International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 02 | February - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

THREE LEVEL SECURITY AUTHENTICATION IN ONLINE BANKING

ARATHY KRISHNAN

DEPARTMENT OF COMPUTER SCIENCE

SREE AYYAPPA COLLEGE, ERAMALLIKKARA

arathyanoop2306@gmail.com

ABSTRACT

Authentication, security, and confidentiality are some of the most important topics of cyber security. There have been many solutions presented to users for strengthening the security of login password-based authentication methods. Primarily this has been through the use of two-factor authentication methods. Two-factor authentication is the combination of single factor authentication mechanisms. The growing popularity and acceptance of two-factor methods are driven by the increasing need for privacy and security in this technological age. The success and popularity of adapted security measures are largely dependent on their ease of implementation and convenience to the user. The focus of this research is to address and analyze the implications of using a three-factor authentication model for added security in websites and mobile apps. This paper will present an app we created which could provide a potential method for three-factor authentication that could potentially ensure added authentication assurances without loss of convenience.

I. INTRODUCTION

Almost every network authentication, server side authentication system is used and this is performed using user id (usernames) and passwords. Each user login to the system by using allocated or self-declared passwords. Usernames are commonly a mixture of a person's first and last names, which is predictable to an external user. Password-based verification and Knowledge- Based authentication (KBA) are vulnerable than system using multiple methods. Client side authentication is the verification done by user himself/herself. By using this each client will feel that he is also a part of the security system. The system uses only client side authentication provides a limited security. In the case of network system client side authentication method is less preferable. In recent days more secure biometric client side authentication mechanisms are implemented. Three factor authentications is a combination of both client side and server side authentication mechanisms. It uses three factors- first one is auto generated plain text passwords, second one is auto generated QR code and third one is biometric passwords (fingerprint lock).

The system lets the user to input the OTP, if the user is authorized one then an encrypted string consisting of IMEI number of the user is displayed in the form of QR code. The user verifies his/her fingerprint using an application lock to open the android application. If the entered fingerprint matches with the fingerprint stored in the phone database then the user can scan the QR code using the application. If the encrypted string contains the IMEI number of the device the user will authenticated.

The core objective of the proposed system is to design and implement a three factor authentication system using OTP, fingerprint and QR code for online transactions. The current online transaction is performed using a computer system and a website of a particular bank which helps to interact with the bank. The verification of each user is performed by using an OTP which is sent to the user through SMS or email.

The main intention of the proposed system is to include the android phones in the authentication process, because it is common in these recent days. Each individual possess android phones which is uniquely identified by its IMEI (International Mobile Equipment Identification) number. We are utilizing this uniqueness of android phones to uniquely identify the users who possess it.

Mainly there are three types of factors are used to perform authentication. Something you know (knowledge factor), something you have (possession factor), and something you are (the inherent factor). The idea of three factor authentication aims to use both the three factors to perform the verification, which enhances the security. It also aims to give an important role to individual users in the process of authentication. In the existing system only server side authentication is performed. Proposed system verifies

fingerprint security at client side, so that the user will more satisfied because he/she is also a part of the authentication process.

II. THEORETICAL BACKGROUND

Three factor authentication system put forwards a system which replaces the current OTP based one factor authentication system used in verification of online transactions. In this project we are implementing a three factor authentication system using QR code and the fingerprint verification, so that the design put forwards a system that includes server side and client side authentication. QR code is validated at server side and fingerprint authentication is performed at client side by setting it as an application lock.

The proposed system uses two contents to perform authentication. A website to validate OTP and perform transactions and an android application to perform fingerprint and QR code validation.

The system lets the user to input the password, if the user is authorized one then an encrypted string consisting of IMEI number of the user is displayed in the form of QR code. The user verifies his/her fingerprint using an application lock to open the android application. If the entered fingerprint matches with the fingerprint stored in the phone database then the user can scan the QR code using the application. If the encrypted string contains the IMEI number of the device the user will authenticated. The result of QR code verification is sent to the server. The three factor authentication is continuous security verification and the user is permitted to perform transaction if and only if the three levels of authentication is satisfied.

