

Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments

J.K. Mohsin
School of Computing, Mathematics &
Digital Technology
Manchester Metropolitan University
Manchester
UK
jawad.k.mohsin@stu.mmu.ac.uk

Liangxiu Han, Mohammad
Hammoudeh and Rob Hegarty
School of Computing, Mathematics &
Digital Technology
Manchester Metropolitan University,
Manchester,
UK

ABSTRACT

Mobile devices offer a convenient way of accessing our digital lives and many of those devices hold sensitive data that needs protecting. Mobile and wireless communications networks, combined with cloud computing as Mobile Cloud Computing (MCC), have emerged as a new way to provide a rich computational environment for mobile users, and business opportunities for cloud providers and network operators. It is the convenience of the cloud service and the ability to sync across multiple platforms/devices that has become the attraction to cloud computing. However, privacy, security and trust issues may still be a barrier that impedes the adoption of MCC by some undecided potential users. Those users still need to be convinced of the security of mobile devices, wireless networks and cloud computing. This paper is the result of a comprehensive review of one typical secure measure-authentication methodology research, spanning a period of five years from 2012 - 2017. MCC capabilities for sharing distributed resources is discussed. Authentication in MCC is divided in to two categories and the advantages of one category over its counterpart are presented, in the process of attempting to identify the most secure authentication scheme.

CCS CONCEPTS

• Security and privacy → Multi-factor authentication • Security and privacy → Mobile and wireless security

KEYWORDS

Authentication; Mobile Cloud Computing; SSO; Two Factor; Multi-factor; Security; Wireless; Networks; Man-in-the-middle Attack; Sniffing; Biometrics.

1 INTRODUCTION

Mobile Cloud Computing (MCC) refers to the combination of three main technologies including mobile devices, wireless

networks and cloud computing. The main purpose of MCC is to augment the capability, capacity and battery time of the mobile devices and enable the transfer of intensive computations and data storage in the 'cloud infrastructure'.

Mobile devices are sophisticated multi-purpose devices that represent part of a large wireless ecosystem. These devices have a massive amount of on board resources [1-3]. They have powerful processors, large amounts of memory, an ever-increasing number of sensors, some with advanced imaging components, and high-resolution displays. Current mobile devices are flexible, customisable, programmable, and highly sophisticated wireless multi-purpose - multi-function devices. Yet, the complexity of today's mobile applications and the massive amount of generated data makes some of the most powerful mobile devices still incapable of delivering many applications to mobile users. In 2013 it was reported that the vast majority of mobile devices did not have adequate communication security [4]. Furthermore, mobile devices are at risk of theft, or data leakage via installed mobile applications.

The cloud is a dynamic, flexible and configurable, self-service, on-demand, pool of shared network resources, which can be commissioned with minimal effort [5]. It is a convenient and cost effective model for many private and corporate users. The lack of on-board resources on mobile devices can be complemented with the on-demand commissioned resources of the cloud. However, there are many drawbacks to cloud computing, such as data dispersal, loss of direct control over data infrastructure, data ownership issues, the potential for increased attacks from hackers, and insider threats from cloud providers.

As well as improving efficiency and reliability of the network, with the advent of broadband services there has been a rapid development in wireless networking technologies. Communication development in the last few decades has seen a rapid increase, spanning many technological generations, namely 1G, 2G, 3G and 4G. Today, 3G is the widely accepted mobile technology, although 4G is being deployed very rapidly across the world to take over as the mainstream technology for mobile communication; 5G is currently in the developmental stage but is expected to be introduced by 2020.

Alongside this rapid development in wireless networking technologies, there has also been a rapid increase in the number of mobile devices in use. These factors combined play a

significant part in threats which target both mobile devices and wireless networks. Such threats include viruses, worms, Trojans, and rootkit to name just a few [6-8].

MCC offers many opportunities and possible gains by the exploitation of remote resources to improve efficiency and performance, as well as enhancing link and network performance, such as the security of data, data throughput, and reliability. MCC can also have a positive impact on the energy consumption of devices involved in the process. An important aspect of MCC is the sharing of distributed resources across the cloud, the enhancement of processing capabilities, access to storage and security enhancement software such as antivirus software. For mobile users, the advent of MCC brings the ability to use the power of the cloud to compensate for any shortfall in the computing and storage powers of their mobile devices.

This paper introduces three constituent component technologies of MCC namely, the cloud, the mobile devices, and the wireless telecommunication and networking standards. It also explores authentication problems for MCC, digesting and analysing a number of authentication research proposals ranging from 2012 to 2017, according to several authentication factors. The analysis categorises the surveyed research papers in to Two Factor Authentication and Multi-Factor Authentication.

The remainder of this paper is organised as follows: Section 2 gives background knowledge. Section 3 describes and compares the strengths and weaknesses of each reviewed authentication method. This is followed in Section 4 by a reasoning of the benefits of two factor authentication over multi-factor authentication techniques, basing arguments on many factors such as efficiency, usability, and other factors, which will also be discussed in more detail. Section 5 concludes the paper.

2 BACKGROUND

The following subsections present a discussion of some of the security vulnerabilities of mobile devices and wireless network technologies and cloud computing, as well as an outline of challenges that researchers in authentication should be aware of. The concept of authentication is also introduced.

