing: A survey," Research Journal of Applied Sciences, Engineering and Technology, vol. 9, no. 8, pp. 655-664, 2015.

[9] P Padma and S Srinivasan, "A survey on biometric based authentication in cloud computing," in Inventive Computation Technologies (ICICT), International Conference on, vol. 1, 2016, pp. 1-5.

[10] G Reshmi and CS Rakshmy, "A survey of authentication methods in mobile cloud computing," in Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for, 2015, pp. 58-63.

[11] Lishan Kang and Xuejie Zhang, "Identity-Based Authentication in Cloud Storage Sharing," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, Nov 2010, pp. 851-855.

[12] A.J. Choudhury, P. Kumar, M. Sain, Hyotaek Lim, and Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in Services Computing Conference (APSCC), 2011 IEEE Asia-Pacific, 2011, pp. 110-115.

[13] R.H. Khan, J. Ylitalo, and A.S. Ahmed, "OpenID authentication as a service in OpenStack," in Information Assurance and Security (IAS), 2011 7th International Conference on, 2011, pp. 372-377.

[14] B. Zwattendorfer and A. Tauber, "Secure cloud authentication using eIDs," in Cloud Computing and Intelligent Systems (CCIS), 2012 IEEE 2nd International Conference on, vol. 01, 2012, pp. 397-401.

[15] Sang-Ho Shin, Dong-Hyun Kim, and Kee-Young Yoo, "A lightweight multi-user authentication scheme based on cellular automata in cloud environment," in Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on, 2012, pp. 176-178.

[16] Mostafa Hajivali, Faraz Fatemi Moghaddam, Maen T. Alrashdan, and Abdualeem Z.M. Alothmani, "Applying an agent-based user authentication and access control model for cloud servers," in ICT Convergence (ICTC), 2013 International Conference on, 2013, pp. 807-812.

[17] J.K. Chiang, E.H.-W. Yen, and Yen-Hua Chen, "Authentication, Authorization and File Synchronization in Hybrid Cloud: On Case of Google Docs, Hadoop and Linux Local Hosts," in Biometrics and Security Technologies (ISBAST), 2013 International Symposium on, 2013, pp. 116-123.

[18] J. Bong, Y. Suh, and Y. Shin, "Fast user authentication method considering mobility in multi clouds," in 2016 International Conference on Information Networking (ICOIN), Jan 2016, pp. 445-448.

[19] J. Panneerselvam, S. Sotiriadis, N. Bessis, and N. Antonopoulos, "Securing Authentication and Trusted Migration of Weblets in the Cloud with Reduced Traffic," in Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on, 2012, pp. 316-319.

[20] Wei Xie, Lei Xie, Chen Zhang, Quan Zhang, and Chaojing Tang, "Cloud-based RFID authentication," in RFID (RFID), 2013 IEEE International Conference on, 2013, pp. 168-175.

[21] D. Umanandhini, L. TamilSelvan, S. Udhayakumar, and T. Vijayasingam, "Dynamic authentication for consumer supplies in mobile cloud environment," in Computing Communication Networking Technologies (ICCCNT), 2012 Third International Conference on, 2012, pp. 1-6.

[22] Yu-Jia Chen and Li-Chun Wang, "A security framework of group location-based mobile applications in cloud computing," in Parallel Processing Workshops (ICPPW), 2011 40th International Conference on, 2011, pp. 184-190.

[23] A. Ahmed-Nacer and M. A. N. Samovar, "Strong authentication for mobile cloud computing," in 2016 13th International Conference on New Technologies for Distributed Systems (NOTERE), July 2016, pp. 1-6.

[24] Ming-Huang Guo, Horng-Twu Liaw, Li-Lin Hsiao, Chih-Yuan Huang, and Chih-Ta Yen, "Authentication using graphical password in cloud," in Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on, 2012, pp. 177-181.

[25] Kao Zhao, Hai Jin, Deqing Zou, Gang Chen, and Weiqi Dai, "Feasibility of Deploying Biometric Encryption in Mobile Cloud Computing," in ChinaGrid Annual Conference (ChinaGrid), 2013 8th, 2013, pp. 28-33.

[26] S.M. Gurav, L.S. Gawade, P.K. Rane, and N.R. Khochare, "Graphical Password Authentication: Cloud Securing Scheme," in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on, Jan 2014, pp. 479-483.