II.I IMEI NUMBER

The main concern here is the IMEI number, and based on IMEI, a dedicated application is required to be built on every mobile phone by the manufacturing company.The idea is to have IMEI application on every mobile device and it must be mandatory to install IMEI application by the consumer for smooth functioning of device.

 Registration of IMEI Application

The idea is to process the online transaction request with dedicated hardware only. The device with IMEI number which has been registered with bank server will receive the OTP, in case when any online query is prompted by registered user. It will happen with the help of IMEI application, which has been installed with user's mobile phone. The mobile manufacturing companies should provide the IMEI application as a mandatory installation whenever user inserts the SIM to activate the phone.

Before activating the proposed algorithm, following steps are required to follow by the consumer:

Step1: IMEI Application Installation To activate a SIM in mobile device, a mandatory IMEI application has to be installed by the consumer in the mobile phone. The IMEI number is hard coded on the device means it is already provided by the mobile manufacturing companies and it must never be changed by the consumer.

Step2: Bank Registration Here the consumer will provide all the details which are given in step 1, to the authorized bank.

Step3: Data Transmission through IMEI Application After sharing the details with bank, consumer will send the request to bank server to authenticate the same.

Step4: Verification Bank will verify the data and it will add the IMEI application request number in its record.

 Reason of Choosing IMEI

Through this research, the author wants to suggest to all mobile manufacturing companies to create their own IMEI application. Therefore, it can be installed mandatorily when the consumer wants to activate his mobile device. This app will store all the details of consumer and send it to bank server. The intention of this research is that, the OTP must reach on the only mobile device whose IMEI number with all details is stored on the bank server. IMEI number plays a vital role in this regard, as it is unique. All the other parameters like mobile number, address, and account number may change but it will not change. In case if IMEI number does not match, the bank server will not send any OTP and the transaction will fail.

II.II QR CODE

The QR codes stands for the Quick Response Code. The barcode mentioned earlier was a one dimensional authentication method. The QR code is a barcode that is two dimensional. It is a barcode that uses a matrix and was first designed in Japan for automotive industry. A barcode has details of the object to which it is affixed and can be interpreted by a machine known as a barcode reader. To efficiently store data, a QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary); extensions can also be used. As compared to general UPC barcodes, QR codes can be scanned faster and can store a greater amount of data. These characteristics made the QR code famous outside the Japanese automotive industry. Quick Response codes are used for managing documents, recognisability of objects, general marketing and tracking of products and time. A QR code consists of a white background along with square shaped modules that are blank in colour and arranged in a square shaped matrix, which are in the foreground. This code can be read by scanners and cameras and mistakes are removed by the Reed-Solomon technique till the image is aptly scanned. Vertical and horizontal components of the image contain patterns that can be chosen and selected to obtain needed data

. A. Finder Pattern:

The finder pattern is used to trace the exact location of the QR code. Geometric properties of the code, such as the dimension and the angle can also be examined. A more significant use of the finder pattern is in the detection of the code in angles that are round the clock. Distortion post scanning is made correct using Alignment patterns which are very useful. The correction of this distortion is facilitated by the black module in the central area of the Alignment Pattern.

B. Timing Pattern:

If an error pitch is present in the middle part of cell, it can be recognised in both, vertical and horizontal directions using supporting patters called Timing Patterns.

C. Quiet Zone:

The function of the data embedding technique can be simplified by recognising the QR code from it's relatively complicated backgrounds using this zone.

D. Data Area:

Confidential information can be stored in this section. The black and white sections can be allotted zeros and ones in either of the two possible combinations and thus, information can be hidden in binary format. For the rectification of mistakes and the respective embedding of data ,the Reed-Solomon codes can be used. C. Links and Bookmarks All hypertext links and section bookmarks will be removed from papers during the processing of papers for publication. If you need to refer to an Internet email address or URL your paper, you must type out the address or URL fully in Regular font.

