Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey on "An Authentication System for Online Banking Using Smart Phones"

Ashwini Jagdale, Sayali Shelar, Poojita Sahani, Anjali Sonsale, Shailesh Bendale
Department of Computer Engineering, STES's NBNSSOE, Pune,
Pune, Maharashtra, India

Abstract: ***The Internet was born with the ideology to share information at a huge extent and to connect people across the globe. It is the most useful technology of the modern times which helps us not only in our daily lives, but also our personal and professional lives developments in several different ways. Internet indeed is a major advancement in the modern era.One of the most crucial and advantageous use of Internet isthat we can perform all our financial transactions online. Online transaction of money has become the norm with almost all kinds of businesses.But everything has a negative aspect to it and so does the Internet. Security is the biggest threat to Internet due to which the existing internet banking system is being exposed to danger because of major hacking techniques and theories. There are no fail-proof ways to securing names, account numbers, addresses, photos and credit card numbers from being stolen or misused by thieving websites and individuals.***

Hence, to solve these problems of Online Banking, we propose an innovative method to authenticate the customer's identity by using the QR-Code (Quick Response), OTP (One-Time Password) and the IMEI (International Mobile Equipment Identity) Number of the customer mobile device. It is also needed that while using the Internet, the data must be secured and personal. Thus, in this method we encrypt the data using the TTJSA Encryption and Decryption Algorithm.

Keywords: Online Banking, QR-Code, OTP, IMEI, TTJSA.

I. INTRODUCTION

The age of Google and Wikipedia has ensured that we do most of our activities online. What is absolutely incredible is we can rely for almost everything on the Internet. More business than we can ever imagine is done online. Internet Banking or Online Banking is the latest in the series of technological wonders of the recent past. With the introduction of latest technologies in the banking sector a lot of new initiatives are oriented to provide a better customer service and facilities with the help of Information Technology. Banking is now no more limited in going and visiting the bank in person for various purposes. Now we can do all thesetransactions and many more using the online services offered by the banks. To access a financial institution's online banking facility, a customer with internet access would need to register with the institution for the service and set up some password for customer verification. This makes the life easy for the customers and convenient for them to access the bank account from anywhere in the world.

But nothing comes with disadvantages and everything has its pros and cons, same is with the online banking. Online Banking too comes with its share of flaws. Due to the increase in technology usage, the number of customers of the domestic banking system has been increased steadily in the first quarter of 2009. Umpteen problems are taking place recently in online banking transactions related to security, privacy, confidentiality and authenticity of the customer's data.Attacks on online banking used today are based on deceiving the customer so as to steal the login data and account details. Two well-known examples for those attacks are Phishing and Pharming. Hence, so security of a customer's financial information is very important, without which online banking could not operate. Financial institutions have set up various security processes to reduce the risk of unauthorized online access to a customer's records, but there is no consistency to the various approaches adopted. Though, single password authentication is still in use, it by itself is not considered secure enough for online banking. At the same time, there is no scientific method to test the authenticity of data from any printed document.

Thus to promise security in transactions, financial institutions in the present are applying a security card and a public key certificate for confirming customer identity and have introduced OTP, recently. One-Time Password is a password system where passwords can only be usedonce and the customer has to be updated with a new password key each time. This guarantees safety if the attacker is tapping the password in the network or even if the customer loses it. Besides, OTP features anonymity, portability, and extensity and prevents the information from being leaked. But, however merely using a security card for safety does not suit the modern mobile environment because we do not know when and how online banking would become a victim of the attacks. Thus, to overcome such vulnerabilities and inconveniences, we propose an Online Banking Authentication System which makes use of QR-Code, OTP and IMEI Number of the customers mobile device.

II. PROPOSED SOLUTION

In this paper, we propose an Online Banking Authentication System which provides greater security, efficiency and convenience through the use of QR-Code, one of the 2D barcode adopted by current international and national standards, OTP (One-Time Password) a unique password for single-use authentication credential and the IMEI (International Mobile Station Equipment Identity) Number of the user mobile device for identifying the device.

