VOL. 14, NO. 10, MAY 2019 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

LITERATURE REVIEW OF AUTHENTICATION LAYER FOR PUBLIC CLOUD COMPUTING: A META-ANALYSIS

Abdalla Eldow[1], Mohanaad Shakir[2], Mohammed Ahmed Talab[3] and Ahmed Kh. Muttar[4]
[1]Department of Information Technology, Al Buraimi University College, Oman
[2]College of Computer and Information Technology, University Tenaga National, Malaysia
[3]Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang, Malaysia
[4]Applied Science University, College of Administrative Sciences, Bahrain
E-Mail: abdalla@buc.edu.om

ABSTRACT

Cloud computing is a rapidly growing technology due to its highly flexible uses and applications. It also has other features such as simplicity, quick data access and reduced data storage costs. Consequently, it has been widely used by many organizations. This widespread use of cloud computing among organizations causes many security issues. Moreover, cloud computing layers are likely to be jeopardized by many security risks such as privileged user access, data location, data segregation, and data recovery. This paper aims to prepare an ample debate of a literature review-based studies that provided important insights to researchers in the scope of security cloud computing. The researcher applied a relevant set of keywords. These keywords are limited to the title, abstract and keywords search archives published between 2010 and June 2018. The database search returned a total of 308 publications. In addition, we conducted backward-forward searches from the reference lists of relevant, quality previous works on the security framework in public cloud computing studies. Then, the researcher filtered the publications to only full text access articles that were written in English only. Finally, this study obtained a many publication. The findings of this paper address many important points such as in this study is recommended to apply behavior recognition with password for improving authentication layer performance in cloud computing. This study finds most of current studies neglected the present of human factor in password-based authentication, and learnability in password-based authentication is highly weak. Despite this, very few studies have adopted the behavior recognition with password in public cloud.

Keywords: authentication, public cloud computing, security in cloud computing, password-based authentication.

1. INTRODUCTION

Cloud computing is a rather new computing model. Its main advantages lie in its upgraded hardware power efficiency and resource use. At the same time, it gives users the opportunity for universal access and the privilege to pay only for the services they receive. It has been defined in multiple ways due to its relatively young history. However, in the current study, we will abide by NIST's thorough definition, which states that cloud computing is "a model for enabling convenient, on-demand network access to a shared of pool configurable computing resources (including networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1]. The essence of cloud computing extends to a wide range of information, software, and resources that are made available to consumers through their very own browsers. The deployment model is a one of cloud computing services, it is consist of three types Public, Private, and Hybrid [1].

This paper presents the current authentication framework in public cloud computing. Multi-factor authentication is considered as a top of authentication methods in public cloud computing [2]. This paper aims to discover the main multifactor authentication methods and pointed drawbacks in current multifactor authentication methods. This paper has six sections. This section introduces the literature work paper. Section2 covers the top general topic in the field of study through defines the security and privacy specifications in public cloud computing, for narrow down according to the top of security concerning in this area. Section 3 defines the authentication in public cloud computing, and it draws the path of the research from the top surface to our research field. Section 4 covers the current related works (description and critical analysis) for determining the main drawbacks points in current multifactor authentication. Section 5 covers the results, which is including meta-analysis on this paper related works by determining the main research questions. 6. The last section shadow light on the main knowledge which is conclude in this paper according to the answer of research question.

2. AUTHENTICATION IN PUBLIC CLOUD

User authentication in public cloud computing is the process of validating the identity of the user to ensure that the user is legitimate to access public cloud resources [19]. Authentication as a critical aspect of security enforcement approaches in public cloud computing is essential to protect users against existing security and privacy issues by preventing unauthorized access to the public cloud user information [20] [21]. According to Correlation Matrix of Latent Variables (Security Risk Construct) in page 68, the author conducted study to assessment the risk in public cloud computing. The result of this study is considered the diagnosis the authorized user for access in to cloud as a top concerning among group of security risk in cloud computing [22]. The purpose of authentication layer in cloud computing is diagnosing an authorized user and grant him authority to

access into data which saved in cloud computing. Authentication in public cloud computing (PCC) is classified into six types Username and Password Authentication (password-based Authentication), Multifactor Authentication, Mobile Trusted, Single Sign On, Public Key Infrastructure, and Biometric Authentication. Despite the growing number of innovative ways to authenticate users, password-based authentication is still one of the most popular methods of all [23].

3. PASSWORD-BASED AUTHENTICATION

Passwords-based authentication can easily be memorized and users at no cost are able to use them in their daily life [23]. In contrast, not only do personal computer users witness an annual increase in motivated cyber-attacks from different unknown directions but also governmental computers such as parliamentary computers of Australian federal ministers and many other examples were reportedly compromised [29]. In this respect, a number of authentication systems which are recognizable in today security engineering are susceptible to some attacks such as denial-of-service, replay, and deception attacks [30]. Traditional password-based authentications have several problems, in Campbell and Bryant research, they found that a personal computer can guess approximately 80% of common passwords in a week [31]. This task subsequently became harder by combining different symbols in a passphrase. Florencio and Herley, conducted a study to understand users' habits in the web-based environment; they found out that nearly half a million users showed a tendency to only use the lower-case password [32]. Moreover, password strength was higher on websites such as Microsoft and PayPal in comparison with that of New York Times' which has fewer rules to mandate password. Similarly, Cazier and Medlin analyzed a dataset of 500 people's password from an E-business website. They found that the cracking time of 60 percent of users could be done less than 10 h and just 38 percent of them took longer than 10 h. The majority of the passwords that could be cracked less than one hour were simply a mix of alpha or alphanumeric characters and only 0.8 percent of the passwords could not be cracked due to the utilization of special symbols and alphanumeric characters [33]. The password-based authentication threats are listed in Table-1 below [34].

Table-1. Password-based Authentication Threats.

Password-based Authentication Threat/Attack	Description	Examples
Duplication	The subscriber's authenticator has been copied with or without their knowledge.	Passwords written on paper are disclosed. Passwords stored in an electronic file are copied.
Eavesdropping	The authenticator secret or authenticator output is revealed to the attacker as the subscriber is authenticating.	A hashed password is obtained and used by an attacker for another authentication (pass-the-hash attack).
Offline Cracking	The authenticator is exposed using analytical methods outside the authentication mechanism.	A software PKI authenticator is subjected to dictionary attack to identify the correct password to use to decrypt the private key.
Phishing or Pharming	The authenticator output is captured by fooling the subscriber into thinking the attacker is a verifier or RP.	A password is revealed by subscriber to a website impersonating the verifier.
Social Engineering	The attacker establishes a level of trust with a subscriber in order to convince the subscriber to reveal their authenticator secret or authenticator output.	A memorized secret is revealed by the subscriber to an officemate asking for the password on behalf of the subscriber's boss.
Online Guessing	The attacker connects to the verifier online and attempts to guess a valid authenticator output in the context of that verifier.	Online dictionary attacks are used to guess memorized secrets.
Stolen password [35]	The attacker stealing the active password manually	Brute Force Attacks; Spidering; Keyloggers; Shoulder Surfing [36].
Impersonation Attacks [37]	The attacker tries to login as an authorized user	Business Email Compromise (BEC) or "CEO fraud" that continues to manipulate companies by using false identities. This can severely damage a company's reputation. This blog from last year explains BEC in detail.
Man-In-The-Middle (MITM) [38]	Man-in-the-middle attacks are a common type of cybersecurity attack that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation they should normally not be able to listen to, hence the name "man-in-the-middle."	IP spoofing DNS spoofing HTTPS spoofing SSL hijacking Email hijacking Wi-Fi eavesdropping Stealing browser cookies

According to what have been declared as password weaknesses, many Identity and context-based authentications such as Two factor authentication and Multi-factor authentication method are aiming at enhancing the security of different applications and websites has become more popular [39] [40] .

