Authentication Using Mobile Phone as a Security Token

Professor T.Venkat Narayana Rao, Vedavathi K
Department of Computer Science and Engineering
Hyderabad Institute of Technology and Management [HITAM]
Hyderabad, A.P, India

Abstract— **Today security concerns are on the rise in all areas industries such as banks, governmental applications, healthcare industry, militaryorganization, educational institutions etc, with one common weak link being "passwords". Several proper strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's security concerns. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Two factor authentication uses elements or devices such as tokens and ATM cards. We have proposed to resolve the password problem, which could be inconvenient for the user and costly for the service providers to combat otherwise. To avoid the usage of additional device, the mobile phone is adopted as security token. In this paper several different authentication solutions using the mobile as authentication token are discussed, where these solutions vary in complexity, strength, security and user friendliness. One of the authentication schemes (OTP solution) is implemented to verify their usability. Hence, a classification and evaluation of the different solutions is provided according to defined criteria.**

Keywords- **Two-factor authentication, Security token, UPIF, IMSI, IMEI, one time password (OTP).**

I. INTRODUCTION

With the increase in popularity of the Internet the number of frauds and abuses is literally exploding. Most serious is the theft of identity which causes grave damages both for the victim and also his entourage such as employee, banks, hobby clubs, etc. The protection of digital identities is getting more and more crucial. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Strong authentication solutions require often two identification factors i.e., in addition to the first factor "something you know" represented by passwords it is introduced a second factor "something you have" materialized by a security token. The introduction of the additional device could be costly for the service providers in terms of deployment and administration at the same time as it could be inconvenient for mobile users. Furthermore, there is very little re-use or sharing such that the same security token can be used for several systems. To remedy the situation, here we have proposed a authentication solution to avoid usage of extra device by re-using existing devices, namely the mobile phone or the SIM cards. This paper starts with a clarification of the notion of authentication in section II. The architecture of the two factor authentication solutions using mobile phone is given and the different authentication solutions are successively described in the sections III. The design implementation for the authentication system is provided in the sections IV and V along with the evaluation schemes.

II. AUTHENTICATION

Authentication is the assurance that the communicating entity claims to be genuine. According to Fermi Lab [1], authentication is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network. The four levels of authentication [2] defined by NIST as follows:

1. Little or no confidence in the asserted identity's validity. There is no need for identity proofing on this level, on this level it is sufficient with a simple password challenge-response protocol.
2. Some confidence in the asserted identity's validity. "Level 2 provides single factor remote network authentication [3]". At this level there is a need for identity proofing and need for a secure authentication protocol to prove the identity.
3. High confidence in the asserted identity's validity. "Level 3 provides multi-factor remote network authentication [3]". At this level there is need for a proof of possession and a minimum of two authentication factors.
4. Very high confidence in the asserted identity's validity. "Level 4 is intended to provide the highest practical remote network authentication assurance [3]". At this level there is need for proof of possession through a cryptographic protocol.

It is not specified which authentication level can be considered as strong but level 3 with multi-factor authentication is definitely considered as a strong authentication. It is also clear that strong authentication does not have to be multi-factor. According to strong authentication can start with two-factor authentication which combines of the following authentication options [4]:

- Something you know, e.g. Passwords.
- Something you have**,** e.g. One-time password tokens and Digital certificates.
- Something you are, e.g**.** Biometrics.

Most of two-factor authentication solutions combine "something you know" and "something you have". They require the usage of an additional device, which demands administration from the service provider and extra care from the user. Multi-channel communication is another way to further improve the security of an authentication scheme.

III. THE DIFFERENT MOBILE PHONE AUTHENTICATION SOLUTIONS

To authenticate users through a mobile phone requires certain components to be placed. Figure 1 shows the required components and the general architecture [6] needed for the solutions described in this paper to work.

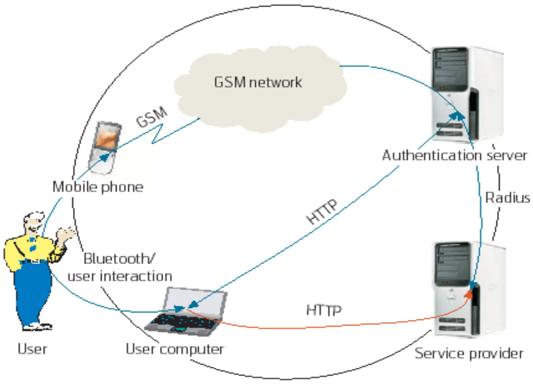

Figure 1, A general architecture of mobile authentication

The user must access to a computer connected to the internet and be in possession of a mobile phone with a working SIM card. If the computer and mobile phone are equipped with Bluetooth, higher usability can be obtained. Through the Internet browser on the computer the user can access web services provided by service providers. The service provider (SP) is connected to an Authentication Server (AS) that will handle the authentication on behalf of the SP. The AS is connected to the GSM network which enables it to communicate with the user's mobile phone and the operator's Authentication Center (AUC).The AS is composed of two parts, an authenticator and an AAA server. The authenticator communicates with the client and relays messages to the AAA server which handles the authentication.

