IUG Journal of Natural and Engineering Studies
Peer-reviewed Journal of Islamic University-Gaza

ISSN 2409-4587

IUGNES
Vol 24, No 1, 2016, pp 1-13

The Two secured Factors of Authentication

Hatem M. Hamad[1]**, Waleed A. Abudalal**[1,*]

[1]Department of Computer Engineering, Faculty of Engineering, Islamic University of Gaza, Gaza Strip, Palestine

Received on (26-05-2015) Accepted on (28-08-2015)

Abstract

One of the popular challenges that faces the Cloud Computing is the authentication problem. Authentication is a mechanism to establish proof of identities to get access of information in the system. There are several solutions to overcome this issue that it can be gathered in three authentication mechanisms which lead to a multifactorial authentication schema. The multi factor is proposed in this paper confirms the user's identity without sending it to the cloud server, which will gain our solution more security and fast response over other solutions that depend on sending the user identity to the server to be authenticated. The User's credentials have never exchanged with the server, it is only saved in the user's mind. We present an efficient authentication schema which based on two authentication factors, the first is the password-based authentication, which is processed in the user's machine, and the second is the biometric-based authentication which adds more secure factors to the authentication process. We use the Elgamal Elliptic Curve Cryptosystem and the symmetric encryption to overcome the security threads on the authentication process. Furthermore; we use the 3D face image as a second challenge response factor in our proposed algorithm. In addition, to save the bandwidth and computation, we use a mobile agent to pass the first factor of the authentication code to be executed in the client machine, and let the second factor to be executed in the cloud server.

Keywords Cloud Computing, Authentication Issue, Two Authentication Factors, Biometric Authentication, Mobile Agent.

اثنان من العوامل الضامنة لعملية المصادقة في الحوسبة السحابية

ملخص

أحد التحديات الشائعة التي تواجه الحوسبة السحابية هي المشاكل الأمنية. وأحد هذه التحديات الأمنية هي مشكلة المصادقة. عملية المصادقة هي الأساس لأمن المعلومات، وهي آلية تهدف للتثبت من هويات المستخدمين للوصول للمعلومات في النظام. هناك عدة حلول للتغلب على هذه المشكلة التي يمكن جمعها في ثلاث آليات للمصادقة التي تؤدي إلى تصميم نظام للمصادقة متعدد العوامل. تم اقتراح بعض العوامل المتعددة في هذه الورقة لنظام المصادقة، حيث أنه يقوم بالتأكد من هوية المستخدم دون إرسالها إلى خادم السحابة. حيث أن المعلومات الخاصة بالمستخدم التي يستخدمها للولوج الى النظام لا تتبادل مطلقا مع الخادم، بل يتم حفظها فقط في ذاكرة المستخدم. نحن نقدم مخطط للتوثيق الفعال مبني على عاملين من عوامل التوثيق، الأول هو المصادقة على أساس كلمة السر، والتي تتم معالجتها في جهاز المستخدم، والثاني هو المصادقة المستندة إلى البيومترية، وهو ما يجعل النظام المقترح أكثر أمنا لعملية المصادقة. لقد قمنا باستخدام وادارة العديد من الأدوات والتقنيات المختلفة لإنشاء تصميم آمن لعملية المصادقة. واستخدمنا Elgamal Elliptic Curve Cryptosystem للتشفير الغير متماثل، أيضا استخدمنا التشفير المتماثل للتغلب على المواضيع الأمنية في عملية المصادقة. وعلاوة على ذلك؛ استخدمنا صورة الوجه ثلاثية الأبعاد كتحدي ثاني في النظام المقترح. بالإضافة إلى ذلك، لحفظ عرض النطاق الترددي وتقليل كمية الحسابات، قمنا بتمرير التحقق للعامل الأول الى جهاز المستخدم ليتم تنفيذه في جهازه، والسماح للعامل الثاني ليتم تنفيذه في خادم الحوسبة السحابية.

كلمات مفتاحية: الحوسبة السحابية، المصادقة المتعددة، عوامل التوثيق والتحقق، التحقق عن طريق صورة الوجه ثلاثية الأبعاد، وكيل برمجي للسيرفر.

[*] Corresponding author e-mail address: wabudalal@students.iugaza.edu.ps

1. Introduction:

Virtualization technology was introduced in the late of 1960s by IBM [1]. Virtualization is defined as the abstraction of hardware resources to facilitate the sharing of resources well. So, virtualization helps enterprises reduce investments and operational cost. The term of virtualization means the ability to run entire virtual machine components, including the Guest Operating System (VMs), on another operating system called Host Operating System. The Hypervisor is the layer of software that emulates the hardware interface seen by the VM. The hypervisor completely controls system resources.

Virtual Migration (VM) migration is defined as the movement of virtual machine from one physical host to another. In the cloud environment, the VM live migration is introduced to obtain multiple benefits which mainly include high availability, hardware maintenance, fault takeover and workload balancing.

This makes the cloud provider puts the client's data outside of his control that leads to many security problems. The cloud computing inherits all computer security aspects that are not specific only to the cloud system. For example, data has to be protected from attackers and malware wherever its location and storage is, however, there are some cloud security issues which are specific to this field [3]. Security comes in the first rank as the greatest challenge or the issue of the cloud computing by 74.6%, then you find the performance and availability by 63.1%. [4]. According to a survey in Japan, 70% of the respondents mentioned the security as the reason of why they were wary of the cloud computing [5].

The security responsibilities are distributed between the cloud provider and the customer according to the cloud computing models. For example, the Amazon's AWS EC2 provides the infrastructure as a service, so his security responsibilities hold on physical security, environment security and virtualization security, but the responsibilities of securing the operation, application, and data hold on the customer. Another inverse example is that the salesforce.com offers the (SaaS) software as a service, and so all the security responsibilities hold on it [6].

There are several security challenges in the cloud computing that we must be aware of them. We divide the security problems into five groups which are: security problems related to Security Standard, Cloud Infrastructure, Cloud Network, Data, and Access Control.

1.1 The Security Challenges of the Cloud Computing:

1. Security Problems Related to Security Standards:

Security Standards refer to the management of the governing bodies and regulatory authorities that elaborate the cloud security policies in order to ascertain a safe environment for working over the cloud. This group comprises service level agreements, service providers, auditing and other agreements among the users and other stakeholders. This group can contain problems such as the cloud Standards [7], the abuse and nefarious use of the cloud Computing [8], Legal Compliance and governance [4], uncertain ability to enforce the provider's security policies [9], Insufficient Due Diligence [8] and the Accountability problems actions [4].

2. The Security Problems Related to The Cloud Infrastructure:

This group of challenges includes the security problems within the Cloud Infrastructure as a service, the platform as a service, and the software as a service. This group contains problems such as Virtualization [3, 10], Multi-tenancy, Shared technology vulnerabilities, and VM-Based Malware Attack [4].

3. The Security Problems Related To The Cloud Network:

This group discusses the channel source through which the users can interlink with the cloud networks in order to perform desired calculations. That includes network connections, browsers and information exchange by means of registration processes. [11]. The network attack remains the biggest challenge of the network security. The cloud computing will be more vulnerable to network attacks and frauds. Therefore, security experts predict that the cloud computing will be the target of the hackers in the next five years [12]. Some of these problems are: DDOS Attacks [13], Flood Attacks [14], IP Spoofing [13], Sessions and services hijacking [8], and Timing attack [15].