- QR code generation and scanning:

After entering hexaflip password it sends request to generate QR code. Once the request is sent to the server, it generates QR code which will be displayed on the client machine. First random number is encrypted using public key. The encrypted string generates the Quick Response Code using it's generation function in java. Now, the client machine displays this image of the QR code. This QR code is scanned by the user using cell phone. By scanning the QR code, he extracts the information (random no.) stored in the QR code. This random no gets combined with the IMEI no. of the user's mobile and a string is generated. This string is matched with the string generated in database. The string in database is generated by combining IMEI no that client has entered while registration and the random no. If both the strings i.e. string sent by user and string generated in database matches then it can be confirmed that user is authenticated. For login each time, new QR code is generated. So in our system there is no need to remember the password which is combination of your IMEI number and the random number. After successful login the home page of the bank is opened. User can check his mini statement, can transfer money to another account holder from the home page.

II.III FINGER PRINT

A fingerprint is an impression left by the friction ridges of a human finger. The recovery of partial fingerprints from a crime scene is an important method of forensic science. Moisture and grease on a finger result in fingerprints on surfaces such as glass or metal. Deliberate impressions of entire fingerprints can be obtained by ink or other substances transferred from the peaks of friction ridges on the skin to a smooth surface such as paper. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, though fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster.

 FingerPrint Authentication

With the release of Android 6.0 (Android M), there has been a significant amount of changes to the APIs, one of them is Fingerprint Authentication. Now, we can easily implement Fingerprint Authentication in our application in the devices having the Fingerprint sensor. The whole process of Fingerprint Authentication can be summarized into the below steps:

1. Requesting Fingerprint Authentication permission within the project's manifest file.

2. As fingerprints can only be registered on the devices which have its lock screen protected by a PIN, pattern or password. So, we have to check if the lock screen of the device is protected by a PIN, pattern or password.

3. Then, create an instance of the Fingerprint Manager class.

4. You have to gain access to the storage area that is used to store the cryptographic keys on Android devices i.e. Keystore. So, create an instance of the Keystore to gain access of the Android Keystore container. After that, generate an encryption key with the help of keyGenerator class and store it in the Keystore container.

5. With the help of the key generated and stored in the Keystore container, initialize the instance of the Cipher class and use this instance to create a CryptoObject and assign it

to Fringerprint Manager instance that you have created earlier.

6. Call the authenticate method of the FingerprintManger class and implement methods to handle the callbacks.

II.IV ONE TIME PASSWORD (OTP):

A one-time password (OTP), also known as one-time pin or dynamic password, is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two-factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows (such as a PIN).

The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

OTPs have been discussed as a possible replacement for, as well as enhancer to, traditional passwords. On the downside, OTPs are difficult for human beings to memorize. Therefore, they require additional technology to work.

 OTP Generation:

OTP generation algorithms typically make use of pseudo randomness or randomness, making prediction of successor OTPs by an attacker difficult, and also cryptographic hash functions, which can be used to derive a value but are hard to reverse and therefore difficult for an attacker to obtain the data that was used for the hash. This is necessary because otherwise it would be easy to predict future OTPs by observing previous ones. Concrete OTP algorithms vary greatly in their details.

Various approaches for the generation of OTPs are listed below:

 Based on time-synchronization between the authentication server and the client providing the password (OTPs are valid only for a short period of time)

 Using a mathematical algorithm to generate a new password based on the previous password (OTPs are effectively a chain and must be used in a predefined order).

 Using a mathematical algorithm where the new password is based on a challenge (e.g., a random number chosen by the authentication server or transaction details) and/or a counter.

There are also different ways to make the user aware of the next OTP to use. Some systems use special electronic security tokens that the user carries and that generate OTPs and show them using a small display. Other systems consist of software that runs on the user's mobile phone. Yet other systems generate OTPs on the server-side and send them to the user using an out-of-band channel such as SMS messaging. Finally, in some systems, OTPs are printed on paper that the user is required to carry.