4. MULTI-FACTOR AUTHENTICATION (MFA)

To make information more secure in cloud computing environment, a combination of authentication techniques needs to be used. This scheme is more secure because it does not just validate the username and password pair but also requires another factor e.g. biometric authentication. It is one of the stronger authentication techniques. Actually, the expectation of authenticity rises exponentially when additional factors are involved in the process of verification. For cloud computing environment, a multifactor biometric authentication system was proposed that includes finger print and palm vein [41]. The aim is to handle the biometric data in a protected fashion by keeping the data of fingerprint in the central database of the cloud security server and the biometric data of palm vein in multi-component smart cards. Typical MFA scenarios include [42]:

a) Security tokens (Hardware) in the form of smart cards or small devices with USB technology (password + smart card).

b) Security tokens (Software) that generate a single-use login PIN has device-based possession factor. For example, Google Authenticator (password + pin).

c) Mobile authentication such as SMS or calls for one-time password (password+ SMS).

d) Biometric authentication methods such as fingerprint, facial recognition uses Inherence factor. For example, Dell Defender (password+ Face, Voice, Fingerprint).

A. Password with smart card

In this method, the authentication performance is works according to two factors Password and smart card. Some more recent smart card based password authentication schemes have also been proposed in [43] [44] [45] [46]. Shoup-Rubin [47] proposed extension of Bellare-Rogaway model which is based on three-part key distribution protocol. Smartcard is used to store the long-term secret key and it is assumed that the smartcard is never compromised. Therefore, the scheme falls in one factor category as two factor schemes can be broken by compromising both the factors only. Liao *et al*. [44] [43] tried to consolidate a number of passwords and smartcard based properties and proposed two factor smartcard and password authentication scheme, which is still vulnerable to many attacks such as offline guessing attack, stolen password attack and impersonation [44] [48]. The limitations of this method are present below [49]:

a) Users must be educated in their use;

b) Cards along with any assigned PINs must be issued and tracked;

c) Can be lost, stolen, or shared;

d) Must be kept close at hand;

e) Cause some problems for users who forget their PINs or make typographical errors;

f) Not very robust and can be easily broken.

B. Password with SMS

Code generation apps are a worthy alternative to SMS codes. The most common among such applications is the Google two factor authentication solution - Google Authenticator. Such software One-Time Password (OTP) tokens generate codes independently based on a particular algorithm or random sequence. The main algorithms for generating such one-time codes are the HOTP (hash-based one-time password, RFC4226), TOTP (time-based one-time password, RFC6238) and OCRA (OATH challenge-response algorithm, RFC6287) that were developed and are supported by the OATH (Initiative for Open Authentication) [50]. The limitations of this method are listed below:

a) Expensive (need to use a smartphone or other similar device);

b) Application can be hacked;

c) Smartphone battery can discharge;

d) If the smartphone is factory reset or lost, or authenticator application is deleted accidentally, the token would be lost and its recovery is a great pain.

C. Password with biometrics

Facial recognition, voice recognition, and fingerprint scans all fall under the category of biometrics. Systems use biometric authentication when it's imperative that you really are who you say you are, often in areas that require security clearance (e.g. the government). The biggest downside, and the reason why biometrics are rarely used as a two-factor method, is that a listed below:

a) you can't change your password (if compromised)

b) Expensive (Extremely high cost of implementation and deployment);

c) Forgery method

d) Man In The Medial (MITM) attack;

e) Accuracy issue

f) Surgery and scars

g) To date, the risk of inaccurate recognition is still quite high (meaning that the system can deny access due to an erroneous determination of the user's biometric parameters). For example, the pattern of the fingers can easily be damaged by common cuts; in addition, there is a category of people - with features of temperature and body moisture - for which it is very difficult to take the print.

5. MULTI-FACTOR AUTHENTICATION FRAMEWORK IN PUBLIC CLOUD COMPUTING

To access cloud services over the Internet, it is necessary for a user to enroll himself with the Cloud Service Provider (CSP). After enrolment, the end user can access any service remotely over the Web. Usually, CSP stores the secret information in the Key Distribution Center (KDC), where a single point of comptonization makes the whole system jeopardized, and it is also vulnerable to on/offline dictionary attack. For example, existing approaches [51] [52] [53] enroll an end user by asking his "username" and password. This username is used as the primary credential, which is verified at the time of user authentication. In fact, selecting a "username" is not enough to be considered as a strong private entity. As a result, an adversary can easily incorporate different attacks, such as impersonation attack and identity comptonization attack by sniffing the "username" from the insecure media. Moreover, the existing password-based enrolment strategy is vulnerable to password guessing (dictionary) attack, stolen-verifier attack and so on. Additionally, the existing approaches [51] [54] derive client's secret key as the hash value of its password.

Therefore, the key will remain same until client changes the current password. However, changing this password needs updating in enrolled data maintained by the KDC and this, in fact, invites many key rollover problems [55].

In [56], Chang and Wu proposed a remote password authentication scheme with a smart card based on the Chinese Remainder Theorem (CRT). The scheme does not need to store verification table and is secure against attacks of replaying previously intercepted requests. However, the user's password of this scheme cannot be chosen and changed freely by the owner. A similar problem also occurs in some schemes proposed by [57] [58] [59]. Chan *et al*. [60] 2003 and Shen *et al*. [58], respectively, further pointed out that Hwang et al.'s scheme[57] is insecure. In [61], Yamaguchi et al. proposed a simple but efficient authentication system, SPLICE/AS. Later, Hwang *et al.* pointed out that SPLICE/AS system is vulnerable to the guessing attack [62]. In [63], Wu proposed an efficient scheme based on the geometric Euclidean plane. The merits of this scheme are its simplicity of geometry and the property that users can freely choose their own passwords. However, the scheme is insecure as indicated in [64]. In [65], Jan and Chen proposed a new scheme without verification table. Users can freely choose and change their own passwords in the scheme. However, the scheme is not efficient because it uses the public key cryptosystem. The computational cost is very high. In [66], Yang and Shieh proposed two methods to prevent replay attack. Their schemes do not store passwords or verification tables in the server, and let users freely change their own passwords. However, two papers [67] [68] pointed out that Yang and Shieh's schemes have a drawback in that an intruder is able to impersonate a legal user by constructing a valid login request from an intercepted login request. Therefore, Yang and Shieh's schemes cannot prevent modification attack. Hwang *et al.* [69]and Chien *et al*. [43] proposed an efficient and practical smart-card-based schemes based on secure one-way hash function. In those schemes, the authors claimed that their schemes can achieve the following characteristics: (1) the verification or password tables are not required in the server; (2) the communication cost and the computational cost is very low; (3) the replay attack problem is completely solved; and (4) users can freely choose their passwords. However, in [13], their scheme cannot achieve mutual authentication. And in [43], their scheme did not let users freely change their passwords.

Chow in [70] proposed an authentication method known as Trust Cube [71] by integrating the implicit authentication [72] to perform mobile client authentication(both the initial method and extended method feature common name of Trust Cube). Trust Cube is a cloud-based authentication solution that is policy-based and utilizes an open standard. It also supports the combination of different authentication methods for the sake of robustness and adaptability. The policy-based authentication has several unique advantages such as the utilization of policies that are user-specific and finely grained, which can be immediately updated according to users' preferences. In addition, TrustCube uses a framework with federated authentication, more similar to the OpenID; the algorithms of the implicit authentication are not specified, and the top-level system description is provided. This system is developed with an implicit authentication, which utilizes mobile data such as SMS messages, calling logs, location, and website accesses, in the current public cloud environment. The public cloud constraints in input requirements make using complicated passwords more difficult, and this leads to select short passwords and PINs, which has the higher rates of security risks such as stolen password and impersonation attacks [37] [35].

Grzonkowski *et al*. [73] proposed the SeDiCi 2.0 protocol, which is another form of Zero Knowledge Proof (ZKP) technique. This technique provides mutual authentications, which are supposed to be more secure when it comes to phishing attack as compared to the present system of using third party protocols. SeDiCi 2.0 is part of the protocol known as the TTP (Third Trusted Party) protocol, which uses the ZKP technique. The main goal is to provide an improved solution for phishing attempts by offering mutual authentication, where users do not have to disclose their passwords at each of the websites that they visit. The user runs his authentication on the browser that domain is controlled Third Trusted Party (TTP), and can login to the system if the name of a service is on the trusted list. There are three parties that are participating in the protocol, including Service (S), Authentication Service (AS), and Client (C). The client communicates with both authentication and consumer services to start authentication procedure. The same policy of typical web-browsers is applied in the case of using web-based applications. In SeDiCi 2.0 protocol, a plug-in-based implementation is utilized to allow the application to bypass the browsers' policy. The URI or other identifiers is required to find user location. The URI has two useful characteristics; it contains authentication service and user name, and it is also globally unique. Furthermore, the users are required to have control over the authentication domain, which can be considered as a second factor for authentication [74]. The user never type password at his visited websites, which is the only revealed information in login step. On the other hand, if malicious servers obtain the login information, the adversary will attack the user. One of the SeDiCi 2.0 protocol advantages is that the physical token is not required. Nonetheless, a plug-in is required in the case of utilizing the user browser, which overwrites the standard websites' security mechanisms because a web-browser communicates with external services in this way.

