Contemplation of Effective Security Measures in Access Management from Adoptability Perspective

Tehseen Mehraj
Dept. of Computer Science & Engineering
Islamic University of Science and Technology
Awantipora, Kashmir

Bisma Rasool
Dept. of Computer Science & Engineering
Islamic University of Science and Technology
Awantipora, Kashmir

Burhan Ul Islam Khan
Dept. of Computer Science & Engineering
Islamic University of Science and Technology
Awantipora, Kashmir

Asifa Baba
Dept. of Electronics & Communication Engineering
Islamic University of Science and Technology
Awantipora, Kashmir

Prof. A. G. Lone
Dept. of Computer Science & Engineering
Islamic University of Science and Technology
Awantipora, Kashmir

***Abstract*—With the extension in computer networks, there has been a drastic change in the disposition of network security. Security has always been a major concern of any organization as it involves mechanisms to ensure reliable access. In the present era of global electronic connectivity where hackers, eavesdroppers, electronic frauds, viruses are growing in number, security has proved to be indispensable. Although numerous solutions have been put forth in literature to guarantee security, they have botched with related traits like efficiency and scalability. Despite the range of security solutions that have been presented by experts, not a single approach has been wholly agreed upon to provide absolute security or standardized upon unanimously. Furthermore, these approaches lack adoptable user implementation. In this paper, various approaches and techniques that were introduced in the past for the purpose of enhancing the authentication and authorization of the user while performing sensitive and confidential transaction are discussed. Each of works performed by the researchers is taken single-handedly for debate followed by analysis. Finally, the open issues in the current domain of study are formulated from the review conducted.**

Keywords—Access Management; Authentication; One-Time-Password (OTP); OTP generation; User adoptability

I. INTRODUCTION

Access management includes diverse ways a user can gain access to an identity and the various technologies that offer protection to that identity. Moreover, the access to an identity by the right user at the right time is also taken care of in Access Management [1]. Access management in public and private networks is a serious concern in the field of Information Technology. The exponential growth in computer networks has led to the emergence of a range of security issues [2]. As information happens to be more substantial and a large figure of people joining the Internet, the security of information about various sectors of society has become vital [3]. Although, security is a serious concern in the present day scenario in sectors like educational institutions, governmental applications, financial institutions, military organization, etc., it needs to be ensured that the security measures should be user ergonomic and adoptable. Therefore, enhanced security measures should be taken for safeguarding computer networks while operating network applications [4]. Further, there is a need for performing secure commercial and business transactions that make access management a top security requirement that involves authentication and authorization [3]. Moreover, a security system relies on Access Management that is found to be the first checkpoint in network security [5].

A. Authentication and Authorization:

In IT security, Authentication is the essential building block as well as the crucial line of defense [6]. Authentication is used as a fundamental technology that is the process of validating the identity of someone or something. On the other hand, authorization is the process of determining whether the user has permission to access, read, insert, delete or modify certain data, or to execute certain programs [3][7]. In general, authentication necessitates the user to present the credentials to prove what he claims to be. Conventionally, the various authentication mechanisms have been categorized as:

1) Something the individual knows, e.g., a password, a Personal Identification Number (PIN), a passphrase

2) Something the individual possesses, e.g., electronic key cards, physical keys, smart cards, cryptographic keys

3) Something the individual is (static biometrics), e.g., recognition by Iris pattern face, fingerprint and other biometrics

4) Something the individual does (dynamic biometrics), e.g., recognition by handwriting characteristics, typing rhythm and voice pattern.

The last couple of years has brought news of a variety of distinguished security breaches focused on authentication, in some cases, severe consequences. A not uncommon pattern could be a revelation that some server is hacked, and an outsized variety of account passwords have been probably exposed. As a result of, whereas, we tend to know files containing things like countersign hashes were traced, there's typically no succeeding data on the actual fallacious use of the information or real harm done. An example of a security breach where the damage resulted is that the attack on the Associated Press Twitter account of Apr 2013 [8]. A counterfeit tweet about explosions at the White House caused a quick, but serious, disruption to the monetary markets. The business is slowly reacting to password attacks and is commencing to try and notice higher ways to stop them.

In the current era of security modernization, password-based authentication i.e. single factor authentication system still finds a use for the processes of authentication and authorization. As passwords form the utmost level of sensitive and confidential information, consequently unauthorized access of user-sensitive password in large scale networking system has been exceedingly studied in the past research works [9][10][11][12]. One of the momentous issues with traditional password-based security system is that users have a higher proclivity to select intrinsically unsafe passwords for the sake of easy memorization, etc. This phenomenon directly leads to surfacing of dictionary attacks [13], where the adversary over the network attempts various permutation and combination of strings leading them finally to arrive at the correct password by the genuine user. With the current availability of various password hacking tools [14][15][16] as well as keylogger software [17], the task of password retrieval has become much easier for the attacker. Not only public network but also private network is not secure in existing set of hacking methodologies and tools. Various events have been reported in the past, where it is found that number of reputed enterprises like eBay, ICICI Bank, World Bank, Walmart, etc. have been literally hacked costing massive loss of property and highly confidential data [18].

Above all, every publicized password attack is sometimes followed by a series of articles decrying the “end of the password” and business for the implementation of Multi-Factor Authentication (MFA) [19]. MFA proves to be a more secure remedy that piggybacks multiple authentication items from multiple factors [20]. A website using MFA is tougher to attack – to “break into” – than a website authenticating users with solely one issue like a password. The widespread adoption of MFA would improve on-line security and facilitate a reduction in fraud. Moreover, MFA is not a replacement plan rather it has been enforced in online systems for several years. Till recently, however, MFA has seldom been deployed with success in very large-scale websites meant for communities like consumers within the light-weight of the increasing word attacks, practices are setting out to an amendment.

Combining multiple factors for authentication enhances the accuracy and usability of the authentication process. It also reduces the False Rejection Rate (FRR) of genuine users [3].

One such technique is Two Factor Authentication (2FA) that combines any of the two above-mentioned authentication factors. For the reason of high cost and complex design, biometric-based security systems are not widely adoptable [3]. Currently, the usage of One-Time-Password in 2FA is extremely popular [21]. OTP authentication, also known as session authentication, utilizes a password that can be used only once unlike the traditional re-usable passwords which are being used over relatively longer periods of time. Moreover, OTPs are encrypted before being transmitted to reduce their interception [3].

B. OTP Generation and Distribution:

To ensure the security of the system, the generated OTP should not be traced, guessed or retrieved easily by the intruders. Thus, a secure authentication mechanism needs to be developed for OTP generation. OTP generation can be achieved by any of the three mechanisms:

1) Use of a mathematical algorithm for generating a new password on the basis of previous password,

2) Use of a time-synchronous scheme, where the designed algorithm executes in both the client and the authentication server for generation of password,

3) Use of a challenge-response schemes in that the server or any other authenticating system issues a challenge to the host seeking authentication and expects a response. In addition to this, a counter is employed instead of the previous password [22].

Though the generated One Time Passwords are immensely employed but at the same time they face with several limitations including synchronization problem and the inability of the algorithms to provide security with continued existence.

Distribution of OTP to the user is achieved in two ways: i) the client can request the service provider i.e. a bank or authentication server to provide the OTP. The server can deliver the OTP via GSM network or it can provide the client with hardcopy of OTPs i.e. TAN lists (Transaction Authentication Number) [23][24], ii) Alternately, the service provider provides client with tokens that can generate OTP on client side i.e. EMV Card and Reader, Hardware/Software OTP Tokens, etc. [25][21].

