Securely Eradicating Cellular Dependency for E-Banking Applications

Bisma Rasool Pampori, Tehseen Mehraj
Department of Info. Tech.
Central University of Kashmir
Srinagar, Kashmir, India

Asifa Mehraj Baba
Department of ECE
School of Technology
IUST, Awantipora, Kashmir

Burhan Ul Islam Khan
Department of CSE
School of Technology
IUST, Awantipora, Kashmir

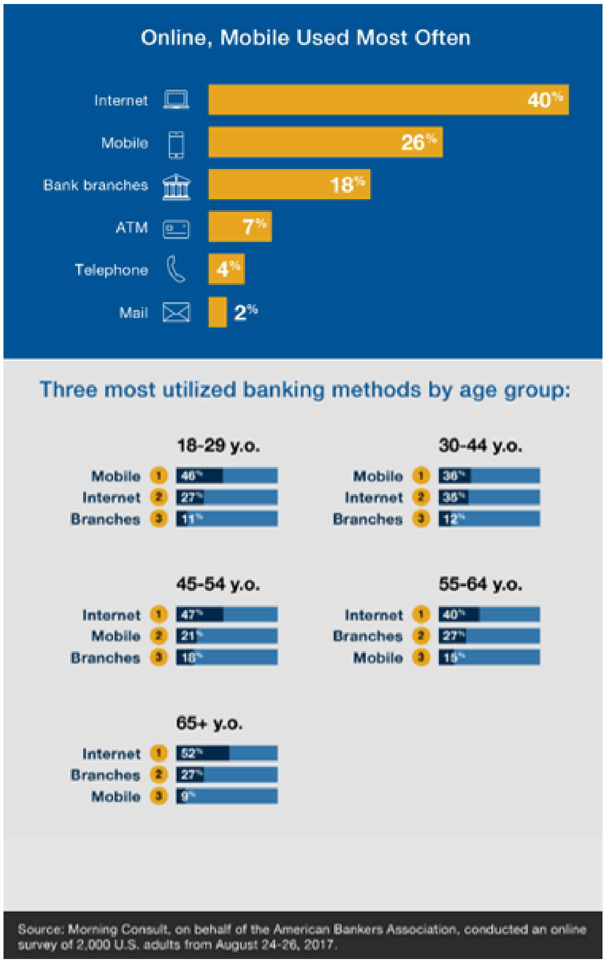
Zahoor Ahmad Najar
Department of Info. Tech.
Central University of Kashmir
Srinagar, Kashmir, India

***Abstract*—Numerous applications are available on the Internet for the exchange of personal information and money. All these applications need to authenticate the users to confirm their legitimacy. Currently, the most commonly employed credentials include static passwords. But people tend to behave carelessly in choosing their passwords to avoid the burden of memorizing complex passwords. Such frail password habits are a severe threat to the various services available online especially electronic banking or e-banking. For eradicating the necessity of creating and managing passwords, a variety of solutions are prevalent, the traditional ones being the usage of One-Time-Password (OTP) that refers to a single session/transaction password. However, the majority of the OTP-based security solutions fail to satisfy the usability or scalability requirements and are quite vulnerable owing to their reliance on multiple communication channels. In this paper, the most reliable and adoptable solution which provides better security in online banking transactions is proposed. This is an initiative to eradicate the dependency on Global System for Mobile communication (GSM) that is the most popular means of sending the One-Time-Passwords to the users availing e-banking facilities.**

***Keywords*—E-banking; one time password (OTP); global system for mobile communication (GSM); authentication**

I. Introduction

The Internet has proved to be the fastest emerging medium in the present day for delivering services in both retail and corporate banking sectors [1]. Electronic banking (E-Banking) is one of the significant developments that have revolutionised the banking sector. Electronic banking is defined as "the technology which allows customers to access the banking services electronically like to pay bills, transfer funds, and view the accounts details and advices" [2]. It provides automatic delivery of conventional and new banking services/products directly to users via interactive and electronic communication channels. Electronic or online banking comprises of the systems that facilitate the customers of financial institutions and individuals for accessing their accounts, performing business transactions, or acquiring information on commercial products/services by using a private or public network. E-banking is a standard term that encompasses mobile banking, internet banking, telephone banking, etc. Furthermore, the evolvement of E-banking services using numerous electronic communication channels such as cell phone, telephone, internet, etc. has presented a convenient and feasible way of providing banking services [3].



Source: Morning Consult, on behalf of the American Bankers Association, conducted an online survey of 2,000 U.S. adults from August 24-26, 2017.

Fig. 1. Preferred banking method (*Adopted from source*[1]).

The emergence of e-banking is not just coerced by the banks’ need to minimise costs, but it is an actualisation of customers' demand who crave for online access to their bank services anytime and anywhere [1]. Numerous reasons make the importance of E-banking evident. First and foremost, it provides unparalleled convenience to its customers by accrediting 24×7 access to a wide variety of services. Moreover, it presents a cost-efficient alternative to branch and telephone banking owing to the comparatively low maintenance and capital cost, along with its ability to offer entirely automated processing of transactions [1].

With the analysis, it has been observed that most of the users all over the world prefer to use net-banking. Fig. 1 illustrates the use of net-banking which gives the fair idea of the popularity of Internet banking among various age groups in the United States.

As per survey [1], 40% of nationals in America prefer managing their bank accounts online as compared to other methods. About 26% customers perform their banking transactions using mobile phones whereas only 18% visit the bank branches on their own.

Even in Canada, more than 68% of the citizens prefer mobile and online banking. Although online banking is popular, mobile banking is gaining popularity. About 51 percent of Canadian nationals make use of the Internet as the primary banking method which is 4 percent less than the margin in 2014. This is due to the rise in mobile banking among them with 17 percent of the individuals utilizing mobile phones as their principal banking mode which is 9 percent higher than that in 2014[2].

In India, online banking has brought about a significant change in the banking industry with the introduction of National Electronic Funds Transfer (NEFT), Real Time Gross Settlement (RTGS), Immediate Payment Service (IMPS), mobile banking, credit cards, prepaid cards, debit cards, etc. [4]. There has been a drastic jump in the values of transactions conducted on mobile wallets and PPI (Prepaid Payment Instruments) cards from Rs. 82 billion and Rs. 105 billion respectively in 2014-2015 to Rs. 532 billion and Rs. 277 billion respectively in 2016-2017[3].

It is thus evident that banking industry has made unparalleled success in delivering its services ranging from telephone banking to computer-based banking applications progressing to Automated Teller Machine (ATM) and Internet banking. There has been a dramatic development in the field of mobile communication technologies with the introduction of WAP, 3G technology, SMS, etc. which has led to the broad expansion of mobile telecommunication. The latest developments in technology in conjunction with the increased rate of acceptance of mobile phones have persuaded the business enterprises to launch and develop a variety of services via mobile phones [5]. On the same lines, the banking sector resolved to build banking applications on mobile devices in order to provide mobility in addition to the inherent features of mobile technology to their customers which was absent in the conventional electronic banking methods. Mobile banking – a subset of E-banking – provides personalisation, dissemination, flexibility and ubiquity which promises unmatched productivity, profitability and market potential to businesses. Moreover, the users find mobile banking more convenient and feasible on the ground of security and adoptability as compared to the traditionally employed approaches [6]. Furthermore, in India, the Governor of Reserve Bank of India (RBI) is sturdily in favour of making use of mobile phones as devices for carrying out bank transactions. Keeping in view the drastic fall in tariffs associated with mobile phones coupled with the flawless connectivity of mobile and fixed lines, mobile banking has evolved as a cost-efficient banking channel today [2].

Despite the numerous facilities offered by the internet banking, it is not devoid of shortcomings. The existing internet banking system has been found to be open to the danger of hacking and a range of other attacks [7], [8]. Although the various attack methods are diverse, the primary objective of the intruders is to acquire confidential information of users, e.g., social security numbers, usernames and passwords, credit card numbers, etc. All these are static credentials, i.e. these do not change. Primarily, the users tend to select passwords which are unsafe but easy to memorise. As a result, these are vulnerable to a variety of attacks such as dictionary attacks. With the current availability of numerous powerful and sophisticated hacker tools as well as keylogger software, it has become an easy task for the intruder to retrieve the password. In the existing system, neither private nor public network is fully secure. There have been numerous events in the past where reputable enterprise agencies such as Walmart, eBay, World Bank, ICICI Bank, etc. have been hacked which resulted in massive loss of both confidential information and property [9]. Thus, there is an urge to adopt a strategic and long-term approach which can meet the much-desired security concerns of the users.

A. *OTP Utilization in Banking*

With the rapid expansion in computerisation of small and large businesses, authentication is the need of the hour to provide security against the emerging threats. Authentication assures secure online transactions and facilitates the development of trust among the trading partners dealing online [9]. Authentication is a procedure by which an entity establishes a claimed property to another entity. In other words, it deals with testing or verifying who an information resource or person claims to be, which adequately convinces the authenticator that the claimed identity is valid. It is followed by authorisation which evaluates whether the authenticated entity has the privilege to access the resources [10]. In general, authorisation can be referred to as the permission to access and the determination of privileges that an entity has on a system and what the entity is allowed to do with the resources [11].

[1] "Survey: Online, Mobile are Most Popular Banking Channels", Aba.com, 2017. [Online]. Available: https://www.aba.com/Press/Pages/092117ConsumerSurveyBankingPreferences.aspx. [Accessed: 15- Jan- 2018].

[2] "Issue Brief: How Canadians Bank", *Cba.ca*, 2017. [Online]. Available: https://www.cba.ca/technology-and-banking. [Accessed: 15- Jan- 2018].

[3] "Digital revolution in the Indian banking sector | Forbes India", *Forbes India*, 2017. [Online]. Available: http://www.forbesindia.com/article/weschool/digital-revolution-in-the-indian-banking-sector/47811/1. [Accessed: 15- Jan- 2018].