Hao *et al*. [75] presented a time-bound ticket-based mutual authentication scheme for cloud computing. The purpose of using the time bound tickets is to reduce the performance degradation.The proposed authentication scheme achieves mutual authentication between the server and the client. The use of timebound tickets reduces the server's processing overhead efficiently. The correspondence relationship between the digital ticket and the client's smart card prevents user masquerade attack

effectively. Unfortunately, Jaid- har [76] identified that Hao *et al*.'s scheme is insecure against denial-of-service attack during the password change phase and impersonation attacks[77]. Wazid *et al*. [78] also proposed a provably secure user authentication and key agreement scheme for cloud computing environment. Their scheme resists the weaknesses of the existing schemes and it also supports extra functionality features, such as user anonymity, and efficient password and biometric update phase in multi-server environment. The greatest disadvantages of this scheme are invasion of privacy, costs of implementation, need long time, surgery can be problematic and influence the accuracy of the system [79] [80].

Omri *et al* [81], proposed to use user handwriting as an authentication factor to access the cloud securely. The mobile user writes his password manually using his smartphone touch screen and sends the image to cloud server to be check the validity of password. There are two criteria to check authentication of users, first the unique handwriting of the user and the second is the password. In the proposed method, the connection between the cloud and the mobile phone is established by a Hadoop server. The uniqueness of biometrics features is useful beneficial in improving the security of different authentication methods; however, some usability and privacy issues are risen by using of these features. However, some usability and privacy issues are risen by using of these features. Moreover, the privacy risk for handwriting is lower than other biometrics; however, the accuracy of using handwriting is low as well. It is recommended that low accuracy authentication metrics such as handwriting can be applied to other methods such as using ID and Password together, if hand writing authentication fails, the system can ask for other methods.

Le in [82], proposed an authentication method called NemoAuth based on the mnemonic multimodal approach. NemoAuth utilizes different mobile device sensors such as gyroscopic, gravity, orientation, proximity, pressure, ambient light, temperature, touch screen, and moisture sensors as well as other facilities such as microphone and camera to measure and extract the biometric features of mobile device user. In general, the dynamic knowledge and biometric based approaches are combined to improve accuracy of authentication method in NemoAuth. The procedure of NemoAuth is similar to biometric based methods that predefines and trains user's signature profile during system setup step. The user's signature includes a set of multimodal signatures, and each signature is composed of a set of mnemonic and atomic motions. The atomic actions that associate with the mnemonics help users to memorize the secret keys more conveniently. There are varied types of atomic actions that can be utilized according to types of mobile device sensors. As an example, the set of atomic actions for touch screen can be taped, line, hold, circle, and cross, and a mobile user can use a fingertip to tap at specific position or hold the fingertip for certain duration on the mobile screen that shows the mnemonic image. The mnemonic image is composed of 16 elements, and each element is located at a determined position of the mobile screen. There is no need to remember the position of image that user wants to tap or hold for certain duration of time, because the user can just remember the memorized elements of mnemonic image. Furthermore, the user can select desirable signature profile according to preferable level of security and usability. In addition, each signature profile consists of a set of duple that shows the kind of authentication method and the trigger time. The user can set signature profile to use different authentication methods in the different period of the day; for example, the mobile device can automatically enable voice signature during non-bed time and GPS authentication at home. The main objective of the Nemo Auth is to utilize different capabilities of the mobile device to improve the usability of authentication by using mnemonic images. However, this method simplifies remembering a password for users and provides different options according to mobile device capacities, but the performance and accuracy of authentication are in question because the performance metrics such as False-Acceptance Rate (FAR), False-Rejection Rate (FRR), Relative Operating Characteristic (ROC), and Crossover Error Rate (CER) are not evaluated in this study. Furthermore, applying a multi-modal method needs enough processing and storage power that can be provided by the cloud server; however, the framework to transfer these intensive processing steps is not provided. The suitable algorithm to transfer intensive processing phases to cloud can be designed to improve performance.

Dey *et al*. [83] proposed an authentication scheme using message digest (MD) called MDA. This method is designed based on existing mobile device hardware and platforms to protect mobile user against different potential security attacks. The vulnerability of the system is computed by vulnerability score, Sv, which is a measure of the number of attacks that the method can prevent. The Sv is calculated according to the following equation:

$$Sv = (N\ success)/ (N)$$

where N is the number of attacks that are launched on the authentication method, and Nsuccess is the number of recorded successful attacks. The amount of Sv is between 0.0 and 1.0. Mutual authentication is an important security countermeasure that is considered in this method. The procedure of this method includes two phases; in the first phase, cloud server checks mobile user authentication and subsequently the mobile device verifies authenticity of the cloud in the second phase. The user has two message digests, MDcloud and MDuser that are used to create MD. The password is hashed and XORed by user ID, to protect user from an attacker during authentication. The Pseudo Random Number Generator (PRNG) is an algorithm to generate random number using seed and State Identifier (SI). The mobile node sends ♯C‖ETk {Eauth_keyi{MD} ‖SI} to the cloud server. In this message, ♯CF is a column reference of stored mobile user and Eauth_keyi is the nth sequence of bits, which are generated by PRNG. The ETk is calculated by XOR-ing hashed user password and user ID. The cloud server checks user authentication after

receiving mobile device authentication request message. Firstly, the cloud server checks ♯CF, to find user ID and hashed password. Then, it generates Tk to decrypt the received message from the mobile device. After decrypting the message, the cloud server obtains MD, and compares both message digests to check user authenticity. The authenticity of the mobile device is verified only if MD and MDn messages is match. Once the mobile user is authenticated to the cloud server, the procedure of cloud server authentication will be initiated. The cloud server sends its digital signature that is encrypted by its private key, Pkpriv_cloud, to the mobile device. The mobile device decrypts the cloud server message to check the authenticity of the cloud server. If the MD matches with mobile device MD, then the cloud server is authenticated. In MDA method, a secure authentication scheme based on message digest is proposed. Furthermore, most of security and privacy criteria that must be achieved to propose a suitable authentication algorithm are applied. One of the important security criteria is mutual authentication that is achieved in this method by authenticating both mobile device and the cloud server together. Furthermore, user privacy is preserved by hashing user ID and Password. Nevertheless, the security and privacy of this method are protected compared to other methods, but the procedure of this authentication scheme is somehow complicated. Additionally, it is recommended to transfer some processing steps that are processed in the mobile device, to the cloud server to improve the performance of the scheme, however, doing such kind of improvement will be more complicated.

Banyal *et al.* [84] In this study the authors suggested multi-factor authentication consists of three layers key entities and Key Approaches Used. Authentication according secret key. The algorithm of this framework is consisted from Registration phase, Login Phase, Authentication Phase, Change Authentication, and Secret Phase Change. The main drawback in this framework is user should memorized complicated password [85], and the Processing several patterns such as SMS activities, calling pattern, and location, needs many computation power, make the authentication procedure more complicated. In addition, it needs many devices such as PC, Smart phone, and server that lead to framework process be highly cost. Finally, this framework is vulnerable to impersonation attack [86].

Yang and Lin [87] proposed ID-based user authentication scheme in a cloud environment. The proposed scheme is consisting of three rules: the user, the server, and the ID provider. The authentication procedure under ID provider responsibility. This scheme is classified into two phases: registration phases and mutual authentication phases. However, Chen *et al.* [88] pointed out the security pitfalls in Yang *et al.*'s scheme [87]that it is vulnerable to insider and impersonation attacks. To with stand these security loopholes in Yang et al.'s scheme, Chen et al. then designed a dynamic ID-based authentication scheme for cloud computing environment, which is based on the elliptic curve cryptography (ECC). Wang *et al.* reviewed Chen et al.'s scheme, and proved that their scheme is vulnerable to offline password guessing as well as impersonation attacks. In addition, it was found that Chen et al.'s scheme does not provide user anonymity and it also has clock synchronization problem [88].