It needs to be ensured that the method used for OTP generation and distribution should be acceptable widely i.e. it should be user ergonomic. The methods used should be intuitive, simple, and economical. Also, the cost of devices used should be taken into consideration in the case of device failure i.e. they should be reliable and robust.

The prime objective of the paper is to study various security measures that were introduced in the past for effective access management. Section II is entirely devoted to the concise survey of numerous current authentication/authorization techniques. Section III highlights the prominence of open issues from the discussed literature and finally the paper is concluded with some clinching remarks in Section IV.

II. RELATED WORK

A detailed study of the relevant literature that has been introduced in the past for the purpose of mitigating security issues about authentication and authorization are discussed in this section. The study involves authentication schemes that are characterized into two categories: OTP based and non-OTP based schemes.

A. Review of OTP Based Schemes

Many authentication schemes have been studied by researchers but the strongest of all have been found to be the ones based on the concept of One-Time-Password. There are numerous schemes of generating One-Time-Passwords.

In [22] a noisy password technique has been implemented that results in passwords that are robust against any shoulder surfing or eavesdropping. This technique enables users to use passwords suitable for them to remember. The password provided by the user together with the noisy part is used to generate complex and different password at each login. The noisy password imbeds the actual password within it. Noisy password, in particular, has four parts that make it extremely challenging computationally to deduce password from the noisy part. User is authenticated with a different password for each login by employing proposed technique. The system achieves user authentication by permitting the user to enter the username i.e. an ID and a noisy password. The technique utilizes two algorithms; first algorithm is used for choosing the password and its storage in a database. The second algorithm is employed for the extraction of the password and its recognition. The proposed work has also limited the number of incorrect login entries to five attempts. The system has made use of noisy passwords that exponentially increase the processing time.

In [26] authors have put forward a scheme known as ‘Infinite Length Hash Chains’ to increase the efficiency and extensibility of the conventional chaining idea with the help of public-key techniques. The ILHC scheme is the scheme where the length of the hash chain can be increased infinitely thereby facilitating its use without the need of system restart or bootstrapping. The proposed ILHC scheme employs a public-key algorithm to produce an infinite one-way-function that forms the one-time-password production core. Unlike the one-way function chains, the proposed system allows the owner of the chain to go in whatever direction any time and doesn’t limit the length of the hash chain. Usually, certificates expire after certain interval of time; say a year or two but the usage of ILHC scheme enables the user to use server-supported signatures whereby the user is no longer restricted by the number of messages to be signed. In the proposed scheme, there is an increase in the computation cost as a consequence of operations involved in public-key algorithms. This can be owed to the exceedingly large number of cascaded exponentiations. As a result, this scheme is difficult to be employed in devices with restricted computational resources (say, mobile phones).

An algorithm proposed by authors in [27] implements a knock sequence that is secure and employs AES (Advanced Encryption Standards) encryption scheme. Thus, the proposed scheme cannot be sensed by sniffing or spoofing. This authentication scheme is an improvement over the port-knocking mechanism in place. The authors have proposed a novel framework that further enhances the security level in the prevailing port-knocking models by making it more complex for the attackers to reveal the correct port knocking sequence. In this system, the concept of One Time Password (OTP) is used that acts as the One Time Key for complete AES encryption technique in addition to Quadratic Residue Cipher (QRC) to spoof the source IP addresses a number of times thereby leading to raised complexity in discovering the sequence of IP addresses and packets. Also, the pseudo random number generator (PRNG) is being used to produce the random numbers in real time that shall be used both in QRC and as a key for the AES encryption. Using this scheme, various problems like out-of-order-delivery problem of packets are swept away since all the packets irrespective of their source being assembled at the server at first and then decrypted to obtain the correct knock sequence. The system makes use of SMS to send OTP and a random number to the client. However, sending an OTP over an SMS to the user has certain restrictions like cost, lateness, security, etc. In addition to this, the SMS-based OTP can be compromised.

A secure and quite compatible web/mobile-based authentication mechanism is presented in [28] with an attempt to enhance multifactor authentication. The authors put forward a method of generating one-time password keys in OTP clients with the help of PingPong128 stream cipher. Stream ciphers have been developed to approximate the behavior of one-time code. The proposed system makes use of an innovative approach for producing an authentication method that employs IC’s (Identification code) to implement an additional security level in the conventional login system. IC’s are the identification codes that are unique to each user and each transmission and are provided by companies, banks or other financial institutions to the user. In this scheme, the authentication server produces a secret code only once and then changes the value of the secret code in the next instance. The system makes use of Advanced Encryption Scheme (AES) for encrypting the generated OTP. The protocol employs multifactor authentication for verifying the user and the current transaction. The client side has been simulated using The Sun J2ME Wireless Toolkit, that comprises of build tools, utilities, and a device emulator.

The authentication server is based on J2EE technology with web server Glassfish and database Mysql. Module IC codes are pseudo-random codes that can be generated employing pseudo-random number generation algorithm. It is only an authorized person who distributes the IC’s to the user’s phone through the web browser or a Bluetooth device. The distribution process also includes the encryption of IC’s. Once implemented, the proposed protocol does not add to the expenses of users considerably as it has an easy implementation and can be executed on the current costs that the servers incur from users. However, this model involves two communication channels viz. TCP/IP and GSM.

A novel OTP authentication scheme based on true random numbers has been put forward in [29]. In the proposed scheme, the true random numbers are generated using physical methods i.e. from digital physical noise sources and are then applied in the process of secure authentication. The generation of random numbers in this scheme is based on the characteristics of the common digital-analog hybrid circuit. The random numbers generated by this method are non-repetitive, stochastic and unpredictable that ensures that it is almost impossible to crack those random numbers. This scheme provides a defense against attacks of human sources and can be viably used in the areas where efficiency and high security is needed such as stock exchange system, finance system, etc. The authentication scheme uses the true random numbers as the password that is encrypted and decrypted by the client and server twice respectively. The proposed authentication mechanism is a two-way authentication scheme i.e. both the server and the client authenticate each other. The client uses challenge/response method to ask authentication each time and the encryption algorithm used is RSA public key cryptography. The cryptographic algorithm employed in this scheme is easy to implement as there is not an involvement of third party. A large amount of random numbers can be generated using this scheme at a fast rate that decreases the expenses paid by the server. This, in turn, enhances the efficiency of the server as well as the entire authentication process. However, the proposed system is found to be vulnerable to phishing attacks.

A secure authentication scheme has been proposed in [30] using smart cards that preserves the properties of previous authentication schemes but does not put any restriction on the number of login attempts. At the same time, the proposed scheme can be said to provide resistance against stolen-verifier attack, replay attack, password guessing attack. As a result, this scheme has been found to improve both the applicability of OTPs as well as the security level in the system using this concept. The proposed scheme is composed of three phases: the registration phase, the login phase, and the proof phase. It is the server that issues the smart card to the user that holds the initial secret seed. A one-way hash function was employed in this scheme that is collision resistant. The server also transmits a timestamp to the user along with the previous results of the computation. It is this timestamp that is used to check the legality of the server. The proposed scheme has been found to be resistant to several attacks, e.g., server spoofing attack, user impersonation, replay attack, password guessing attacks (offline as well as online), stolen-verifier attack. Moreover, this authentication system ensures a high level of security since both the server and the user authenticate each other. The proposed authentication system is reliable and complete in terms of the fact that the important data cannot be retrieved even after analyzing the data transmitted. However, the use of an extra device i.e. a smart card in the proposed authentication scheme can cause inconvenience to the user and at the same time may prove expensive to the service provider.