Authentication can be achieved in one of the three ways [12], [13]:

a) Something the user only knows, e.g., a private key, a password, a Personal Identification Number (PIN) or a secret key.

b) Something possessed by the user or a physical item exclusively owned by the user, e.g. a driver's license, a credit card, a passport, a smart card or an identification card.

c) Something the user is, e.g. facial characteristics, retinal pattern, or fingerprints.

d) Something the user produces, e.g. voice pattern, handwriting characteristics and current signature.

It has been observed that the authentication based only on the first type, i.e. something a user knows (static password) is vulnerable to phishing attacks. Online banking applications require rigorous user authentication. Most often, user authentication is realized by employing two-factor authentication (2FA) technique, which is a two-level security approach -- based on something the user only knows, viz. a static password, and something the user possesses, viz. a One Time Password (OTP) [14]. Biometrics is not used for authentication purposes in banking for reasons like cost, reliability, privacy, and complexity. It has been found that the most commonly used authentication technique is based on the usage of passwords as they are easy to implement, convenient, inexpensive and highly adopted by masses but they are relatively simple to be stolen or broken [11], [9]. Consequently, a reliable and hard-to-crack authentication is needed which can be provided by one-time-password system [15]. One-time-passwords, also referred to as single-use passwords, are dynamic, i.e. these are changed every time they are used. OTPs are considered to be the most reliable variant of passwords and provide an effective solution for security [10]. In internet banking, one-time passwords play a prominent role in providing authentication to enhance the security. OTPs impart an additional layer of security above the conventional static passwords which are vulnerable to replay attacks. OTPs offer immunity against replay attacks as the unique password generated once can never be repeated which implies that even if the attacker procures the OTP, it will be futile [16]. In banks, OTPs are used in conjugation with static passwords which offer a strong defence against numerous online attacks [9]. Regardless of this win-win proposal, the distribution of OTPs to the concerned user is a significant issue. There are certain pitfalls in the existing method of delivery of OTPs particularly in regions like Kashmir where most of the time SMS service is banned. Our proposed work is an initiative to eradicate those issues by putting forward an alternate solution for distribution of OTP to the user.

This paper is comprised of five sections. Section 2 discusses the variety of authentication/authorization schemes currently employed followed by the architecture of the proposed system in Section 3. Section 4 covers the illustration of the implementation details of the authentication mechanism proposed. Section 5 provides the analysis of results, and finally, the concluding remarks along with future scope have been elucidated in Section 6.

II. Evaluation of Existing Security Solutions

There has been a considerable change in the security means of online banking since the short span it has been in use. Particularly, the authentications schemes utilized in previous systems have been found to be susceptible to numerous attacks like man-in-the-browser, phishing, password sniffing, malware, etc. This section investigates the prevailing authentication and authorization schemes concerning the usability and security of online transactions.

Authors in [17] have set forth a novel two-factor authentication mechanism based on OTP using mobile phones. Two nested hash functions, i.e., SHA-1 and MD-5 have been employed in this system to provide online authentication. In this system, SMS based OTPs are eradicated as OTP is generated on a user mobile phone thus eliminating the use of separate tokens providing usability. However, the proposed system fails to give efficient storage and user ergonomic authentication as the generated OTP is 128-bit data which is difficult to be entered manually by the user.

A scheme has been put forward in [18] referred to as 'Infinite Length Hash Chains' to enhance the extensibility and efficiency of the traditional idea of hash chaining by employing public key techniques. In this scheme, the hash chain length has been extended infinitely thus avoiding the need to reboot the system. A one-way hash function based on a public key algorithm provides an infinite source that forms the core of OTP production.

In [9], authors have performed a detailed study of various authorisation and authentication systems proposed beforehand, with the goal to highlight the numerous issues still prevailing in the existing field. The paper embroils schemes offered to alleviate the number of security threats present in access management both in private as well as public networks. The review has been carried out by categorising numerous authentication techniques and approaches into non-OTP and OTP based schemes. Although OTP based methodologies were found to be more robust in providing the required security than non-OTP-based schemes, all the techniques surveyed in this paper have been found to have some loopholes ranging from the type of communication medium used, to the computational complexity of the technique, to their technical adoptability. Some methods have been found to be costly for the service provider along with the associated customer, hence proving deficient in user ergonomics and obstructing their technical adaptability in general. Many issues have been highlighted resulting from techniques which involve dependency on outside parties, for instance, GSM or certain authorised entities either for OTP distribution or communication with the user, all of them are found to face obstructions. Further, some techniques discussed in this paper have been found to make use of multiple communication channels which burdens the customers with substantial service charges and at the same time have proven to be infeasible. The paper concludes that a major portion of the considered authentication mechanisms was found to be weak in providing security owing to various password generation schemes like MD-5, SHA-1, and AES, etc. employed by the techniques, which have been found to be unsuccessful both in providing strong security and in maintaining their continual existence as there exists an exponential growth in the network security issues.

A system has been presented in [19] that makes use of OTP as the One Time Key to perform AES encryption along with Quadratic Residue Cipher (QRC). This leads to spoofing of the source IP addresses multiple times, therefore, increasing the complexity required to find the sequence of packets and IP addresses. The OTP and the random numbers generated are transmitted to the user via SMS which poses several restrictions to the client in terms of cost, security and transmission.

An authentication technique based on mobile/web has been put forward in [20] to enhance multi-factor authentication which is used for verification of the user as well as the current transaction. The proposed system makes use of PingPong 128 stream cipher for the generation of OTP keys which are encrypted using Advanced Encryption Scheme (AES). The dissemination of ICs to the end user's device is done by an authorised person via the web browser, or Bluetooth enabled device.

Authors in [21] have presented a novel authentication scheme which generates OTP by using time as well as location information of mobile device. The proposed scheme enhances security by restricting the validity of OTP generated to a confined geometrical location and a definite time-period. The user is facilitated with transparent authentication provided the user moves consistently, hence enabling the user to avoid entering credentials manually every time. This system provides user authentication for accessing crucial online services for instance e-banking transactions and e-commerce; resistance against numerous attacks, e.g., replay, man-in-the-middle (MIM), brute force, eavesdropping, user impersonation and dictionary attacks. However, clock synchronization between server and mobile device is difficult to acquire as mobile phones are likely to go out of network coverage resulting in failure in synchronization.

In [22], an OTP based authentication mechanism was introduced that eliminates the issue of counter de-synchronisation by implementing the one-way hash function and symmetric encryption algorithm. Further, the proposed system has successfully been able to minimise several attacks such as replay, Denial of Service (DoS) and guessing attacks. Symmetric encryption technique, i.e. Advanced Encryption Standard (AES) in conjunction with one-way hash function (MD5) has been employed by the system. The scheme offers easy implementation in current enterprise applications, and server-side security requirements are also minimised.

An authentication mechanism designed for home networks has been introduced in [23]. The framework employs OTP-based smart cards which offer secure authentication. Mutual authentication is achieved using three-way challenge-response handshake. The system makes home networks resilient against various passive attacks as well as phishing attacks. System security is centred on the one-way characteristic of the hash function and a nonce that has been used to thwart the problem of time synchronisation. However, this system fails to protect against numerous active attacks.

A technique was proposed in [24] that extend the password generator to improve OTP-manageability. The proposed system presents better performance in terms of computation cost related to the generation and verification of password in addition to the bandwidth associated with transmission. A Manageable One Time Password (M-OTP) module has been used in this scheme that may be some firmware module or any software program on the user device. Advanced Encryption Standard (AES) algorithm used in this system provides the necessary encryption along with one-way functionality.

A One-Time-Password (OTP) MIDlet has been put forward by authors in [25] that work on the user's mobile phone to provide integrated authentication for various critical internet services. The proposed system uses two different channels, i.e., GSM and internet to send and receive authentication messages. A challenge-response approach is employed by the system for OTP generation. This model uses Java MIDlet embedded on the Java-enabled mobile phone on the user side and an applet on the user's computer to transmit OTP to servlet acting as an authentication server. The fundamental characteristic of the scheme is that it involves closed loop formation among system components. HTTPS connection is used by the authentication server to connect applet and SMS facility provided by GSM to connect the mobile phone. Moreover, the mobile phone needs to possess Bluetooth facility to enter the credentials else the user has to enter those manually.

In [26], authors have put together the advantages of software as well as hardware tokens by embedding both on mobile phones with hardware Mobile Trusted Module (MTM) enabled in them. This technique offers better usability along with security and scalability options for OTP generation based on mobile phones embedding trusted computing technology. The system presented uses SHA-1 for OTP generation. Two different channels, i.e. GSM network and the internet, used in this system, result in a considerably complex system making it difficult for the intruder to carry out a man-in-the-middle attack.

The limitations as well as the main contributions of the researches conducted by various authors so far in the field of authentication and authorization have been presented in Table I.