2.1 Security Challenges in Mobile Devices

Smart mobile devices are different from standard PCs in that these devices integrate a variety of technologies, which gives the user the ability to access the internet from anywhere, and at any time. This feature requires complex software and varying operating systems, an infrastructure that makes these devices vulnerable as they are therefore more attractive than 'normal' PCs to being attacked. Furthermore, smartphones are limited in

resources compared to PCs, which limits the sophistication and range of security measures available to them.

Mobile devices do have limitations, such as limited battery life when compared to PC's, and in those cases, security measures that can be implemented on the smartphone will be power sensitive. Where there is a limitation in computational power, therefore, sophisticated security algorithms, including authentication, should be carried out within the cloud [9].

2.2 Security Challenges in Mobile Networks

Compared to wired devices, which are static in nature, mobile devices roam between multiple heterogeneous networks, IP networks and cellular networks. These networks employ a variety of technologies, to varying degrees of security standard, and they use a variety of authentication protocols. This heterogeneity may lead to connectivity delays or signal loss.

A wireless medium is by nature prone to many threats such as eavesdropping, unauthorised access and jamming and, due to the number of built in sensors in the mobile device, sensitive personal data such as username and password, mobile identification, or other personal data can be compromised. Additionally, there are many types of break-in attacks that can exploit vulnerabilities in installed applications, or the operating systems, on the mobile device. Any attack on the cellular network can compromise the integrity of sensitive user information; attacks, such as IMSI catchers that feign man-in-the-middle attacks, can target user sensitive information, thereby breaching confidentiality through unauthorised access. Confidentiality and integrity of communication therefore, should not be taken for granted in any application relating to mobile communication. Figure 1 outlines various security services that may run on different layers to provide a more secure MCC environment for the smartphone.

2.3 Security Challenges in the Cloud

In the cloud, factors that can pose serious vulnerabilities include virtualisation, vulnerability succession and service hindrance. These relate to the sharing of resources, data flows using terminals, and other difficulties that may be experienced when applying updates or security fixes, due to the distributed processing of large amounts of data.

Different measures can be implemented to improve the security of the services offered in the cloud and these are summarised in Table 1. However, when implementing any of these measures, consideration would need to be given to the ability of these systems to ensure security of authentication and access control.

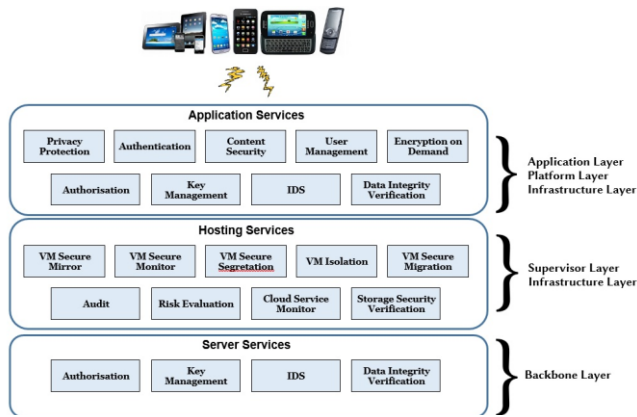


Figure 1: Multi-layered security services

2.4 Authentication

Access to sensitive information by anyone, from anywhere, means that user authorisation and authentication are critical factors to maintain the security of information. Any solution that is to be implemented, to address any of the security challenges identified above, will need to ensure that a suitable method of authentication forms an integral part of that solution.

Authentication, the main focus of this paper, is the process that confirms the identity of a user. Firstly, it identifies who the user is, and secondly it seeks to verify that the user is who she/he claims to be. A unified and strong form of authentication mechanism is required to reduce security risks.

Authentication, authorisation, and confidentiality are the three key elements that should be present in any strong security policy.

Table 1: Measures to improve security of services in MCC

Security service	Consideration
Data backup	Effective backup, verification processes, policies and procedures are needed.
Encryption	Secure and effective key management and distribution policy is needed to control the generation of encryption keys, specific to an organisation or country.
Communication network	Prevent wiretapping, encryption needs to be employed; Protect from repudiation, any transmitted or received data must be prepared; Check identity and authenticate users' needs to be employed; Protect against interlocking in a heterogeneous network; Protect against service refusal attacks; Protect the system from network hindrance.
System software	Protect the integrity of data and the installed software; Software updates to protect against any bugs or vulnerability in the software; Maintain operating systems and virtual systems vaccinations; Maintain software proficiency by applying service patches.
System virtualisation	Control virtual machine resources; Apply and maintain service patches to prevent malignant code from becoming a problem; Define clear boundaries between the host operating system and the virtual machine; Maintain log and image histories of virtual instances.
Data centre, disaster recovery policies	Policies to cover for all eventualities and risks, such as floods, fires and earthquakes.
Access management and authentication - Wireless access	Encrypt communication sessions; Control mobile terminal authentication and log session management.
Access management and authentication - Login sessions	Implement mechanisms to verify user identity; Minimise user authority.
Access management and authentication - Account	Implement an organisation policy with restrictions on number of attempts in case of login failure

Authentication represents a fundamental security building block, and forms an integral part of the access control of a security policy. It holds the user accountable for his/her actions when accessing resources, while still maintaining the integrity and authenticity of data during the communication process.

Research work on the subject of authentication falls in to two main categories depending on how the authentication process is performed. This could be either on the mobile device or on the internet/network side. The two categories are:

2.4.1 *Two factor authentication* - a verification technique using two means of identification chosen from two categories

of credentials. They are based on something that the user knows (knowledge factor) and either something the user has (possession factor), or something the user is (inherence factor).