An efficient end-to-end one-time-password authentication scheme has been put forward in [31] that eradicates the drawback of the existing authentication protocols. The proposed scheme utilizes two cryptographically strong base elements viz. the Authentication Key Exchange (AKE) protocol and the keyed Hash Message Authentication Code (HMAC). Such an authentication protocol has been found to provide transparency in the mutual authentication between the two participating end-points. In this authentication system, the various operations involved like Key Setup, Key Scheduling, and Key Update are performed independently at the two end-points with no interaction between them. As a result, the proposed authentication scheme ensures a high level of security since there is no involvement of a trusted third party. Moreover, this scheme is highly secure cryptographically owing to its resistance against a range of attacks that the present OTP authentication schemes encounter. The proposed scheme makes use of HMAC-SHA512, that is based on the cryptographic hash function SHA3. HMAC is used for message authentication and to verify data integrity. This authentication protocol can be operated independently in various scenarios because it is relatively simple and has less computational overhead as compared to the previous protocols. Owing to the simple operation of the proposed scheme, it can be very suitably adapted by resource-constrained mobile devices. However, this authentication mechanism suffers from a limitation that it is not much strong cryptographically as it cannot be used in cases when the number of iterations exceeds the length of the mutually agreed upon Master Key. Furthermore, the security of the system relies on secure handling and storage of Master key i.e. the Master key should not be stolen or compromised.

In [32] authors have put forward a novel authentication mechanism based on Chebychev chaotic mapping. The chaotic mapping has various characteristics such as sensitive dependence on the initial condition and structural parameters; and unpredictability that are the key factors of authentication. The proposed system has designed an authentication mechanism between intelligent electronic devices (IEDs) in substation automation. This system has been proposed taking into consideration three protocols—GOOSE, SMV and GSE, that have rigorous performance requirements as a result of that encryption or various other security measures can drastically affect their rate of transmission. The proposed chaotic sequence based authentication scheme has been found to be efficient than the general OTP authentication schemes since there is no need to store the whole sequence thus utilizing less memory. The chaotic mapping employed in this scheme being an identity mark sequence ensures that the sequence generated cannot be imitated by others. The use of one-way function F ensures secure and easy authentication, since it is practically infeasible for anyone to generate the initial seed ‘s’ from the value y = F(s). The chaotic sequence that is generated in the proposed authentication scheme is found to be responsive to the initial condition such that a small change in y_0 produces large changes in the sequence y_n. Although, the chaotic sequence based authentication schemes have been found to be fast and secure but a large number of those systems have been effectively cryptanalyzed owing to the finiteness in its computing precision that is used as a means to represent the floating point output of the system, thus making the current system susceptible to attacks.

The paper [33] has proposed a novel authentication mechanism that exploits location and time information of mobile device as physical parameters to generate the One-Time-Password (OTP). The framework restricts the validness of OTP in a definite time-period along with the tolerant geometrical location, thus enhancing security. Present statistics of moving directions and movement of the mobile device are employed to improve the precision of location prediction. Transparent authentication of the user is presented, provided the user moves steadily thus avoiding manual typing of credentials every time while being transparently logged into the server. The authors have utilized both event based and time synchronized OTP mechanisms. In event-based, the system considers that the user should be in the tolerant region while in time-based, mobile device and server are clock synchronized. An assumption is made in the system that the users are already registered on the application server and are organized in Public Key Infrastructure (PKI). The system involves two phases. In the first phase, it calculates the user-tolerant range of expected future location, from the user's current location and time. For user to login the server, the location obtained from GPS receiver and the current time is used to generate OTP. The generated OTP and the International Mobile Subscriber Identity (IMSI) are concatenated and encrypted by a public key and then sent to the server. The server decrypts the received message using a secret key. OTP is extracted by the server and from it, the time and location coordinates are retrieved. If the coordinates are in the tolerant region of predicted destination, the server authenticates the user otherwise it rejects the login request. System provides secure user authentication while accessing crucial Internet services such as e-commerce and online banking transactions; immunity against several types of attacks like eavesdropping, replay, man in the middle, dictionary, brute force, and other user impersonation attacks. The proposed authentication mechanism works with GPS-enabled mobile phones. Further, clock synchronization between the server and the mobile device is required, that is difficult to achieve in the case of mobile phones as mobile phones are certain to move out of the network due to that synchronization fails.

A novel OTP authentication mechanism that resolves counter de-synchronization problem by employing symmetric encryption algorithm and one-way hash function was proposed in [34]. It has effectively minimized Denial of Service (DoS), guessing, and replay attacks. The approach makes use of symmetric encryption scheme i.e. AES, that offers resistance to differential and linear cryptanalysis in coordination with a one-way hash function i.e. MD5. The symmetric cryptographic algorithm provides one-way functionality. The symmetric cryptographic algorithm encrypts counter value to generate OTP. Further, the symmetric encryption algorithm generates an output that is capable of carrying the counter value to the server thus avoiding the counter de-synchronization problem. A single comparison is done by the server so as to solve counter desynchronization problem. Using only symmetric encryption algorithm will result in a successful attack. To avoid such attack, the system makes use of a digest that are the verification bits of counter need to be added i.e. MD5. In the scheme, OTP has two parts P = C | | D, where C signifies cipher text, D signifies verification bits. 48 bits one-time password using 24 bits of C and 24 bits of D are used in the system, MD5 calculates one part and AES calculates another part of the password. Illegal submission is recorded by the server if password authentication fails. The server restricts a user if the number of illegal submissions reaches a specific threshold. The scheme has minimized the security requirement of server and provides an easy integration in the present enterprise applications.

The paper [35] has proposed a scheme that makes use of one-time-passwords as dynamic passwords that change according to time, user ID and some other factors unique to user i.e. Media Access Code (MAC). The scheme has utilized time and space factor to provide secure authentication mechanisms. In this system, various problems associated with the current 2FA scheme have been eliminated by minimizing user's effort or/and the high overhead associated with the generation of one-time-password. It has employed software for OTP generation thus providing easy user adoption and an economical solution. Proposed dynamic authentication mechanism involves four steps: sign-up, OTP generation, transferring authentication information to the server and finally, the verification. In this technique, the OTP generation and user authentication are performed on the same machine. In the sign-up phase, the user enters the static password provided by the server that holds the master key. The hash function is used to generate Password Digest (PD) from the static password entered by the user and the digest is saved in server's database. The second phase comprises of small software that is used to generate the OTPs from the static passwords of the user. The generated PD is XORed with a master key that is present in the software, so as to generate Master-key and Password Digest (MPD). The generated digest together with MAC and time are concatenated and fed to hash function to generate an OTP. This phase may include compression of the generated OTP into a smaller length OTP. The generated OTP is considered user's signature at specific machine and time and helps to obtain time and space dynamism. The generated OTP at user side is denoted as U-OTP (user side OTP). The third phase involves transferring authentication information to the server. Since, the hash function generates output as binary strings therefore encoding technique Radix64 is utilized to present the user an OTP that can be typed and read easily. The generated U-OTP is manually entered or copied on the login screen of website. In addition to other authentication information, MAC also has to be transferred to server. MAC can be captured using JavaScript techniques by a web page. The final phase involves verification. The server will extract the MAC address of the user and generate OTP by the same mechanism and compare the details upon reception of authentication information. The server side retrieves MAC and PD easily retrieved but for obtaining time synchronization information it may use any of the two strategies: add a time factor to OTP and server guesses method. As the scheme has utilized space and time dynamism it enables the proposed authentication mechanism to resist Perfect-Man-in-the-Middle and replay attacks. In the proposed scheme, the hashed output of static password is stored in server's database that enables the proposed authentication mechanism to resist stolen-verifier attack. However, this system has been found to be resistant to basic phishing attack as the user is not allowed to enter the password on login form.