Cindhamani *et al.* [89] This study is proposed security framework consist of two stages: 1) How securely we storing the data? and 2) How securely we retrieving the data by using encryption algorithm. The authentication in this algorithm checks by send the password to owner with security question. The main downside in this framework is user should memorize some secrets makes the procedure more difficult, and using both password and secret question makes procedure more difficult for the users [85]. In addition, processing several parameters such as ID/password, IMEI, IMSI, voice and face recognition, make the authentication procedure more complicated, highly cost, surgery can be problematic and influence the accuracy of the system [79].

Zhang *et al.* [90] proposed an authentication algorithm based on finger print. In this method, the finger print image is captured by existing mobile device camera, which does not need to implement sensors in the mobile device. The whole process of capturing and matching finger print is hosted on the cloud server to take all benefits from cloud. The main idea of this method is alike to other normal finger recognition methods that use mobile device camera to capture fingerprint. The procedure is initiated with the capturing fingerprint image to be processed on the cloud server. After capturing, the preprocessing of the image is applied to convert RGB to gray-scale image and other steps such as reducing the blur effect, ridge enhancement, and segmentation are completed. This preprocessed image is sent to feature extraction phase, and in the final phase, the server checks the similarity of the extracted features to store information of user fingerprint. The privacy issues of using biometrics introduce the requirement of applying privacy preserving approaches. In a similar situation, some cryptographic algorithms should be applied to the captured image by the mobile device before sending it to the cloud server, however, the fingerprint image is sent in plain text in this method. Furthermore, the details of utilizing MCC processing and storage resources are not clearly explained in this approach, and the fit utilization framework for MCC is advised to be designed. In the other word, the adapt ability to MCC is not clearly defined in this method. In addition, the accuracy of finger print that is captured by mobile device camera is lower than using sensors to capture the finger print images; therefore, it is recommended to add other authentication factors such as using ID and Password to this method.

V. Chang *et al.* [91] This study is proposed a security framework for business cloud computing under the name cloud computing adoption framework (CCAF), which includes three layers. Firstly, tasks for layer 1 are password protection, network, and IP-based firewall and access control. Secondly, tasks for layer 2 are out-of-band authentication and openID serving for identity management. Finally, tasks for layer 3 encryption and

decryption for authentication file. The insufficiency of this framework is memorizing some secrets makes the procedure more difficult for a user. In addition, several authentication factors are utilized for user authentication, which increases the authentication procedure time. This framework is vulnerable to impersonation and stolen password attacks [37] [35].

Gope and Das [92] proposed an anonymous mutual authentication scheme for ubiquitous mobile cloud computing services, in which allows a legitimate mobile cloud user to enjoy *n* times all the ubiquitous services in a secure and efficient way, where the value of *n* may differ based on the principal he/she has paid for. In addition, Odelu *et al.* [93] reviewed Tsai- Lo's scheme [94] and pointed out that their scheme does not provide the session-key security and also strong user credentials' privacy. To remove the security weaknesses found in Tsai-Lo's scheme, Odelu *et al*. designed a provably secure authentication scheme for distributed mobile cloud computing services. According to the current practice, a user makes an authentication request to an authentication server (*AS*) by means of a plain text containing "username"[51]. In this context, an attacker can eavesdrop the "username" and later expose himself to the *AS* as a legitimate user. In other word, an attacker can easily determine from the transmitted message that which users are currently online. In this situation, an attacker has scope to make man-in- the-middle attack as well as replay attack [95]. Further, an eavesdropper can make identity comptonization attack and impersonation attack by stealing the "username" if the channel is insecure [96] [97]. Moreover, the *AS* issues an authentication ticket (AT) to an end user after verifying only its "username" without verifying user's password or other security credentials [96]. However, as "username" is not a confidential credential, there is an opportunity for an attacker to get multiple authentication tickets by simply sending a "username" to the (*AS)*. As a consequence, a cryptanalyst can decrypt the ciphertexts (i.e., ATs) using some knowledge about underlying user's password. Thus, this scheme is vulnerable to Ciphertext-only Attack (COA). In spite of this, in the existing authentication approaches [51] [98] [99], a user blindly trusts the authentication server (*AS*) or the service server (*SS*) (more precisely the so called trusted third party) without verifying any cross parameters (e.g., message authentication code, server-side generated one-way hash chain based onetime identifier [100], etc.) after receiving the authentication ticket or service ticket. To the best of our knowledge, there is no solution to verify the originality of *AS* or *SS* except the timestamp and visualization of password or session key protected authentication ticket or service ticket [51] [101]. Hence, this shortcoming opens a possibility of byzantine attack [102], where a compromised principle can falsify the primitive operations on the authentication system. In order to ensure mutual authentication and session key distribution between two parties, several solutions have been proposed in the literature. For example, in possession based (also called token based) approach, a trusted server distributes a token with a number of authentication parameters, that is, more parameters are included into the constitution of an authentication token (AT) and authorization token or service token (ST). Hence, AT and ST verification increases the overhead to the existing authorization server and service server, respectively. In addition to this, tokens and session keys are stored into user's credential cache [103] [96] in the respective workstation, and each token has its own lifetime. So, it leads to workstation comptonization attack, disclosure of session key as well as misuse of tokens. Moreover, an end user blindly accepts the services of the server (i.e., KDC's *AS*) without checking the authenticity of the server. Therefore, if the server is compromised, a byzantine attack can be induced into the system which ca n falsify its primitive operations and it can also lead to the wrong desires. Nonetheless, some mutual authentication schemes use time synchronization for joint authentication between end user and the service servers [104] [105]. The summarize of multifactor authentication as shown as in Table-2 below.

Table-2. Summarize of Multifactor Authentication.

Scheme	Threats	Cons
Chen *et al.*'[88]	1. Impersonation attacks; 2. Stolen password attack; 3. Offline password guessing.	Scheme does not provide user anonymity and it also has clock synchronization problem
Chow *et al.* [70] Song *et al.* [71] V. Chang *et al.* [91]	1. Stolen password attack; 2. Impersonation attack	- Memorizing some secrets makes the procedure more difficult for a use; Several authentication factors are utilized for user authentication, which increases the authentication procedure time
Cindhamani *et al.* [89]	1. Stolen password attack; Impersonation attack	- User should memorize some secrets makes the procedure more difficult; - Using both password and secret question makes procedure more difficult for the users - Processing several parameters such as ID/password, IMEI, IMSI, voice and face recognition, make the authentication procedure more complicated; Highly cost, surgery can be problematic and influence the accuracy of the system
Omri *et al.* [81]	1. MITM attack; 2. Replay attack	- Handwriting pattern is the error-prone method as the mobile user may write the same digits in different styles - The accuracy of using handwriting is low; - Need more hardware - Highly cost - Suitable for mobile cloud rather than others Surgery and scars
Rassan *et al.* [90]	1. MITM attack; Replay attack	- The accuracy of finger print that is captured by mobile device camera, is lower than using sensors to capture the finger print images - The mobile device processes resource intensive task such as processing the user fingerprint image - Need more hardware - Highly cost Surgery and scars
Le *et al.* [82]	1. MITM attack; Replay attack	- Need more hardware - Highly cost - Surgery and scars - Suitable for mobile cloud rather than others - User should memorize some secrets makes the procedure more difficult; - Several authentication factors are utilized for user authentication, which increases the authentication procedure time

Dey *et al.* [83]	-Stolen password attacks	- User should memorize complicated password to achieve high level of security; - The procedure of this authentication scheme is complicated; - The mobile device must process several steps to send an authentication request to the cloud; - The number of communication messages is high because of applying mutual authentication, which increases the authentication procedure overhead;
Hao *et al*. [75]	1. Denial-of-service attack during the password change phase; 2. Impersonation attacks; 3. Stolen password.	- User should memorize some secrets information; - several authentication factors are utilized for user authentication, which increases the authentication procedure time.
Odelu *et al.* [93]	1. Eavesdropper; 2. Offline password guessing; 3. Impersonation attacks; 4. Stolen password attack; 5. Man-in- the-middle attack.	- Attacker can easily determine from the transmitted message; - Username" is not a confidential credential - Vulnerable to Ciphertext-only Attack (COA). - There is no solution to verify the originality of *AS* or *SS*
Banyal *et al*. [84]	1. Stolen password attack; 2. Impersonation attack	- User should memorize complicated password; - The processing several patterns such as SMS activities, calling pattern, and location, needs many computation powers; - Needs many devices such as PC Smart phone, and server; - Highly cost
- Yang *et al*. [87]	1. Impersonation attacks 2. Stolen password attack; 3. Offline password guessing.	- Scheme does not provide user anonymity and it also has clock synchronization problem
- Grzonkowski *et al*. [73]	2. Stolen password attack;	- If malicious servers obtain the login information, the adversary will attack the user - If an unauthorized user uses authorized device the authentication process grants him authority to login into data saved in public cloud

6. RESULTS

Of the 14 studies published on multifactor authentication framework in public cloud computing security from 2010 to 2017, frequency of publication focused on Multifactor-based authentication in public cloud computing. Below I detail the results of our meta-analysis based on three research question.