4. Security Problems Related To Data:

This class includes matters related to data integrity and confidentiality. Some problems refer to this class such as Data Loss and leakage, Data Storage [13], Data geolocation, Third party access [16], Data Boundary, Big Data [17, 18], and Data Remanence [19].

5. Security Problems Related To Access Control:

This group of challenges refers to the user's oriented class, and involves the issues of authentication, identification and authorization such as the System Monitoring [7], Access Control, Authentication and Auditing [20].

1.2 The Authentication Problem in the Cloud Computing:

Authentication is the determination of the identity or the role that someone has. This determination can be done in a number of different ways, but it is usually based on a combination of something the person has (like a smart card), something the person knows (like a password), or something the person is (like a human with a fingerprint). [21] The user's authentication in the cloud computing environments has been divided to two main processes: The first one is investigating unique identifiers of the users during the initial registration phase, and the second one is the authentication and validation of the user's legal identities, and acquiring their access control privileges for the cloud resources and services during the service operation phase. As the number of the end-users has increased, the challenge of controlling accesses and operations in shared files has increased too [22]. The current user's authentication models such as the password-based authentication could not satisfy the users and enterprises and make sure that the safety of this process decreases the rate of efficiency and reliability in the cloud computing system [12].

Nowadays, the cloud providers depend on the password authentication mechanism to authenticate their clients. However, the password-based authentication only depends on something the user knows (i.e. PIN, or password), so it suffers from many problems, such as it can be forgotten or stolen or guessed [23, 24]. Adding complexity to the password (i.e. combining the case with sensitive letters, numbers, symbols), may be helpful in the prevention of stealing or guessing. But this will bring another problem which is the hardness of remembering the complex passwords for the different applications. Hence, the users tend to use the same password for a long time, and among the different applications. In addition to the limitations above, password-based authentication can be compromised by different types of hack, such as the Key logger, Sniffing, Dictionary Attack and Brut Force Attacks [25].

The rest of the paper is organized as following: Section 2 presents a brief description of the authentication mechanisms. Section 3, discusses the related work. Section 4 presents our motivation. Section 5 presents our proposed schema. Section 6 presents a brief description of the system principles and technologies which are selected, the Cryptography and Biometric techniques, and what guides us to use them. Section 7 presents the algorithm of our proposed schema. Section 8 shows the security analysis of our proposed algorithm. Finally our conclusion is presented in Section 9.

2. Authentication Mechanism:

Authentication mechanisms can be categorized into three groups: the biometric authentication, token-based authentication, and knowledge-based authentication. In this section we will summarize these types including the weakness points of each of them.

2.1 The Biometric Authentication:

The biometric authentication includes behavioral biometrics such as the keystroke latency or signature dynamics, and physiological characteristics that study physical characteristics such as the fingerprint, voice or vein pattern. The Biometrics cannot be easily changed but they are easy to manage. However, we cannot consider the biometrics as the best choice to the cloud environment for the following reasons: 1) they need professional and excessive devices such as a fingerprint scanner, which requires extra costs as well as troubles in combining them to the cloud computing environment; 2) when a large number of customers is being verified at the same time, the mechanism will be slow 3) it may not work well when the physical characteristic changes (i.e. the changed voice when someone catches a cold) [26, 27].

2.2 Token-based authentication:

The token-based authentication may be a physical device that an authorized user of the computer services is given to make the authentication easier. An example of the token is the bank cash card. Tokens can be easily stolen and used for malicious purposes, and they are not convenient for using in the web environment because special devices are needed. [26]

2.3 Knowledge-based authentication:

The knowledge-based authentication can be a text-based password or a graphical password. The text-based passwords include un-cued and cued passwords. The un-cued passwords use a random sequence of characters and digits either generated randomly or selected by each user. The cued password relies on the memory of a concept or a phrase that the user selects. The weakness of this password is that the users tend to select phrases from music lyrics, movies, literature, or television shows. These text sources are often available in the Internet and there is a possibility to build a dictionary for a mnemonic password [26-28].

The graphical passwords include recognition-based passwords and position-based passwords. When using recognition-based techniques, the user is presented with a set of images and the user passes the authentication by recognizing and identifying the images he or she selected during the registration stage.

Using position-based techniques requires the user to identify the target objects within an individual picture or draw a previously drawn object on a grid, which relies on both visual memory and spatial recall ability [26, 28].

There are also some drawbacks of recognition-based passwords. Firstly, they have a smaller space than the text-based passwords so it might be less secure.

Secondly, they take a longer time than the text passwords under the same network speed. Some other drawbacks include the users who tend to choose faces of people from the same race. They likely choose the faces of females more than the other faces [29, 30].

In general, the knowledge-based authentication still suffers from the malicious attacks such as the brute force attacks, dictionary attacks, replay attacks, and Man-in-the-Middle attacks.

3. Related Work:

The term "biometrics" is commonly used today to refer to the authentication of a person by analysing physical characteristics, such as fingerprints, or behavioral characteristics such as signatures. The biometric authentication relies on something a user is, therefore it identifies the users based on their biological or behavioral characteristics, which cannot be easily stolen or guessed, and doesn't require remembering a long and complex password [25].

Since many physical and behavioral characteristics are unique to an individual, the biometrics provides a more reliable system of authentication than the ID cards, keys, passwords, or other traditional systems [31]. Biometric authentication can be a solution for most of the password authentication problems.

Recently, the biometrics authentication are applied as a solution for cloud authentication users, and there are a lot of researches in this topic. Now, we will survey the work done on an applying biometric authentication in the cloud computing.

In this section, we focus on the related works that are done in the biometric authentication for the cloud computing and present their weakness points.

3.1 Biometric Authentication without Protecting Biometric Template:

To preserve the user's privacy, the biometric template has to be protected against attacks. Some research are done on using the biometric authentication to authenticate the cloud clients without securing the biometric templates. In this section, we survey some examples for this work as:

Kesava. R. [24] applies the iris authentication for authenticating users of the cloud software as a service (SaaS), which stores users' iris patterns in a database on the cloud without any protection.

In [32], an application is proposed to secure the email in the MS Outlook kind of environment. They used a combination of the password, fingerprint scanner, and e-token device (USB device) for the authentication users. And also used a 448 bit symmetric key algorithm for the data encryption.

The drawback of the proposed application is the dependency on external devices to achieve authentication, a scanner for fingerprint and a USB e-token device.

Mohammed [33] proposed an authenticated system by integrating a multifactor authentication with multilayer authentication techniques in order to produce a standard of multilayered factor of authentication model which is suitable for different internet banking services based on a risk assessment criteria. The produced model consists of 5 levels in which each level contains one or a combination of authentication factors such as knowledge-based, possession-based or Biometric-based factors. They deploy the user's authentication schemes of level 5 by developing a web application using Asp.net and SQL Server in integration of the Silver Light technology which allow the add-ons of the face recognition capabilities. They deploy a web application tested under a local host machine, but the recent studies show that there are limitations for the applying face recognition function while running on the server's hosting.