Traditional hash chains suffer from updation problem in that seed should be updated after generating finite hash values. In [36] authors have introduced an enhanced self-updating hash chain that eliminates the practicality and security issues associated with the conventional Infinite Length Hash Chains (ILHC). The authors have demonstrated a self-updating hash chain, which is based on Linear Partition Combination Algorithm (LPCA). LPCA, which is a data distribution scheme, splits the data or seed in 'm' parts and then departs those parts. No information about the seed can be obtained from these parts as they do not hold any information about the seed. This scheme eradicates the shortcomings of traditional infinite length hash chains used for authentication that are associated with increased computational cost in case of public key based infinite length hash chains and weak security due to leak of part of next hash seed value at every transmission in case of one bit information exchange algorithm. The model has made use of LPCA algorithm, the computations for data dispersal and data restoration functioned in Galois Function (2). Further, the technique requires additional storage than the conventional authentication mechanisms. Also, the security of the system is centered on LPCA scheme and one-way functionality of the hash function. OTP has solved the security issues associated with static passwords, but the manageability of same is a problem for consumers.

A novel authentication mechanism has been presented in [37] for home networks by using smart cards based on One-Time-Password (OTP). The proposed scheme provides strong authentication mechanism by using OTP and one-way hash function that reduces the computation load enabling the system to meet the security requirements of home networks. Mutual authentication is established using three-way challenge-response handshake. The scheme has accepted the current home networks based on one-time-passwords. Authors have designed this system between the user and home gateway. The proposed authentication mechanism involves three major phases: registration phase, login phase and authentication/service request phase. In this model, the secret key has to be shared between Home Gateway (HGW) and Internet Authentication Server (IAS). The system enables the server to verify multiple access requests from a home user in single verification. It makes the home networks resistant against passive attacks such as eavesdropping, replay, Man-in-the-middle and Denial of Service and Stolen-verifier attacks. Mutual authentication between the home user and the authentication server is done thus avoids phishing attacks. The system discards timestamp to eradicate serious time synchronization problem. Further, Session key agreement is used in every session to provide secure connection and minimizes the burden on systems involved in authentication mechanism as no verification tables need to be stored. The security of the system is based on the non-invertible property of hash function and a nonce that is used to prevent time synchronization problem. However, this system proves to be unsuccessful to offer protection against various active attacks.

OTP has solved the security issues associated with static passwords, but the manageability of OTP is a problem for consumers. In [38] authors have proposed a technique that has extended the password generator to increase the manageability of OTP. The system generates website specific passwords by applying a one-way cryptographic hash function over website domain name and password. The proposed scheme has proved to provide superior performance by taking into consideration transmission bandwidth and computational cost of password verification/generation. The scheme makes use of Manageable One Time Password (M-OTP) module that can be any firmware module or some software program on the consumer device. The user submits only one password to this module and obtains a website-specific OTP. The web browser transmits the generated OTP to the web server, which performs authentication. In this scheme, Advanced Encryption Standard (AES) algorithm is used as to provide one-way functionality as well as for encryption. A large number of iterations of one-way cryptographic hash function has been employed to generate the password, due to that the proposed system has been able to resist offline dictionary attacks.

The manageability of credentials and identities for different internet services has become difficult for users. A One-Time-Password (OTP) MIDlet working on a mobile phone for integrated authentication designed for various types of internet services is presented in [39]. The proposed system minimizes the burden on users by automating the solution. This technique results in reliable multi-channel authentication mechanism by combining internet connection and GSM to give-and-take authentication messages. In this technique, challenge-response mechanism is employed to generate OTP. The model comprises of Java MIDlet installed on java supported mobile phone, an applet on the user terminal to pass the OTP to Authentication Server (AS) i.e. a servlet. The core of the scheme is that there exists a closed loop among all components in the system. The user accesses the internet services through the browser having a java applet on the user computer, equipped with internet connection. The service providers are associated with authentication servers to handle authentication mechanism. The authentication server connects to the applet on HTTPS connection and with the mobile phone through SMS over GSM network. Finally, the mobile phone inputs the credentials via Bluetooth or if there is no Bluetooth, user enters the credentials manually.

The paper [40] aggregates the advantages of both software and hardware tokens by integrating them on mobile phones equipped with hardware mobile trusted module (MTM). The technique presented provides usability with strong security and scalable OTP solution using mobile phones as hardware tokens together with trusted computing technology. In the proposed scheme, the trust factor is established between the service provider and the Mobile Local Owner Trusted Module (MLTM) equipped mobile phone. The MLTM acts as a secure processor to create a series of OTPs. MLTM supports SHA-1 as OTP generator function. The proposed model considerably reduces the cost and need of having separate hardware tokens for different service providers and thus allows users to handle multiple OTP service providers on a single mobile phone hence, eliminating problem of economics and scalability. In the presented scheme, user authentication as well as data origin authentication is taken into consideration. Usage of two separate channels concurrently i.e. the internet and the mobile network lead to a complex system that will minimize the man in middle attack. The separation of the mobile phones from the user client terminal restricts the usability that necessitates the user to copy the OTP manually from mobile phone to the client terminal.

Top military commands, government agencies, etc. require absolute privacy and security that lasts endlessly. The intervention of “Top Secret” in a month or after 100 years can prove disastrous. In [41] authors have proposed a framework that delivers absolute security by making use of one-time-pad and supplying the random keys by using a high throughput binary random sequence generator. The framework has introduced an up-to-date usage of one time pads for achieving absolute security by introducing 100Mbit/s hardware binary random generator. The proposed scheme has solved the problem of availability of long one time keys (OTK) or one time pads (OTP). It presents an infinite source of one time keys by making use of the random generator. However, this system involves a high cost for secure physical distribution of keys thus, hampering adoptability.

The various problems about security and authentication of accessing private and highly privileged information studied by many researchers are tabulated below for benchmarking. The contributions and associated shortcomings of the various OTP based authentication approaches already discussed are formulated in Table I as follows:

TABLE I. REVIEW OF OTP-BASED SCHEMES

AUTHOR	CONTRIBUTION	RESULT OBTAINED	LIMITATIONS
(Bicakci and Baykal, 2002)[26]	Proposed Infinite Length Hash Chains that use a public-key algorithm to generate one-time-password	• Network overhead and system-restart complexity is evaded. • Owner of the hash chain is allowed to go in whatever direction anytime with no limit on the length of the chain. • Enables the user to use server-supported signatures whereby user is no longer restricted by number of messages to be signed.	• Increase in computation complexity as a consequence of public key operations makes it difficult to be employed in devices with restricted computational resources e.g., mobile phones.
(Chang et al., 2004)[30]	A secure authentication scheme using smart cards with no restriction on the number of login attempts	• One-way hash function and XOR operations employed ensure its efficiency. • Defensive against a number of attacks e.g., server spoofing, user impersonation, replay attack, password guessing attacks(offline and online), stolen-verifier attack. • Highly secure since both server and user authenticate each other. • Important data cannot be retrieved even after analyzing the data transmitted.	• Extra hardware token involvement.
(Long and Blumenthal, 2007)[38]	Designed Manageable-OTP by extending password generator for consumer applications.	• Increased consumer convenience by offering manageability for OTP based authentication systems. • Resistant against offline dictionary attacks.	• Employed symmetric encryption algorithm (AES-128) and one-way hash function (MD-5) that have already been compromised.
(Hallsteinsen and Jorstad, 2007)[39]	Presented a unified authentication scheme based on mobile phones	• Increases user adoptability and eliminates the weakness associated with many existing time synchronization based OTP schemes. • Reduces cost and burden of managing hardware token compared to other OTP schemes. • Offers resistance against eavesdropping, man-in-middle, replay, hacking, sniffing and guessing attacks.	• SMS has been used by the authentication server to perform key exchange and communication with user, that can be compromised. • Reduces user friendliness when client terminal does not possess Bluetooth facility.
(Jeong et al., 2008)[37]	Provided a novel authentication mechanism for home networks by using smart cards based on one time passwords.	• Minimized the computational overhead and communication cost. • Immune against various passive attacks viz. passive eavesdropping, replay, Man-In-The-Middle, Denial of Service and stolen verifier attacks. • Discards timestamp to eradicate serious time synchronization problem. • Offers user convenience by enabling home user to freely choose the password. • Avoided phishing attacks by providing mutual authentication between home user and authentication server. • Minimized burden on the systems involved in authentication mechanism as there is no need to store verification tables.	• Fails to preserve the privacy of transmitted data. • Protection against active attacks is not provided. • Smart cards are used for achieving authentication, that are not devoid of short comings.
(Li and Zhu, 2009)[32]	Designed a novel authentication mechanism between IEDs in substation automation based on Chebychev chaotic mapping	• Utilizes less memory as there is no need to store the whole sequence. • Chaotic sequence generated cannot be imitated by others. • One-way function employed ensures secure and easy authentication. • Chaotic sequence is sensitive to initial condition.	• Large number of chaotic sequence based authentication systems have already been cryptanalyzed effectively.
(Alghathbar and Mahmoud, 2009)[22]	Designed a novel one time password authentication	• Robust against shoulder surfing or eavesdropping.	• Usage of noisy passwords

	mechanism based on noisy password technique.		exponentially increases the processing time. • Less user-friendly.
(Liao et al., 2009)[34]	Presented a one-time-password authentication mechanism eliminating counter de-synchronization problem.	• Resolved counter de-synchronization problem. • Minimized security requirements of the server and provided easy integration in present enterprise applications. • Effectively minimized guessing and replay attacks.	• Employed symmetric encryption algorithm (AES-128) and one-way hash function (MD-5) that have already been compromised.
(Davaanaym et al., 2009)[28]	Proposed a secure and market-compatible mobile/web based authentication mechanism that generates OTP using PingPong128 stream cipher	• Resistant to attacks based on basic key-stream properties like period and linear complexity. • Overcomes time-memory tradeoff. • Easy implementation and can be executed on current costs incurred by servers from users.	• AES has been employed for encryption of generated OTP.
(Tao et al., 2009)[29]	Designed a novel two-way authentication scheme based on true random numbers generated by physical methods	• Password generation is random, fast and dynamic • Provides defense against many attacks e.g., interception, forgery, server-forged attacks, etc. • Improved efficiency of the server as well as the entire authentication process	• Cannot thwart guided phishing attack.
(Min-Qing et al., 2009)[36]	Introduced an enhanced self-updating hash chain based on LPCA.	• Eliminates practicality and security issues associated with the conventional infinite length hash chains (ILHC).	• Additional storage than the conventional authentication mechanisms is required since a part of next root seed is stored at each process
(Alzomai and Josang, 2010)[40]	Presented mobile phone as scalable OTP device based on trusted computing.	• Provided solution for achieving scalability and usability. • Minimized man in the middle attacks.	• SHA-1 has been employed as OTP generator on that theoretical attacks have been reported. • Restricts the user to generate valid OTPs when attacker masquerades the service provider. • Separation of mobile phones from user client terminal restricts usability. • Wide technical adoptability of the proposed system is not supported.
(Srivastava et al., 2011) [27]	Proposed an algorithm that implements a knock sequence employing AES capable of withstanding spoofing or sniffing attacks	• Almost impossible to detect and interpret the successive knock sequences • Implementation of multi-packet authentication mechanism prevents data to be divulged • Eliminates out-of-order delivery problem of packets • A range of attacks viz. man-in-the-middle attack, denial of service attack can be avoided	• OTP generated is sent over a GSM network
(Hsieh and Leu, 2011)[33]	Proposed an authentication mechanism based on time and location of mobile phone.	• Provided secure user authentication for accessing crucial internet services • Immune against various attacks such as eavesdropping, replay, brute force, and user impersonation attacks • Transparent user authentication • Improved precision of location prediction.	• GPS enabled mobile phones are required • Clock synchronization is required between mobile device and server
(Ren and Wu, 2012)[35]	Provides a secure authentication mechanism utilizing time and space factors	• Minimizes user's effort or/and the high overhead associated with generating OTP • Easy user adaption • Effectively resists Perfect-Man-in-the-Middle, stolen-verifier, replay and basic phishing attacks.	• Susceptible to phishing and other attacks that are highly sophisticated and on rise.
(Borowski and Lesniewicz, 2012)[41]	Presented an up-to-date usage of old one time keys or pads by introducing 100Mbits/sec binary generator.	• Provides absolute security by making use of 100Mbits/sec hardware binary random generator • Provides infinite source of one time keys	• Involves high cost for secure physical distribution of keys thus hampering adoptability
(Castiglione et al., 2014)[31]	An efficient end-to-end OTP authentication scheme involving AKE protocol and the keyed HMAC	• Simple and less computational overhead thus can be operated independently. • Provides transparency in addition to efficiency. • Resistant against wide range of attacks e.g., password guessing attack, offline dictionary attack, brute-force attack, replay attack, eavesdropping, stolen-verifier attack and denial-of-service attack • Suitably adoptable.	• Cannot be used when the number of iterations exceeds the length of the mutually agreed upon Master Key. • Security of the scheme relies on secure handling and storage of the Master Key.

B. Review of Non-OTP Based Schemes

Other than OTP based authentication schemes, researches have been conducted on security solutions that are based on biometrics, fuzzy vault schemes, chaotic mapping, etc.

The paper [5] demonstrates the usage of speech for identity authentication i.e. they make use of speech features obtained from speech recognition. Usage of speech features is highly beneficial as the same are having stability and uniqueness characteristics. Moreover, it is difficult to be forged and can be easily carried by the user, resulting in better user ergonomics. Speech authentication is associated with speech recognition that incorporates two fundamental phases, viz., feature extraction and matching. The security of speech authentication system can be easily compromised if the intruder succeeds in recording the voice of the authenticated user and uses this recorded voice to break the system.

In [42] authors have proposed a federation Single Sign-On (SSO) authentication scheme based on network identity. The one-pass authentication technique presented is very fast and secure since it ties together two authentication schemes viz. Network Attachment Control Function (NACF) and IP Multimedia Subsystem (IMS). The bundled authentication scheme is useful for the mobile users in the Next Generation Network (NGN). In NGN, the Federation SSO is a method used for authenticating IMS service and web application service, i.e., even if, only network operator is authenticated, there is no need to authenticate application service. It is thus evident that this method reduces the complexity as compared to previous approaches. To realize the federated SSO scheme, the prerequisites are Service Control Function (SCF), Network Access Control Access Function (NACF), Web Application Service Control Function (WASCF) and NGN Terminal Function (NTF). In this scheme, authors have introduced the Authentication and Key Agreement (AKA) vector in 3GPP that comprises of an Integrity Key (IK), a Cipher Key (CK), and a credential for authentication. The access network operator is there to provide the unified access authentication to both wired and wireless networks. The service network operator is there to provide IMS service authentication for the user equipment making use of SIP REGISTER. Here, MD5-Digest and MD5-AKA are employed for authentication purposes. The proposed scheme proves to have higher security and reliability as against the previous SSO authentication mechanisms owing to the use of a reliable network operator—NACF with Identity Provider. Thus, unlike the earlier systems where authentication is provided between application services, this federated single sign-on considers authentication between web application service and NACF. This scheme prompts the user to select or subscribe the bundled authentication process; hence the user is given privilege over the federation operator. It can prove beneficial when the user has to access the network about multiple service network operators. But it has been found that the proposed scheme fails to provide security against spoofing attack as it only involves information about the location of the user equipment and does not consider security operations. Moreover, some access identifiers need to be added to the profile of user equipment to identify the user because it is devoid of fixed line information.