6.1 Research question 1

Major Research Purposes, articles citations

a) Distribution of research purposes

Author classified each paper into one of three categories according to the research purpose: (1) Password with smart card, (2) Password with SMS, (3) Password with Biometric, (4) Password with security question, (5) Password with others. As seen in Figure-2.2 below, those pertaining to the percentage of password with smart card was (7%). The password with SMS has the percentage (43%). The password with biometric has the percentage (14%). The percentage of password with security question was (7%). Additionally, the Password with others percentage was (4%). The main purpose of this section to show we covered in this study the majors of multifactor authentication methods.

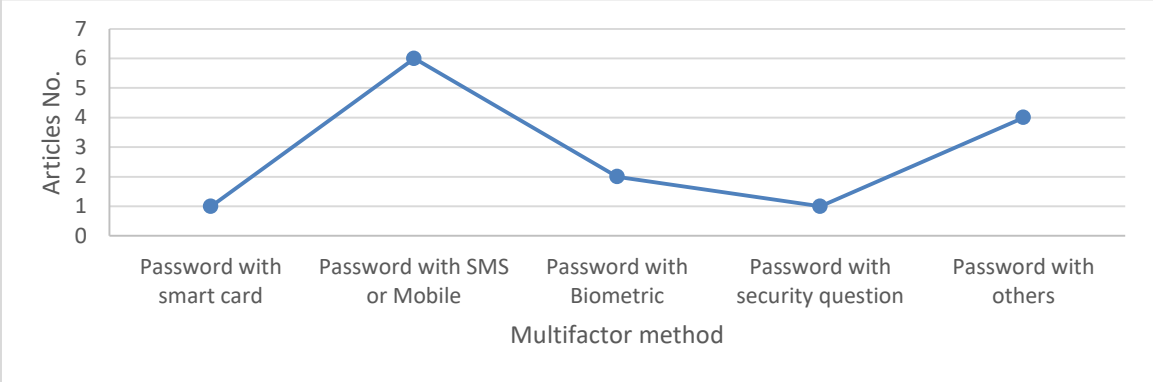

Figure-1. Distribution Based on Research Purposes.

b) Distribution of articles citations

As seen in Figure-2.3, articles have been distributed based on the number of citations in the search engines of the google scholar. The main purpose of this analysis to determine the dependability level of researchers on these articles. The analysis results are appearing the 80% from these articles got up to 15 citations. Therefore, these articles have a high accreditation in scientific researchers' range. Thus, these articles are considering in this study.

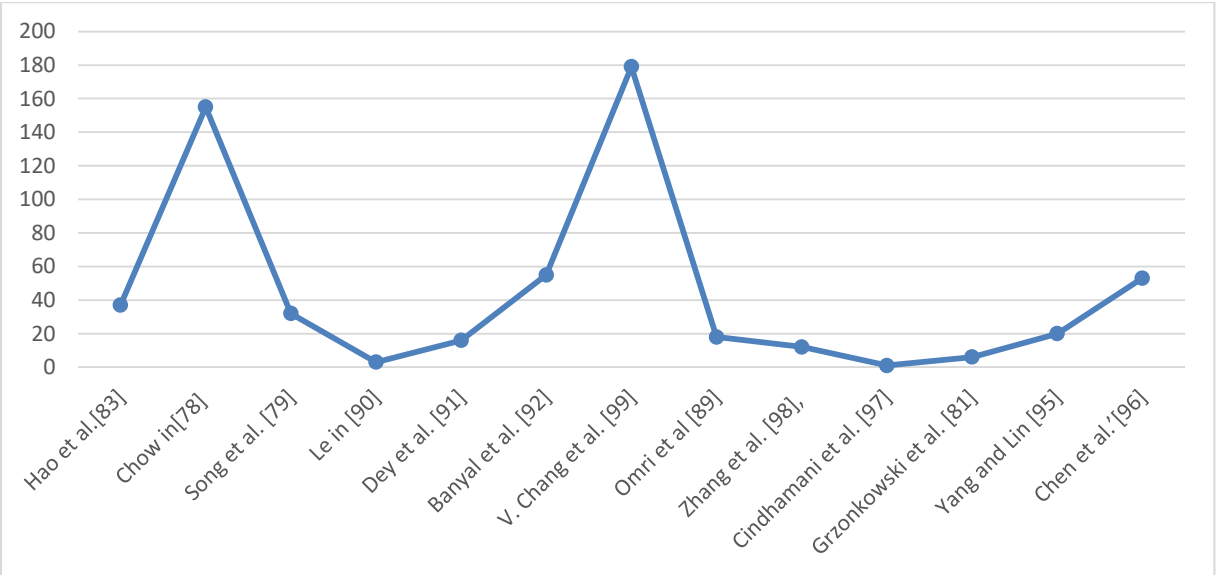

Figure-2. Distribution Based on Articles Citations.

6.2 Research question 2

What are the main threats and drawbacks?

a) Distribution based on threats

This section presents the distributions of articles based on threats methods on authentication framework in public cloud computing. Those pertaining to the percentages of stolen of password was (35%), the impersonation attack was (26%), MITM, and reply attacks was (13%), offline password guessing was (9%). The percentage of Denial-of-service attack was (4%). Accordingly, (35%) was the percentage for the stolen of password. Thus, the threats stolen of password attacks is considered as a major threat in multifactor authentication in public cloud computing followed by Impersonation as seen in Table-3 below.

Table-3. Articles Distribution Based on Threats.

No.	Articles	Denial-of-service	Reply	MITM	Offline password guessing	Impersonation	Stolen PW	Eavesdropper;
1	Hao *et al*.[75]	X				X	X	
2	Chow in [70]					X	X	
3	Song *et al*. [71]					X	X	
4	Le in [82]		X	X				
5	Dey *et al*. [83]						X	
6	Banyal *et al*. [84]						X	
7	V. Chang *et al*. [91]					X	X	
8	Omri *et al* [81]		X	X				
9	Zhang *et al*. [90],		X	X				
10	Cindhamani et al. [89]					X	X	
11	Grzonkowski *et al*. [73]						X	
12	Yang and Lin [87]				X	X	X	
13	Chen *et al*.'[88]					X	X	X
14	Odelu *et al.* [93]			X	X	X	X	X

b) Distribution based on drawbacks

This section presents the distribution of studies based on drawbacks in authentication framework in public cloud computing. The main aim of this analysis is to determine the most common drawbacks in current authentication framework scheme in public cloud computing.

A. Drawbacks password with biometric

According to Omri *et al* [81], Zhang *et al.* [90], Password with biometric is considered as a best multifactor authentication method from security side [106]. Unfortunately, highly cost is represented as a biggest drawback in this method, followed by Surgery and scars. In addition, this method has a medium usability level because it has many tools must be applied in authentication process [107]. Moreover, several authentication factors are utilized for user authentication, which increases the authentication procedure time [107]. Thus, in this study we did not have the potential or high budget to deal with this method, and others drawback especially in usability level make us to exclude this method in our research.

B. Drawbacks password with SMS or mobile

Password with SMS was the most widely used data application, with an estimated 3.5 billion active users [108]. According to Chow *et al*. [70], Song *et al.* [71], and Chang *et al*. [91], the main drawback in these scheme the user must be memorizing some secrets that makes the authentication process more difficult for user and need long time [107]. In Le in [82], Dey *et al*. [83], they suggested multifactor authentication scheme for applying with mobile, the main drawback highly cost implemented, surgery and scars, and need to apply many security procedures that makes more difficult for user and long time as well [107] [109]. In our research, the highly cost is considered as a main factor to exclude this method. In addition, this scheme is suitable for mobile cloud rather than others.