[27] L.B. Jivanadham, A.K.M.M. Islam, Y. Katayama, S. Komaki, and S. Baharun, "Cloud Cognitive Authenticator (CCA): A public cloud computing authentication mechanism," in Informatics, Electronics Vision (ICIEV), 2013 International Conference on, May 2013, pp. 1-6.

[28] A. Mansour, M. Sadik, E. Sabir, and M. Azmi, "A context-aware Multimodal Biometric Authentication for cloud-empowered systems," in 2016 International Conference on Wireless Networks and Mobile Communications (WINCOM), Oct 2016, pp. 278-285.

[29] Richard Chow et al., "Authentication in the clouds: a framework and its application to mobile users," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop, 2010, pp. 1-6.

[30] R.K. Banyal, P. Jain, and V.K. Jain, "Multi-factor Authentication Framework for Cloud Computing," in Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, 2013, pp. 105-110.

[31] A.A. Yassin, Hai Jin, A. Ibrahim, and Deqing Zou, "Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing," in Cloud and Green Computing (CGC), 2012 Second International Conference on, 2012, pp. 282-289.

[32] H.A. Dinesha and V.K. Agrawal, "Multi-level authentication technique for accessing cloud services," in Computing, Communication and Applications (ICCCA), 2012 International Conference on, 2012, pp. 1-4.

[33] Mojtaba Alizadeh, Wan Haslina Hassan, and Touraj Khodadadi, "Feasibility of Implementing Multi-factor Authentication Schemes in Mobile Cloud Computing," in Intelligent Systems, Modelling and Simulation (ISMS), 2014 5th International Conference on, Jan 2014, pp. 615-618.

[34] F. Fatemi Moghaddam, N. Khanezaei, S. Manavi, M. Eslami, and A. Samar, "UAA: User authentication agent for managing user identities in cloud computing environments," in Control and System Graduate Research Colloquium (ICSGRC), 2014 IEEE 5th, Aug 2014, pp. 208-212.

[35] J.A Larcom and Hong Liu, "Authentication in GPS-directed mobile clouds," in Globecom Workshops (GC Wkshps), 2013 IEEE, Dec 2013, pp. 470-475.

[36] Elaine Shi, Yuan Niu, Markus Jakobsson, and Richard Chow, "Implicit authentication through learning user behavior," in Information Security.: Springer, 2011, pp. 99-113.

[37] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow, "Implicit authentication for mobile devices," in Proceedings of the 4th USENIX conference on Hot topics in security, 2009, pp. 9-9.

[38] Reza Fathi, Mohsen Amini Salehi, and Ernst L Leiss, "User-Friendly and Secure Architecture (UFSA) for Authentication of Cloud Services," in Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on, 2015, pp. 516-523.

[39] A.A. Yassin, A.A. Hussain, and K.A.-A. Mutlaq, "Cloud authentication based on encryption of digital image using edge detection," in Artificial Intelligence and Signal Processing (AISP), 2015 International Symposium on, March 2015, pp. 1-6.

[40] Ann Cavoukian, Alex Stoianov, and Fred Carter, "Keynote Paper: Biometric Encryption: Technology for Strong Authentication, Security and Privacy," in Policies and Research in Identity Management.: Springer, 2008, pp. 57-77.

[41] F. Omri, S. Foufou, R. Hamila, and M. Jarraya, "Cloud-based mobile system for biometrics authentication," in ITS Telecommunications (ITST), 2013 13th International Conference on, Nov 2013, pp. 325-330.