As can be observed from the findings in Table I, the prevailing authentication solutions face potential threats and may not be able to support in the long run with the advancements in attacks conducted by intruders and introduction of quantum computing. Other significant issue includes the distribution of OTP via GSM networks which face issues like delay and cost associated with SMS, roaming constraints, weak security, government regulatory restrictions, etc. Also, the existing authentication solutions fail in terms of providing scalability, flexibility, cost-effectiveness, reliability and technical adoptability. To tackle these challenges, the alternative solution proposed has been given in the following section:

TABLE I. SUMMARY OF FINDINGS

AUTHOR	CONTRIBUTION	RESULT OBTAINED	LIMITATIONS
(Eldefrawy et al., 2011) [17]	Designed a novel two-factor authentication mechanism using mobile phones.	• Less computation time offered since no dependence on public key techniques.	• 128-bit OTP generated is neither storage efficient nor user-friendly. • Reported attacks on SHA-1 make it impractical to be used for security purposes.
(Bicakci and Baykal, 2002) [18]	Presented a flexible Infinite Length Hash Chain based on a public-key algorithm for OTP generation.	• The user is granted the freedom to move in any direction in the chain further offering no restriction on the length of the chain • Complexity because of restarting the system and communication overhead is averted.	• Low computation devices (e.g. mobiles phones) fail to implement this technique due to higher complexity offered by system owing to use of public key operations.
(Long and Blumenthal, 2007) [24]	Proposed an efficient Manageable One Time Password (M-OTP) via the extension of the password generator.	• Successfully thwarts offline dictionary attacks. • Enhances the manageability of OTP for consumer applications thereby resulting in better user convenience.	• Usage of MD-5 and AES-128 is not apt which have eventually proven to be compromised.
(Hallsteinsen and Jorstad, 2007) [25]	Designed a mobile phone-based OTP-MIDlet for unified authentication.	• Lowers management cost of hardware tokens than previous OTP-based approaches. • Provides resilience against a range of attacks like hacking, eavesdropping, man-in-the-middle, replay, guessing and sniffing attacks.	• Dependence of the client terminal on Bluetooth facility hampers user-friendliness. • Exchange of keys and user communication is done by authentication server making use of GSM network.
(Davaanaym et al., 2009) [20]	Designed an OTP authentication mechanism based on PingPong128 stream cipher	• Execution can be done with no extra expense charged from the user, thus easily implementable. • Provides immunity against attacks based on key-stream properties.	• Usage of AES as the encryption algorithm for the OTP generated. • Employment of two channels of communication viz. GSM and TCP/IP
(Jeong et al., 2008) [23]	Presented smart card-based OTP authentication scheme for the home network.	• Eliminates serious time synchronisation problem by making use of timestamp. • Offers immunity against phishing attack and a range of passive attacks like Man-In-The-Middle, passive eavesdropping, stolen verifier, Denial of Service, and replay attacks. • A decrease in computational overhead along with communication cost. • The home user has free will to choose password thus improving convenience.	• The system fails to provide security against active attacks. • Smart card – a hardware token, is used for authentication which hampers user convenience.
(Liao et al., 2009) [22]	Proposed an authentication scheme that eradicates counter de-synchronisation.	• Successfully eliminates counter de-synchronization problem. • Effectively thwarts replay as well as guessing attacks. • Easily implementable in enterprise applications and offers reduced server security requirements.	• AES-128 in conjunction with MD-5 has been employed which have proven to be compromised previously.
(Alzomai and Josang, 2010) [26]	Presented usage of mobile phone as scalable, trusted computing-based OTP device	• OTP generation providing usability and scalability. • Reduced man in the middle attacks.	• SHA-1 acts as an OTP generator that has been compromised. • An attacker can masquerade the server resulting in the generation of useless OTPs at the user side. • User terminal to connect service provider and mobile phone used to generate OTP are separate which restricts usability. • Not widely adoptable.
(Srivastava et al., 2011) [19]	Proposed an improved knock sequence algorithm using AES	• Avoids attacks like denial of service (DoS), man-in-the-middle (MIM), etc. • Detection and interpretation of consecutive knock sequences is difficult • Disclosure of data is prevented via multi-packet authentication mechanism • Out of sequence delivery of packets is eradicated.	• Transmission of OTP via GSM network
(Hsieh and Leu, 2011) [21]	Presented an authentication framework based on two parameters, i.e. location and time of the mobile phone.	• Provided secure authentication of user to access crucial internet services • Resilience against a range of attacks, e.g. brute force, eavesdropping, user impersonation, and replay attacks. • Offers transparent user authentication.	• The requirement of mobile phones with GPS facility. • Mobile phone and server should be clock synchronised.

(Moon et al., 2012) [27]	Three solutions for fuzzy fingerprint vault were proposed to enhance the security of biometric information.	• Biometric information that is highly reliable can't be lost, duplicated, changed or speculated. • Since it works with unordered sets, it is apt for crypto-biometric frameworks. • Since polynomial reconstruction is quite infeasible, thus guaranteeing its security. • Immune to correlation assault. • Improved execution of GAR is brought about without influencing FAR.	• Fuzzy vault cannot be repudiated, once it has been compromised. • Some modern assaults can compromise biometric data. • Since this framework can't scale well to a huge service pool, so it is more relevant to restricted applications.
(Ma et al., 2013) [28]	An authentication mechanism based on identity was designed which puts the speech features into use.	• Better client ergonomics is provided.	• It can be rendered useless if an attacker gets access to authentic user's pre-recorded voice.
(Castiglione et al., 2014) [29]	An effective end-to-end OTP validation mechanism which involves AKE convention and the keyed HMAC.	• Since it is quite simple and involves less computational overhead, it can work independently along these lines. • In addition to efficiency, it also provides transparency. • Immune to extensive variety of assaults, e.g., offline dictionary attack, password guessing attack, replay attack, brute force attack, stolen verifier attack, denial of service attack and eavesdropping • Its adoptability is quite suitable.	• It can't be utilized when the number of iterations surpasses the length of the commonly settled upon Master Key. • Security of the mechanism depends entirely upon storage and secure handling of the Master Key.
(Avhad and Satyanarayana, 2014) [30]	A password/user ID, single biometric and OTP based authentication scheme is proposed.	• Improved assurance information at reduced cost. • Preserves privacy of client in distributed systems. • Easily implementable configuration.	• Dependence on GSM network for transmission of OTP. • Vulnerable to imitation and MIM attacks.
(Oruh, 2014) [31]	Presented a system for ATMs that integrates biometric authentication with user PIN and smartcard.	• Relatively more secure, reliable and accurate user authentication technique for ATMs.	• No complete exclusion of false matches and non-matches in the biometric feature (i.e., fingerprint).
(Boonkrong, 2017) [32]	Designed and developed a multi-factor authentication protocol, starting from a registration system, which generates authentication factors, to an actual authentication mechanism.	• Requires only three messages between the bank's server and the client to complete the authentication process. • Utilizes a username, a password, number of iterations, a public key, a private key, a symmetric key, a digital signature and an IP address as factors of authentication, all being unique to each user.	• Vulnerable to the threat of password reuse since password is not changed every time the user logs in. • Usage of SHA1 and MD5 which have been reported to be vulnerable.
(Akinyede and Esese, 2017) [33]	Proposed a model that performs hashing using Salted SHA 512, authentication using OTPs, encryption and decryption using AES.	• More advantageous and comfortable model to help conquer challenges to online banking. • Validity and dependability of the model was ensured using a password recovery tool.	• SHA-2 has been employed which makes the system susceptible to length extension attacks. • Usage of AES for encryption/decryption.

III. Proposed Security Architecture

A. Problem Formulation

Short Message Service (SMS) is the most common approach used by the traditional systems to distribute the OTPs to the users for performing online transactions [11]. The 2FA technique based on SMS is the most widely used approach in India, particularly in banks because of reasons like end-device liability and zero logistics charges [34]. However, there are various limitations associated with SMS-based 2FA which are discussed as follows:

1) Delay in SMS delivery:

Though SMS transmission occurs in no time in normal circumstances, there may be a delay associated with the transmission of SMS in cases of network congestion. Since SMSs are not transmitted point to point, instead these are queued and sent to the desired network cell where they are again queued before being sent to the end user. It is this queuing which accounts for SMS delays. This delay may lead to session time-out which may last for few minutes thus impeding the transaction/authentication to happen [35].

2) Low security:

Various possible security concerns are associated with SMS-based OTP. The SMS encryption employed in India is generally basic in nature. At the outset, in between user and service provider, there are various mobile phone operators who happen to be part of the trust chain and as such, have to be trusted. A major security breach is possible if and when a gateway is attacked in the instance of roaming. Moreover, SMS encryption is easily decrypted by an intruder. SIM swap attack is another emerging danger faced by SMS-based OTPs [11].

3) Service unavailability/Coverage areas:

SMS-based 2FA OTPs result in inconvenience to the users in the reception of incoming SMSs when they move outside the network coverage [35].

4) Roaming Restrictions:

It is one of the significant shortcomings of SMS-based systems that a user travelling abroad faces restrictions and may be deprived of availing SMS facility. Even if the services are available, users have to pay high roaming costs resulting in constraints on SMS services. When the roaming services are turned off, then banks will fail in SMS-OTP distribution to users, which leads to the conclusion that users are stopped from continuing any further processes. Roaming facility for global GSM mobile phones is not permitted in Kashmir. Moreover, pre-paid GSM connections in the valley can't benefit roaming facility in the rest of India, restricting customers stationed outside the state from availing net-banking services offered by banks [17], [35].

5) *Government Regulatory Regulations*

In critical emergency and sensitive conditions, the government of India has to follow some set of standard rules which involves blocking bulk SMS services thus affecting facilities provided by SMS-based authentication mechanisms [16], [36]. In Kashmir, a similar situation was observed in the year 2010, when the government announced to block SMS service in Jammu & Kashmir. On June 30, 2010, SMS facility on mobile phones was snapped by the government, however, only after a short duration of 6 months, the SMS services were resumed on post-paid networks, but pre-paid network continued to face the ban. The ban on SMS services for pre-paid subscribers which formed 70% customers to telecom companies were deprived of using the SMS service, and lastly, the ban was lifted after four years on May 20, 2014[4].

Though user authentication is ensured by employing OTP when OTP generation is based on GSM, it is vulnerable to compromise [9]. Thus, a serious cost-effective solution and a secure authorisation mechanism which caters the much-needed convenience of customers without compromising on security aspect are required. To overcome all the short falls, device-details based two-way authentication mechanism needs to be developed; further improvements need to be achieved by considering SHA3, truncated SHA1 and RIPEMD-128 in place of SHA1 and MD5 and overcoming human ease of short-data entries as opposed to large length data.

B. *Design Methodology*

The proposed system is much more secure than the before-mentioned approaches since it provides security and supports the performance with continued existence. The proposed system is cost-effective and ensures privacy, confidentiality, non-repudiation as it employs secure hash algorithms (SHA3 and truncated SHA1) which can produce One Time Passwords (OTPs) on Android environment thereby providing password security besides improved protection.