An authentication scheme has been put forward in [43] to ensure secure user authentication in a cloud computing environment. Enormous volume of data has to be handled in real time in cloud computing, therefore it is imperative to devise an authentication system that is lightweight, cost-effective, fast and most importantly secure i.e. robust against attacks. Thus, the authors have presented a lightweight and efficient multi-user authentication mechanism that is based on Cellular Automata (CA) in cloud computing environments. The proposed scheme works in almost the same way as the One-Time-Password (OTP) authentication, the only difference being use of non-linear Cellular Automata (CA) for the purpose of random key generation.

The process of authentication has been illustrated between the user and the authentication server and is accomplished in two distinct phases: a setup phase and an authentication phase. The proposed system makes use of a CA-based Pseudo-Random Number Generator (PRNG) that gives the system several properties like vast area complexity, uniform structure, fast operation, prompt hardware implementation, uniform structure, etc. The security of the proposed scheme has been experimentally proven with the help of a DIEHARD test suite. The DIEHARD test has generated the p-value pass rate ≥ 85% that is measured as “good”. As a result, this authentication system proves to be secure. However, the security of this system can be further enhanced by improving the randomness of the pseudorandom generator. Furthermore, this authentication system is based on non-linear CA whereas linear CA could provide a much higher degree of randomness.

The paper [44] introduces a system that makes use of a fuzzy vault scheme for the protection of biometric information. The user authentication with the help of biometric data can prove to be a stronger security measure. The proposed scheme makes use of biometric information for authentication purpose that makes it more reliable since a biometric data cannot be lost, changed, copied and guessed. The fuzzy fingerprint vault has been found to be the most accepted solution to safeguard the fingerprint features. With the help of fuzzy vault scheme, the data can be made secure by combining it with a biometric template in such a way that only the user who is authorized can be granted access to the secret data after providing the genuine biometric. In previous systems, it was assumed that the fingerprints were already aligned but this was not a rational assumption regarding authentication systems based on fingerprints.

As a result, three solutions have been put forward by the authors for fuzzy fingerprint vault that make the biometric-based data authentication more secure and efficient i.e. automatic alignment of fingerprints based on a geometric hash table; a better and secure fuzzy fingerprint vault that can provide resistance against correlation attack; fuzzy fingerprint vault employing One-Time-Template (OTT) producing a diverse biometric template every time, just like One-Time-Password (OTP). These solutions have been proposed to improve the security of biometric data.

The proposed system has shown a performance of 91.17% Genuine Accept Rate (GAR) without affecting False Accept Rate (FAR) (0.6%) with an 8-degree polynomial in FVC2002 DBI. Also, the performance of 92.1% GAR and FAR (0%) has been reported with a 7-degree polynomial. In this scheme, there is no need to store additional information, e.g., geometry hash table, helper data, etc. that may otherwise degrade the security level of the system. The proposed scheme makes sure that the access to secret data is granted only to the authorized user, but there remains liability that some sophisticated attacks may compromise the secret data or biometric information. Moreover, this scheme is suitable for restricted applications only as the system cannot scale well to large service pool.

In [45] authors have presented a secure and efficient authentication system based on a smart card to protect against the vulnerabilities as well as to improve the security in the existing systems. The proposed authentication system allows the user to choose a password very conveniently and even modify it offline. This system blocks stolen user smart card attack because the smart card does not hold any important information. Also, the server attack has been eliminated by shifting the user authentication from the server to registration center that ensures that each server possesses a unique private key. Thus, this system provides high-level security and is more practical. There are three participating entities in this system i.e. user, server and registration center. The proposed system works on four protocols viz. the registration protocol, the login protocol, the authentication protocol and the password change protocol. The proposed scheme is flexible for the users in a way that it is the concealed identity that is transmitted and not the actual identity of the user. It provides an efficient and secure mechanism for changing the password because the user can very conveniently change his password without relying on the registration center. The proposed system was found to be more cost-efficient after performing a comparative analysis with other systems.

A new identity authentication scheme has been proposed in [46] with employs a Contactless Smart Card (CSC) that holds a multitude of biometric features. This authentication scheme is aimed to enhance airport security by securing logical access. The contactless smart card is useful for authentication because of its various features like the low mechanical complexity of the reader-writer unit, fast speed, reduced maintenance cost and secure physical access. The proposed authentication system makes use of fingerprint recognition and iris scanning for providing support to many fields such as airline passengers, border security, transportation security, law enforcement and logical access. In the proposed work, a Two Stage Random Number Generator (TSRG) has been employed that makes use of randomized encryption techniques to design a TSRG cryptosystem that is secure functionally. The fundamental biometric feature used in the proposed scheme is the fingerprint. For users who are not comfortable to enroll using fingerprint template, iris recognition has been recommended. Then, biometric authentication is performed to determine the identity of the user. This authentication scheme enrolls the biometric live features of the user. Moreover, the usage of Ferroelectric Random Access Memory (FRAM) technology in smart cards augments the efficiency of the proposed system as it consumes less power, has a higher write speed and greater rewrite endurance as compared to its counterpart i.e. EEPROM. Despite its numerous features, there lies further scope for improvement in the design paradigm of the proposed system by focusing on coordination, cooperation and interoperability.

In [47], the authors have re-examined the security claims of Predicate-based Authentication Service (PAS) and successfully indicated PAS was insecure against probabilistic attack and brute force attack. The PAS system claims security against three attacks: random guess, SAT (satisfiability solver) and brute force attacks that is highly over-estimated. The proposed system introduces probabilistic attack, which even with a small session of authentication breaks part of the password.

Further, it was also found that the PAS system is poor in terms of complexity and security against low complexity than Cognitive Authentication Scheme (CAS). The attack is also computationally efficient and reduces the PAS system to challenge-response based OTP system. Thus, it has less security as well as usability than OTP systems. However, the probabilistic attack introduced on PAS is unable to completely break the password or secret key shared between server and user.