This paper isorganized asfollows:

1) In Section 2, we introduceQR-Code, OTPand IMEI Number.

2) In Section 3, we describe our new scheme and analysis of proposed authentication system which makes use of TTJSA Algorithm for Encryption and Decryption purpose.

III. RELATED WORK

A. QR-Code (Quick Response-Code)

A QR code consists of black modules (square dots) arranged in a square grid on a white background, which can be read by an imaging device (such as a camera) and processed using Reed–Solomon error correction until the image can be appropriately interpreted. The required data are then extracted from patterns present in both horizontal and vertical components of the image.

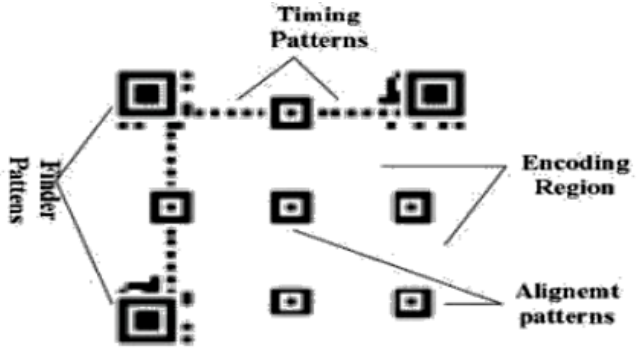

Figure 1 - The structure of QR-Code.

A QR code uses four standardized encoding modes (numeric, alphanumeric, byte / binary, and kanji) to efficiently store data; extensions may also be used.The amount of data that can be stored in the QR code symbol depends on the data-type (mode, or input character set), version (1, …, 40, indicating the overall dimensions of the symbol), and error correction level. The maximum storage capacities occur for 40-L symbols (version 40, error correction level L).

Number of bits per length field

Encoding	Ver. 1–9	10–26	27–40
Numeric	10	12	14
Alphanumeric	9	11	13
Byte	8	16	16
Kanji	8	10	12

Figure 2 – Standardized Encoding Modes Of QR-Code.

The QR code system was invented in 1994 by Denso-Wave. Its purpose was to track vehicles during manufacture; it wasdesigned to allow high-speed component scanning. Although initially used for tracking parts in vehicle manufacturing, QR codes now are used in a much broader context, including both commercial tracking applications and convenience-oriented applications aimed at mobile-phone users (termed mobile tagging). QR codes may be used to display text to the user, to add a vCard contact to the user's device, to open a Uniform Resource Identifier (URI), or to compose an e-mail or text message. Users can generate and print their own QR codes for others to scan and use by visiting one of several paid and free QR code generating sites or apps. It can also be used in storing personal information for use by organizations. The technology has since become one of the most-used types of two-dimensional barcode .There was still another factor that contributed greatly to spreading the use of the code, and that was DENSO WAVE's decision to make the specifications of the QR Code publicly available so that anyonecould use it freely. It was in 2002 that use of the code became widespread among the general public in Japan. What facilitated this trend was the

marketing of mobile phones with a QR Code-reading feature. These phones make it possible for people to access a website or obtain a coupon by just scanning a strange, eye-catching pattern. The sheer convenience helped to rapidly heighten the popularity of the code among the general public. And now, it is an indispensable tool for businesses and in people's daily lives, used in all sorts of ways including for issuing name cards and electronic tickets and in flight ticket issuing systems implemented at airports.

The QR-Codes can be used in Google's android, BlackBerry OS, Nokia Symbian Belle, Apple iOS devices (iPhone/iPod/iPad), Microsoft Windows Phone, Google Goggles, 3rd party barcode scanners and the Nintendo 3DS. These devices support URL redirection which allows QR-Codes to send metadata to existing applications on the device.