The proposed work makes use of SHA3, truncated SHA1 and RIPEMD128 as standard algorithms for generation of One-Time-Passwords (OTPs) from an initial germ with no dependence on GSM network. The hardware profiles (IMEI, IMSI and timestamp) and software profile (index number) form the initial seed. Two random numbers ‘N' and ‘M' are generated which specify the number of SHA3 and RIPEMD128 iterations. A third coordinate, i.e. |N - M%N| determines the number of iterations of truncated SHA1. RIPEMD128 results in 128-bit data which is later collapsed into the 64-bit result. The 64-bit key may be converted into six words in a user readable format using FRC 1751. This system, however, does not employ any traditional encryption/decryption method. The proposed work is implemented on an Android platform using Java as a programming tool. The proposed work has been built and tested on Android which is gaining popularity among the users globally as compared to tablet PCs and other smart-phones. The Android market share is 87.7%, which is the highest than the market share of any mobile OS [37]. Thus, the proposed work is highly adoptable technically.

The principal objective of the proposed work is to design a model for OTP authentication. The whole process can efficiently be visualized with the help of modules which have been described as follows:

1) *Registration Phase*

The primary module in the proposed system comprises of the registration phase which is given in Fig. 2. In this phase, the user registers or enrols for the proposed authentication system. The generation of a user interface on Android is followed by the formation of unique initial seed from the hardware profiles of the user (comprising of Timestamp, IMSI and IMEI) and the software profile (consisting of the index number).

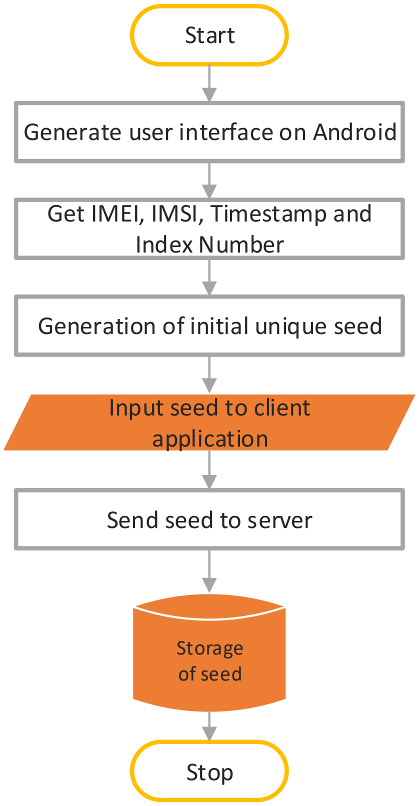

Start
Generate user interface on Android
Get IMEI, IMSI, Timestamp and Index Number
Generation of initial unique seed
Input seed to client application
Send seed to server
Storage of seed
Stop

Fig. 2. Registration of user.

[4] "Jammu and Kashmir government lifts ban on SMS on pre-paid mobiles | Latest News & Updates at Daily News & Analysis", *dna*, 2014. [Online]. Available: http://www.dnaindia.com/india/report-jammu-and-kashmir-government-lifts-ban-on-sms-on-pre-paid-mobiles-1990107. [Accessed: 17-Jan- 2018].

2) OTP Generation Phase

The next phase involves the generation of OTP for authentication purposes as illustrated in Fig. 3. In this phase, a one-time-password that can be easily read by a human is generated on the user's mobile device. It begins with the user logging-in to the website of the service provider using a distinct username-password combination. Then, the server is allowed to compute the seed from the status as submitted by the user. This is followed by the transmission of a random challenge to the client by the server for computing OTP at his/her side.

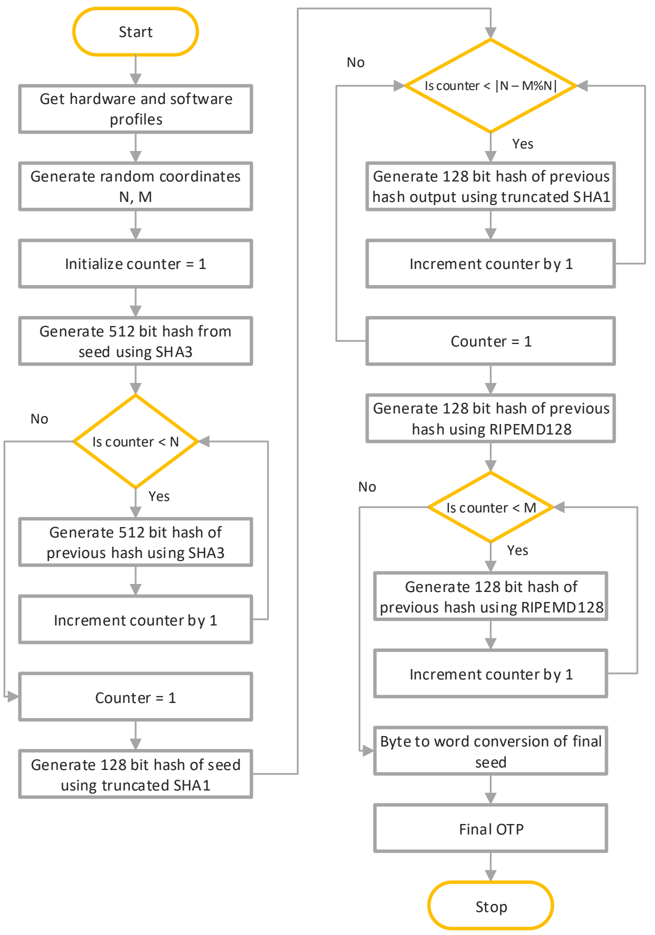

Start
Get hardware and software profiles
Generate random coordinates N, M
Initialize counter = 1
Generate 512 bit hash from seed using SHA3
No
Is counter < N
Yes
Generate 512 bit hash of previous hash using SHA3
Increment counter by 1
Counter = 1
Generate 128 bit hash of seed using truncated SHA1
No
Is counter < |N – M%N|
Yes
Generate 128 bit hash of previous hash output using truncated SHA1
Increment counter by 1
Counter = 1
Generate 128 bit hash of previous hash using RIPEMD128
No
Is counter < M
Yes
Generate 128 bit hash of previous hash using RIPEMD128
Increment counter by 1
Byte to word conversion of final seed
Final OTP
Stop

Fig. 3. OTP generation on the client side.

At the client side, this challenge is read and used for generating the final hash with the help of SHA-3. The output value of SHA-3 is input to truncated SHA1 whose output is in turn fed to RIPEMD128. Byte to word conversion is performed on the resulting output yielding a human-readable OTP.

3) OTP Authentication Phase

In this phase, the final authentication of the OTP generated is performed as shown in Fig. 4. This is done by comparing the OTP generated at the client side and that at the server side. Only when the two match, the user is provided access to the online services by the service provider.

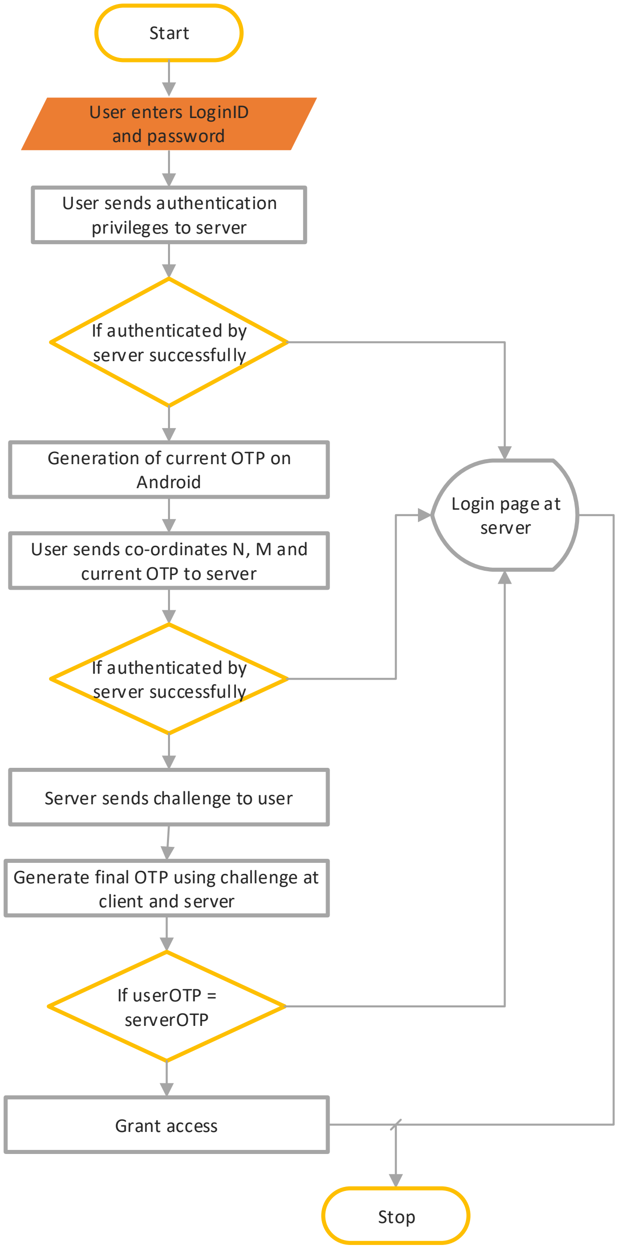

Start
User enters LoginID and password
User sends authentication privileges to server
If authenticated by server successfully
Generation of current OTP on Android
User sends co-ordinates N, M and current OTP to server
If authenticated by server successfully
Server sends challenge to user
Generate final OTP using challenge at client and server
If userOTP = serverOTP
Grant access
Stop
Login page at server

Fig. 4. Final authentication of generated OTP.