The prominent pros and cons of a variety of Non-OTP based security techniques have been framed in Table II as follows:

TABLE II. REVIEW OF NON-OTP BASED SCHEMES

AUTHOR	CONTRIBUTION	RESULT OBTAINED	LIMITATIONS
(David et al., 2003)[46]	A new identity authentication scheme employing contactless smart card that holds biometric features aimed to enhance airport security	• High reliability provided by features of contactless smart card. • Usage of FRAM augments efficiency. • Contactless smart card widens the arena of its applications from logical access to physical access. • High security ensured by combining TSRG data with several cryptographic methods.	• Additional research needs to be carried out to examine its adoptability. • Further scope for improvement in the design paradigm of the system by focusing on coordination, cooperation and interoperability.
(Li et al., 2009)[47]	Re-examined the security claims of PAS by inducing Probabilistic attack over the same.	• Successfully illustrated weakness associated with PAS towards probabilistic and brute force attacks.	• Fails to provide satisfactory solution to tackle the security issues with PAS thus hampering adoptability.
(Kim et al., 2010)[42]	Proposed a federation oriented single sign-on authentication scheme based on network identity	• Eliminates issues like message overhead and latency by bundling together NACF and IMS authentications. • Higher security and reliability as authentication is being provided between web application service and NACF. • Proves beneficial when user has to access network with regard to multiple network service operators.	• Access identifiers need to be added to the profile of user equipment to identify the user. • Only one Proxy Call Session Control Functional Entity (P-CSC-FE) is connected to NACF that is not feasible in real time. • Vulnerable to spoofing attack.
(Moon et al., 2012)[44]	Proposed three solutions for fuzzy fingerprint vault to improve the security of biometric data	• Highly reliable as biometric data cannot be lost, copied, changed or guessed. • Suitable for crypto-biometric systems since it works with unordered sets. • Infeasibility of polynomial reconstruction ensures its security. • Resistant to correlation attack. • Improved performance of GAR is fetched without affecting FAR.	• Once compromised, fuzzy vault cannot be revoked. • Biometric information may be compromised by some sophisticated attacks. • Suitable for restricted applications as the system cannot scale well to large service pool.
(Shin et al., 2012)[43]	Proposed a lightweight multi-user authentication mechanism based on non-linear cellular automata for cloud based environments	• Use of CA-based PRNG makes the system fast and implementable architecture-wise. • Resistant to various attacks like replay attack, reflection attack and eavesdropping.	• Based on non-linear CA whereas linear CA could provide much higher degree of randomness.
(Ma et al., 2013)[5]	Designed an identity authentication mechanism based on speech features.	• Provides better user ergonomics.	• Can be compromised if intruder used recorded voice of authenticated user.
(Aboud, 2014)[45]	Presented a secure and efficient authentication system based on smart cards	• Resistant to multitude of attacks e.g., stolen attack, offline dictionary attack, user attack, server attack, etc. • System turns out to be more flexible to the user as user anonymity is taken care of in the same. • No reliance on registration centre for password change. • Cost-efficient as compared to existing systems.	• Usage of an extra token shall cause inconvenience to users and may even prove to be expensive solution for service provider.

III. OPEN ISSUES

After performing the study of numerous security techniques taken up in access management as have been conducted by researchers, it can be concluded that there are still some loopholes in the proposed security solutions. The limitations have been found to be about several areas ranging from technical adoptability to computational complexity to communication media employed for the said purpose. Finally, the progressive survey conducted in this paper ends with the inference of open issues as mentioned below:

- As can be observed from the study of various authentication schemes [33][37][45][30][40][39][22], special featured hardware tokens, smart cards and other chip modules have been projected that lead to user inconvenience and may prove expensive to the service provider. Thus, these systems lack user ergonomics and this impeding their technical adoptability.
- OTP distribution is a grave issue as ascertained from the review of prevalent authentication mechanisms. It is observed that there is a dependence on external parties such as GSM or some authorized individuals [39][41][27][28].
- Numerous issues have been uncovered with the existing authentication systems [36][22][26][44] like

high storage, elevated processing time and computational cost and degradation of system speed owing to public key operations, self-updating hash chains and fuzzy vault schemes.

- Although there are some systems like [38][40][42] that allow a user to access services from multiple service providers from a single token, but majority of the authentication mechanisms discussed in the literature fall dumpy in this aspect. As a result, users craving for amenities from multiple service providers shall have to maintain different tokens for each service provider.
- There are several systems for authentication [44] that are suitable for restricted applications only, given the fact that they cannot scale well to larger service pools.
- Majority of authentication mechanisms in place [28][38][34][40], offer weak security by employing password generation schemes like SHA-1, AES, MD-5 etc, that prove to be insecure and fail on the lines of continual existence.
- It has been found that some of the authentication and authorization systems discussed in the literature employ multiple communication channels [28][40] that becomes quite infeasible to catch up in real life scenarios and further will burden the user on lines of service charges.

IV. Conclusion

The paper presents the explicit discussion of the prior research works introduced in the past for the purpose of incorporating secure authentication and authorization for any legitimate members attempting to perform secure transactions. Both significant contributions and weaknesses of these security schemes have been elaborated upon overtly. It was observed that all the authentication mechanisms aim at providing complete security but have failed in one context or the other. Some of authentication schemes employ complex cryptography that degrades system performance by increasing complexity, and are even unable to conform upon user ergonomics in an effective manner. At the same time, these authentication schemes cannot provide continued support as they bow down to advancement in the computation. It can be safely concluded that although large volume of research has been conducted in the discussed domain, but there still exist some gaps that need to be crammed because of the advent of new hacking tools and techniques on the part of hackers.

Acknowledgment

We would like to express gratitude towards Prof. Abdul Rashid Trag (*Vice Chancellor Islamic University of Science & Technology*) for his support throughout the many years of our stay at *IUST*. We are sincerely thankful to Sheikh Asif (*Assistant Registrar Academics* at *IUST*) for his aspiring guidance, invaluably constructive criticism and friendly advice during this research.

References

[1] M.A. Thakur and R. Gaikwad, "User identity and Access Management trends in IT infrastructure-an overview", in *Pervasive Computing (ICPC), 2015 International Conference on*, Pune, 2015, pp. 1 - 4.

[2] S. Xiaoling, "The study on computer network security and precaution", in *Computer Science and Network Technology (ICCSNT), 2011 International Conference on (Volume:3)*, Harbin, 2011, pp. 1695 - 1698.

[3] J. Kizza, *Computer network security*. New York: Springer, 2005.

[4] C. Yan-ping, L. Dong-liang and G. Rui, "Security and precaution on computer network", in *Future Information Technology and Management Engineering (FITME), 2010 International Conference on (Volume: 1)*, Changzhou, 2010, pp. 5 - 7.

[5] H. Ma, S. Yan, X. Bai and Y. Zhu, "The Research and Design of Identity Authentication Based On Speech Feature", in *Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on*, Nangang, 2013, pp. 166 - 169.

[6] W. Stallings, *Cryptography and Network Security*, 5th ed. India: Pearson Education, 2011.

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

[8] W. Highleyman and S. Associates, Inc, "Hacked AP Tweet Crashes Markets", availabilitydigest, 2013. [Online]. Available: http://www.availabilitydigest.com/. [Accessed: 21- May- 2015].

[9] Z. Zhao, Z. Dong and Y. Wang, "Security analysis of a password-based authentication protocol proposed to IEEE 1363", *Theoretical Computer Science*, vol. 352, no. 1-3, pp. 280-287, 2006.

[10] A. Conklin, G. Dietrich and D. Walz, "Password-Based Authentication: A System Perspective", in *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, 2004.

[11] P. Elftmann, "Secure Alternatives to Password-based Authentication Mechanisms", 1st ed. RWTH Aachen University Aachen, Germany, 2006.

[12] B. K. Marshall, "Tips for Avoiding Bad Authentication Challenge Questions", 1st ed. White Paper, 2007.

[13] A. Narayanan and V. Shmatikov, "Fast Dictionary Attacks on Passwords Using Time-Space Trade-off", in CCS '05 Proceedings of the 12th ACM conference on Computer and communications security, New York, NY, USA, 2005, pp. 364-372.

[14] C. Goel and G. ARYA, "Hacking of Passwords in Windows Environment", International Journal of Computer Science & Communication Networks, vol. 2(3), pp. 430-435, 2012.

[15] N. Adhikary, R. .Shrivastava, A. Kumar, S. Verma, M. Bag and V. Singh, "Battering Keyloggers and Screen Recording Software by Fabricating Passwords", International Journal of Computer Network and Information Security, vol. 5, pp. 13-21, 2012.