II.V AVOID PHISHING ATTACK IN BANKING INDUSTRY

The word “phishing” is an attempt, originally via a message or email, to lure computer users to reveal sensitive personal information such as passwords, birthdates, credit cards, and social security numbers. To perpetrate this type of con, the communication pretends to be from an official representative of a website or another institution a person has likely done business with (e.g., PayPal, Amazon, UPS, Bank of America, etc.). The communication may have an “iPad giveaway,” “fraud alert”, or other type of intriguing subject line. The email itself may contain the company’s logo and phone number, and otherwise look completely legitimate; another common tactic is to make it look like a personal email from a friend or relative who wants to share something with you. However, once victims click on the provided link, instead of being directed to the real website, they are routed to a fake, where they unwittingly enter all their information as prompted. This information is captured by the thieves and used immediately, sold on the black market for nefarious purposes, or both. Many times the user’s computer is also infected, sending out phishing emails from their address books and continuing the rampage. Phishing is one the oldest cyber security scams. It is often perpetrated via emails, and it is an attempt to deceive users in some way. Hackers can trick their targets into opening an attachment containing malicious code or into visiting a spoof webpage where they enter their personal data, or into simply sending information to the sender. This fairly simple scam has gotten much more sophisticated in recent years. Phishers, in fact, have become more resourceful and with access to more information on their victims via corporate websites and social networks, they are able to effectively personalize messages and websites or install malware to target specific victims

Phishing steals identities and wrecks lives. It affects everyone, from a senior bank manager to a minor who has

never heard of internet scams. The worst part is that though phishing is now more than a decade old, many people are not familiar with how it works and still fall victim to this scam.

Let us look at some of the ways in which successful phishing works. Using data to access a victim's account and withdrawing money or making an online transaction, e.g. buying a product or service.

 Using data to open fake bank accounts or credit cards in the name of the victim and using them to cash out illegal checks, etc.

 Using the victim's computer systems to install viruses and worms and disseminating phishing emails further to their contacts.

 Using data from some systems to gain access to high value organizational data such as banking information, employee credentials, social security numbers, etc.

III. MEASURES TAKEN TO PREVENT PHISHING

Phishing can take many forms and can be achieved with many tools and techniques. Here, we highlight the most common tools and techniques that are used to carry out phishing scams.

III.I Link Manipulation

Link manipulation is a widely used technique for phishing scams. It is done by directing a user through fraud to click a link to a fake website. Generally, many users are now aware that they do not need to click on links that may seem suspicious in first look. Hence, hackers are now using manipulative ways to get the users to click. Let us look at some of the ways hackers use link manipulation to their advantage:

1. Use of Sub-Domains

For nontechnical users who may not be familiar with sub-domains, this trick works like magic for the hacker. Consider for example, you get an email from a renowned xyz bank that asks for your credentials and requests you to click on the URL www.xyzbank.user.com. A nontechnical person will

consider that the link would direct to a "user" section of the xyz bank. In reality, the link takes you to the "xyzbank" section of the website www.user.com. Though the domains are unique, sub-domains are not, and hence no domain owner can prevent anyone from using their name as a sub-domain of their domain. Whether technical or nontechnical, one should always remember that the URL hierarchy always goes from right to left. Hence a link that says mail.yahoo.com will take you to domain of yahoo with sub-domain as mail, whereas yahoo.mail.com will lead you to the domain mail.com with subdomain as yahoo.

2. Hidden URLs

Another commonly used link manipulation technique is when a phisher hides the actual URL under plain text. This means that rather than displaying the actual URL, they use sentences such as "Click Here" or "Subscribe". In reality, the URL hiding behind the text leads you to phishing websites. A more convincing email could even display the actual link, such as www.americanexpress.com, but if you click the link it would lead you to an unexpected website. Another method of hiding the URL is by using shortening tool such as tiny url or bit.ly. (You don't need to worry about clicking these links, as all of them take you to Security IQ's PhishSim tool portal). With more users now on social media networks, phishers are able to cast wider nets with greater opportunities to succeed. With social media, the trust factor for which phishers otherwise work very hard is already there. People follow and receive messages from other people and services they trust. Skeptical users may easily spot rogue messages, but most of the time these go undetected and tempt users into clicking. With only one malicious link, a hacker can easily target many users in one go. Since URL shorteners are extensively used on social media, it is hard to tell in advance where the link will actually take us. To avoid clicking a manipulative hidden URL, always hover your cursor over the link and check to see the actual link where the URL is directing you to. In case the link seems "phishy," do not click it.