C. Drawbacks password with smart card

Scheme in Hao *et al*. [75], has many drawbacks such as smart card readers are expensive to produce. These readers are not available in all locations and may have compatibility issues due to the differences of each smart card brand [110]. In addition, user must be works according to memorize some secrets information which increases the authentication procedure time[107]. Smart cards are individually encrypted and can only be accessed by pin number. However, there is concern about privacy and whether or not information on the card could be accessed or used illegally by the government or other third-party sources [110]. In our research, the highly cost is considered as a main factor to exclude this method. In addition, this scheme needs many hardware.

D. Drawbacks password with security question

According to Cindhamani *et al*. [89], they proposed security framework in public cloud computing. The authentication in this framework is constract according to password with security question. This scheme has many drawbacks such as user should be memorize many secrets information which is makes the procedure

more difficult for user and need long time. Morever, in 2015 two Google security researchers in analyzed the weaknesses of the approach and concluded, "Secret questions are neither secure nor reliable enough to be used as a standalone account recovery mechanism. That's because they suffer from a fundamental flaw: their answers are either somewhat secure or easy to remember" [111].

E. Drawbacks password with others

Grzonkowski *et al*. [73], proposed the SeDiCi 2.0 protocol. This scheme is suffering from many drawbacks the top one, if malicious servers obtain the login information, the adversary will attack the user. In addition, Yang and Lin [87] and Chen *et al*.'[88], they suggested authentication scheme in public cloud. This scheme does not provide user anonymity and it also has clock synchronization problem. Odelu *et al.* [101], they suggested authentication in cloud environment. The main limitations in this scheme are attacker can easily determine from the transmitted message, Username" is not a confidential credential, there is no solution to verify the originality of AS or SS.

7. CONCLUSIONS

In public cloud computing, the multi factor authentication is considered more secure [112]. Nevertheless, most of current multi factor authentication methods have extremely high cost of implementation and deployment. Thus, the multi factor authentication in public cloud computing needs to add new factor has high security, easy to use, and cheap. In the other side, Oracle is recommended to move from traditional authentication strategies to intelligent authentication operations [113] through adapting learning mechanisms for behavior recognition that can mitigation to threats automatically [114].

Behavior recognition technique is considered as a cheap "no need more hardware", and easy to use" no need to add any new authentication procedure" technique. Furthermore, many researchers recommended to apply behavior recognition in authentication processes to improve its performance[115] [114] [116] [117] [118] [113]. These researchers are recommended to apply user behavior recognition with password for avoid many threats in authentication. Belk *et al*. [119] in this study investigates the interactivity between humans, technology and user authentication. These study findings highlight the necessity to improve current approaches of knowledge-based user authentication research by incorporating human cognitive factors in both design and run-time. Hoonakker *et al*. [120] this study is collects information on non-malicious computer and information security deviations by end users and possible reasons for these deviations. This research can help identify solutions for improving computer and information security related behaviors of end users (i.e. reducing the occurrence of deviations or mitigating their impact on computer and information security). The focus in this paper on computer authentication and how it can make computer and information systems more vulnerable. In this study recommended finding balance between the limitation of human beings and the desire to increase security that mean the authentication layer be easy to use from human and more secure.

Jayawardana [116], in this study is recommended to apply behavior recognition with password for improving authentication layer performance in cloud computing. This study finds most of current studies neglected the present of human factor in password-based authentication, and learnability in password-based authentication is highly weak. Despite this, very few studies have adopted the behavior recognition with password in public cloud. Accordingly, the objectives of this study are to improve password-based authentication performance through adopting learning mechanisms for behavior recognition as a matching factor with password during authentication process.

REFERENCES

[1] P. Mell, T. Grance, and others. 2011. The NIST definition of cloud computing.

[2] I. Velásquez, A. Caro, and A. Rodríguez. 2018. Authentication schemes and methods: A systematic literature review. Inf. Softw. Technol. 94(September 2016): 30-37.

[3] R. K. L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang and B. S. Lee. 2011. TrustCloud: A framework for accountability and trust in cloud computing. in Services (SERVICES), 2011 IEEE World Congress on. pp. 584-588.

[4] F. Sabahi. 2011. Cloud computing security threats and responses. in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. pp. 245–249.

[5] D. Teneyuca. 2011. Internet cloud security: The illusion of inclusion. Inf. Secur. Tech. Rep. 16(3): 102-107.

[6] A. Youssef and M. Alaqeel. 2011. Security Issues in Cloud Computing. GSTF J. Comput. 1(3).

[7] M. Carroll, A. Van Der Merwe and P. Kotze. 2011. Secure cloud computing: Benefits, risks and controls. in Information Security South Africa (ISSA). 2011, pp. 1-9.

[8] K. Popović and Ž. Hocenski. 2010. Cloud computing security issues and challenges. in MIPRO, 2010 proceedings of the 33rd international convention. pp. 344-349.

[9] Z. Wang. 2011. Security and privacy issues within the Cloud Computing. in Computational and Information Sciences (ICCIS), 2011 International Conference on. pp. 175-178.

[10] E. Mathisen. 2011. Security challenges and solutions in cloud computing. in Digital Ecosystems and Technologies Conference (DEST), 2011 Proceedings of the 5th IEEE International Conference on. pp. 208-212.

[11] D. Zissis and D. Lekkas. 2012. Addressing cloud computing security issues. Futur. Gener. Comput. Syst. 28(3): 583-592.

[12] D. Abraham. 2009. Why 2FA in the cloud? Netw. Secur. 2009(9): 4-5.

[13] F. Scott, M. Itsik and S. Adi. 2001. Weakness in the key scheduling algorithm of RC4. in Proceedings of the 8 Annual Workshop on SAC.

[14] S. Ramgovind, M. M. Eloff and E. Smith. 2010. The management of security in cloud computing. in Information Security for South Africa (ISSA).2010, pp. 1-7.

[15] S. Subashini and V. Kavitha. 2011. A survey on security issues in service delivery models of cloud computing. J. Netw. Comput. Appl. 34(1): 1-11.

[16] E. C. Amazon. 2010. Amazon elastic compute cloud (Amazon EC2). Amaz. Elastic Comput. Cloud (Amazon EC2).

[17] A. Tripathi and A. Mishra. 2011. Cloud computing security considerations. in Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on. pp. 1-5.

[18] A. E. Youssef. 2012. Exploring cloud computing services and applications. J. Emerg. Trends Comput. Inf. Sci. 3(6): 838-847.

[19] D. Schwab and L. Yang. 2013. Entity authentication in a mobile-cloud environment. in Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop. p. 42.

[20] E.-Y. Jang, H.-J. Kim, C.-S. Park, J.-Y. Kim and J. Lee. 2011. The study on a threat countermeasure of mobile cloud services. J. Korea Inst. Inf. Secur. Cryptol. 21(1): 177-186.

[21] H. Suo, Z. Liu, J. Wan and K. Zhou. 2013. Security and privacy in mobile cloud computing. in Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International. pp. 655-659.

[22] L. Bernard. A Risk Assessment Framework for Evaluating Software-as-a-Service (SaaS) Cloud Services Before Adoption," ProQuest Diss. Theses. p. 129-n/a.

[23] C. Shen, T. Yu, H. Xu, G. Yang and X. Guan. 2016. User practice in password security: An empirical study of real-life passwords in the wild. Comput. Secur. 61: 130-141.

[24] T. Acar, M. Belenkiy and A. Küpçü. 2013. Single password authentication. Comput. Networks. 57(13): 2597-2614.

[25] D. P. Sidlauskas and S. Tamer. 2008. Hand geometry recognition. in Handbook of Biometrics, Springer. pp. 91-107.

[26] M. Kim, H. Ju, Y. Kim, J. Park and Y. Park. 2010. Design and implementation of mobile trusted module for trusted mobile computing. IEEE Trans. Consum. Electron. 56(1).

[27] V. Radha and D. H. Reddy. 2012. A survey on single sign-on techniques. Procedia Technol. 4: 134-139.

[28] D. Bhattacharyya, R. Ranjan, F. Alisherov, M. Choi and others. 2009. Biometric authentication: A review. Int. J. u-and e-Service, Sci. Technol. 2(3): 13-28.

[29] K.-K. R. Choo. 2011. The cyber threat landscape: Challenges and future research directions. Comput. Secur. 30(8): 719-731.

[30] D. Ding, Q.-L. Han, Y. Xiang, X. Ge and X.-M. Zhang. 2018. A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing. 275: 1674-1683.