IV. Design Implementation

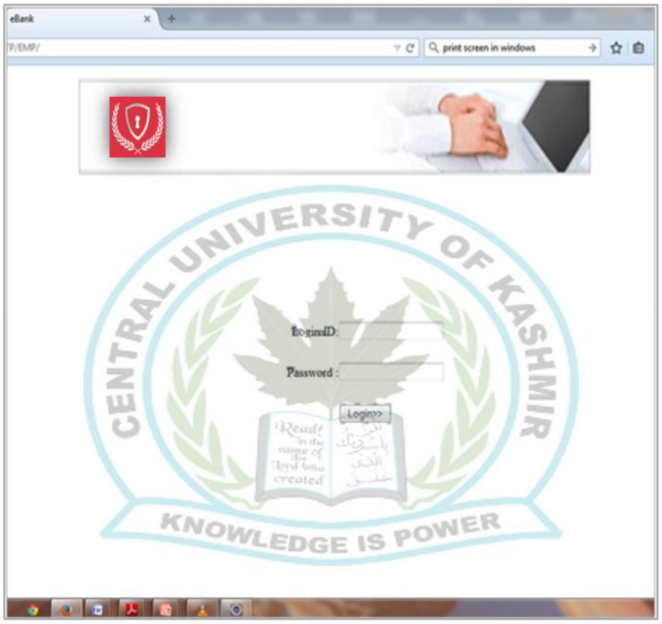
The implementation details have been highlighted in this section including the installations required. For writing the Android application, the requirements comprise of Java Development Kit (JDK), the Android SDK, an Editor or Eclipse (an Integrated Development Environment for Java) for making the development process easier. Besides, a plug-in is also required for Eclipse, i.e. Android Development Tools (ADT) for providing added support. The list of One-Time-Passwords has been computed before-hand to enhance the efficiency and performance. This is done using SQLyog as the database management tool owing to the ease of use and automaticity it provides.

A. *Illustration of the Proposed System*

The screenshots that follow illustrate the process of authentication of the user in a stepwise manner. Each of the steps that are involved has been described with the help of corresponding figures. These have been given as under:

a) Bank Employee Login:

At the server (bank) site, the employee who is privileged can log in to the system. The employees and their details, i.e. employee id and passkey are stored on the server. It is only the registered employee who can manage the customers/users who want to avail the online banking services. The login page of the employee appears as shown in Fig. 5. After logging in successfully, the employee can open an account for the user or can credit amount.



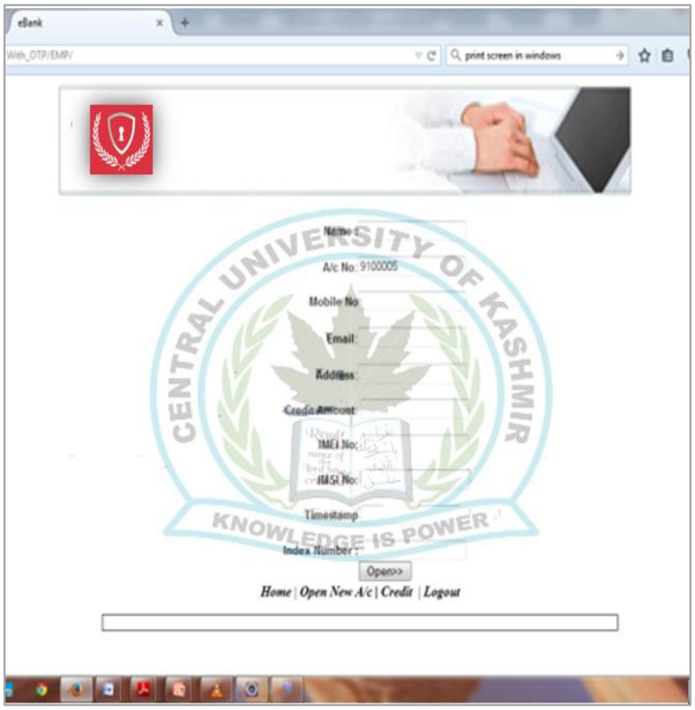
LoginID:

Password :

Fig. 5. Employee login page.

b) Open new account for user:

Only the registered employees can add the user's account after obtaining the hardware/software profiles and other details of the user as shown in Fig. 6. The authentication details of the user must be submitted manually by the users to the server (bank) which is considered as the most secure form of passing on the details. The hardware profiles constitute the IMSI (International Mobile Subscriber Identity), the IMEI (International Mobile Equipment Identity), the Timestamp and the software profile comprises of the Index number that uniquely identifies your application. These details are taken from the user's device and are placed under System Info as shown in Fig. 7. Even if the application is uninstalled on the device, the index number remains there with the server. It shall be flushed only if the user removes the application file (.apk) from his/her device. In that case, the user will have to request for the application from the server (bank) again and re-register his/her details manually. After registering, the user is provided with an account number to be used for accessing the online services. The details of all the users registered are stored at the server side.


eBank
With_OTP/EMP/
print screen in windows
CENTRAL UNIVERSITY OF KASHMIR
KNOWLEDGE IS POWER
Open>>
Home | Open New A/c | Credit | Logout

Name :

A/c No: 9100005

Mobile No

Email:

Address:

Credit Amount:

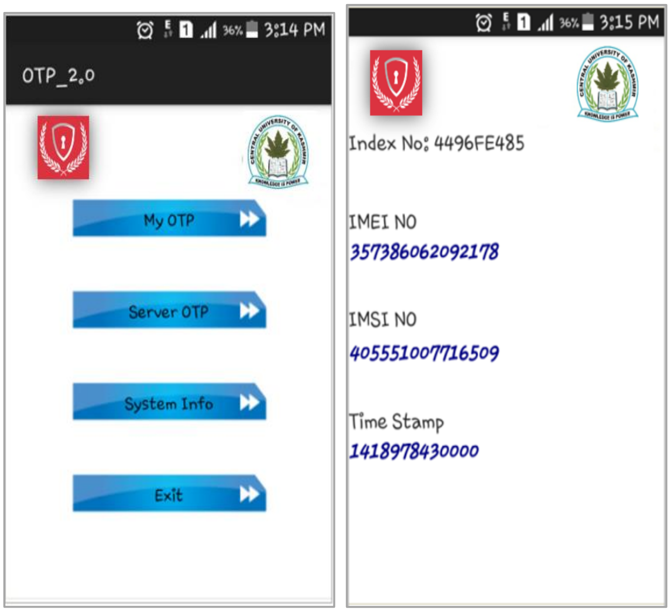
IMEI No:

IMSI No:

Timestamp

Index Number :

Fig. 6. Screenshot showing how to open a new user account.



Index No: 4496FE485

IMEI NO
357386062092178

IMSI NO
405551007716509

Time Stamp
1418978430000

Fig. 7. Screenshots showing system info on the user device.

c) Credit amount:

Again, it is the employee who has the privilege to credit amount to any account which is shown in Fig. 8 below.

d) User login page:

When provided with an account by the server (bank), a new user submits his/her login id and password to account for the first layer of authentication. The user must activate his/her account by logging in to his/her account at first. The login page for user appears as in Fig. 9.

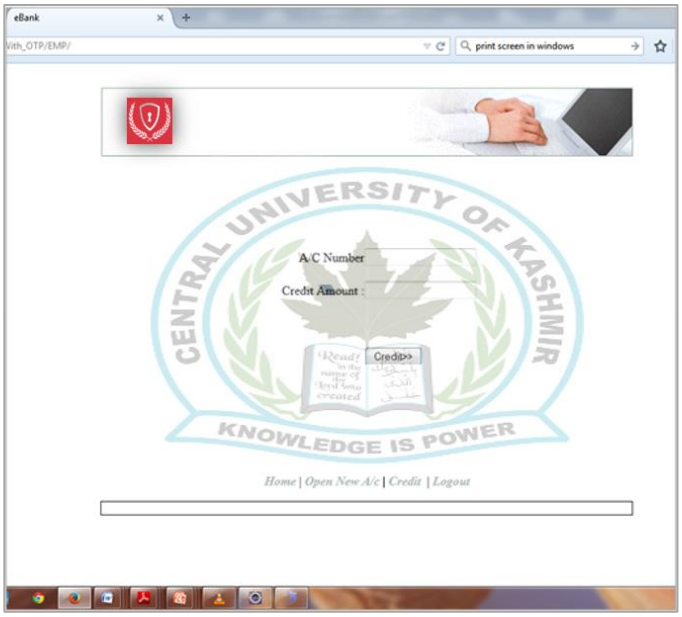


Fig. 8. Screenshot for crediting amount.

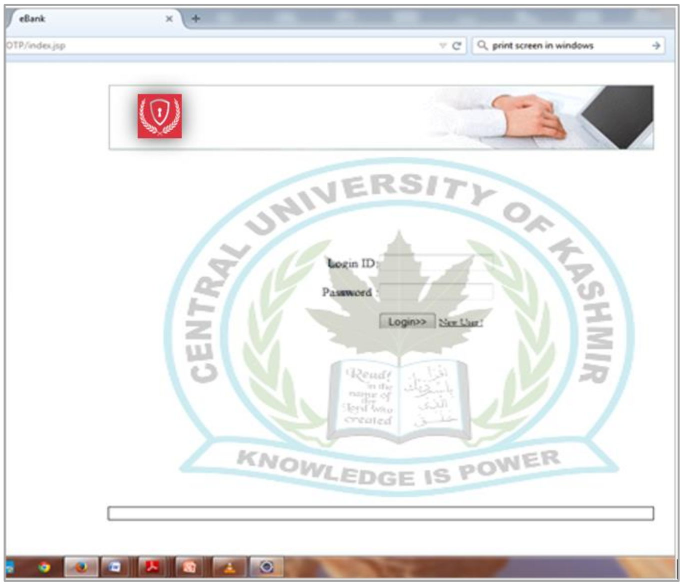
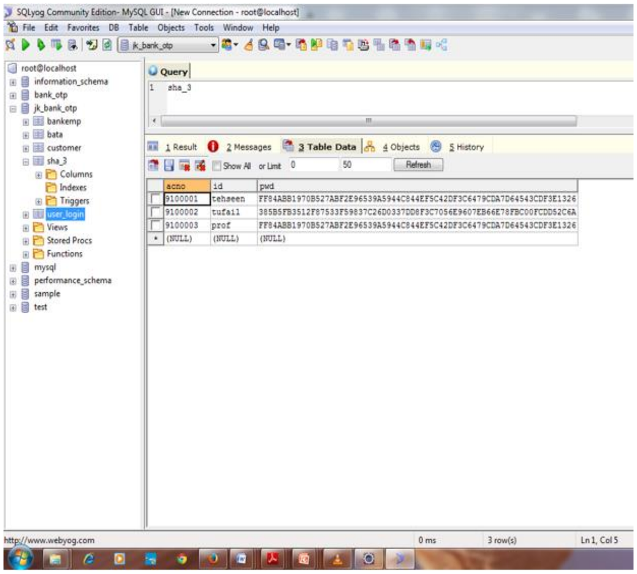


Fig. 9. User login page.