3. Misspelled URLs

Another common link manipulation technique is when a hacker will buy domains with a variation in spellings of a popular domain, for example, facebok.com, googlle.com, yahooo.com, etc. They then fool the users by making similar looking websites and asking for personal information. This technique

is also known as URL hijacking or typosquatting. The advantage it gives to a malicious user is that they don't even need to be sent via email to be accessed. Rather, a little carelessness in typing can lead many users to them. 4. IDN Homograph Attacks In this technique, a malicious individual misguides a user towards a link by taking advantage of similar looking characters. For example, a user who frequently visits Citibank.com may be directed to click a link in which Latin C is replaced by Cyrillic C. Moreover, characters that seem similar may also be used to deceive. For example, capital of i (I) and small L (l), both look the same. Similarly, zero (0) and capital o (O) also look much the same.

III.II Website Forgery

Website forgery is another phishing technique that works by making a malicious website impersonate an authentic one, so as to make the visitors give up their sensitive information like account details, passwords, credit card numbers, etc. Web forgery is mainly carried out in two ways: cross-site scripting and website spoofing. 1. Cross-Site Scripting Cross-site scripting, or XSS, is an attack in which a hacker executes malicious script or payload into a legitimate web application or website. It is a very common and widely used technique in which the victim is not directly targeted. Rather, the attacker exploits a vulnerability in a web application or website that is visited by a user. Eventually, a malicious script is delivered to the victim's browser. Though hackers can take advantage of XSS within ActiveX or VBScript also, the most commonly abused is JavaScript, primarily because it is used by nearly all websites of today. In order to make it work, an attacker will need to inject a payload into a page visited by the victim. To make you visit a page, the attacker uses social engineering or link manipulation techniques. To make it further successful for the attacker, the user then needs to input their data directly into the fake website's pages. After this, the attacker will insert a string to be used in the webpage and treated by the user's browser as code. When the browser loads the page, the malicious script executes without the victim even knowing that such an attack has taken place.

Protection against XSS is possible, though it may not be totally avoidable. Some browsers come with built-in XSS protection, so it is always a good practice to check your browser's security options and update the browsers to the latest versions. Some add-ins like NoScript for Firefox let you allow or deny permission. NoScript also lets users reject websites other than the ones chosen by them for their usage.

2. Website Spoofing

Another technique used for web forgery, website spoofing, is done by creating a fake website that looks similar to a legitimate website that the user actually intends to access. A spoof website has a similar user interface and design and often has a similar URL. If you are in a hurry and not paying much attention, you can easily fall prey to such sites that appear identical to their legitimate versions. If you have not manually typed a URL and are landing on a webpage by clicking a certain link, you need to be particularly skeptical about it. As already discussed in our Link Manipulation section, you should always look out for the possibility of URL cloaking. To be sure, hover your cursor over the link to check the actual URL where the link is taking you to.

III.III Pop-Ups

Pop-up messages are one of the easiest techniques to conduct successful phishing scams. They allow hackers to steal login details by sending users pop-up messages and eventually leading them to forged websites through these pop-ups. A variant of phishing attacks, also known as "in-session phishing," works by displaying a pop-up window during an online banking session and appears to be a message from the bank.

A typical "in-session phishing" scenario would look like this: You log into your online banking account.

 You may leave your browser open and check another website in another window.

 A pop-up appears after some time, supposedly from your bank, and asks you to retype your username and password as your previous session has expired.

 You enter your details, not expecting the popup to be a fraud, since you had already logged into the bank's website.

Another recently widespread pop-up phishing scam is the "popup tech support." When browsing the Internet, you will suddenly receive a pop-up message that your system is infected and you need to contact your vendor for technical support.