[31] J. Campbell and K. Bryant. 2004. Password composition and security: an exploratory study of user practice. ACIS 2004 Proc. p. 80.

[32] D. Florencio and C. Herley. 2007. A large-scale study of web password habits. in Proceedings of the 16th international conference on World Wide Web. pp. 657-666.

[33] J. A. Cazier and B. D. Medlin. 2006. Password security: An empirical investigation into e-commerce

passwords and their crack times. Inf. Syst. Secur. 15(6): 45-55.

[34] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr and J. P. Richer. 2018. NIST Special Publication 800-63B. Digit. Identity Guidel. Authentication Lifecycle Manag.

[35] Stolen password lets hackers into Deloitte's systems. 2017. Industry News. [Online]. Available: https://www.securenvoy.com/en-gb/blog/stolen-password-lets-hackers-deloittes-systems.

[36] "4 Ways Hackers Can Steal Your Password. 2017. Diverge IT. [Online]. Available: https://www.divergeit.com/4-ways-hackers-can-steal-password/%0D.

[37] Kanika Sharma. 2018. How Dangerous are Impersonation Attacks. AT&T Completes Acquisition of AlienVault. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/how-dangerous-are-impersonation-attacks.

[38] Symantec employee. 2018. Man-in-the-Middle (MITM) Attacks. Norton by Symantec. [Online]. Available: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html.

[39] N. Aboudagga, M. T. Refaei, M. Eltoweissy, L. A. DaSilva and J.-J. Quisquater. 2005. Authentication protocols for ad hoc networks: taxonomy and research issues. in Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks. pp. 96-104.

[40] D. Dasgupta, A. Roy and A. Nag. 2016. Toward the design of adaptive selection strategies for multi-factor authentication. Comput. Secur. 63: 85-116.

[41] S. Ziyad and A. Kannammal. 2014. A multifactor biometric authentication for the cloud. in Computational Intelligence, Cyber Security and Computational Models, Springer. pp. 395-403.

[42] R. Nikam and M. Potey. 2017. Cloud storage security using Multi-Factor Authentication. 2016 Int. Conf. Recent Adv. Innov. Eng. ICRAIE 2016.

[43] H.-Y. Chien, J.-K. Jan and Y.-M. Tseng. 2002. An efficient and practical solution to remote authentication: smart card. Comput. Secur. 21(4): 372-375.

[44] I. E. Liao, C. C. Lee and M. S. Hwang. 2006. A password authentication scheme over insecure network. J. Comput. Syst. Sci. 72(4): 727-740.

[45] E. Yoon, E. Ryu and K. Yoo. 2004. Efficient remote user authentication scheme based on generalized elgamal signature scheme. IEEE Trans. Consum. Electron. 50(2): 568-570.

[46] E.-J. Yoon and K.-Y. Yoo. 2005. New Authentication Scheme Based on a One-Way Hash Function and {Diffie}-{Hellman} Key Exchange. CANS 05\ifnum\shortbib=0{: 4th}\fi\ifnum\shortbib=0{International Conference on Cryptology and Network Security}\fi. 3810: 147-160.

[47] V. Shoup and A. Rubin. 1996. Session key distribution using smart cards. in International Conference on the Theory and Applications of Cryptographic Techniques. pp. 321-331.

[48] G. Yang, D. S. Wong, H. Wang and X. Deng. 2008. Two-factor mutual authentication based on smart cards and passwords. J. Comput. Syst. Sci. 74(7): 1160-1172.

[49] H. Abie. 2006. Different Ways to Authenticate Users with the Pros and Cons of each Method.

[50] K. Skračić, P. Pale and Z. Kostanjčar. 2017. Authentication approach using one-time challenge generation based on user behavior patterns captured in transactional data sets. Comput. Secur. 67: 107-121.

[51] J. Kohl and C. Neuman. 1999. The Kerberos network authentication service (V5).

[52] R. M. Needham and M. D. Schroeder. 1978. Using encryption for authentication in large networks of computers. Commun. ACM. 21(12): 993-999.

[53] L. O'gorman, A. Bagga and J. Bentley. 2005. Query-directed passwords. Comput. Secur. 24(7): 546-560.

[54] B. C. Neuman and T. Ts'o. 1994. Kerberos: An authentication service for computer networks. IEEE Commun. Mag. 32(9): 33-38.

[55] X. Yi, S. Ling and H. Wang. 2013. Efficient two-server password-only authenticated key exchange. IEEE Trans. Parallel Distrib. Syst. (9): 1773-1782.

[56] C.-C. Chang and T.-C. Wu. 1991. Remote password authentication with smart cards. IEE Proc. E (Computers Digit. Tech. 138(3): 165-168.

[57] M.-S. Hwang and L.-H. Li. 2000. A new remote user authentication scheme using smart cards. IEEE Trans. Consum. Electron. 46(1): 28-30.

[58] J.-J. Shen, C.-W. Lin and M.-S. Hwang. 2003. A modified remote user authentication scheme using smart cards. IEEE Trans. Consum. Electron. 49(2): 414-416.

[59] H.-M. Sun. 2000. An efficient remote use authentication scheme using smart cards. IEEE Trans. Consum. Electron. 46(4): 958-961.

[60] C.-K. Chan and L.-M. Cheng. 2000. Cryptanalysis of a remote user authentication scheme using smart cards. IEEE Trans. Consum. Electron. 46(4): 992-993.

[61] S. Yamaguchi, K. Okayama and H. Miyahara. 19990. Design and implementation of an authentication system in WIDE Internet environment. in Computer and Communication Systems, 1990. IEEE TENCON'90., 1990 IEEE Region 10 Conference on. pp. 653-657.

[62] M.-S. Hwang, C.-C. Lee and Y.-L. Tang. 2001. An improvement of SPLICE/AS in WIDE against guessing attack. Informatica. 12(2): 297-302.

[63] T.-C. Wu. 1995. Remote login authentication scheme based on a geometric approach. Comput. Commun. 18(12): 959-963.

[64] M.-S. Hwang. 1999. Cryptanalysis of a remote login authentication scheme. Comput. Commun. 22(8): 742-744.

[65] J.-K. Jan and Y.-Y. Chen. 1998. ﷺ password authentication scheme without verification tables. J. Syst. Softw. 42(1): 45-57.

[66] W.-H. Yang and S.-P. Shieh. 1999. Password authentication schemes with smart cards. Comput. Secur. 18(8): 727-733.

[67] J.-J. Shen, C.-W. Lin and M.-S. Hwang. 2003. Security enhancement for the timestamp-based password authentication scheme using smart cards. Comput. Secur. 22(7): 591-595.

[68] B. Wang, J.-H. Li and Z.-P. Tong. 2003. Cryptanalysis of an enhanced timestamp-based password authentication scheme. Comput. Secur. 22(7): 643-645.

[69] M.-S. Hwang, C.-C. Lee, Y.-L. Tang and others. 2002. A simple remote user authentication scheme. Math. Comput. Model. 36(1-2): 103-107.

[70] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi and Z. Song. 2010. Authentication in the clouds: a framework and its application to mobile users. in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. pp. 1-6.

[71] Z. Song, J. Molina, S. Lee, H. Lee, S. Kotani, and R. Masuoka. 2009. Trustcube: An infrastructure that builds trust in client. in Future of Trust in Computing, Springer. pp. 68-79.

[72] E. Shi, Y. Niu, M. Jakobsson and R. Chow. 2010. Implicit authentication through learning user behaviour. in International Conference on Information Security. pp. 99-113.

[73] S. Grzonkowski. 2010. Sedici: an authentication service taking advantage of zero-knowledge proofs. in International Conference on Financial Cryptography and Data Security. p. 426.

[74] B. Adida. 2007. Beamauth: two-factor web authentication with a bookmark. in Proceedings of the 14th ACM conference on Computer and communications security. pp. 48-57.

[75] Z. Hao, S. Zhong and N. Yu. 2011. A time-bound ticket-based mutual authentication scheme for cloud computing. Int. J. Comput. Commun. Control. 6(2): 227-235.

[76] C. D. Jaidhar. 2013. Enhanced mutual authentication scheme for cloud architecture. in Advance Computing Conference (IACC), 2013 IEEE 3rd International. pp. 70-75.