When designing an authentication scheme which uses two separate devices that communicate over two different networks it is very important to ensure that it is the same user that controls both devices .This is done by ensuring that there is a "closed loop" going through all the components involved in the authentication as illustrated in Figure 1. The loop starts in the device requesting the service, the user's computer, goes through the network with SP and AS and then via mobile phone and back to the initial device, either by user interaction or Bluetooth.

A. SMS Authentication with Session-ID Check

This solution exploits that a user with a valid mobile subscription is already authenticated through the GSM system. Session IDs are used to ensure that it is the same user that controls both the computer and the mobile phone. When the user accesses a service provider a unique session ID is created and sent both to the user's computer and to the mobile phone. The session ID is sent over the Internet to the computer and shown in the web browser and sent to the phone by SMS. Then the user can confirm that the session IDs match and send a confirmation by SMS to the service provider. When receiving the confirmation from the user the AS knows that the user is in possession of the phone and the authentication is successful.

The comparison of the session ID can be made by the user or automatically by software if the phone is connected to the computer by Bluetooth.

B. User Verification of Session ID

The user accesses the service provider through the Internet browser and chooses to be authenticated by his mobile phone. The user identifies him with his mobile phone number and the request is redirected to the authentication server. The authentication server then creates a unique session ID and sends this to the user by SMS and over the Internet to the computer. The user checks that the session ID in the SMS is the same as the one shown in the browser. If this is the case the user replies by sending an SMS back to the AS confirming that the session IDs match. When receiving the confirmation the authentication server redirects the browser back to the service provider and the user is given access to the service. The message exchange is shown in Figure 2.

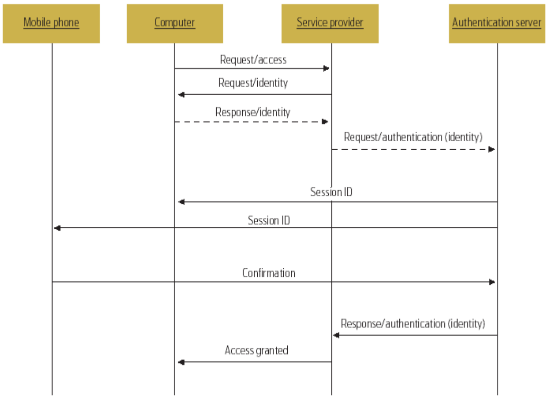

Figure 2. Session ID check

C. Automatic Check of Session ID

To make it even easier for the user the session ID can be checked automatically. This can be done by pair- ing the mobile phone and the computer by Bluetooth.

D. One-Time-Password

One-Time Password is one of the simplest and most popular forms of two-factor authentication today. This solution builds on the same principle as the session ID check, that a user with a working phone is already authenticated through the GSM network. The difference is that the check is done by the server and therefore relieves the user from this burden. The user starts the authentication procedure by entering his username. The session is redirected to the AS which creates an OTP based on the user's identity by a cryptographic hash function. The OTP is then sent to the user by SMS. When receiving the SMS the user types the OTP in the browser. The AS verifies that the OTP is correct and redirects the browser back to the service provider and the user is logged in. Figure 3 shows the message exchange of this solution

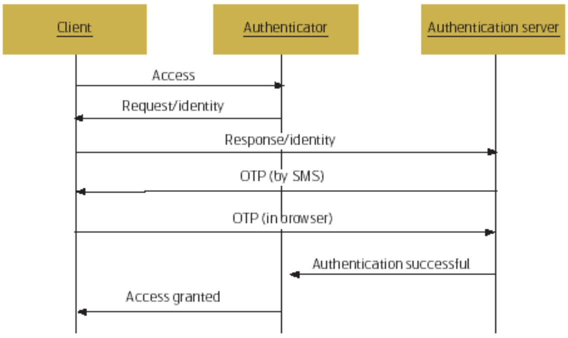

Figure 3. OTP Check

In this paper, we proposed a design implementation of OTP [5].