Bhattasali [34] proposed the two factors of the authentication mechanism provided by the cloud provider as a service for authenticating access to the sensitive healthcare data in the cloud. They combined the secret PIN verification with a dynamic keystroke analysis to enhance accuracy level of the authentication. The first factor uses simple and effective behavioral biometrics and keystroke analysis model while the second factor uses the secret PIN mechanism. The results show that accuracy level is enhanced in the two factors of authentication which is compared to use only one factor keystroke.

The drawback of this solution is the scalability. The scalability is a considerable issue in the keystroke dynamics. It is difficult to differentiate the users accurately when the number of users is increasing.

Haqani in [35], addressed the issue of access control to the critical data on a cloud by the use of the biometric iris verification and authentication for a controlled flow of data. They used a biometric iris verification for the purpose of authentication of the users. The results showed that the percentage which the biometric iris verification /authentication system can perform correctly is around 97%.

The drawback of this solution is that the iris template is not protected.

Gunasekaran [36], proposed a multimodal biometric authentication to the authorized users with a secure and easy access to information and services for the personal identification system. The unimodal biometrics suffer from the noise, intra class variations, spoof attacks and non-universality. To avoid these attacks, the multimodal biometrics, which are the combination of many modalities, are adapted. They used fingerprint and palmprint biometrics for a multimodal biometric system. They achieved a percentage of 98% when the number of samples is 600.

The drawback of this solution is that the multimodal biometrics template is not protected.

3.2 Biometric Authentication with Protected Biometric Template:

To keep the biometric template safe and secure from the different hack methods, it has to be encrypted. Several researchers attempt to encrypt the biometric template by different encryption methods, and some others use the cancellable template. The work in this field is still being developed. In this section we survey some of the work done in secured biometric templates.

Wang [37], proposed a method for securing the face biometric template in the cloud computing. The cloud operates the face recognition and matching under an encrypted condition, and the result is encrypted again before encrypting the transmission to the user. In this way, the cloud neither knows the user's real face data, nor which face and the face matches in templates. Ensure that there is no leakage in the user's privacy data, compare numbers in the encrypted domain, allow the user to obtain the same and correct result as it's under non-encrypted conditions.

The method is divided into three parts: the user, the cloud initialization and the cloud private which is matching the identification part. The user's part uses a series of face pre-processing method to be done with original images, using the Paillier encryption algorithm encrypts the processed images, the cloud initialization's part uses the processed original images to establish subspaces and face templates database through the PCA algorithm, and the cloud private which is matching the identification part, has a projection, distance calculation and a minimum distance finding combined to achieve a face matching and a recognition under encrypted conditions. The cloud and user's communication is also in the encrypted domain.

One of the drawbacks of this solution is the time consuming, it takes 240 seconds for an image of 92*112 dimension. The best result they gained of face recognition is 94%.

Zhu. [38] proposed a voiceprint authentication scheme for authenticating the cloud's users with a homomorphic encryption as a template protection mechanism. The homomorphic encryption is used to encrypt the users' biometric templates and to allow the biometric matching process to be done in the encoded space (i.e. biometric templates do not need to be decrypted for matching). However, this voiceprint authentication scheme achieves a high FRR of 4% when the size of the voice codebook is 32. The drawback of this solution is when the size of codebook is larger, the FRR is lower, and the time of the encryption is longer.

Joshi [39], proposed a system that uses three tiers of security in the cloud environment. A set of biometric features is firstly extracted from the user's face image. The extracted features are then quantized and mapped to a binary representation for a feature point matching. The produced features and the secret key (which will restrict the unauthorized access) are bound by using the Face fuzzy vault scheme. The first tier is to classify the priority of data, the second tier is to categorize the clients into three rings, each of them contains a secret key, and the third tier (Face fuzzy vault technique) is to bind the ring secret key with the user's face feature to provide a controlled data access to the authorized user i.e. the fuzzy vault provides a unique identification.

In [40], presented a two-factor authentication scheme for the cloud environment to authenticate the users, which depends on the features' extraction of the fingerprint and Schnorr digital signature.

In the registration phase, a user submits the hash of his username, password, and fingerprint to the data owner inside the cloud server in a secure channel. The data's owner sends back the credential (the keys derived from the username, password, and the features' extraction of the fingerprint) to the user. This credential contains the two main factors that will be used by the user in the next phases. In the login and mutual authentication phases, the user sends his first factor to the cloud server who ensures the authority of the user's first factor. After that, the cloud server sends back the request to the user, asking him to submit the second factor. Then, the user checks the validity of the cloud server at first and provides his second factor to the cloud server. Finally, the user gains a permit to reach the cloud server's resources when his second factor possesses the validity in the cloud server.

In [41] an approach is proposed for using a cancellable biometric authentication system. In this concept, a distorted biometric image, derived from the original, is used for the authentication to keep the biometric safe from a situation if it is compromised. This is achieved by using

One-Way function, which allows the generation of non-invertible transforms. Additionally, a data hiding technique is used to embed the demographic information in the biometric image to keep it secret against the replay attacks.

In [42], an approach is proposed for using a fingerprint authentication, and storing a biometric template in a database in a cloud, then they use a bio hash function to secure the stored biometric template. The results show that an enhancement of 25% is gained in the security performance in the cloud compared with the Crypto-Biometric Authentication approach.

4. Motivation:

From above, we see that all used authentication processes depend on sending the user's identity to the server or to a third party server, in order to be authenticated. Because of insecure of transmission media, there are several motivations are done in order to secure the user's credential as much as possible. Although there are several attempts to protect the user's credential, they are still susceptible to be attacked and discovered.

Our solution depends on the idea of non-existence user credentials. This means that the user has never needed to send his username and password to the server, therefore, the authentication process is locally done at the user's machine. First of all, at the registration phase, the user's credential is encrypted by the user's public key, then it is hashed, and after that, it is encrypted again by the server's public key, then the user sends this message to the server. The server can decrypt the message using his private key, and he stores the hash value of the user's encrypted credential in a database. So, the cloud service provider himself cannot get any information about the user's identity. When the user wants to login to the system, he sends his encrypted ID to the cloud server, and keeps his username and password on his mind. The cloud server selects the user's stored and hashed credential from the database, and concatenates with others. Then he encrypts it again by using the user's public key, then he sends it as a challenge/response message. This challenge message is sent to the user who has to response correctly to this message. The challenge /response message is a mobile agent which is sent to the local object in the user's machine. The local object gets the username and password from the login fields, then it calls the local function to make a decision about whether the user is authorized or not, according to the return value.

Our solution has the following properties, which make it different, efficient, and more secure than the other solutions:

1. No exchange of user credential (username and password)
2. No one except the user can know or even get the username and password
3. The process of authenticating the username and password is done in the user's machine.

5. Proposed Schema:

In order to increase the security of our solution, we design an authentication schema which consists of two factors of authentication. The 2-Factors of Authentication (2FA) is more suitable for the cloud authentication principles. We choose the first factor to be a knowledge-based authentication, which contains the username and password. The second factor is introduced when the user successes and passes the first factor, and hence, the cloud server asks the user to send his second factor. We choose the second factor to be a biometric-based authentication. When it is being authenticated, the user gains an access to the cloud server’s resources.