2.4.2 *Multi-factor authentication* - a verification technique using more than two categories of credentials. The additional security increases the difficulty an intruder faces to access system resources. It incorporates one or more of the following authentication methods to identify the identity of the user during the login process:

1. Knowledge based identification: this is based on something the user knows such as, username/password, or personal identification number (PIN)
2. Possession based identification: this is based on something the user has such as a hardware or software token, user ID card, International Mobile Terminal number (IMEI), and the International Mobile Station Identification number (IMSI)
3. Tertiary identification: this is based on the user's physical features, i.e. biometric identifiers, such as face, palm, finger or voice recognition

3 A REVIEW OF AUTHENTICATION TECHNIQUES IN THE LITERATURE

Industrial and research communities are actively seeking to address the security challenges in the field of MCC. In the following subsections, authentication research is analysed according to the following criteria:

1. Computing intensity on the mobile side
2. Techniques having unpredictable values
3. Techniques having a frequent change of values
4. Authentication data not stored in devices
5. Technique is strong and able to withstand attacks
6. Mutual authentication between communicating parties is present
7. Technique is immune to external factors such as a lost/stolen mobile

3.1 Two Factor Authentication Methods

This subsection reviews recent and prominent two factor authentication techniques.

In 2012 a two factor authentication system was proposed that used hand writing recognition techniques to provide authentication [10]. The system comprised pre-processing, an extraction of features to provide authentication. It used three classifiers: Euclidean distance classifier, Artificial Neural Network (ANN) and K-Nearest Neighbour (KNN) to improve accuracy on hand writing recognition and error rate processes. In this system, a web interface was deployed on the mobile device which captured the user's ID and handwritten password. The encrypted credentials were then transmitted over the public network. A centralised authentication server contained a database of user sample signatures and the user was either accepted or rejected according to whether there was a match between the handwritten password, provided by the user during the login process, and the user's signature from the database.

A major advantage of this system was that the login process was simplified by using a handwriting imaging process. Furthermore, the processing of the image was performed on the cloud to reduce the time needed for the authentication, which in turn enhanced the efficiency of the authentication process. However, there were serious security concerns with this method. A web interface was used to log in to the cloud. Web applications tended to cache user authentication information and measures to eliminate this security risk were not addressed. Conventional encryption methods could not protect the data [11]. This was because the process of comparing the captured biometric image with the stored image was not performed in an encrypted environment, which meant that the images were exposed and no protection was applied during the authentication process. Therefore, a biometric specific defence needed to be implemented. No mutual authentication was present either between the mobile device and the authenticating server, which would have protected from many different attacks such as masquerading attacks and man-in-the-middle attacks. Also, measures to protect against mobile loss were not addressed.

A palm recognition biometric system, which ran completely on the mobile device, was introduced in 2014 [12]. This is demonstrated in Figure 2.

This system used an Orthogonal Line Features (OLOF) extraction method to provide a template for the biometric recognition. It provided good tolerance to illumination variations, and template shift to improve on misalignment captured by the mobile device. This model divided the processing of the authentication between the mobile device and the authenticating server.

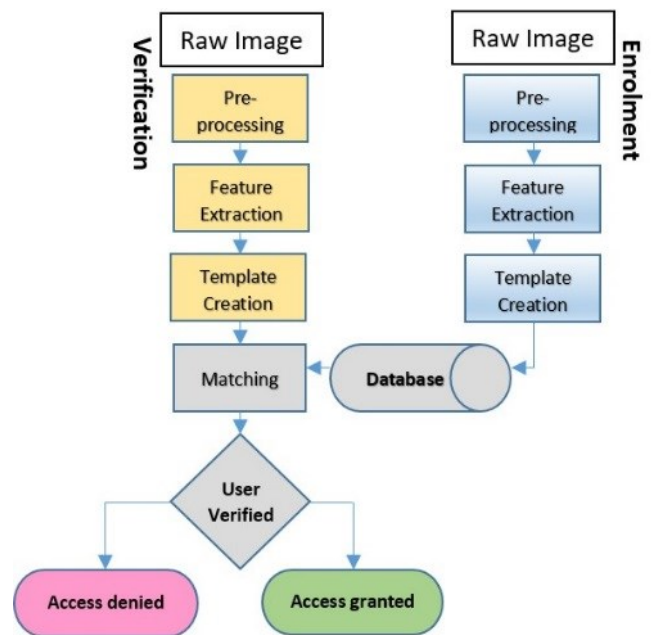


Figure 2: System architecture, adopted from [12]

With the image captured on the mobile device, the authentication server would conduct the processing of the image, and compare the information obtained to that stored on its database to authenticate the user.

A significant advantage of this system was the use of palm recognition biometrics with information that was unique to the user, while a serious effort was made to reduce reading error rates. However, there were also disadvantages associated with this method. Although the processing was divided between the mobile device and the cloud server, the capturing of the image, the correction of alignment functions, and the collection of data in display image and transmission, were all carried out by the mobile device. This energy intensive processing introduced time delay in handover of the image to the cloud server, which in turn lead to a delay in authentication.

In addition, we know that an increase in processing leads to more power consumption and less battery life. Therefore, along with bandwidth limitations, these factors could also have been the cause of delays. Furthermore, the speed of data transmission between the mobile device and the base station may not always be constant, and therefore the image data may be disrupted or become unavailable if the mobile user moves to a signal blind zone.