IV. DESIGN IMPLEMENTATION

The proposed system is secure and consists of three parts: (1) software installed on the client's mobile phone, (2) server software, and (3) a GSM modem connected to the server. The system will have two modes of operation:

A. Connection-Less Authentication System

A one time password (OTP) is generated without connecting the client to the server. The mobile phone will act as a token and use certain factors unique to it among other factors to generate a one-time password locally. The server will have all the required factors including the ones unique to each mobile phone in order to generate the same password at the server side and compare it to the password submitted by the client. The client may submit the password online or through a device such as an ATM machine. A program will be installed on the client's mobile phone to generate the OTP.

B. SMS-Based Authentication System

In case the first method fails to work, the password is rejected, or the client and server are out of sync, the mobile phone can request the one time password directly from the server without the need to generate the OTP locally on the mobile phone. In order for the server to verify the identity of the user, the mobile phone sends to the server, via an SMS message, information unique to the user. The server checks the SMS content and if correct, returns a randomly generated OTP to the mobile phone. The user will then have a given amount of time to use the OTP before it expires. Note that this method will require both the client and server to pay for the telecommunication charges of sending the SMS Message.

C. OTP Algorithm

In order to secure the system, the generated OTP must be hard to guess, retrieve, or trace by hackers. Therefore, it's very important to develop a secure OTP generating algorithm. Several factors can be used by the OTP algorithm to generate a difficult-to-guess password. Users seem to be willing to use simple factors such as their mobile number and a PIN for services such as authorizing mobile micropayments. Note that these factors must exist on both the mobile phone and server in order for both sides to generate the same password. In the proposed design implementation the following factors were chosen:

•*IMEI number*: The term stands for International Mobile Equipment Identity which is unique to each mobile phone allowing each user to be identified by his device. This is accessible on the mobile phone and will be stored in the server's database for each client.

•*IMSI number***:** The term stands for International Mobile Subscriber Identity which is a unique number associated with all GSM and Universal Mobile Telecommunications System (UMTS) network mobile phone users. It is stored in the Subscriber Identity Module (SIM) card in the mobile phone. This number will also be stored in the server's database for each client.

- *Username:* Although no longer required because the IMEI will uniquely identify the user anyway. This is used together with the PIN to protect the user in case the mobile phone is stolen.
- *PIN:* This is required to verify that no one other than the user is using the phone to generate the user's OTP. The PIN together with the username is data that only the user knows so even if the mobile phone is stolen the OTP cannot be generated correctly without knowing the user's PIN. In order for the PIN to be hard to guess or brute- forced by the hacker, a minimum of 8-characters long PIN is requested with a mixture of upper- and lower-case characters, digits, and symbols.
- *Hour:* This allows the OTP generated each hour to be unique.
- *Minute***:** This would make the OTP generated each minute to be unique. Note that the software can modified to allow the administrators to select their preferred OTP validity interval.
- *Day:* Makes the OTP set unique to each day of the week.
- *Year/Month/Date***:** Using the last two digits of the year and the date and month makes the OTP unique for that particular date.
- *UPIF:* User personal identification factor. This allows the user choose a few categories of things they can easily remember - such as cars, food and flowers .At the time of OTP Check, user identity is verified with this UPIF.

The time is retrieved by the client and server from the telecommunication company. This will ensure the correct time synchronization between both sides. The above factors are concatenated and the result is hashed using MD5/SHA which returns a 256 bit message. The message is then XOR-ed with the PIN replicated to 256 characters. The result is then Base64 encoded which yields a 28 character message. The message is then shrunk to an administrator-specified length by breaking it into two halves and XOR-ing the two halves repeatedly. This process results in a password that is unique for a ten minute interval for a specific user. Keeping the password at 28 characters is more secure but more difficult to use by the client, since the user must enter all 28 characters to the online webpage or ATM machine. The shorter the OTP message the easier it is for the user, but also the easier it is to be hacked. The proposed system gives the administrator the advantage of selecting the password's length based on his preference and security needs.