We use a combination of a knowledge-based authentication and biometric-based authentication. We can manage a requirement for smart cards, tokens, PINs and passwords, which can provide a powerful deterrent to spoofing, however, it can increase a processing time and may reduce the convenience of the biometric systems.

We can use iris or finger print or 2D face feature extraction as a second factor for authentication, furthermore, we can use a multiple biometric such as a combination of fingerprint and iris, but the multiple biometric increases processing time that cannot be a good choice for the cloud environment. We use 3D face feature extraction to improve the systems' performance against the pose and expression variations, and the changing environmental conditions, such as the light and heat. Furthermore it increases the complexity of the data set by the incorporation of the subtle variations, particularly in the facial images, thus it makes spoofing extremely difficult.

One choice to protect the biometric data in the cloud database is to store it as an encrypted data. In order to match the encrypted data, firstly, we have to decrypt the data then compare it with the taken one. Another solution is to use the Homomorphic cryptography which is a good mechanism to match the encrypted data without decrypting it. The problem of this solution is the high computation and time consuming. The second choice is to store the data without encryption, but it can be compromised by the attackers. We choose to store the biometric data without encryption since our framework is proposed to be software as a service in the cloud computing, in which the fast response is a major concern. At the same time, we introduce a framework that overcomes our solution from the various security risks.

6. System Principles and Technology:

To secure the transmission media between the user and the cloud server, it has to be encrypted. Cloud computing environments have many applicable cryptosystems, as the symmetric cryptosystems (Stream Ciphers, Block ciphers - AES), and asymmetric cryptosystems (RSA, Knapsack, ECC) and others like Homomorphic, Identity-Based Encryption and Biometric-Based Cryptography.

We can use Homomorphic or Identity-Based Encryption to encrypt the data used to authenticate the user. But we choose elliptic curve cryptography system since it is recommended by [43] to be the best system among the tested systems used in the cloud computing because of the following reasons:

1. It is more efficient.
2. It has a small volume because it depends on generating a curve by choosing random points instead of a key generation like in traditional public key systems (RSA, and ... etc.).
3. It is stronger than traditional systems in the secure ensuring.
4. This system can be executed in a relatively easy mode.
5. Because it has not a big computational effort, it needs a small energy (battery) when being executed.

6.1 Using Elgamal Elliptic Curve Cryptosystem:

The ElGamal Elliptic Curve Cryptography is a public key cryptography analogue of the ElGamal encryption schemes which uses Elliptic Curve Discrete Logarithm Problem. Elliptic curve cryptosystem can match the security of other cryptosystems while using a smaller key. For example, an elliptic curve cryptosystem with a public key of size 160 bits is as secure as RSA and DSA cryptosystems with a public key of size 1024 bits. With a smaller key size, the elliptic curve cryptosystem can offer a lower memory requirement, faster implementation and lower bandwidth requirement. [44, 45]. This encryption uses points on an elliptic curve for the encryption parameters of the ElGamal Encryption except the private key. It randomly selects points from the elliptic curve. The mathematical operations of the ECC is defined over the elliptic curve y2 = x3 + ax + b, where 4a3 + 27b2 ≠ 0. Each value of the 'a' and 'b' gives a different elliptic curve. Both points (x, y) which satisfy the equation above plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G and the curve parameters 'a' and 'b', together with a few more constants, constitute the domain parameter of the ECC [46].

In [47], the ElGamal Elliptic Curve Cryptosystem is implemented by using a C language. They divide the whole cryptosystem into seven different phases which are: System Setup, Key Generation, Public Key Validation, Message Encoding, Encryption, Decryption, and Message Decoding.

6.2 Using face recognition:

Perhaps the most common biometrics are the fingerprints and iris, but many other human characteristics which have been studied in the last years: fingerprint, palm geometry, voice, signature and face. However, biometrics have drawbacks. Iris recognition is extremely accurate, but expensive to implement and not very acceptable by people. Fingerprints are reliable and non-intrusive, but not suitable for non-collaborative individuals. On the contrary, face recognition seems to be a good compromise between reliability and social acceptance, and balances security and privacy well.

The 3D capturing process is becoming cheaper and faster, and for this reason, the recent works attempt to solve the problem directly on a 3D face model [48]. In [49], a new approach is presented for the 3D face recognition and authentication. They used a modified PCA algorithm for the feature's extraction of the facial image and they gained a high recognition rate of 99%.

7. Algorithm for Proposed Schema:

Our proposed schema consists of two phases: the Registration phase, and the Login & Authentication Phase. The second phase is divided into two levels of authentication, (i.e. two factors of authentication), which have to be passed successfully by the user to be authorized by the cloud server, and access its resources.

In this section, the algorithm of the two phases and the activities of secure authentication are discussed in detail. The notations used in this paper are defined in Table 1.

Table 1 *List of Notations*

Notation	Description
Un	User of Cloud Services
ID	User's unique identity
PW	User's password
K_S	Symmetric Shared Secret key- session key
H	Hash function for arithmetic captcha
‖	The string concatenation operation
K_{SP}	Cloud Server Public Key
K_{SS}	Cloud Server Secret Key

K_{UP}	User Public Key
K_{US}	User Secret Key
3DFI	3D Face Image
IFF	3D Image Feature Extraction

7.1 Registration phase:

In the registration phase, the user needs to register at the server by providing identification information. The server processes the user’s data for the authentication. The algorithm for the new user's registration is shown in Figure 1 and described as:

1. The user requests the cloud server for a new registration.
2. The ElGamal Elliptic Curve Algorithm [46] is established; both the user and server generate their public key and private key.
3. The user selects a unique ID, and encrypts it by using the public key of the server $\mathrm{E_{SP}}$(ID), then sends the message to the server.
4. The cloud server decrypts the message by using his private key $D_{\mathrm{SS}}(\mathrm{E_{SP}}(\mathrm{ID}))$ and gets the user's ID to check the uniqueness of the requested ID. If not, it goes on to step 3.
5. The cloud server generates the one-time password (OTP), and the dynamic symmetric shared key then encrypts both the OTP and symmetric shared secret key (session key) by using the user's public key, M1= E_{UP}(OTP, K_S.) ,then he sends the M1 to the user to continue.
6. The user decrypts the message by using his private key, and keeps the OTP and shared symmetric key (OTP, K_S) = D_{US}(M1).
7. The user encrypts his username and password with his public key E_{UP}(Un), E_{UP}(PW)
8. Then he computes the hash value of both username and password H (E_{UP}(Un)), H (E_{UP}(PW)).
9. The user keeps his credential information UCR= H (E_{UP}(Un)) || H (E_{UP}(PW)) on an external storage such as USB. This step is only required if the user's credential information is lost, or forgotten
10. The user constructs a message that contains the hash values of the encrypted username and password with his public key, and the user ID. M2= [H (E_{UP}(Un)), H (E_{UP}(PW)), ID].
11. Then he encrypts M2 with the public key of the server Y= E_{SP}[M2], to authenticate the server, then he sends the encrypted message Y to the cloud server for registration.
12. The cloud server decrypts the sent message with his private key M2= D_{SS}[Y].
13. The cloud server stores the user's ID, H (E_{UP}(Un)), and H (E_{UP}(PW)), on the user's ID, Username and Password fields in the database
14. The cloud server asks the user to turn on the 3D camera and capture a user face image.
15. The user uses a session key to encrypt the saved OTP, user's ID, and the hash value of the 3D face image then he constructs a message that contains the encrypted hash value of his 3D face image, the plain image without hashing, the encrypted OTP, and the user's ID. M3= (E_{SK}(H (3DFI)), (3DFI), E_{SK}(OTP), $\mathrm{E}_{SK}(ID)$). Then he sends the M3 to the cloud server.
16. The cloud server uses the session key to decrypt the user's ID, OTP, and H(3DFI) such as $D_{SK}(\mathrm{E}_{SK}(\mathrm{ID}))$, $D_{SK}(\mathrm{E}_{SK}\mathrm{OTP}))$, $D_{SK}(\mathrm{E}_{SK}(\mathrm{H(3DFI)}))$ then he verifies the OTP. Verify that the sent OTP = stored OTP. If it succeeds, he checks the integrity of the face image by computing the hash value of the plain 3D face image. Then compare it with the sent hashing value. Verify that H (3DFI) = H'(3DFI), if it is true then continue to else terminate.
17. The server processes the user face image, normalizes it, and extracts the feature by using the modified PCA algorithm explained in [48], and stores the image feature IFF on the database with the user's identity in the cloud.
18. The server clears the memory buffer that can be compromised by an attacker.

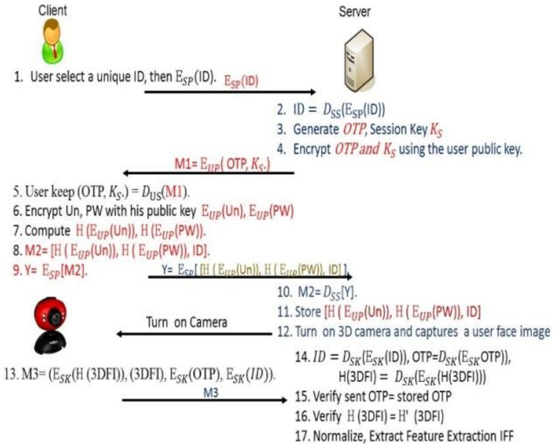
Client
Server
1. User select a unique ID, then E_{SP}(ID). $\mathrm{E_{SP}}$(ID)
2. ID = $D_{SS}(\mathrm{E_{SP}}(\mathrm{ID}))$
3. Generate *OTP*, Session Key K_S
4. Encrypt *OTP and* K_S using the user public key.
M1= E_{UP}(OTP, K_S.)
5. User keep (OTP, K_S.) = D_{US}(M1).
6. Encrypt Un, PW with his public key E_{UP}(Un), E_{UP}(PW)
7. Compute H (E_{UP}(Un)), H (E_{UP}(PW)).
8. M2= [H (E_{UP}(Un)), H (E_{UP}(PW)), ID].
9. Y= E_{SP}[M2].
Y= E_{SP}[[H (E_{UP}(Un)), H (E_{UP}(PW)), ID]]
10. M2= D_{SS}[Y].
11. Store [H (E_{UP}(Un)), H (E_{UP}(PW)), ID]
Turn on Camera
12. Turn on 3D camera and captures a user face image
13. M3= (E_{SK}(H (3DFI)), (3DFI), E_{SK}(OTP), $\mathrm{E}_{SK}(ID)$).
M3
14. ID = $D_{SK}(\mathrm{E}_{SK}(\mathrm{ID}))$, OTP=$D_{SK}(\mathrm{E}_{SK}\mathrm{OTP}))$,
H(3DFI) = $D_{SK}(\mathrm{E}_{SK}(\mathrm{H(3DFI)}))$
15. Verify sent OTP= stored OTP
16. Verify H (3DFI) = H' (3DFI)
17. Normalize, Extract Feature Extraction IFF

Figure 1 *Registration Phase*

7.2 Login And Authentication Phase:

In this phase, the user login into the system for authenticating and access the cloud services. The process of authentication phase is divided into two phases. The first phase is the first factor authentication, which aims to authenticate the user by the user name and password. In this phase, the process of authentication is executed in the user's machine by using the mobile agent concept. The second phase is the second factor of authentication which aims to authenticate the user by the 3D face image. In this phase, the process of authentication is processed in the server's machine. Figure 2 shows the login and authentication phase.

7.2.1 First Factor Authentication:

The algorithm of the first factor of authentication is introduced as following:

1. The user requests the cloud server for login, and enters his encrypted user's ID by using the public key of the server M4= E_{SP}(user's ID).
2. The cloud server decrypts the message by using his private key ID= D_{SS}(M4), and gets the user's ID.
3. The cloud server checks the existence of the user's ID, if it is not found, he gives the user two choices, 1) to enter his ID again for one more time, or 2) to register a new user .but if it's found, continue to else terminate.
4. The cloud server gets the stored hash values of the username and password that correspond to the user's ID $H(\mathrm{E}_{US}(\mathrm{Un}))$, and $H(\mathrm{E}_{US}(\mathrm{PW}))$.
5. The cloud server generates a new shared secret key K_S(session key) and the OTP
6. The cloud server encrypts the hash values of the username, password, OTP and the session key K_S by using the user's public key
7. The cloud server constructs a message that contains $S =$ E_{UP} $(H(\mathrm{E}_{UP}(\mathrm{Un}))$ || $H(\mathrm{E}_{UP}(\mathrm{PW}))$, OTP, K_S).
8. The cloud server sends a mobile code that contains a challenge/response of S
9. The mobile code sends the S to a local object in the user's machine to verify the user.
10. The local object decrypts the S by using the user's private key. *P1*= $D_{US}(S)$.
11. The local object gets the input username and password from the their fields in the login browser, then calls a function that computes *P2*= $H(\mathrm{E}_{UP}(\mathrm{Un}))$ || $H(\mathrm{E}_{UP}(\mathrm{PW}))$
12. The local object compares the first field of P1 with P2. If P1= P2, he encrypts the OTP by using the session key$K_S(OTP)$, and passes it to the mobile code. But if P1 != P2 , terminate the process.
13. The mobile agent activates the 3D camera, and captures a new face image.
14. The mobile agent uses the sent session key to encrypt the user's ID and the hash value of the 3D face image as E_{SK}(ID), E_{SK}(H(3DFI)),

The mobile code constructs M5= [3DFI, K_S(H(3DFI)), $K_S(OTP)$, K_S(ID)]. Then he sends M5 to the cloud server.