The server (bank) stores the login details of the users which comprises of the user id and the password. It is worth mentioning that it is the hash value of the password (shown in Fig. 10) that is stored rather than the password itself. This protects the system from various attacks such as stolen-verifier attack where it may be possible that the intruder gets access to the password file stored on the server.



```
1   sha_3
```

0 50

acno	id	pwd
9100001	tehseen	FF84ABB1970B527ABF2E96539A5944C844EF5C42DF3C6479CDA7D64543CDF3E1326
9100002	tufail	385B5FB3512F87533F59837C26D0337DD8F3C7056E9607EB66E78FBC00FCDD52C6A
9100003	prof	FF84ABB1970B527ABF2E96539A5944C844EF5C42DF3C6479CDA7D64543CDF3E1326
(NULL)	(NULL)	(NULL)

Fig. 10. Screenshot showing users' login details.

e) *Sending current OTP to server:*

As soon as the user logs in, the server prompts the user (shown in Fig. 11) for the current OTP, the coordinate N (number of SHA3 iterations) and the coordinate M (number of RIPEMD128 iterations). The current OTP and the values of M, N are generated at the user device in 'My OTP' as depicted in Fig. 12. Every time the user taps 'My OTP', a new set of OTP, M and N is produced. The OTP generated comprises of 6 human-readable words which provide increased user convenience.

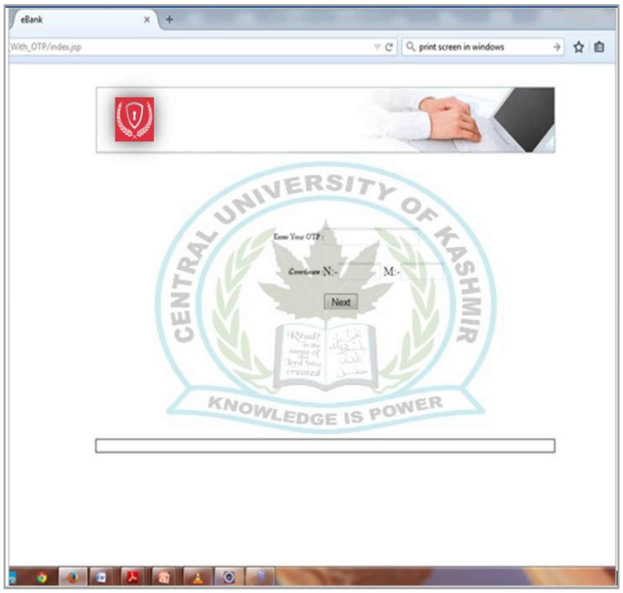
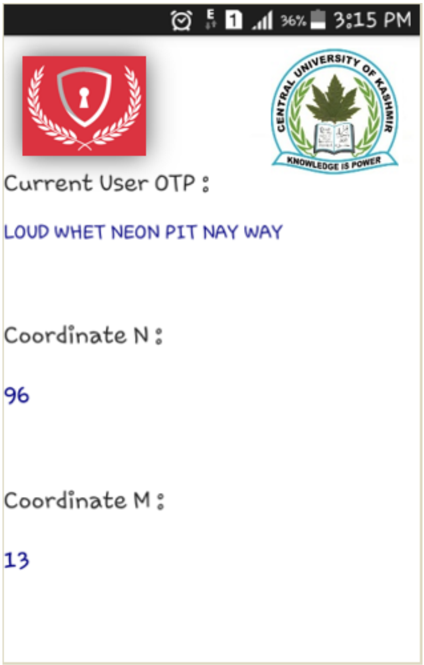


Fig. 11. Screenshot showing how current OTP is sent to the server.



Current User OTP :

LOUD WHET NEON PIT NAY WAY

Coordinate N :

96

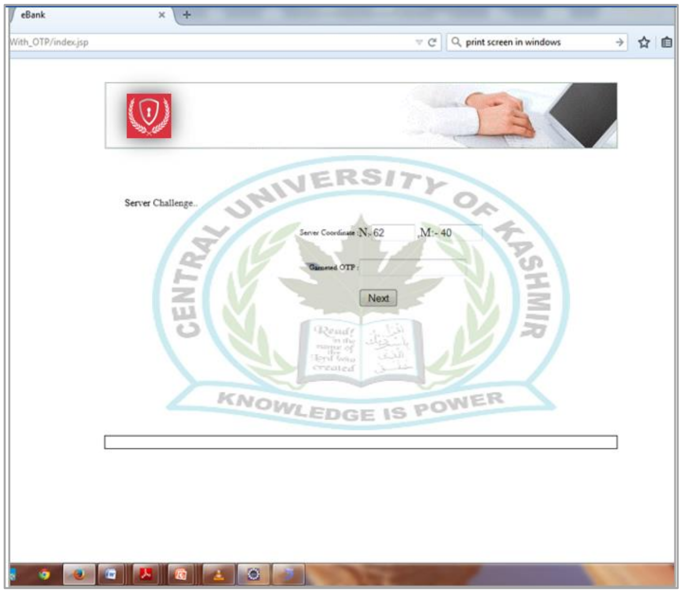
Coordinate M :

13

Fig. 12. Screenshot showing OTP generation on the client side.

f) Server challenge:

The next step in the authentication process consists of a challenge sent by the server to the user to validate the user by his/her response. In the challenge, the server sends the coordinates M and N to the user and asks it to generate the final OTP on his/her handheld device. The server challenge has been shown in Fig. 13, and the generation of new/final OTP at client side has been illustrated in Fig. 14. When the server receives the OTP from the client, it matches this OTP with the one generated at the server side. Only when the two matches, the server grants access privileges to the user, i.e. only when the user shall be allowed to transact from his account.

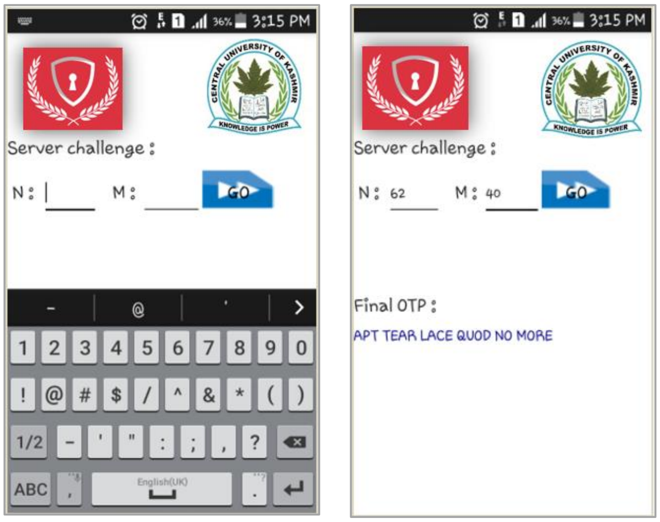


Server Challenge.

Server Coordinate N:-62 M:-40

Generated OTP:

Fig. 13. Screenshot showing challenge sent by the server.



Server challenge :

N: M:

Server challenge :

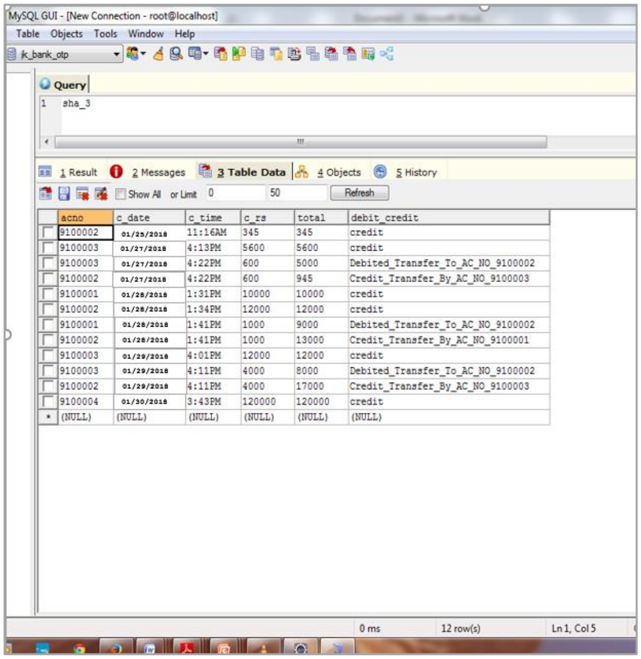
N: 62 M: 40

Final OTP :

APT TEAR LACE QUOD NO MORE

Fig. 14. Screenshots of final OTP generation on the client side.