This method did not address a proper mechanism for protecting the biometric data from exposure during the authentication process. In addition, it was not clear whether the biometric image was deleted from the mobile device once the authentication had been performed. It was vitally important that a low-level deletion of these data were performed. As an alternative, the biometric data could be loaded only on the RAM and deleted from RAM once the authentication had been performed. That way, if the mobile was lost or stolen, there would be no trace of the data. None of these issues were addressed. Finally, this method could have been made more secure by implementing encryption, and the addition of mutual authentication between the communicating parties, to improve the method's ability to withstand external attacks. No defence mechanism was offered to eliminate the threats imposed in the event of loss of mobile device.

A two factor authentication scheme using an encrypted password and mobile phone token stored on the mobile device was introduced in 2015 [13]. In this scheme, an identity provider (IdP) undertook the tasks of registering, storing and managing the user identity information and issuing the user with a token to access the services of the Cloud Service Provider (CSP). The IdP would execute the proposed two factor protocol using Secure Assertion Markup Language (SAML) to provide a Single Sign On (SSO) concept. A user agent, a web browser application installed on the user's mobile device, regulated the user access. This scheme did not require a password table to be maintained by the authentication server. A 'three-phase' authentication scheme was utilised: a registration, a login and authentication, and a password change phase.

The scheme further proposed that a PAAS (Password as a Service) provided by the CSP should consist of three Virtual

Machines (VMs), two to provide the functionality of the SP and a third to provide the IdP functions.

This scheme was a positive attempt to address SSO issues. Although the SSO had many security concerns, it was very popular with both mobile users and service providers. Furthermore, it provided mutual authentication between the IdP and the mobile user, which added further security to the authentication process. The authentication process did not require any computation on the smartphone side, therefore saving on power consumption. It used tokens to authenticate the user, adding security to the process. It also provided a detailed design architecture covering the implementation of the scheme on the cloud side. In addition, it encrypted the user credentials prior to transmission which further added to the security of the scheme. However, the scheme proposed that the encrypted password and token be stored on the mobile and used a web browser application to provide an interface to manage the login process. The combination of the above two elements represented a heightened security risk. A mobile device could be lost or stolen and, in the wrong hands, the system could be compromised using the user credentials stored on the device.

A message digest authentication scheme (MDA) [14] used the hardware of the mobile device to protect against any threats or attacks. To measure the number of possible attempts to infiltrate the system, a system vulnerability score threat, s_y , was calculated by dividing the number of successful attacks by the total number of attempts made on the system, where $0.0 \leq s_y \leq 1.0$.

There were two stages in this scheme. In the first stage was a mutual authentication process between the user and the cloud provider. Figure 3 shows the second stage of authentication, where two message digests, MD_{cloud} and MD_{user} , were used to create MD. To protect the authentication process during the login stage, the user-generated password was 'hashed' and a process of XOR applied on both the user name and password. A random number was generated and an authentication key used to encrypt the Message Digest MD by hashing MD_{cloud} and MD_{user} .

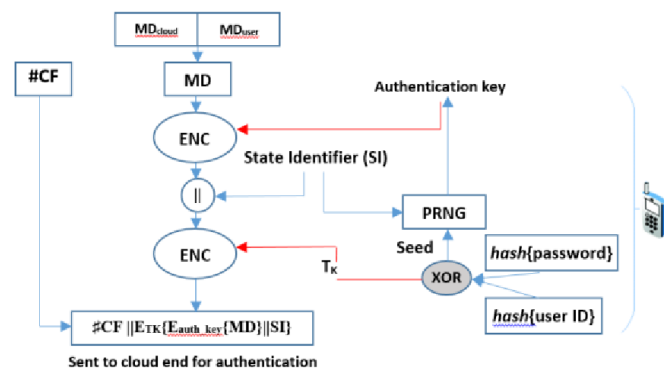


Figure 3: Message digest authentication scheme, adopted from [14]

$CF \parallel E_{TK}\{E_{auth_key}\{MD\}\parallel SI\}$ was sent by the mobile to the SP.

CF was a column reference, which was sent in text format with the encrypted message, and E_{auth_key} was the n^{th} sequence of bits. The E_{TK} represented the resultant of the XOR process of the password and the username during the first stage.

After user authentication, a mutual authentication process was initiated by the cloud server, communicating its own encrypted digital signature to the mobile device. The digital signature comprised an MD, which was encrypted using the server private key PK_{priv_cloud} . The mobile decrypted the received MD with the cloud public key. If the newly decrypted MD matched with the MD stored in its database, then successful authentication was granted on both sides.

Despite its complexity, this method was a good example of a privacy oriented authentication scheme. Serious effort was taken to improve the method's ability to withstand security attacks, by addressing mutual authentication between the mobile user and the cloud server, and also the security of transmitted authentication data. However, the method used was still complex and required a lot of processing. Any error in the received data, or break in transmission, would result in restarting the process, adding to the length of the overall process and resulting in further user frustration. This method required that the authentication data processing be partially carried out by the smartphone, which lead to increased power consumption, and therefore a significant reduction in battery life. In 2013 many smart devices did not have enough CPU and memory capabilities to carry out this level of processing. In addition, there were no countermeasures to deal with the threat from mobile device loss.