[77] M. Safkhani, N. Bagheri, M. Naderi, Y. Luo, and Q. Chai. 2011. Tag impersonation attack on two RFID mutual authentication protocols. Proc. 2011 6th Int. Conf. Availability, Reliab. Secur. ARES 2011, no. September, pp. 581–84.

[78] X. L. and F. W. Mohammad Wazid, Ashok Kumar Das1, Saru Kumari. 2016. Provably secure biometric-based user authentication and key agreement scheme in cloud computing. Int. J. Appl. Eng. Res. 9(22): 5968-5974.

[79] S.-N. Cheong, H.-C. Ling and P.-L. The. 2014. Secure encrypted steganography graphical password scheme

for near field communication smartphone access control system. Expert Syst. Appl. 41(7): 3561-3568.

[80] A. Babich. 2012. Biometric Authentication. Types of biometric identifiers. pp. 1-56.

[81] F. Omri, R. Hamila, S. Foufou and M. Jarraya. 2012. Cloud-ready biometric system for mobile security access. in International Conference on Networked Digital Technologies. pp. 192-200.

[82] Z. Le, X. Zhang and Z. Gao. 2013. NemoAuth: a mnemonic multimodal approach to mobile user authentication. in TENCON 2013-2013 IEEE Region 10 Conference (31194). pp. 1-6.

[83] S. Dey, S. Sampalli and Q. Ye. 2013. Message digest as authentication entity for mobile cloud computing. in Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International. pp. 1-6.

[84] R. K. Banyal, P. Jain and V. K. Jain. 2013. Multi-factor authentication framework for cloud computing. Proc. Int. Conf. Comput. Intell. Model. Simul. pp. 105-110.

[85] A. Singer, W. Anderson and R. Farrow. 2013. Rethinking Password Policies (Uncut). Login. 38(4): 14-19.

[86] K. Sharma. 2018. How Dangerous are Impersonation Attacks?. ALIENVAULT IS NOW AN AT&T COMPANY. [Online]. Available: https://www.alienvault.com/blogs/security-essentials/how-dangerous-are-impersonation-attacks%0D.

[87] J. H. Yang and P. Y. Lin. 2014. An ID-based user authentication scheme for cloud computing. in Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on. pp. 98-101.

[88] T.-H. Chen, H. Yeh and W.-K. Shih. 2011. An advanced ecc dynamic id-based remote mutual authentication scheme for cloud computing. in Multimedia and Ubiquitous Engineering (MUE), 2011 5th FTRA International Conference on. pp. 155-159.

[89] J. Cindhamani, N. Punya, R. Ealaruvi and L. D. Dhinesh. 2014. An enhanced data security and trust management enabled framework for cloud computing systems.

[90] I. Al Rassan and H. AlShaher. 2014. Securing mobile cloud computing using biometric authentication (SMCBA). in Computational Science and Computational Intelligence (CSCI), 2014 International Conference on. 1: 157-161.

[91] V. Chang, Y.-H. Kuo and M. Ramachandran. 2016. Cloud computing adoption framework: A security framework for business clouds. Futur. Gener. Comput. Syst. 57: 24-41.

[92] P. Gope and A. K. Das. 2017. Robust anonymous mutual authentication scheme for n-times ubiquitous mobile cloud computing services. IEEE Internet Things J. 4(5): 1764-1772.

[93] V. Odelu, A. K. Das, S. Kumari, X. Huang and M. Wazid. 2017. Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Futur. Gener. Comput. Syst. 68: 74-88.

[94] J.-L. Tsai and N.-W. Lo. 2015. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Syst. J. 9(3): 805-815.

[95] G. S. Sadasivam, K. A. Kumari and S. Rubika. 2012. A novel authentication service for Hadoop in cloud environment. in Cloud Computing in Emerging Markets (CCEM), 2012 IEEE International Conference on. pp. 1-6.

[96] S. M. Bellovin and M. Merritt. 1990. Limitations of the Kerberos authentication system. ACM SIGCOMM Comput. Commun. Rev. 20(5): 119-132.

[97] I.-E. Liao, C.-C. Lee and M.-S. Hwang. 2006. A password authentication scheme over insecure networks. J. Comput. Syst. Sci. 72(4): 727-740.

[98] G. H. Wettstein, J. Grosen and E. Rodriquez. 2006. IDfusion, an open-architecture for Kerberos based authorization. in AFS and Kerberos Best Practices Workshop, Michigan.

[99] J. Astorga, E. Jacob, M. Huarte and M. Higuero. 2012. Ladon: end-to-end authorisation support for resource-deprived environments. IET Inf. Secur. 6(2): 93-101.

[100] Y.-C. Hu, M. Jakobsson, and A. Perrig. 2005. Efficient constructions for one-way hash chains. in International Conference on Applied Cryptography and Network Security. pp. 423-441.

[101] W. Stallings. 2006. Cryptography and network security: principles and practices. Pearson Education India.

[102] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen and D. E. Culler. 2002. SPINS: Security protocols for sensor networks. Wirel. Networks. 8(5): 521-534.

[103] Y. Yang, R. H. Deng and F. Bao. 2006. A practical password-based two-server authentication and key exchange system. IEEE Trans. Dependable Secur. Comput. (2): 105-114.

[104] N. T. Abdelmajid, M. A. Hossain, S. Shepherd, and K. Mahmoud. 2010. Location-based kerberos authentication protocol. in Social Computing (SocialCom), 2010 IEEE Second International Conference on. pp. 1099-1104.

[105] S. T. F. Al-Janabi and M. A. Rasheed. 2011. Public-key cryptography enabled kerberos authentication. in Developments in E-systems Engineering (DeSE). 2011, pp. 209-214.

[106] S. Almuairfi, P. Veeraraghavan and N. Chilamkurti. 2013. A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices. Math. Comput. Model. 58(1-2): 108-116.

[107] M. Alizadeh, S. Abolfazli, M. Zamani and S. Baharun. 2016. Authentication in mobile cloud computing : A survey. J. Netw. Comput. Appl. 61: 59-80.

[108] What is a SMS Password? SMSPassword, Netherlands. [Online]. Available: https://smspassword.com/sms-password/. [Accessed: 18-Oct-2018].

[109] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad. 2018. Authentication systems: A literature review and classification. Telematics and Informatics. 35(5): 1491-1511.

[110] S. Robinson. 2018. Advantages & Disadvantages of Using Smart Cards. Techwalla, 2015. [Online]. Available: https://www.techwalla.com/articles/advantages-disadvantages-of-using-smart-cards. [Accessed: 18-Oct-2018].

[111] Lily Hay Newman. Time to Kill Security Questions-or Answer Them With Lies. WIRED, 2016. [Online]. Available: https://www.wired.com/2016/09/time-kill-security-questions-answer-lies/. [Accessed: 18-Oct-2018].

[112] S. Asad, M. Fatima, A. Saeed and I. Raza. 2016. Multilevel classification of security concerns in cloud computing. Appl. Comput. INFORMATICS.

[113] Oracle Corporation. 2018. Machine learning-based adaptive intelligence: The future of cybersecurity Executive summary. no. January.

[114] J. Oeltjen. Authentication and Machine Learning: Taking Behavior Recognition to a New Level. RSA Identity Reimagined. [Online]. Available: https://www.csoonline.com/article/3209917/identity-management/article.html.

[115] W. Paper and W. Paper. ADAPTIVE AUTHENTICATION SUPERIOR USER EXPERIENCE AND GROWTH THROUGH INTELLIGENT.

[116] V. Jayawardana. 2017. Adaptive Authentication and Machine Learning. Towards Data Science. [Online]. Available: https://towardsdatascience.com/adaptive-authentication-and-machine-learning-1b460ae53d84.

[117] J. Shepherd. 2016. Duo + OneLogin: Adaptive Authentication. Product and technology, security & compliance. [Online]. Available: https://www.onelogin.com/blog/what-is-adaptive-authentication.

[118] A. Ferdowsi and W. Saad. 2018. Deep Learning for Signal Authentication and Security in Massive Internet of Things Systems. pp. 1-30.

[119] M. Belk, C. Fidas, P. Germanakos and G. Samaras. 2017. The interplay between humans, technology and user authentication: A cognitive processing perspective. Comput. Human Behav. 76: 184-200.

[120] P. Hoonakker, N. Bornoe and P. Carayon. 2009. Password Authentication from a Human Factors Perspective: Results of a Survey among End-Users. Hum. Factors Ergon. Soc. 53: 459-463.