The user when authenticated can access his banking services online. A user may transfer funds, view his/her account summary or change his/her password very conveniently. The account summary includes the date and time of transactions made from and to the user account. This can be seen from Fig. 15.



```
1  sha_3
```

0 50

acno	c_date	c_time	c_rs	total	debit_credit
9100002	01/25/2018	11:16AM	345	345	credit
9100003	01/27/2018	4:13PM	5600	5600	credit
9100003	01/27/2018	4:22PM	600	5000	Debited_Transfer_To_AC_NO_9100002
9100002	01/27/2018	4:22PM	600	945	Credit_Transfer_By_AC_NO_9100003
9100001	01/28/2018	1:31PM	10000	10000	credit
9100002	01/28/2018	1:34PM	12000	12000	credit
9100001	01/28/2018	1:41PM	1000	9000	Debited_Transfer_To_AC_NO_9100002
9100002	01/28/2018	1:41PM	1000	13000	Credit_Transfer_By_AC_NO_9100001
9100003	01/29/2018	4:01PM	12000	12000	credit
9100003	01/29/2018	4:11PM	4000	8000	Debited_Transfer_To_AC_NO_9100002
9100002	01/29/2018	4:11PM	4000	17000	Credit_Transfer_By_AC_NO_9100003
9100004	01/30/2018	3:43PM	120000	120000	credit
(NULL)	(NULL)	(NULL)	(NULL)	(NULL)	(NULL)

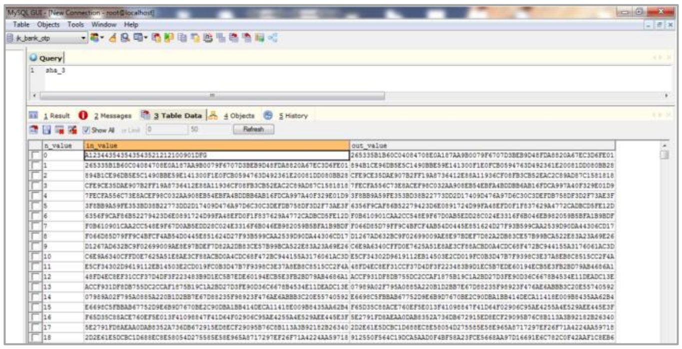
0 ms 12 row(s) Ln 1, Col 5

Fig. 15. Screenshot showing users' transaction details.

The server keeps a record of the transaction details of all the customers in its database.

g) List of One-time passwords:

The initial seed is formed by the concatenation of IMEI, IMSI, timestamp and index number. The values of SHA3 from 0-99 are pre-calculated to enhance efficiency. In this way, reliable and efficient One-Time-Passwords are generated which have been shown in Fig. 16.



```
1    sha_3
```

n_value	in_value	out_value
0	A12344354354354352121210090 1DFG	265335B1B60C04084708E0A187AA9B0079F6707D3BEB9D48FDA8820A67EC3D6FE01
1	265335B1B60C04084708E0A187AA9B0079F6707D3BEB9D48FDA8820A67EC3D6FE01	894B1CE96DB5E5C1490BBE59E141300F1E0FCB0594763D492361E20081DD080BB28
2	894B1CE96DB5E5C1490BBE59E141300F1E0FCB0594763D492361E20081DD080BB28	CFE9CE35DAE907B2FF19A8736412E88A11936CF08FB3CB52EAC2C89AD87C1581818
3	CFE9CE35DAE907B2FF19A8736412E88A11936CF08FB3CB52EAC2C89AD87C1581818	7FECFA556C73E8ACEF98C032AA908EB54EBFA4BDDBB6AB16FDCA997A40F329E01D9
4	7FECFA556C73E8ACEF98C032AA908EB54EBFA4BDDBB6AB16FDCA997A40F329E01D9	3F8BB9A59FE353BD38B22773DD2D17409D476A97D6C30C3DEFDB758DF3D2F73AE3F
5	3F8BB9A59FE353BD38B22773DD2D17409D476A97D6C30C3DEFDB758DF3D2F73AE3F	6356F9CAF86B52279423D6E0891724D99FA48EFD0F1F837629A4772CADBCD5FE12D
6	6356F9CAF86B52279423D6E0891724D99FA48EFD0F1F837629A4772CADBCD5FE12D	F0B610901CAA2CC548E9F67D0AB5EDD28C024E3316F6B046EB982059B5BFA1B9BDF
7	F0B610901CAA2CC548E9F67D0AB5EDD28C024E3316F6B046EB982059B5BFA1B9BDF	F066D85D79FF9C4BFCF4AB54D0445E851624D27F93B599CAA2539D90DA44306CD17
8	F066D85D79FF9C4BFCF4AB54D0445E851624D27F93B599CAA2539D90DA44306CD17	D1267AD632BC9F02699009AE8E97BDEF7D82A2DB83CE57B99BCA522E83A23A69E26
9	D1267AD632BC9F02699009AE8E97BDEF7D82A2DB83CE57B99BCA522E83A23A69E26	C6E9A6340CFFD0E7625A51E8AE3CF88ACBD0A4CDC68F472BC944155A3176061AC3D
10	C6E9A6340CFFD0E7625A51E8AE3CF88ACBD0A4CDC68F472BC944155A3176061AC3D	E5CF34302D9619112EB14503E2CD019FC0B3D47B7F9398C3E37A8EB8C8515CC2F4A
11	E5CF34302D9619112EB14503E2CD019FC0B3D47B7F9398C3E37A8EB8C8515CC2F4A	48FD4EC8EF31CCF37D4DF3F223483B9D1EC5B7EDE60194ECB5E3FB2BD79AB4686A1
12	48FD4EC8EF31CCF37D4DF3F223483B9D1EC5B7EDE60194ECB5E3FB2BD79AB4686A1	ACCF931DF8DB755DC2CCAF1875B19C1A2BD27D3FE90D36C6678B4534E11DEADC13E
13	ACCF931DF8DB755DC2CCAF1875B19C1A2BD27D3FE90D36C6678B4534E11DEADC13E	07989A02F795A0885A220B1D2BB7E67D88235F98923F476AE6ABBB3C20E55740592
14	07989A02F795A0885A220B1D2BB7E67D88235F98923F476AE6ABBB3C20E55740592	E6698C5FBBAB67752D9E6B9D7670BE2C90DBA1BB414DECA11418E009B8435AA62B4
15	E6698C5FBBAB67752D9E6B9D7670BE2C90DBA1BB414DECA11418E009B8435AA62B4	F65D35C88ACE760EF5E013F41098847F41D64F02906C95AE4255A4E529AEE445E3F
16	F65D35C88ACE760EF5E013F41098847F41D64F02906C95AE4255A4E529AEE445E3F	5E2791FD8AEAA0DAB8352A736DB672915ED8ECF29095B76C8B113A3B92182B26340
17	5E2791FD8AEAA0DAB8352A736DB672915ED8ECF29095B76C8B113A3B92182B26340	2D2E61E5DCBC1D688EC8E58054D275585E58E965A8717297EF26F71A4224AA59718
18	2D2E61E5DCBC1D688EC8E58054D275585E58E965A8717297EF26F71A4224AA59718	912550F564C19DCA5AAD0F4BF58A23FCE5668AA97D16691E6C782C0F42AAF1C8EB6

Fig. 16. Screenshot showing OTP list.

V. Results and Analysis

The primary usage of the proposed system is that it can be utilized for an efficient identification of a legitimate member for having access rights to their privilege account. As the entire framework is based on the enhanced operation of One-Time Password (OTP) as well as updated cryptographic hash functions (SHA3, truncated SHA1) and RIPEMD128, so the system excels some of its security measures. It should be also known that although there are abundant micro stages of implementation of the system, the fundamental concept of the framework basically uses the trusted handheld devices as a medium to perform authentication procedure of the system. Underlying concepts of SHA3, truncated SHA1 and RIPEMD128 makes all the differences in the security incorporations that make the authentication more robust as compared to the standard techniques adopted so far. Therefore, this section discusses the performance analysis of the system using processing time as a parameter for performance evaluation.

A. *Processing Time*

An effective time required to process the complete OTP generation for performing the user authentication is termed as 'processing time'. The effectiveness of the system against mitigating common types of attack/intrusion from an illegitimate member and an effective processing time required to perform the procedure is the attribute of performance analysis.

The OTP generator is installed on 100 Android mobile phones from various vendors with varying hardware specifications for the evaluation of the processing time of the application which is defined with regard to our application as the time it takes for an OTP generator to create an OTP from the initial seed. The time it takes in OTP generation is dependent on the values of random numbers N and M. This is because these values specify how many times the hash functions SHA3, truncated SHA1 and RIPEMD128 are to be used. These hash functions are used for the calculation in which the values for N and M are randomly being taken by the OTP generator. This random feature in selection of coordinates lends credibility to our results. In Fig. 17, it can be seen that irrespective of the hardware specification, it does not take more than 49 ms for the application to generate OTP. The results have been formulated using a timer. Furthermore, the average time it takes for a mobile to generate an OTP is 26.72 ms. Both the time calculations conform to the tolerable time thus proving the efficiency of the system. It is important to mention here that the correctness of the timer depends on the internal threads of the CPU; thus, to eradicate that factor influencing the final application throughput, the running application were stopped on all the test beds. Fig. 17 shows the final results accomplished while evaluating the system processing time.

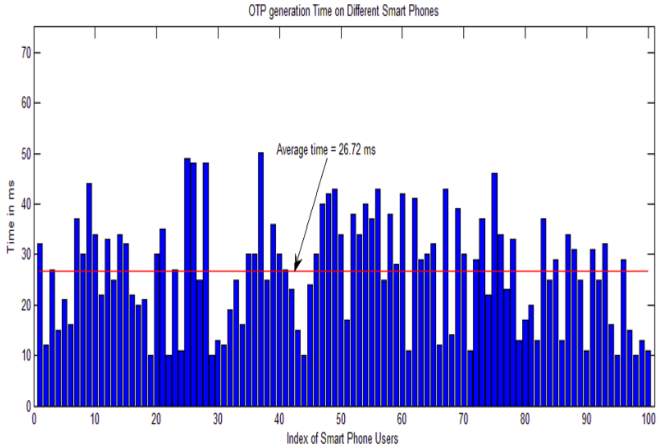


Fig. 17. Total processing time.

To emphasize on the user friendliness of the same by inclusion of Byte to word conversion, a survey was conducted where 40 users were asked randomly to key in the original 128 generated OTP to be entered as 32 digits. The analysis of the results shows that it takes on an average 30.185 seconds for the user to enter the same into his/her computer via keyboard. That is not all, 17.5% of the times an error occurred with it. Errors in keying the mobile generated OTP are shown by red rectangles in Fig. 18.