Fuzzy vault authentication was proposed in 2013 [15], based on digital signatures and zero knowledge (FDZ). In this method, the authentication between the server and the mobile user was achieved using RSA. A fuzzy picture password method was used to authenticate the user. Once authentication of all parties was completed successfully, a secure communication encrypted channel was set up between the mobile user and the cloud server. This protocol involved six steps: 1) a Diffi-Hellman public value was created by the server and communicated to the client; 2) The mobile client processed the received Diffi-Hellman public value and a session key; 3) The mobile client signed and encrypted those values, and transmitted them to the server; 4) The server then calculated the session key and verified the mobile client signature; 5) The server applied its digital signature, encrypted the Diffi-Hellman public value, and resent it to the mobile client; 6) The mobile finally verified the server's digital signature.

This method provided better security by using the Diffi-Hellman discrete function, and by protecting the keys using an RSA digital signature. This provided resistance to man-in-the-middle and impersonation attacks. Both the client and the server made use of the digital signature. Furthermore, this method provided defence against reply attacks, as the Diffi-Hellman key exchanges were randomly generated during the setup of the secure channels between the mobile client and the server. Additionally, it was resistant to sniffing attacks due to

encryption of data before transmission between the mobile user and the server. Finally, the use of Advanced Encryption Standard (AES) protected against brute force attacks.

However, no defence was put forward to protect from Record Multiplicity attacks, which targeted fuzzy vault. The heavy processing on the mobile client side required intense use of resources and invariably resulted in higher power consumption and lower battery life. In addition, there was no attempt to delete the fuzzy image data from the mobile device, which could then be exposed, exported, or copied in the case of device loss.

3.2 Multi-factor Authentication Methods

For organisations such as banks, in need of greater security in their day-to-day operations, multi-factor authentication has for many years been the preferred method for authentication. The industry is now actively encouraging research activities to improve the efficiency and security of the multi-factor authentication process. Examples of research undertaken to date are presented in the following subsection.

One proposal in 2015 was for a five factor authentication scheme [16]. Factors used were: 1) User name/password; 2) Voice recognition; 3) Face recognition; 4) Mobile identity number (IMEI); 5) International Mobile Subscriber Identity (IMSI). The components of the proposed system included the mobile devices, the cloud host, the management server and the storage. One assumption was that Transport Layer Security protocol (TLS/SSL) was used to communicate between the wireless network access point and the authenticating server. To improve efficiency and speed of the authentication process it attempted to gather all those processes together to be performed simultaneously on the cloud, rather than processing them individually as separate processes. To improve security and efficiency of the authentication process, the authentication factors were processed in VMs in the cloud. Additionally, IMEI and IMSI were used to protect against the loss of mobile devices. However, there was no attempt to delete the biometric data from the mobile device, which could potentially be exported or copied by an attacker.

There were many positive efforts towards a secure authentication process presented in this approach. It enforced a number of measures to ensure the authenticity of the user. It grouped the authentication processes to be performed simultaneously by the authentication server, improving the speed and efficiency of the process. At the same time, it saved the precious resources of the mobile device and reduced power consumption. It used the VM's resources to improve security and efficiency and finally, it protected the integrity of the system by providing measures in case of loss of the device by using the IMEI and IMSI. It did however, use a complicated and long authentication process, although this could have been considered to be a price worth paying for peace of mind.

A multi-factor, multi-phase, authentication scheme that used the One Time Password (OTP) authentication method was proposed in 2013 [17]. This was aimed at large companies such as Google. In this scheme, users were required to go through a

registration phase, whereby the user registered their credentials including user name/password, a 4-6 digit Personal Identification Number (PIN), an ID card and email address, mobile number and IMEI. The login process was a multi-phase process, whereby the user had to first log in using their user name and password. The next phase of authentication then ensured non-repudiation, as the user was required to input a PIN number, mobile number and IMEI. This process ensured that the mobile device was in the hands of the right user. The user was then given the choice to receive an encrypted OTP by SMS or email. At this stage, the user was directed to another screen where she/he would be required to input the OTP received.

This system ensured that only authorised users could access the system and it detected when to block lost or stolen mobiles by using the mobile number and IMEI. One of the advantages of this method was that the user was not permitted to have multiple accounts with the same mobile number as it allowed only one user per mobile number. This improved user account management control and reduced errors created in the user's accounts database. Non-repudiation was mitigated by enforcing a policy that an OTP was sent only when the user had re-confirmed his/her information, which had been supplied during registration. In addition, it confirmed that the authorised person was in possession of the registered mobile device. However, this system added complexity and time overheads. Furthermore, there was no security for the transmission of user information, i.e., no mutual authentication between the server and client was included in the proposed scheme.

A Multi-Factor Architecture Service (MFAS) was proposed for the banking industry in 2015 [18]. This process combined the use of biometric technology on the mobile device with the transaction authorisation process of an ATM (Automated Teller Machine) terminal. The mobile device was used to interface with the ATM terminal. The authentication process spanned three phases. The first phase was the registration phase, where the user registered his/her mobile device directly with the bank; a biometric processing tool would be installed by the bank on the user's mobile device and this tool was then used to capture face and finger biometric images through the registered mobile device. The registration data was stored in a database located in the bank. The second phase combined the existing authentication protocol for the ATM with an added security layer, in which the user provided his/her biometric image using the pre-installed biometric capturing tool installed on the user's mobile. Once the verification process was complete, the user was either accepted or rejected depending on the success or failure of the verification process. The third phase was the transaction authentication protocol. Once authentication had been completed successfully, the user would then be able to conduct his/her business securely. All data transmitted between the customer and the ATM terminal was encrypted.