D. Client Design

A java enabled mobile phone is used to generate the OTP. The program has an *easy-to-use* GUI that is developed using the Net Beans drag and drop interface. The program can run on any J2ME-enabled mobile phone. The OTP program has the option of (1) generating the OTP locally using the mobile credentials, or (2) requesting the OTP from the server via an SMS message. The default option is the first method which is cheaper since no SMS messages are exchanged between the client and the server. However, the user has the option to select the SMS-based method. In order for the user to run the OTP program, the user must enter his username and PIN and select the OTP generation method. The username, PIN, and generated OTP are *never* stored on the mobile phone. If the user selects the connection-less method the username and PIN are used to locally generate the OTP and are discarded thereafter. The username and PIN are stored on the server's side to generate the same OTP. If the user selects the SMS-based method, the username and PIN, in addition to the mobile identification factors, are encrypted via a 256-bit symmetric key in the OTP algorithm and sent via an SMS to the server. The server decrypts the message via the same 256-bit symmetric key, extracts the identification factors, compares the factors to the ones stored in the database, generates an OTP and sends the OTP to the client's mobile phone if the factors are valid. The advantage of encrypting the SMS message is to prohibit sniffing or man-in-the-middle attacks. The 256-bit key will be extremely hard to brute-force by the hacker. Note that each user will have a pre-defined unique 256-bit symmetric key that is stored on both the server and client at registration time.

E. Database Design

A database is needed on the server side to store the client's identification information such as the first name, last name, username, pin, password, mobile IMEI number, IMSI number, unique symmetric key, and the mobile telephone number for each user. The password field will store the hash of the 10 minute password. It will not store the password itself. Should the database be compromised the hashes cannot be reversed in order to get the passwords used to generate those hashes. Hence, the OTP algorithm will not be traced.

F. Server Design

A server is implemented to generate the OTP on the organization's side. The server consists of a database as described in the following section and is connected to a GSM modem for SMS messages exchange. The server application is multithreaded.. In order to setup the database, the client must register in person at the organization. The client's mobile phone/SIM card identification factors, e.g. IMEI/IMSI, are retrieved and stored in the database, in addition to the username and PIN. The J2ME OTP generating software is installed on the mobile phone. The software is configured to connect to the server's GSM modem in case the SMS option is used. A unique symmetric key is also generated and installed on both the mobile phone and server. Both parties are ready to generate the OTP at that point.

G. System testing

The server was implemented using Java. A GSM modem was used for sending and receiving SMS messages on the server side. The smslib3.2.[7] library was used to send the messages and the MD5/SHA 4j [10]library was used to hash the password. MySQL was used as a database. The client was implemented using java enabled mobile phones. Both methods, the connection-less and SMS-based, were tested. In the first method, fake user accounts were setup on both the mobile phone and server. The mobile phone was used to generate 5000 random OTPs at various times of the day and all 5000 generated OTPs matched the OTPs generated on the server side. The use of date and time from the telecommunication company helped solve the synchronization problem. Furthermore, using the first digit of the minute gave the user enough time, i.e. 10 minutes, to compute, read, enter, and send the OTP. The second SMS-based method was also tested. Once the client requests an OTP via an SMS, the server would check the user credentials, generate the OTP, and send it back instantly. The SMS message was also encrypted using a 256-bit unique symmetric key to avoid man-in the- middle attacks. The complete process of receiving the request, checking the factors, generating and sending the OTP was done in less than a second from the server's side. This confirms the efficiency and effectiveness of the proposed system when dealing with many customers. An experiment was done to check the chances of generating two identical hashes for two different users, i.e. generating a hash collision. In this experiment, the database was filled with information for ten fake users. The generated OTP was set to be 14 characters long. The OTP can consist of upper/lower-case characters, digits, and symbols, yielding a total of 4.9E+91 different possible combinations. This is almost impossible to brute force with the existing computing facilities. For each of the ten users, 100,000 OTPs were generated and compared; a total of 1 million OTPs. All million OTPs were unique.

H. The Common Problem with Two-Factor Authentication Solutions

More websites and online businesses today are beginning to rely on mobile as a second factor of authentication. Some online banks have been using SMS-based authentication for transaction verification but recently, major websites and businesses not in regulated industries are recognizing the need for stronger online authentication.

It's great news that more websites are strengthening online authentication. When one considers how much sensitive, personal information people share on the Web, relying on a single layer of password protection simply is not enough. However, sending a one-time password or authentication code by SMS text message is also not very secure, because they are often sent in clear text. Mobile phones are easily lost and stolen and if another person has possession of the user's phone, they could read the text message and fraudulently authenticate. SMS text messages can also be intercepted and forwarded to another phone number, allowing a cybercriminal to receive the authentication code.