B. OTP (One-Time Passwords)

A one-time password (OTP) is a password that is valid for only one login session or transaction. It is a randomly generated, single-use authentication credential. OTP is a form of secondary authentication that is used in addition to standard user name and password credentials to strengthen the existing authentication and authorization process, thereby providing additional security for users. When the user is OTP-challenged, a one-time password is generated and delivered to the user through one of the configured channels. The user must retrieve the one-time password and enter it when prompted, before the one-time password expires.

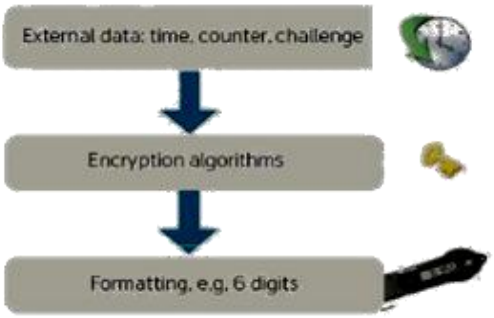

Figure 3 - The Generation Of One-Time Password.

The one-time password may be either numeric or alphanumeric and any configured length and the randomization algorithm is pluggable. One-time password systems provide a mechanism for logging on to a network or service using a unique password which can only be used once, as the name suggests. This prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time. Typically the users logon name stays the same, and the one-time password changes with each logon. One-time passwords are a form of so-called strong authentication, providing much better protection to on-line bank accounts, corporate networks and other systems containing sensitive data.

Today most enterprise networks, e-commerce sites and online communities require only a user name and static password for logon and access to personal and sensitive data. Although this authentication method is convenient, it is not secure because online identity theft – using phishing, keyboard logging, man-in-the-middle attacks and other methods – is increasing throughout the world.Strong authentication systems address the limitations of static passwords by incorporating an additional security credential, for example, a temporary one-time password (OTP), to protect network access and end-users' digital identities. This adds an extra level of protection and makes it extremely difficult to access unauthorized information, networks or online accounts.

One-time passwords can be generated in several ways and each one has trade-offs in term of security, convenience, cost and accuracy. Simple methods such as transaction numbers lists and grid cards can provide a set of one-time passwords. These methods offer low investment costs but are slow, difficult to maintain, easy to replicate and share, and require the users to keep track of where they are in the list of passwords. A more convenient way for users is to use an OTP token which is a hardware device capable of generating one-time passwords. Some of these devices are PIN-protected, offering an additional level of security. The user enters the one-time password with other identity credentials (typically user name and password) and an authentication server validates the logon request. Although this is a proven solution for enterprise applications, the deployment cost can make the solution expensive for consumer applications. Because the token must be using the same method as theserver, a separate token is required for each server logon, so users need a separate token for each Web site or network they use.

More advanced hardware tokens use microprocessor-based smart cards to calculate one-time passwords. Smart cards have several advantages for strong authentication including data storage capacity, processing power, portability, and ease of use. They are inherently more secure than other OTP tokens because they generate a unique, non-reusable password for each authentication event, store personal data, and they do not transmit personal or private data over the network.

C. IMEI (International Mobile Station Equipment Identity)

The International Mobile Station Equipment Identity or IMEI is a number, usually unique to identify 3GPP (i.e., GSM, UMTS and LTE) andiDEN mobile phones, as well as some satellite phones. It is usually found printed inside the battery compartment of the phone, but can also be displayed on-screen on most phones by entering *#06# on the dial-pad, or alongside other system information in the settings menu on smart-phone operating systems.

Figure 4 - An Example Of IMEI Number.

The IMEI number is used by a GSM network to identify valid devices and therefore can be used for stopping a stolen phone from accessing that network. For example, if a mobile phone is stolen, the owner can call his or her network provider and instruct them to "blacklist" the phone using its IMEI number. This renders the phone useless on that network and sometimes other networks too, whether or not the phone's SIM is changed.The IMEI is only used for identifying the device and has no permanent or semi-permanent relation to the subscriber. Instead, the subscriber is identified by transmission of an IMSI number, which is stored on a SIM card that can (in theory) be transferred to any handset.