This method was designed for the banking system, where security of the authentication process was paramount. It required the user to protect their mobile with a strong password, to prevent any unauthorised access, and any related data stored on the mobile device was hashed to protect it from migration or

from being exported by an intruder. This method used fuzzy vault to protect the biometric data. It used the RAM to temporarily load the biometric image when authenticating, and deleted the data soon after, thereby leaving no trace of the biometric image. It also tied the mobile IMEI and IMSI to the biometric image ensuring the coupling of the two for added security. This method was resistant to many attacks, such as Record Multiplicity Attack, which targeted fuzzy vault. It did not require mutual authentication as the protocol was only used when accessing the ATM terminal. Although it was feasible for an attacker in the vicinity to masquerade as the ATM terminal, there were enough security measures to counteract this threat. The only negative aspect of this method was that it required intensive computation on the mobile device to process the face and fingerprint images.

A multi-stage authentication system was proposed in 2016 [19]. User credentials were pre-registered and a procedure followed to collect a set of specific graphical images that would be used in future authentications. An Android-based mobile application was installed on the mobile device and used to coordinate the login process. On authentication, the user would run the installed application. The user would be prompted to enter a username, while the application detected the mobile serial number automatically. This was followed by a graphical task the user needed to perform, which was compared with the image stored in the server database during registration. If there was a match, the user progressed to the third stage where the user must remember a pattern of squares she/he had also chosen in the registration stage. The user was given a number of patterns, and had to choose the right one. When the correct pattern was selected, the user authentication was successful. This was a simple and effective method; it relied on recognition based memory. It only allowed registered devices to access the system, and it protected against loss of device. There were many measures to protect against different attacks. However, it limited the eligible user to using only registered devices. In addition, the transmitted information was not protected and no mutual authentication was proposed.

3.3 Two Factor Vs Multi-factor

A comparison of the key advantages and disadvantages of each of the authentication methods reviewed in this section are given in Table 2 and Table 3.

4 DISCUSSION

A first assessment of the authentication research field reveals that researchers tend to prefer one of two alternative types of authentication schema. In the battle of supremacy between more or less authentication factors, it seems that the notion of 'more means better' is becoming the norm across the mobile industry, the business industry such as in banking, and within the research community. This has been reflected in the amount of research conducted and more emphasis is tending to be put on multi-factor authentication. From the observation of the research activities in the field of authentication since 2012, the growth in

the number of research activities in to multi-factor authentication appears to have been more prominent than two factor authentication. However, despite the pressure from the industry, two factor authentication research shows significant strength and still offers security and efficiency, as well as saving on computing resources such as memory and storage.

Moreover, one might argue that one of the most important savings is on energy consumption. Considering that smartphones consume a considerable amount of energy to stay connected, power limitations can have a profound impact. This is one of the driving factors behind the need to use the cloud resources to subsidise the lack of local resources on mobile devices.

Table 2: Strengths Vs weaknesses of two factor authentication methods

Technique	Strengths	Weaknesses
Handwriting [10]	<ol style="list-style-type: none"> 1. The log in process is simplified by using handwriting 2. Processing of the handwriting image is performed on the cloud to reduce time needed for the authentication 	<ol style="list-style-type: none"> 1. Mutual authentication between the parties is not performed 2. User may alter their writing style, which may lead to an error in authentication 3. There is no mechanism to protect against attacks
Palm recognition [12]	<ol style="list-style-type: none"> 1. Uses the palm to authenticate with functions to minimise errors, which makes it a secure system 	<ol style="list-style-type: none"> 1. No mutual authentication between the parties 2. All processing is on the mobile device, which reduces efficiency because of the device’s lack of resources 3. If the device is stolen, user information can be extracted from the device 4. No mechanism employed to protect against attacks
Password & phone token [13]	<ol style="list-style-type: none"> 1. Provides mutual authentication 2. Passwords are protected in transmission 3. No computation on smartphone, saves on power consumption 	<ol style="list-style-type: none"> 1. Proposes that the encrypted password be stored on the mobile device, which can be a security risk if the mobile is lost or stolen 2. Does not protect against misuse if mobile is lost/stolen
MDA[14]	<ol style="list-style-type: none"> 1. Uses the traditional user name and password, which makes it easy to use 2. Protects against many attacks 3. Employs mutual authentication between the user and the cloud 4. Robustness against various attacks 	<ol style="list-style-type: none"> 1. Employs complicated passwords that are difficult to remember 2. Increased processing by the mobile device has negative impact on power consumption 3. Does not protect against misuse if mobile is lost or stolen
Fuzzy Vault [15]	<ol style="list-style-type: none"> 1. Uses a simple graphical password that reduces time to authenticate 2. Sets up a secure communication channel between the user and cloud to make it more secure 3. Uses RSA digital signature to protect against attacks 4. Data is encrypted before transmission 	<ol style="list-style-type: none"> 1. Employs too many encryption methods, which increases processing time and reduces efficiency due to higher power consumption and lower battery life 2. Data is not deleted from the mobile once authentication is complete

Two factor authentication shows more compatibility with MCC as it often uses less computational processing than multi-factor authentication, while multi-factor authentication tends to require, for the most part, more and more resources due to the complexity of the proposed schemes. An example of multi-factor inefficiency is where a high imaging camera is required to improve the accuracy of the image [16]. In low lighting conditions, the use of flash may be necessary, which in turn would increase power consumption on the mobile device, thereby reducing the efficiency of the scheme.