7.2.2 The Second Factor of Authentication:

The algorithm of the second factor of authentication is introduced as following:

1. The cloud server decrypts the user's ID and OTP by using the session key, $D_S(\mathrm{E}_{SK}(OTP))$, $D_S(\mathrm{E}_{SK}(ID))$ and verifies OTP with the sent one. Verify that the $OTP = OTP'$. If it is true then continue, else terminate.
2. The cloud server decrypts the hash value of the face image $D_S(\mathrm{E}_{SK}(\mathrm{H(3DFI)}))$, then he checks the integrity of the face image by computing the hash value of the plain 3D face image, and comparing it with the sent hash value. Verify that H (3DFI) = H' ' (3DFI), if it is true then continue, else terminate
3. The cloud server processes the user face image then normalizes it, and extracts the feature by using the modified PCA algorithm explained in [48], and verifies the feature extracted from the image (IFF), with the stored one. Verify that (IFF) = (IFF)'.
4. If the user is authenticated then the user is allowed to access the cloud services and resources, else the authenticate process terminates.

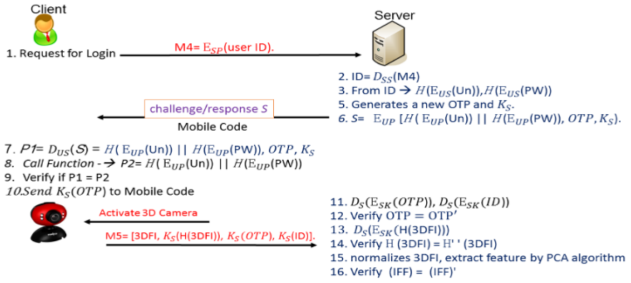
Client
Server
1. Request for Login
M4= E_{SP}(user ID).
2. ID= D_{SS}(M4)
3. From ID → $H(\mathrm{E}_{US}(\mathrm{Un}))$,$H(\mathrm{E}_{US}(\mathrm{PW}))$
5. Generates a new OTP and K_S.
6. S= E_{UP} [$H(\mathrm{E}_{UP}(\mathrm{Un}))$ || $H(\mathrm{E}_{UP}(\mathrm{PW}))$, OTP, K_S).
challenge/response S
Mobile Code
7. P1= $D_{US}(S)$ = $H(\mathrm{E}_{UP}(\mathrm{Un}))$ || $H(\mathrm{E}_{UP}(\mathrm{PW}))$, OTP, K_S
8. Call Function -→ P2= $H(\mathrm{E}_{UP}(\mathrm{Un}))$ || $H(\mathrm{E}_{UP}(\mathrm{PW}))$
9. Verify if P1 = P2
10.Send $K_S(OTP)$ to Mobile Code
Activate 3D Camera
M5= [3DFI, K_S(H(3DFI)), $K_S(OTP)$, K_S(ID)].
11. $D_S(\mathrm{E}_{SK}(OTP))$, $D_S(\mathrm{E}_{SK}(ID))$
12. Verify OTP = OTP'
13. $D_S(\mathrm{E}_{SK}$(H(3DFI)))
14. Verify H (3DFI) = H' ' (3DFI)
15. normalizes 3DFI, extract feature by PCA algorithm
16. Verify (IFF) = (IFF)'

Figure 2 *Login and Authenticating Phase*

8. Security Analysis:

A. **The secure credential management:** The user has never exchanged his credentials with the cloud server, and he keeps it only in his mind. The cloud server stores the hash values of the encrypted user name and password in a database with the user's ID. In this case, the cloud provider himself cannot get the username and password. The server checks the availability of the unique ID for each user at the time of new registration.

B. **The mutual authentication:** This security feature means that an attacker cannot impersonate the legal user to the server, and vice versa. Only the genuine user who possesses the secret factors can successfully bring the factors M1, Y, M3, S1, and M5. In the registration phase, the cloud server uses the user public key to encrypt both the OTP and symmetric shared key, so the legal user is the only one who can decrypt M1 by his private key to get the K_S and OTP. Then the user uses the K_S to encrypt the OTP. On the other side, only the cloud server can authenticate the user by verifying the OTP, and decrypt Y, and M3 by using his private key K_{SS}. In the login phase, the cloud server is the only one who can use his private key to decrypt the M4, and send the challenge mobile code to the client. On the other side, the legal user server is the only one who can response to M5. Furthermore; the OTP, that is passed with the user's 3D face image, is encrypted and decrypted by a new generated symmetric shared key (session key). So our scheme could provide a mutual authentication.

C. **The replay attack:** for each authentication phase, the server generates a new symmetric secret key that encrypts the OTP. Hypothetically, if the adversary detects the old secret keys authentication such as K_S and OTP, he still cannot perform a replay attack on the next authentication session. So, an adversary fails to use the replay attack**.**

D. **Man In The Middle Attack (MITM):** This type of attack intends that an adversary has the ability to intercept the messages between the users and the server. Then he uses this message when the user signs out the server. In our proposed scheme, the factors are securely encrypted. If an attacker tries to eavesdrop on the user's login request, he cannot obtain the user's identity unless he can solve the Elliptic Curve Discrete Logarithm Problem, which is hard to be broken. The generation of $S = \mathrm{E}_{UP}$ $(H(\mathrm{E}_{UP}(\mathrm{Un}))$ || $H(\mathrm{E}_{UP}(\mathrm{PW}))$, OTP, K_S) becomes useless when the user signs out, because it depends on generating a new OTP, and K_S for the next login. Another challenge is the second authentication factor (the 3D face image) which is taken online with the encrypted OTP. As a result, the proposed scheme can resist the MITM attack.

E. **The stolen verifier attack and the unauthorized access attack:** In our proposed scheme, all the authentication factors are not simultaneously available. Thus, if a one credential is stolen or lost, he needs the other, since the legal user needs Un and PW to login. Furthermore, if both the Un and PW are stolen, the stealer cannot authorize to login, since he needs the user's private key to decrypt S1. Now, if we suppose that all the Un, PW, and K_{US} are stolen, authentication needs an online 3D face image for login. Hence, the stolen verifier attack and unauthorized access attack are not applicable in this framework.

F. **The phishing attack:** In this framework, a mutual authentication between the user and the server, which is based on a strong encryption and multi-factor credentials, is performed for authentication. Only the genuine server can send a proper authentication information. And the user's responses can be verified only by the genuine server.

G. **The spoofing Attack:** In this framework, the live detection of the 3D face image is a key defense to spoofing. This ensures that the biometric sample, presented to the server, is from alive person and is not artificial or from a cadaver. The use of 3D feature information is considered to improve a systems' performance against the pose, expression variations, and the changing environmental conditions, such as the light and heat. And increases the complexity of the data set by incorporation of subtle variations, particularly in the facial images. Thus, making spoofing is extremely difficult.

H. **Our proposed scheme can support the user's anonymity:** If an attacker tries to eavesdrop on the user's login request, he can obtain nothing, since the login request only contains the encrypted user ID. Also if he tries to eavesdrop on the server's mobile agent, he cannot obtain the user's identity from the crypto hash function H ($\mathrm{E}_{UP}(\mathrm{Un})$) || H ($\mathrm{E}_{UP}(\mathrm{PW})$ from $S = \mathrm{E}_{UP}$ $(H$($\mathrm{E}_{UP}(\mathrm{Un})$) || H ($\mathrm{E}_{UP}(\mathrm{PW})$), OTP, K_S). Hence, it is impossible for an attacker to reveal the user's identity. Clearly, our proposed scheme can support the user's anonymity.