However, many network and security features are enabled by knowing the current device being used by a subscriber.The IMEI (15 decimal digits: 14 digits plus a check digit) or IMEISV (16 digits) includes information on the origin, model, and serial number of the device. The structure of the IMEI/SV is specified in 3GPP TS 23.003. The model and origin comprise the initial 8-digit portion of the IMEI/SV, known as the Type Allocation Code (TAC). The remainder of the IMEI is manufacturer-defined, with a Luhn check digit at the end. For the IMEI format prior to 2003, the GSMA guideline was to have this Check Digit always transmitted to the network as zero. This guideline seems to have disappeared for the format valid from 2003 and onwards.

	AA	**-**	**BB**	**BB**	**BB**	**-**	**CC**	**CC**	**CC**	**D or EE**
Old IMEI	TAC				FAC					(Optional) Luhn checksum
New IMEI	TAC									
Old IMEISV	TAC				FAC		Serial number			Software Version Number (SVN).
New IMEISV	TAC									

Figure 5. Structure Of IMEI.

Asof2004, the format of the IMEI is *AA-BBBBBB-CCCCCC-D*, although it may not always be displayed this way. The IMEISV drops the Luhn check digit in favour of an additional two digits for the Software Version Number (SVN), making the format *AA-BBBBBB-CCCCCC-EE*.

When mobile equipment is stolen or lost the owner can contact their local operator with a request that it should be blocked from the operator's network, and the operator can be expected to do so if required by law in the operator's jurisdiction. If the local operator possesses an Equipment Identity Register (EIR), it then may put the device IMEI into it, and can optionally communicate this to shared registries, such as the Central Equipment Identity Register (CEIR) which blacklists the device in switches of other operators that use the CEIR. With this blacklisting in place thedevice becomes unusable on any operator that uses the CEIR, making theft of mobile equipment a useless business proposition, unless for parts.The BGAN, Iridium and Thuraya satellite phone networks all use IMEI numbers on their transceiver units as well as SIM cards in much the same way as GSM phones do. The Iridium 9601 modem relies solely on its IMEI number for identification and uses no SIM card; however, Iridium is a proprietary network and the device is incompatible with regular GSM networks.

IV. ALGORITHMS USED

A. TTJSA for Encryption Purpose of the Embedded Data

TTJSA is a combined symmetric key cryptographic method, which is formed of generalized modified Vernam cipher, MSA and NJJSA symmetric key cryptographic methods. Brief study of the methods used in TTJSA algorithm is as follows:

1) Modified Vernam Cipher.

In this step, we break the whole file into different small blocks (like in Block Cipher system),where each block size should be less than or equal to 256 byes. Then we follow these steps:

Step1: Perform normal Vernam Cipher method with the block of randomized key i.e. each byteof blocks of the file+ each byte of the blocks of randomized key.

Step 2: If the pointer reaches the end of each block then after performing Vernam Ciphermethod, pass the remainder of the addition of the last byte of the file block with the last byte ofthe key to the next file block and add the remainder with the first byte of the that file block. (This mechanism is called feedback mechanism).

Step 3: Perform Step 1 and Step 2 until the whole file is encrypted and repeat this step forrandom number of times. After performing the aforementioned steps, we again merge the blocksof the encrypted file and thus we get the final encrypted result of this modified Vernam Ciphermethod.

2) NJJSAA Algorithm.

The encryption number (=secure) and randomization number (=times) is calculated according tothe method mentioned in MSA algorithm.

Step 1: Read 32 bytes at a time from the input file.

Step 2: Convert 32 bytes into 256 bits and store in some 1-dimensional array.

Step 3: Choose the first bit from the bit stream and also the corresponding number (n) from thekey matrix. Interchange the 1st bit and the n-th bit of the bit stream.

Step 4: Repeat step-3 for 2nd bit, 3rd bit...256-th bit of the bit stream

Step 5: Perform right shift by one bit.