Two factor authentication simplifies the authentication process. It shows that the weaknesses associated with the use of the traditional password can be overcome by using biometric information [12] or with handwriting techniques [10]. This

improves usability of the two factor authentication methods. In addition, two factor authentication does not require as many resources as that of the multi-factor authentication schemes, which makes it more efficient than its counterpart. For example, we can draw a direct comparison between the Two Factor message digest authentication scheme [14], which requires only a username and password authentication, with multi-factor five factor authentication scheme [16], which requires five steps to authenticate.

Although multi-factor authentication aims to improve security, the process of dividing the tasks of the authentication process between the server and the client only serves to increase the complexity of the operation, which then requires more resources and adds more time to the process.

Table 3: Strengths Vs weaknesses of multi-factor authentication methods

Technique	Strengths	Weaknesses
Five Factor [16]	<ol style="list-style-type: none"> 1. Uses the cloud to process authentication factors in bulk, which improves efficiency, speed, and time 2. Uses TLS/SSL to improve security of communication 3. Uses IMEI and IMSI to protect against loss of device 	<ol style="list-style-type: none"> 1. Too many factors are employed in authentication making it complicated and overwhelming to users 2. No mutual authentication is employed 3. Biometric data is not deleted from device
OTP [17]	<ol style="list-style-type: none"> 1. Ensures that only authorised users are authenticated 2. Effective user account management control 3. Protects against mobile device loss 	<ol style="list-style-type: none"> 1. Overly complicated, involving many factors, and is less efficient 2. Does not protect against many attacks such as sniffing, or man-in-the-middle attacks 3. Does not provide security to transmitted data
MFAS [18]	<ol style="list-style-type: none"> 1. Multi-phase authentication ensures strong security implementation 2. Biometric data loaded temporarily on RAM to ensure no trace left on mobile device 3. Protects against multiple attacks 4. Does not require mutual authentication 	<ol style="list-style-type: none"> 1. Requires intensive computation on device
Multi-stage [19]	<ol style="list-style-type: none"> 1. Multi-stage authentication process 2. Simple and effective, using image patterns rather than complicated passwords 3. Effective against numerous attacks 	<ol style="list-style-type: none"> 1. User can only use registered device 2. No mutual authentication in place

The strength of authentication scheme can be measured by its robustness against various attacks.

Two factor authentication is susceptible to man-in-the-middle attacks [20]. This means that an attacker can see all messages transmitted between client and server and the attacker is able to alter the data, as well as trace the user. This weakness has been addressed by some of the research papers analysed in this survey [15], which not only provide resistance to man-in-the-middle attacks, but also brute force and impersonation attacks, by setting up a secure channel between the server and client through the use of strong encryption methods. This also protects the user’s and server’s privacy against eavesdropping. Similarly, the MDA authentication scheme [14] provides anonymity of both the client and server, which protects both communicating parties from eavesdropping or impersonation attacks. MDA also provides mutual authentication between the user and cloud server, which further improves privacy.

Another factor that affects the attractiveness of any authentication method is the user acceptance and willingness to embrace that method. Biometric methods have been shown to be more appealing to users than passwords [21] because they require less effort and no complicated words to remember. Hand writing techniques [10], fuzzy vault [15], or the use of biometrics [12] are prime examples of this.

A number of multi-factor research papers analysed during the research for this paper highlighted excellent examples of efficient authentication methods. However, as the number of authentication factors increases, the potential for authentication failure increases exponentially. Below are some of the factors that can affect the process:

1. Moving from one mobile coverage cell to another may incur an ephemeral disconnection
2. Moving in to a mobile shadow area, or no coverage area, may also cause an interruption in communication
3. Environmental factors such as bad lighting, when using biometric authentication, can also result in authentication errors

Any particularly long authentication process would only fuel user frustration, negatively affecting the usability of the authentication scheme, resulting in user distrust of the technology, and in turn impacting negatively upon the adoption of the technology. Multi-factor authentication is most effective when used in a resource rich environment, such as with PCs or laptops. In this environment, any processing requirement can be carried out by the local station using local resources.

One of the principal reasons for using MCC is to exploit the cloud’s resources to subsidise the mobile’s resources for carrying out any required computations. Therefore, two factor authentication should not be abandoned in favour of multi-factor authentication, because it complies with almost all the reasons that form the bases of MCC.

However, in order to design an efficient and reliable two factor authentication system, it would need to comply with all the specifications discussed at the start of the Analysis section of this paper, with a focus on ensuring that all authentication communication is secured using strong encryption. Mutual authentication should also be established between the authenticating server and the mobile client, and finally, all complicated authentication algorithms should be performed on the cloud.