[42] J.A. Larcom and Hong Liu, "Authentication in GPS-directed mobile clouds," in Globecom Workshops (GC Wkshps), 2013 IEEE, Dec 2013, pp. 470-475.
[43] Hoang T Dinh, Chonho Lee, Dusit Niyato, and Ping Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," Wireless Communications and Mobile Computing, 2011.
[44] M Reza Rahimi, Jian Ren, Chi Harold Liu, Athanasios V Vasilakos, and Nalini Venkatasubramanian, "Mobile cloud computing: A survey, state of art and future directions," Mobile Networks and Applications, vol. 19, no. 2, pp. 133-143, 2014.
[45] Hongbin Liang, Dijiang Huang, L.X. Cai, Xuemin Shen, and Daiyuan Peng, "Resource allocation for security services in mobile cloud computing," in Computer Communications Workshops (INFOCOM WKSHPS), 2011 IEEE Conference on, 2011, pp. 191-195.
[46] Tien-Ho Chen, Hsiu lien Yeh, and Wei-Kuan Shih, "An Advanced ECC Dynamic ID-Based Remote Mutual Authentication Scheme for Cloud Computing," in Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on, June 2011, pp. 155-159.
[47] S. Dey, S. Sampalli, and Qiang Ye, "Message digest as authentication entity for mobile cloud computing," in Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International, Dec 2013, pp. 1-6.
[48] D. Jana and D. Bandyopadhyay, "Management of identity and credentials in mobile cloud environment," in Advanced Computer Science and Information Systems (ICACSIS), 2013 International Conference on, Sept 2013, pp. 113-118.
[49] I Al Rassan and H. AlShaher, "Securing Mobile Cloud Computing Using Biometric Authentication (SMCBA)," in Computational Science and Computational Intelligence (CSCI), 2014 International Conference on, vol. 1, March 2014, pp. 157-161.
[50] D. He, N. Kumar, M. K. Khan, L. Wang, and J. Shen, "Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services," IEEE Systems Journal, vol. PP, no. 99, pp. 1-11, 2016.
[51] Jia-Lun Tsai and Nai-Wei Lo, "A privacy-aware authentication scheme for distributed mobile cloud computing services," IEEE systems journal, vol. 9, no. 3, pp. 805-815, 2015.
[52] J.B. Abdo, J. Demerjian, H. Chaouchi, K. Barbar, and G. Pujolle, "Single-Sign-On in operator centric mobile cloud architecture," in Mediterranean Electrotechnical Conference (MELECON), 2014 17th IEEE, April 2014, pp. 151-155.
[53] J. B. Abdo, J. Demerjian, H. Chaouchi, and G. Pujolle, "EC-AKA2 a revolutionary AKA protocol," in Computer Applications Technology (ICCAT), 2013 International Conference on, Jan 2013, pp. 1-6.
[54] J. Roth, Xiaoming Liu, A. Ross, and D. Metaxas, "Biometric authentication via keystroke sound," in Biometrics (ICB), 2013 International Conference on, June 2013, pp. 1-8.
[55] M.B. Bondada and S.M.S. Bhanu, "Analyzing User Behavior Using Keystroke Dynamics to Protect Cloud from Malicious Insiders," in Cloud Computing in Emerging Markets (CCEM), 2014 IEEE International Conference on, Oct 2014, pp. 1-8.
[56] D. Stefan and Danfeng Yao, "Keystroke-dynamics authentication against synthetic forgeries," in Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010 6th International Conference on, Oct 2010, pp. 1-8.
[57] Cheng-Jung Tsai et al., "Work in progress: A new approach of changeable password for keystroke dynamics authentication system on smart phones," in Communications and Networking in China (CHINACOM), 2014 9th International Conference on, Aug 2014, pp. 353-356.
[58] H. Saevanee and P. Bhatarakosol, "User Authentication Using Combination of Behavioral Biometrics over the Touchpad Acting Like Touch Screen of Mobile Device," in Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on, Dec 2008, pp. 82-86.
[59] Hidetoshi Nonaka and Masahito Kurihara, "Sensing Pressure for Authentication System Using Keystroke Dynamics.," in International Conference on Computational Intelligence, 2004, pp. 19-22.
[60] Cristiano Giuffrida, Kamil Majdanik, Mauro Conti, and Herbert Bos, "I sensed it was you: authenticating mobile users with sensor-enhanced keystroke dynamics," in Detection of Intrusions and Malware, and Vulnerability Assessment.: Springer, 2014, pp. 92-111.
[61] Apache Hadoop, , Accessed on 2016.
[62] S Subashini and V Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.
[63] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, and Aoying Zhou, "Security and privacy in cloud computing: A survey," in Semantics Knowledge and Grid (SKG), 2010 Sixth International Conference on, 2010, pp. 105-112.
[64] Chunming Rong, Son T Nguyen, and Martin Gilje Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers \& Electrical Engineering, vol. 39, no. 1, pp. 47-54, 2013.