Step 6: Perform bit(1) XOR bit(2), bit(3) XOR bit(4),...,bit(255) XOR bit(256)

Step 7: Repeat Step 5 with 2 bit right, 3 bit right,...,n bit right shift followed by Step 6 after eachcompletion of right bit shift.

3) MSA Encryption and Decryption Algorithm.

Nath et al. proposed a symmetric key method where they have used a random key generator forgenerating the initial key and that key is used for encrypting the given source file. MSA methodis basically a substitution method where we take 2 characters from any input file and then searchthe corresponding characters from the random keymatrix and store the encrypted data in anotherfile. MSA method provides us multiple encryptions and multiple encryptions. The key matrix (16x16) is formed from all characters (ASCII code 0 to 255) in a random order.The randomization of key matrix is done using the following function calls:

Step-1: call Function cycling ()

Step-2: call Function upshift ()

Step-3: call Function downshift ()

Step-4: call Function leftshift ()

Step-5: call Function rightshift ()

How the above functions will work have been discussed in detail by Nath et al. The idea of thesefunctions is to make elements in a square matrix in a random order so that no one can predictwhat will be the nearest neighbor of a particular element in that matrix. This method is basicallymodified Playfair method. In Playfair method one can only encrypt Alphabets but in MSA onecan encrypt any character whose ASCII code from 0-255 and one can apply multiple encryptionshere which are not possible in normal Playfair method.

V. FUTURE SCOPE

One-Time Password is a password system where passwords can only be used once and this guarantees the safety even if an attacker is tapping password in network. OTP features anonymity, portability, extensibility and enables to keep the information from being leaked. QR-Code is fast, easy, accurate and automatic data collection method. The IMEI Number identifies the valid devices and can be used for stopping the stolen phone from accessing the account. Simply, a smart-phone running on Android or iOS or any other new generation of mobile OS can be used to extract encrypted data from embedded QR-Code and finally that data to be decrypted using the TTJSA decryption algorithm.

VI. CONCLUSION

Online transaction of money has become the norm with almost all kinds of businesses. Hence, the use of electronic banking services has increased gradually in daily life and the existing online banking systems require more security to prevent from various threats. To promise security in transactions, financial institutions in the present are therefore applying a security card and a public key certificate for confirming customer identity, but these prove to be lagging when privacy and safety of user data is concerned. Thus, in order to overcome such discomfort, we propose a new authentication system for online banking that can provide greater security and confidentiality through the use of QR-Code, OTP, and IMEI Number of the user mobile device. These mechanisms make the online transactions comparatively free from security threats. Even in regard to theft or loss, attackers cannot approach due to internal password system and the devices that can be used which have the highest loss recognition.

REFERENCES

[1] Somdip Dey, Asoke Nath and Shalabh Agarwal "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System" 2013 International Conference on Communication Systems and Network Technologies IEEE 2013.

[2] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, Heung Kuk Jo, Hoon Jae Lee "Online Banking Authentication System using Mobile-OTP with QR-code" IEEE 2010.

[3] Young-Gon Kim and Moon-Seog Jun "A Design of User Authentication System Using QR code Identifying Method" IEEE 2010.

[4] Symmetric Key Cryptography using Random Key generator: "Proceedings of International conference on security and management (SAM'10" held at Las Vegas, USA Jull 12-15, 2010), P-Vol-2, 239-244(2010).

[5] Symmetric key cryptosystem using combined cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm " Proceedings of Information and Communication Technologies (WICT), 2011 " held at Mumbai, 11th – 14th Dec, 2011, Pages:1175-1180.

[6] New Symmetric key Cryptographic algorithm using combined bitmanipulation and MSA encryption algorithm: NJJSAA symmetrickeyalgorithm: NeerajKhanna, JoelJames, JoyshreeNath, SayantanChakraborty, AmlanChakrabarti and AsokeNath: Proceedings ofIEEE CSNT-2011 held at SMVDU (Jammu) 03-06 June 2011, Page125-130(2011).