5 CONCLUSION

The advent of MCC has proven to be a valuable asset in the armoury of computing technology. Users can access elastic resources, introducing mobile computing to enable them to access many different services, such as healthcare, finance and transportation. However, MCC is still in its infancy and faces many challenges that need to be addressed. In this survey, we highlighted some of the research afforded in the two factor and multi-factor authentication methods, and we analysed a number of research efforts taking in to consideration important criteria, such as ease of use, efficiency, reliability, security, privacy and trust. MCC will continue for now and the near future to be the trend for accessing and sharing resources. Despite the fact that there are various issues associated with the technology, which have been addressed by a number of researchers, there remains some never ending issues that will always be associated with MCC. The issue of authentication has to a large extent been achieved by modern platforms. However, data leakage and side channel attacks are just two examples of issues that remain a difficult open challenge.

6 REFERENCES

- [1] M. Hammoudeh, R. Newman, C. Dennett, S. Mount and O. Aldabbas. 2015. *Map as a Service: A Framework for Visualising and Maximising Information Return from Multi-Modal Wireless Sensor Networks*. Sensors, Vol 15, Issue 9: p. 22970-23003. Multidisciplinary Digital Publishing Institute.
- [2] A. Abuarqoub, M. Hammoudeh, B. Adebisi, S. Jabbar, A. Bounceur and H. Al-Bashar. 2017. *Dynamic Clustering and Management of Mobile Wireless Sensor Networks*. Computer Networks, Vol 117, p. 62-75. Elsevier.
- [3] M. Hammoudeh, F. Al-Fayez, H. Lloyd, R. Newman, B. Adebisi, A. Bounceur and A. Abuarqoub. 2017. *A Wireless Sensor Network Border Monitoring System: Deployment Issues and Routing Protocols*. IEEE Sensors Journal, IEEE.
- [4] I. Al Rassan and H. Al Shaher. 2013. *Securing Mobile Cloud using Finger Print Authentication*. International Journal of Network Security & Its Applications (IJNSA), Vol 5 no 6. Academy & Industry Collaboration Centre (AIRCC)
- [5] L. Badger, T. Grance, R. Patt-Corner and J. Voas. 2011. *Draft Cloud Computing Synopsis and Recommendations*. National Institute of Standards and Technology (NIST), Special Publication 800-146. US Department of Commerce. <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf>
- [6] I. Ghafir, V. Prenosil, J. Svoboda and M. Hammoudeh. 2016. *A Survey on Network Security Monitoring Systems*. IEEE International Conference on Future Internet of Things and Cloud Workshops (FiCloudW). IEEE, p.77-82.
- [7] I. Ghafir, V. Prenosil, A. Alhejailan and M. Hammoudeh. 2016. *Social Engineering Attack Strategies and Defence Approaches*. 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, p. 145-149.
- [8] I. Ghafir, V. Prenosil and M. Hammoudeh. 2016. *Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution*. theIRED.
- [9] H. Khan, A. Atwater and U. Hengartner. 2014. *An implicit authentication framework for Android*. Proceedings of the 20th Annual International Conference on Mobile Computing and Networking, MobiCom '14. ACM, New York, NY, USA, pp. 507– 518.
- [10] F. Omri, R. Hamila, S. Foufou and M. Jarraya. 2012. *Cloud-ready biometric system for Mobile Security Access*. Networked Digital Technologies, communications in computer and information science. p. 192-200.
- [11] C. Rathgeb, and A. Uhl. 2011. *A Survey on biometric cryptosystems and cancelable biometrics*. EURASIP Journal on Information Security, Springer.
- [12] N.F. Moco, P.L. Correia and L.D. Soares. 2014. *Smartphone-Based Palmprint Recognition System*. 21st International Conference on Telecommunications (ICT).
- [13] S. Binu, A. Mohan, K.T. Deepak, S. Manohar, M. Mohammed and R. Pethuru. 2015. *A Proof of Concept Implementation of a Mobile Based Authentication Scheme without Password Table for Cloud Environment*. IEEE International Advance Computing Conference (IACC).
- [14] S. Dey, S. Sampalli and Q. Ye. 2013. *Message digest as authentication entity for mobile cloud computing*. 32nd international performance computing and communications conference. San Diego, USA: IEEE
- [15] D. Schwab and L. Yang. 2013. *Entity authentication in a mobile-cloud environment*. In: 8th annual cyber security and information intelligence research workshop: federal cyber security R and D program thrusts. Oak Ridge, United States: ACM.
- [16] Y.S. Jeong, J.S. Park and J.H. Park. 2015. *International Journal of Communication Systems*. Int. J. Commun. Syst. 2015; 28:659–674.
- [17] K.W. Hussein, N.F.M. Sani, R. Mahmud and M.T. Abdullah. 2013. *Design and Implementation of Multi Factor Mechanism for Secure Authentication System*. International Journal of Computer Science and Information Security 11.7: 31-37.
- [18] N.A. Albahbooh and P. Bours. 2015. *A Mobile Phone Device as a Biometrics Authentication Method for an ATM Terminal*, in Computing Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), IEEE International Conference.
- [19] M. Aldwairi, R. Masri, H. Hassan and M. El Barachi. 2016. *A Novel Multi-Stage Authentication System for Mobile Applications*. International Journal of Computer Science and Information Security. Vol 14, Issue 7.
- [20] B. Schneier. 2005. *The Failure of Two-Factor Authentication*. https://www.schneier.com/blog/archives/2005/03/the_failure_of.html.
- [21] C. Braz and J.M. Robert. 2006. *Security and usability: the case of the user authentication methods*. In: Proceedings of the 18th international conference of the association francophone d'interaction homme-machine. Montreal, Canada: ACM; 2006. p. 199–203.