I. Countermeasure

With more businesses relying on mobile phones for out-of-band authentication, cybercriminals will increasingly target this channel for attack meaning that businesses should use a more secure approach than simple SMS text message. However, the challenge for consumer-facing websites is to balance strong security with usability. Complicated security schemes will not achieve widespread adoption among Internet users. A more secure and easy to use approach is to use User Personal Identification Factor (UPIF) on the user's mobile phone to create a one-time password (OTP).Along with OTP generation and user verification is done very efficiently.. Here's one example of how it can be done: During the user's first-time registration or enrollment with the website they choose a few categories of things they can easily remember - such as cars, food, flower, hobbies.etc

Whenever authentication is needed, trigger an application to display a randomly-generated UPIF on Screen. The user authenticates by tapping the UPIF that fit their secret, pre-chosen categories along with OTP. In this way, the authentication challenge forms a unique UPIF that is different every time for each OTP. Yet, the user only needs to remember their categories (in this case cars, food and flowers).This type of knowledge-based authentication challenge to the user an jus a SMS message with the code displayed in clear text is more secure because the interaction takes place entirely out-of-band of the mobile channel .Because the mobile application communicates directly with the business' server to verify that the user authenticated correctly, it is much more secure than having the user receive a code on their phone but then type it into the web page to authenticate. Additionally, even if another person has possession of the user's phone, they would not be able to correctly authenticate because they do not know the user's secret categories. This secure two-factor authentication will help to mitigate more sophisticated malicious attacks such as man-in-the-browser (MITB) and man-in-the-middle (MITM).

V. EVALUATION

This section provides an evaluation of the different authentication solutions [6] using the mobile phone as authentication token. The evaluation is performed according to the following criteria:

- Strength & vulnerability
- Cost
- User friendliness.

The different authentication solutions can be subject to attacks in several areas, depending on the specific scheme:

1. On the mobile phone
2. Across the Bluetooth connection
3. On the computer
4. Across the Internet connection
5. Across the connection between service provider and authentication server
6. On and between GSM network components and connections.

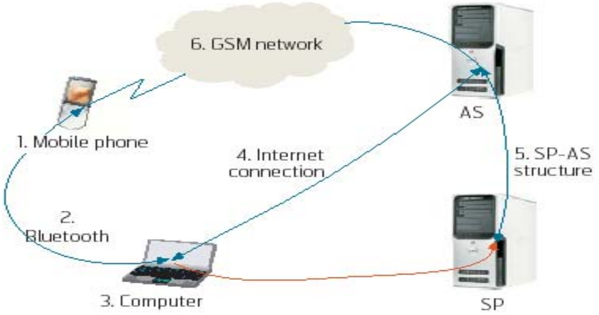

Figure 4. Possible points of attacks

The above figure illustrates the possible points of attacks in the architecture.

A. *Comparison of authentication solutions*

An attacker's possibilities :

There are many different attacks[8] a person could choose to use in order to access information that does not belong to said person. Below are descriptions of few types of attacks .We have chosen these attacks since they are quite common and paint an easy-to-understand image of attacks that threat web authentication.

- *Eavesdropping*

This method is known as a passive method, and means that the attacker simply listens to the traffic and tries to pick up useful information [9]

- *Man-in-the-Middle (MitM***)**

In this method, the attacker goes for the authentication protocol and positions himself between the communicating parties and can therefore read and/or alter all information travelling between the parties

- *Phishing*

This method is basically just asking for the password, in one or more ingenuous way. For example by posing to be a support centre, redirecting the user to an identical page and capture the password when the user tries to log on.

- *Dictionary attack or online guessing attack*

This is a guessing attack where the attacker most commonly has a list of strings, which are words or just probable letter combinations, and do trial and error guesses based on that list.

- *Spoofing attack*

This is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

- *Replay attack*

This is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

- *Sniffing attack*

This means that the attacker is able to view network traffic and will try to steal credentials, confidential information, or other sensitive data. The above Table illustrates some of the security properties of the major categories of authentication solutions discussed in this paper. It shows what type of attacks the different solutions can be susceptible to

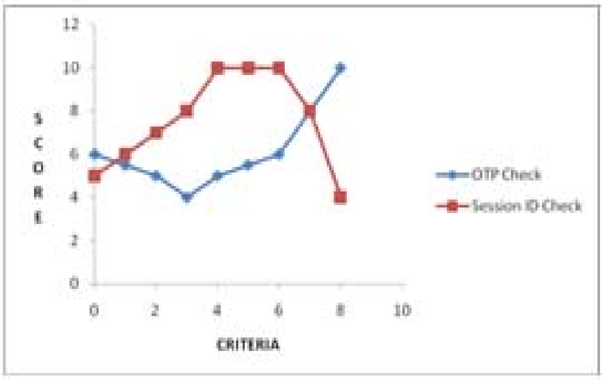

Figure 5. Comparison of the different authentication solutions based on the mobile phone

Table I shows a comparison of the different authentication solutions with respect to four parameters; security, cost, infrastructure and user-friendliness. The comparison is informal and only meant to provide some insight into the properties of the various solutions relating to each other. As with all such solutions, the actual implementations might have other properties than illustrated here.