[16] www.bloggingstocks.com, "headline-reports-ebay-hacked", 2007. [Online]. Available: http://www.bloggingstocks.com. [Accessed: 17- May- 2015].

[17] www.grahakseva.com/complaints, "online fraud happened hacking my icici bank credit card", 2013. [Online]. Available:http://www.grahakseva.com/complaints/130310/online-fraud-happened-hacking-my-icici-bank-credit-card. [Accessed: 01- May- 2015].

[18] www.foxnews.com, "World Bank Under Cyber Siege in Unprecedented Crisis", 2008. [Online]. Available:http://www.foxnews.com/story/2008/10/13/world-bank-under-cyber-siege-in-unprecedented-crisis/. [Accessed: 27- May- 2015].

[19] J. Vacca, *Computer and information security handbook*. Amsterdam: Elsevier, 2009.

[20] J.C. Liou and S. Bhashyam, "A feasible and cost effective two-factor authentication for online transactions.", in *Software Engineering and Data Mining (SEDM), 2010 2nd International Conference on*, Chengdu, China, 2010, pp. 47 - 51.

[21] F. Cheng, "A Novel Rubbing Encryption Algorithm and the Implementation of a Web Based One-time Password Token." in *Computer Software and Applications Conference (COMPSAC), 2010 IEEE 34th Annual*, Seoul, 2010, pp. 147 - 154.

[22] K. Alghathbar and H. A. Mahmoud, "Noisy Password Scheme: A New One Time Password System", in *Electrical and Computer Engineering,*

2009. CCECE '09. Canadian Conference on, St. John's, NL, 2009, pp. 841 - 846.

[23] L. Soares, D. Fernandes, M. Freire and P. Inacio, "Secure user authentication in cloud computing management interfaces", in *Performance Computing and Communications Conference (IPCCC), 2013 IEEE 32nd International*, San Diego, CA, 2013, pp. 1-2.

[24] P. Thiyagarajan, V. Venkatesan and G. Aghila, "Anti-phishing technique using automated challenge response method", in *Communication and Computational Intelligence (INCOCCI), 2010 International Conference on*, Erode, 2010, pp. 585 - 590.

[25] M. Bond, O. Choudary, S. Murdoch, S. Skorobogatov and R. Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack", in *Security and Privacy (SP), 2014 IEEE Symposium on*, San Jose, CA, 2014, pp. 49-64.

[26] K. Bicakci and N. Baykal, "Infinite Length Hash Chains and Their Applications", in *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops on*, Ankara, Turkey, 2002, pp. 57 - 61.

[27] V. Srivastava, A. Keshri, A. Roy, V. Chaurasiya and R. Gupta, "Advanced Port Knocking Authentication Scheme with QRC Using AES", in *Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference on*, Udaipur, 2011, pp. 159 - 163.

[28] B. Davaanaym, Y. Lee, H. Lee and S. Lee, "A Ping-Pong Based One-Time-Passwords Authentication System", in *INC, IMS and IDC, 2009. NCM '09. Fifth International Joint Conference on*, Seoul, 2009, pp. 574 - 579.

[29] F. Tao and S. Ping, "Design of Two-Way One-Time-Password Authentication Scheme Based on True Random Numbers", *Computer Science and Engineering, 2009. WCSE '09. Second International Workshop on*, vol. 1, pp. 11 - 14, 2009.

[30] Y. Chang, C. Chang and J. Kuo, "A secure one-time password authentication scheme using smart cards without limiting login times", *SIGOPSOper. Syst. Rev.*, vol. 38, no. 4, pp. 80-90, 2004.

[31] A. Castiglione, A. De Santis, A. Castiglione and F. Palmieri, "An Efficient and Transparent One-Time Authentication Protocol with Non-Interactive Key Scheduling and Update", in *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on*, Victoria, BC, 2014, pp. 351 - 358.

[32] L. Li and Y. Zhu, "Authentication Scheme for Substation Information Security Based on Chaotic Theory", in *Power and Energy Engineering Conference, 2009. APPEEC 2009. Asia-Pacific*, Wuhan, 2009, pp. 1 - 3.

[33] W. Hsieh and J. Leu, "Design of a Time and Location Based One-Time Password Authentication Scheme", in *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, Istanbul, 2011, pp. 201 - 206.

[34] S. Liao, Q. Zhang, C. Chen and Y. Dai, "A unidirectional one-time password authentication scheme without counter desynchronization", in *Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on (Volume: 4)*, Sanya, 2009, pp. 361 - 364.

[35] X. Ren and X. Wu, "A Novel Dynamic User Authentication Scheme", in *Communications and Information Technologies (ISCIT), 2012 International Symposium on*, Gold Coast, QLD, 2012, pp. 713 - 717**.**

[36] Z. Min-Qing, D. Bin and Y. Xiao-Yuan, "A New Self-Updating Hash Chain Structure Scheme", in *Computational Intelligence and Security, 2009. CIS '09. International Conference on (Volume: 2)*, Beijing, 2009, pp. 315 - 318.

[37] J. Jeong, M. Young Chung and H. Choo, "Integrated OTP-Based User Authentication and Access Control Scheme in Home Networks", in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, Waikoloa, HI, 2008, pp. 294.

[38] M. Long and U. Blumentthal, "Manageable One-Time Password for Consumer Applications", in *Consumer Electronics, 2007. ICCE 2007. Digest of Technical Papers. International Conference on*, Las Vegas, NV, 2007, pp. 1 – 2.

[39] S. Hallsteinsen, I. Jørstad and D. Van Thanh, "Using the mobile phone as a security token for unified authentication", in *Systems and Networks Communications, 2007. ICSNC 2007. Second International Conference on*, Cap Esterel, 2007, p. 68.

[40] M. Alzomai and A. Josang, "The Mobile Phone as a Multi OTP Device Using Trusted Computing", in *Network and System Security (NSS), 2010 4th International Conference on*, Melbourne, VIC, 2010, pp. 75 – 82.

[41] M. Borowski andM. Lesniewicz, "Modern Usage of "Old" One Time Pad", in *Communications and Information Systems Conference (MCC), 2012 Military*, Gdansk, 2012, pp. 1 - 5.

[42] K. Kim, S. Jo, H. Lee and W. Ryu, "Implementation for federated Single Sign-on based on network identity", in *Networked Computing (INC), 2010 6th International Conference on*, Gyeongju, Korea (South), 2010, pp. 1 - 3.

[43] S. Shin, D. Kim and K. Yoo, "A Light-Weight Multi-User Authentication Scheme Based On Cellular Automata in Cloud Environment", in *Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on*, Paris, France, 2012, pp. 176 - 178.

[44] K. Moon, D. Moon, J. Yoo and H. Cho, "Biometrics Information Protection Using Fuzzy Vault Scheme", in *Signal Image Technology and Internet Based Systems (SITIS), 2012 Eighth International Conference on*, Naples, 2012, pp. 124 - 128.

[45] S. Aboud, "Secure Password Authentication System Using Smart Card", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 3, no. 1, pp. 75-79, 2014.

[46] M. David, G. Hussein and K. Sakurai, "Secure Identity Authentication and Logical Access Control for Airport Information Systems", in *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on*, 2003, pp. 314 - 320.

[47] S. Li, H. Jameel Asghar, J. Pieprzk, A. Sadeghi, R. Schmitz, and H. Wang, "On the Security of PAS (Predicate-Based Authentication Service)", in Computer Security Applications Conference, 2009. ACSAC '09. Annual, Honolulu, HI, 2009, pp. 209 - 218.