IV IMPLEMENTATION AND RESULTS

Three factor authentication system put forwards a system which replaces the current OTP based one factor authentication system used in verification of online transactions. In this project we are implementing a three factor authentication system using QR code and the fingerprint verification, so that the design put forwards a system that includes server side and client side authentication. QR code is validated at server side and fingerprint authentication is performed at client side by setting it as an application lock.

The proposed system uses two contents to perform authentication. A website to validate OTP and perform transactions and an android application to perform fingerprint and QR code validation.

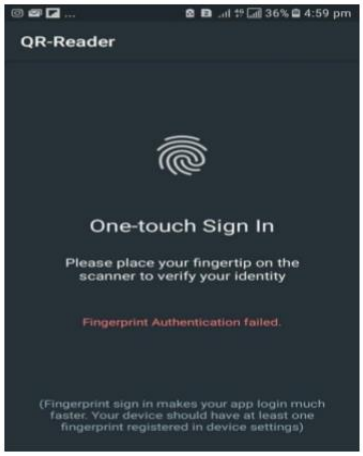

Figure1: FINGERPRINT VERIFICATION

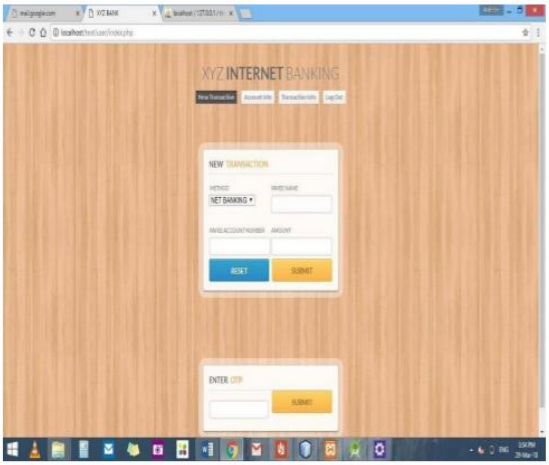

Figure 2: OTP GENERATION PAGE

Figure 3: QR GENERATION PAGE

The system lets the user to input the password, if the user is authorized one then an encrypted string consisting of IMEI number of the user is displayed in the form of QR code. The user verifies his/her fingerprint using an application lock to open the android application. If the entered fingerprint matches with the fingerprint stored in the phone database then the user can scan the QR code using the application. If the encrypted string contains the IMEI number of the device the user will authenticated. The result of QR code verification is sent to the server. The three factor authentication is continuous security verification and the user is permitted to perform transaction if and only if the three levels of authentication is satisfied.

V. CONCLUSION

In recent days network based attacks are widely increasing. The existing password (one factor) based authentication only helps to prevent traditional attacks. To prevent several attacks the currently using method is that increasing the password length or size of the encrypting and decrypting key. But the recently occurred attacks like phishing cannot be prevented using the password based security because the user himself/herself shares their sensitive data.

Here is the need for multiple levels of authentication in online transactions. Three factor authentications is a continuous three levels of validation process which improves the security of online transactions. It uses a combination of a website and an android application for the authentication and transaction. The system uses both the three components of authentication such as knowledge factor, possession factor and the inherent factor.

Since the generated QR code is different for each and every time is different and it is invisible to the user the shoulder attacks, man-in-the-middle attacks, phishing, spoofing can be prevented.

VI. REFERENCES

[1] Olufemi Sunday Adeoye “Evaluating the performance of two-factor authentication solution in the banking sector“. International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[2] Reshmi Maulik,” An Overview of Phishing and ItsIndianPerspective”,Available: https://www.researchgate.net/publication/361541692

[3] Kennedy, William & Olmsted, Aspen. (2017). Three factor authentication. 212-213. 10.23919/ICITST.2017.8356384.

[4] D. DeFigueiredo, "The Case for Mobile Two-Factor Authentication," IEEE Security & Privacy, vol. 9, no. 5, pp. 8185, Sept-Oct 2011

[5] Bharat B. Bhagat, and Latika Kharb, “Phishing and Its Indian Perspective”, The Internet Journal of Medical Informatics, Vol. 3, 2008

[6] Paul Roberts. Multi-Factor Authentication, IEEE. 2004.