VI. CONCLUSION

This paper has suggested several ways to employ the mobile phone as an authentication token, with the purpose of addressing shortcomings of existing authentication solutions on the internet today. It even provides a design implementation for one of the authentication scheme. Using the mobile phone as an authentication token provides very flexible and secure solution. It is therefore a very good alternative to the existing authentication solutions such as directly accessible usernames and passwords. The proposed solution can also be an alternative to existing OTP solutions which require extra hardware and therefore put an extra burden on the user and also impose cost on service providers. The paper also offers a thorough security evaluation which discusses the threat model and security properties of the proposed solutions. The paper also informally illustrates a comparison between the solutions with respect to important criteria. As a further work this implementation with User Personal Identification Factor [UPIF] and user trials at the user end can strengthen the security levels in more robust manner.

Table I. Comparative study of OTP and Session Mechanism

Security requirement	OTP Solutions	Session ID
Online Guessing	✓	✓
Phishing	✓	
Eavesdropping	✓	✓
Shared secrets not revealed	✓	
Man-in-the-middle	✓	
Session hijacking	✓	
Replay	✓	
Spoofing	✓	
Sniffing	✓	
Brute Force attack	✓	

REFERENCES

[I] Fermi National Accelerator Laboratory, Office of Science / U.S Department of Energy: Strong Authentication at Fermilab, Sept 2006

[2] National Institute of Standards and Technology (NIST) U.S.Department of Commerce: Electronic Authentication Guideline -Information Security, Special Publication 800-63-1, December 8, 2008.

[3] W. E. Burr, D. F. Dodson, W. T. Polk. ElectronicAuthentication Guideline. Technical Report 800-63, National Institute of Standards and Technology,2008.<http://csrc.nist.gov/publications/ nistpubs/800-63/SP800-63V1_0_2.pdf>.

[4] CA.Managing strong Authentication: A Guide to Creating an Effective Management System, 2007.

[5 Fadi Aloul, Syed Zahidi and Wassim El-Hajj "Two factor authentication using mobile phones" in Pro 2009 IEEE/ACS International Conference on Computer Systems and Applications, ISBN: 978-1-4244-3807-5.

[6] Do van Thanh; Jorstad, I Jonvik, T, Do van Thuan "Strong authentication with mobile phone as security token" in Pro Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on.

[7] SMSLib. Available at http://smslib.org/

[8] Pernilla Stolpe Johansson "Economic aspects of web authentication" in Project Report for Information Security Course Linköping University, Sweden. In 2011.

[9] Steffen Hallsteinsen,Ivar Jorstad, and Do Van Thanh "Using the mobile phone as a security token for unified authentication" in Pro Second International Conference on Systems and Networks Communications (ICSNC 2007).

[10] Sha4J.Available at http://www.softabar.com/home/content/ view/ 46/ 68/

Professor T.Venkat Narayana Rao, received B.E in Computer Technology and Engineering from Nagpur University, Nagpur, India, M.B.A (Systems), holds a M.Tech in Computer Science from Jawaharlal Nehru Technological University, Hyderabad, A.P., India and a Research Scholar in JNTU. He has 20 years of vast experience in Computer Science and Engineering areas pertaining to academics and industry related I.T issues. He is presently Professor and Head, Department of Computer Science and Engineering, Hyderabad Institute of Technology and Management [HITAM], JNTUH, Gowdavally, R.R.Dist., A.P, INDIA. He is nominated as an Editor and Reviewer to 25 International journals relating to Computer Science and Information Technology. He is currently working on research areas which include Digital Image Processing, Digital Watermarking, Data Mining, Network Security and other Emerging areas of Information Technology.

Vedavathi.K, pursuing M.Tech Final Semester , Department of Computer Science and Engineering, Hyderabad Institute of Technology and Management [HITAM], JNTUH, Gowdavally, R.R.Dist., A.P, INDIA.