I. **Our proposed scheme can withstand the online and off-line guessing attacks:** In an online dictionary attack, the adversary tries the possible passwords by attempting to logging in to the server online. In an offline dictionary attack, the adversary eavesdrops on the communication channel to record the data for a successful protocol execution. The adversary then goes offline and tests the passwords against the recorded protocol execution data without contacting the server at all. In our proposed scheme, the username and password have never been sent to the server, and the user is authorized locally. Actually, there is no user's credential exists. The person ,who wants to login into the system, has to be a legal user, since he sends his user ID to the cloud server who extracts the user's credential and concatenates together, and sends this as a challenge/response. So our schema prevents the online guessing attack. If an attacker can eavesdrop on the communication channel, he can get M4= E_{SP}(user ID), which doesn't contain a user identity information. Furthermore; if he can get the mobile agent, and analyze it, he can get S = E_{UP} (H(E_{UP}(Un)) || H(E_{UP}(PW)), OTP, K_S), which is encrypted twice and hashed once. So it is impossible to be guessed by the off-line guessing attack. For that, our proposed scheme resists the off-line attack.

9. Conclusion and Future Work:

In this paper, an efficient user authentication scheme was proposed according to the challenging issues during the user authentication and access control process in the cloud computing environments. The main idea in our schema is to destroy any refers that lead to discover the user's credential. The user has never exchanged his credential with the cloud server, and hence, he keeps his credential in his mind. Authenticating process is done locally in the user's machine. So the user is the only one who knows his username and password. We take into consideration the needs for both the clients and the cloud service provider. We combine between the realism and security needs as seen as possible. An ElGamal elliptic curve cryptography was used to encrypt the registration phase and the first factor of the transactions between the user and cloud server. The 3D face image is introduced to be the second factor of the authentication. The advantage of using the mobile agent is taken in our proposed work to save the bandwidth and computation, especially when dealing with encrypted and hashed messages. The proposed framework provides a feasible and efficient solution by combining the traditional user's ID and password-based authentication with the biometric-based authentication. It designs a secure authentication system which can resist many types of attacks. In the future work, we plan to implement our proposed solution and make the performance analysis comparing with other schemas.

References:

[1] Verma, J. K., and Katti, C. P. Study of Cloud Computing and its Issues A Review. *Smart Computing Review, **4(5)***, (2014) 389-410.

[2] Bhushan, B. L., and Tiwari, R. A Comprehensive Study on Cloud Computing. *International Journal of Advanced Research in Computer Science and Software Engineering, **2(9)***, (2012) 33-37.

[3] Djenna, A., and Batouche, M. Security Problems in Cloud Infrastructure. *Networks, Computers and Communications, International Symposium on*, Hammamet, IEEE, (17-19 June 2014) 1-6.

[4] Jouini, M., and Ben Arfa Rabai, L. Surveying and Analyzing Security Problems in Cloud Computing Environments. *Computational Intelligence and Security (CIS), Tenth International Conference on*, Kunming, IEEE, (15-16 Nov. 2014) 689-693.

[5] Tanimoto, S., Sato, R., Kato, K., Iwashita, M., Seki, Y., Sato, H., and Kanai, A. S. A Study of Risk Assessment Quantification in Cloud Computing. *Network-Based Information Systems (NBiS), 17th International Conference on*, Salerno, IEEE, (10-12 Sept. 2014) 426-431.

[6] *Cloud Sercurity Alliance*. Security Guidance For Critical Areas Of Focus in Cloud Computing (2011, November 11). Retrieved March 18, 2015, from: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

[7] Abd, S. K., Al-Haddad, S. A. R., Hashim, F., and Abdullah, A. A Review of Cloud Security Based on Cryptographic Mechanisms. *Biometrics and Security Technologies (ISBAST), International Symposium on*, Kuala Lumpur, IEEE, (26-27 Aug. 2014) 106-111.

[8] Cloud Security Alliance. The Notorious Nine Cloud Computing Top Threats in 2013 (2013, February). Retrieved March 18, 2015, from: https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf.

[9] Fotiou, N., Machas, A., Polyzos, G. C., and Xylomenos, G. Access control delegation for the Cloud. *Computer Communications Workshops (INFOCOM WKSHPS), IEEE Conference on*, Toronto, IEEE, (27 April 2014-2 May 2014) 13-18.

[10] Vitti, P., Santos, D., Westphall, C., Vieira, K. Current Issues in Cloud Computing Security and Management. *The Eighth International Conference on Emerging Security Information, Systems and Technologies - SECURWARE*, Lisbon, (16-20 Nov. 2014) 36-42.

[11] Naser, A., Zolkipli, M. F., Majid, M. A., and Anwar, S. Trusting Cloud Computing for Personal Files. *Information and Communication Technology Convergence (ICTC), International Conference on*, Busan, IEEE, (22-24 Oct. 2014) 488-489.

[12] Moghaddam, F., Ravan, R. R., Khodadadi, T., Javadianasl, Y., and Halalzadeh, A. SUAS: Scalable User Authentication Scheme for Secure Accessing to Cloud-Based Environments. *Computer Applications and Industrial Electronics (ISCAIE), IEEE Symposium on*, Penang, IEEE, (7-8 April 2014) 33-38.

[13] Grover, J., Shikha, and Sharma, M. Cloud Computing and Its Security Issues - A Review. *Computing, Communication and Networking Technologies (ICCCNT), International Conference on*, Hefei, IEEE, (11-13 July 2014) 1 - 5.

[14] Webopedia. *Flooding Attack*. Retrieved March 11, 2015. From: http://www.webopedia.com/TERM/F/Flooding.html.

[15] Wikipedia. Timing attack. Retrieved March 16, 2015. From: http://en.wikipedia.org/wiki/Timing_attack.

[16] Mxoli, A., Gerber, M., and Mostert-Phipps, N. Information Security Risk Measures for Cloud-based Personal Health Records. *Information Society (i-Society), International Conference on*, London, IEEE, (10-12 Nov. 2014) 187-193.

[17] Bertino, E., Samanthula, B. K, Security with Privacy- A Research Agenda. *Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), International Conference on*, Miami, IEEE, (22-25 Oct. 2014), 144 - 153.

[18] Mittal, D., Kaur, D., Aggarwal, A. Secure Data Mining in Cloud using Homomorphic Encryption. *Cloud Computing in Emerging Markets (CCEM), International Conference on*, Bangalore, IEEE, (15-17 Oct. 2014) 1-7.

[19] Mo, Z., Xiao, Q., Zhou, Y., and Chen, S. On Deletion of Outsourced Data in Cloud Computing. *Cloud Computing (CLOUD), 7th International Conference on*, Anchorage, IEEE, (June 27 2014-July 2 2014) 344-351.

[20] Jianbing, N., Yong, Y., Yi, M., and Qi, X. On the Security of an Efficient Dynamic Auditing Protocol in Cloud Storage. *Parallel and Distributed Systems, IEEE Transactions on*, ***25(10)***, (2014) 2760–2761.

[21] Goodrich, M., and Tamassia, R. *Introduction to Computer Security*. Addison Wesley, (2010).