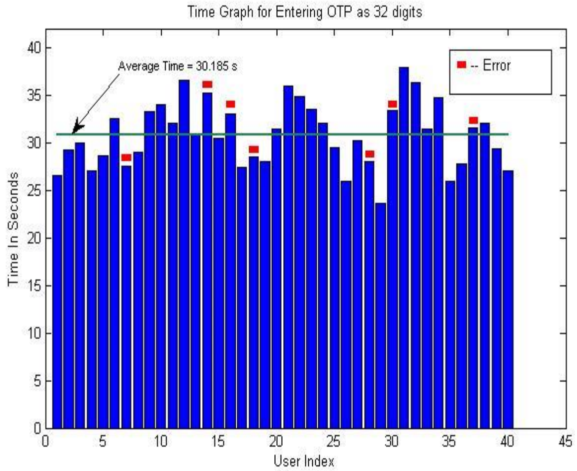


Fig. 18. Time graph for entering OTP as 32 digits.

However, when the same users were asked to enter a OTP as a six-dictionary word, the average time taken by the user decreased to 11.87 seconds (as shown in Fig. 19). Also, the occurrence of errors also diminished to 2.5 % which is extremely low as compared to the previous occurrence and thus shows the user-friendly attribute of the system. Therefore, the inclusion of Byte to Word mechanism is proven to be important while providing applicability from user perspective.

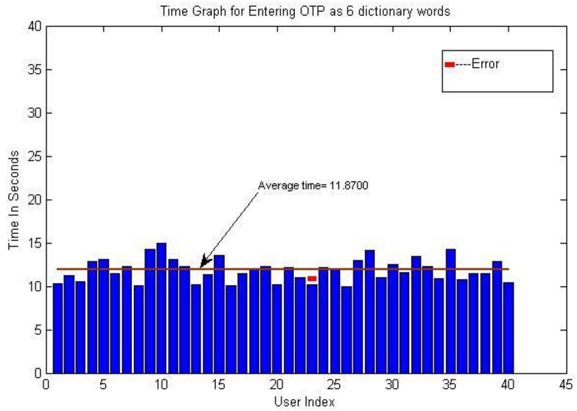


Fig. 19. Time graph for entering OTP as 6 dictionary words.

B. Security Analysis

The evaluation of security analysis critique lies in the efficient operation of the security functionality for performing secure transaction, for the considered application on financial institutions. The OTP authentication implemented makes use of OTP which is valid only for a single session and is generated with the help of strong mechanism performing concatenated cryptographic functions (SHA3, truncated SHA1 and RIPEMD128), which results in a system impossible to break until the quantum computing comes in picture. The proposed scheme can resist an off-line guessing attack because it uses strong passwords generated from strong hash functions. Also, it can protect the online transactions from replay attacks, key-loggers, shoulder surfing attacks, etc. Moreover, replaying reusable passwords are restricted by encoding passwords to be used one time.

While reviewing the base work, it was found that SHA-1 can be a potential security algorithm for mechanizing robust authentication system. However, it is not true as SHA-1 is also explored with multiple security incapability and reported attack evidences found in history. Therefore, the implementation has been carried out using SHA3 and truncated SHA1. SHA3 is designed to mitigate the security loopholes that SHA-0 or SHA-1 couldn’t afford to furnish in a secure and efficient authentication mechanism. Henceforth, SHA3 is adopted in our application taking into consideration the effectiveness in security for longer time (software lifetime). Moreover, the proposed security policy ensures better privacy and confidentiality by not permitting the server and the user to secretly create and exchange the authentication token in external communication environment. Therefore, the system considers the hardware profiles and associates the exclusive generation of one-time password with it, so that it cannot be replicated for other mobile devices for particular session usage. It is almost impossible for an attacker to have the possession of actual mobile device of a legitimate user along with the static password thus rendering the system secured. Furthermore, even if the attacker has the possession of the above credentials he/she again needs to switch ON the stolen mobile phone while keeping the SIM of legitimate user intact before he/she can start using the OTP generator. This will mean that his/her location is known, and he/she can be caught. The system can thus be seen as fool proof because of the employment of the multilayer security factor as illustrated.

The results show that the client can access the privilege account in fast track proving its compatibility in mobile devices too. The performance of the system is tested by installing the application in Android mobile device, which shows no significant changes in the service delivery. Hence, it can be said that a performance which is user-friendly and secure is recorded in this evaluation process. The performance of the system can be stated as better and secure as it has two inherent characteristics: 1) The OTP processing speed is acceptable; 2) using SHA-3, it is almost impossible to explore the message mapping with the pre-determined hash function.

VI. Conclusion and Future Work

Authentication, as well as authorisation, plays an important role in securing transactions conducted on any communication network particularly over the cellular network. As observed from this study, a one-time-password authentication scheme needs to be developed on the mobile platform that provides security as well as performance in the long run. Various authentication schemes have been explored in this study which points out the vulnerabilities in the prevalent GSM-based systems. Thus, a unique password authentication mechanism is presented where the user generates OTPs on his/her mobile phone using its hardware and software profiles. For OTP generation, three hash functions, i.e. SHA-3, truncated SHA-1 and RIPE-MD128 are used which are concatenated with each other. However, the major limitation associated with the proposed scheme is that the mobile phone becomes the only point of failure in case it is stolen or lost or malfunctions. However, one method to overcome the limitation will be to design a backup procedure to restore its status after any untoward incident.

Further plans for the research undertaken include the extension of the authentication mechanism to other mobile phone platforms like Windows, Symbian, iOS, etc. There is a vast scope for researchers to make further enhancements in the solution proposed to have more security in their online transactions. This system has a large expanse in providing secure authentication and authorisation means in banking as well as other finance-based applications calling for higher security. The presented work makes use of two factors of authentication – something you know and something you have. In future, the other factor, i.e. something you are (biometrics), can be made use of to enhance the security further. Moreover, the performance analysis of the authentication system may be conducted based on user ergonomics as compared to prior systems.

References

[1] *Two-Factor Authentication for Banking - Cryptomathic*, 1st ed. Jægergårdsgade 118, DK-8000 Aarhus C, Denmark: Two-Factor Authentication for Banking – Building the Business Case, 2012, pp. 4-16.

[2] P. Vashishta and S. Kapoor, "E-Banking: Perspective for Survival in Current Market", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 1, no. 1, pp. 42-46, 2012.

[3] R. Jatana and R.K. Uppal, *E-banking in India: challenges and opportunities*. New Century Publications, 2007.

[4] B. Khan, R. Olanrewaju, A. Mehraj, A. Ahmad and S. Assad, "A Compendious Study of Online Payment Systems: Past Developments, Present Impact, and Future Considerations", *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 5, pp. 256-271, 2017.

[5] M. Masihuddin, B.U.I. Khan, M.M.U.I. Mattoo and R.F. Olanrewaju, () "A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts", *Indian Journal of Science and Technology*, vol. 10, no. 20, pp. 1-19, 2017.

[6] T. Laukkanen and J. Lauronen, "Consumer Value Creation in Mobile Banking Services", *International Journal of Mobile Communications*, vol. 3, no. 4, pp. 325-338, 2005.

[7] S. Choudhary, R. Temkar and N. Bhatta, "QR Code Based Secure OTP Distribution Scheme for Authentication in Net-Banking", *International Journal of Information Science and Intelligent System*, vol. 2, no. 4, pp. 115-121, 2013.

[8] R.F. Olanrewaju, B.U.I. Khan, M.M.U.I. Matto, F. Anwar, R.N. Mir and A.N.B. Nordin, "Securing Electronic Transactions via Payment Gateways – A Systematic Review", *International Journal of Internet Technology and Secured Transactions*, vol. 7, no. 3, pp. 245-269, 2017. (Accepted to be published)

[9] T. Mehraj, B. Rasool, B.U.I. Khan, A. Baba and A.G. Lone, "Contemplation of Effective Security Measures in Access Management from Adoptability Perspective", *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 8, pp. 188-200, 2015.

[10] J.M. Stewart, E. Tittel and M. Chapple, *CISSP: Certified Information Systems Security Professional Study Guide*. Sybex, 2005.

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

[12] A.F. Behrouz, *Cryptography and network security*. Tata McGraw Hill Education Private Limited, 2010.

[13] D. Salomon, *Elements of computer security*. Springer Science & Business Media, 2010.

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

[15] R.E. Smith, *Internet cryptography*. Addison-Wesley Longman Publishing Co., Inc., 1997.

[16] 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.

[17] M. Eldefrawy, K. Alghathbar and M. Khan, "OTP-Based Two-Factor Authentication Using Mobile Phones", in *Eighth International Conference on Information Technology: New Generations (ITNG)*, Las Vegas, NV, 2011, pp. 327-331.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] P. R. Avhad and R. Satyanarayana, “A Three-Factor Authentication Scheme in ATM”, *International Journal of Science and Research (IJSR)*, vol. 3, no. 4, pp. 656-659, 2014.

[31] J. N. Oruh, “Three-Factor Authentication for Automated Teller Machine System”, *IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS)*, vol. 4, no. 6, pp. 160-166, 2014.

[32] S. Boonkrong, “Internet Banking Login with Multi-Factor Authentication”, *KSII Transactions on Internet & Information Systems*, vol. 11, no. 1, pp. 511-535, 2017.

[33] R.O. Akinyede and O.A. Esese, “Development of a Secure Mobile E-Banking System”, *International Journal of Computer (IJC)*, vol. 26, no. 1, pp. 23-42, 2017.

[34] A. Arara, E.B.E. Fgee and H.A. Jaber, “Securing e-Government Web Portal Access Using Enhanced Two Factor Authentication”, in *Advances in Engineering Sciences & Applied Mathematics (ICAESAM'2015), 4th International Conference on*, 2015, pp. 65-69.

[35] M.H. Eldefrawy, M.K. Khan, K. Alghathbar, T.H. Kim and H. Elkamchouchi, “Mobile One-Time Passwords: Two-Factor Authentication Using Mobile Phones”, *Security and Communication Networks*, vol. 5, no. 5, pp. 508-516, 2012.

[36] W. Stallings, *Cryptography and network security*, 5th ed. India: Pearson Education, 2011.

[37] "Mobile OS market share 2017 | Statista", *Statista*, 2017. [Online]. Available: https://www.statista.com/statistics/266136/global-market-share-held-by-smartphone-operating-systems/. [Accessed: 18- Jan-2018].