[22] Fatemi, M., Gerayeli, S., Rouzbeh, Sohrab, Araghi, and Kohpayeh, S. A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments. *Region 10 Symposium*, Kuala Lumpur, IEEE,(14-16 April 2014) 508-513.

[23] Tang, H. B., Zhu, Z. J., Gao, Z. W., and Li, Y. A Secure Biometric-Based Authentication Scheme Using Smart Card. *Cyberspace Technology (CCT 2013), International Conference on* , Beijing China, IEEE, (23-23 Nov. 2013) 39 - 43.

[24] Kesavaraja, D., Sasireka, D., and Jeyabharath, D. Cloud Software as a Service with Iris Authentication. *Journal of Global Research in Computer Science*, ***1(2)***, (2010) 16-22,.

[25] Albahdal, A. A., and Boult, T. E. Problems and Promises of Using the Cloud and Biometrics. *11th International Conference on Information Technology: New Generations*, Las Vegas, IEEE, (7-9 April 2014) 293-300.

[26] Ma, Y., and Feng, J. Evaluating Usability of Three Authentication Methods in Web-Based Application. *Ninth International Conference on Software Engineering Research, Management and Applications*, Baltimore, IEEE, (10-12 Aug. 2011) 81-88.

[27] Yassin, A. A., Jin, H., Ibrahim, A., and Zou, D. Anonymous Password Authentication Scheme by Using Digital Signature and Fingerprint in Cloud Computing. *Cloud and Green Computing (CGC), Second International Conference on*, Xiangtan, IEEE, (1-3 Nov. 2012) 282-289.

[28] Kuo, C., Romanosky, S., and Cranor, L. Human Selection of Mnemonic Phrase-Based Passwords. *The second symposium on Usable privacy and security*, (2006) 67-78.

[29] Eljetlawi, A. M., and Ithnin, N. Graphical Password: Comprehensive Study of the Usability Features of the Recognition Base Graphical Password Methods. *Convergence and Hybrid Information Technology, ICCIT '08. Third International Conference on*, Busan, IEEE, (11-13 Nov. 2008) 1137-1143.

[30] Davis, D., Monrose, F., and Reiter, M. On User Choice in Graphical Password Schemes. *The 13th conference on USENIX Security Symposium*, Berkeley, *USENIX Security Symposium*, (2004) 151–164.

[31] Dahiya, k., and Kant, C. Biometrics Security Concerns. *Advanced Computing & Communication Technologies (ACCT), Second International Conference on*, Rohtak Haryana, IEEE, (7-8 Jan. 2012) 297-302.

[32] Shukla, R., Prakash, H. O., Bhushan, R. P., and Venkataraman, S. Sahastradhara: Biometric and Etoken Integrated Secure Email System. *Advanced Computing Technologies (ICACT), 15th International Conference on*, Rajampet, IEEE, (21-22 Sept. 2013) 1-4.

[33] Mohammed, M. M., and Elsadig, M. A Multi-layer of Multi Factors Authentication Model for Online Banking Services. *Computing, Electrical and Electronics Engineering (ICCEEE), International Conference on*, Khartoum, IEEE, (26-28 Aug. 2013) 220-224.

[34] Bhattasali, T., and Saeed, K. Two Factor Remote Authentication in Healthcare. *Advances in Computing,*

Communications and Informatics (ICACCI, International Conference on , New Delhi, IEEE, (24-27 Sept. 2014), 380-386.

[35] Haqani, H., Saleem, M., Banday, S. A., and Khan, A. R. Biometric Verified Access Control of Critical Data on a Cloud. *International Conference on Communication and Signal Processing*, India, IEEE, (3-5 April 2014), 981- 984.

[36] Gunasekaran, K., and Mahalakshmi, P. Implementation of Multimodal Biometric Authentication Using Soft Computing Techniques. *Information Communication and Embedded Systems (ICICES),International Conference on* , Chennai, IEEE, (27-28 Feb. 2014) 1-6.

[37] Chenguang, W., and Huaizhi, Y. Study of Cloud Computing Security Based on Private Face Recognition. *Computational Intelligence and Software Engineering (CiSE), International Conference on*, Wuhan, IEEE, (10-12 Dec. 2010) 1-5.

[38] Zhu, H. H., Qian-Hua, H., Tang, H., and Cao, W. H. Voiceprint Biometric Template Design and Authentication Based on Cloud Computing Security. *International Conference on Cloud and Service Computing*, Hong Kong, IEEE, (12-14 Dec. 2011) 302–308.

[39] Joshi, V., and Sanghavi, P. Three Tier Data Storage Security in Cloud Using Face Fuzzy Vault. *Computing, Communication and Applications (ICCCA), International Conference on*, Dindigul Tamilnadu, IEEE, (22-24 Feb. 2012) 1-6.

[40] Soyjaudah, K. M. S., Ramsawock, G., and Khodabacchus, M. Y. Cloud Computing Authentication using Cancellable Biometrics. *Browse Conference Publications, AFRICON*, Pointe-Aux-Piments, IEEE, (9-12 Sept. 2013) 1-4.

[41] Sabri, H. M., Ghany, K. K. A., Hefny, H. A., and Elkhameesy, N. Biometrics Template Security on Cloud Computing. *Advances in Computing, Communications and Informatics (ICACCI, International Conference on*, New Delhi , IEEE, (24-27 Sept. 2014) 672-676.

[42] Sadkan, S. B., and Abdulraheem, F. H. An Analytical Study for Security Evaluation of Cryptosystems used in Cloud Networking. *The First International Conference of Electrical, Communication, Computer, Power and Control Engineering ICECCPCE*, Mosul, IEEE, (17-18 Dec. 2013) 157-162.

[43] Sadkan, S.B., and Abdulraheem, F.H. Efficient Implementation of Elliptic Curve Cryptography Using Low-power Digital Signal Processor. *Advanced Communication Technology (ICACT), The 12th International Conference on*, Phoenix Park, IEEE, (17-18 Dec. 2013) 157-162.

[44] Minfeng, F., and Wei, Ch. Elliptic Curve Cryptosystem EIGamal Encryption and Transmission Scheme. *Computer Application and System Modeling (ICCASM), International Conference on*, Taiyuan, IEEE, (22-24 Oct. 2010) V6-51 - V6-53.

[45] [45] Sodiya, A.S., Onashoga, S.A., and Adelani, D.I. A Secure E-voting Architecture. *Information Technology: New Generations (ITNG), Eighth International Conference on*, Las Vegas, NV, IEEE, (11-13 April 2011) 342-347.

[46] Boruah, D., and Saikia, M. Implementation of ElGamal Elliptic Curve Cryptography Over Prime Field Using C. *Information Communication and Embedded Systems (ICICES), International Conference on*, Chennai, IEEE, (27-28 Feb. 2014) 1-7.

[47] Abate, A., Nappi, M., Riccio, D., and Sabatino, G. 2D and 3D Face Recognition: A Survey. *Elsevier*, ***28(14)***, (2007) 1885–1906.

[48] Khadhraoui, T., Benzarti, F., and Amiri, H. New Approach on PCA-based 3D Face Recognition and Authentication. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, Las Vegas, IEEE, (30 June 2014-2 July 2014) 1-5.