



L OVELY
P ROFESSIONAL
U NIVERSITY

**Enhanced two-step authentication scheme using TLS for secure seed exchange
In
TLS (Transport Layer security)**

A Dissertation-II
Submitted

By Sandeep Singh

To

Department of Computer Science and Engg.
In partial fulfilment of the Requirement for the
Award of the Degree of
Master of Technology in Computer Science

Under the guidance of

Mr. Ravishanker
May 2015



School of SCE

DISSERTATION TOPIC APPROVAL PERFORMANCE

Name of the Student: Sandeep Singh Registration No.: 11100772
Date: 2011 Roll No.: R-02
Session: 2014-2015 Parent Section: K2006
Name of Supervisor: Ravishanker Designation: Asst. prof
UID: 12412 Qualification: M. Tech
Research Experience: 06

SPECIALIZATION AREA: _____ (pick from list of provided specialization areas by DAA)

- DISSERTATION TOPICS
1. Transport Layer Security Protocol
 2. Distributed Denial of Services Attacks
 3. Virtual Private Network

Ravishanker
Signature of Supervisor

PAC Remarks:

11/01/11
Signature: _____ Date: _____

APPROVAL OF PAC CHAIRPERSON:

- *Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)
- *Original copy of this form after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report
- *One copy to be submitted to Supervisor.

CERTIFICATE

This is to certify that Sandeep Singh has completed M.Tech dissertation titled Enhanced two-step authentication scheme using TLS for secure seed exchange under my guidance and supervision. To the best of my knowledge, the present work is the result of his original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and partial fulfilment of the conditions for the award of M.Tech Computer science & Engg.

Date: _____

Signature of Advisor

Name:

UID:

ABSTRACT

In this dissertation, an enhanced two factor authentication scheme has been proposed that will use a secured TLS connection for exchanging the seed between server and client application. The proposed system uses a mobile application that will generate time based one-time passwords (TOTP) for two factor authentication. The system will be capable of working offline except from the registration phase. The system uses an encrypted keystore which will generate OTPs by using a securely exchanged secret seed. App will be password protected to avoid unauthorized access. Our system eliminates the dependency on network which was a major disadvantage of SMS based OTP authentication schemes. The proposed system is easy to deploy on any type of web platform and mobile application can be developed for almost all operating systems available.

ACKNOWLEDGEMENT

It is true that people and institutions do help in research projects, it has been more so in my case. The words cannot really convey my gratitude to Mr. Ravishanker whose able guidance and invaluable suggestions has inspired me to work on this research. His scholarly wisdom has instigated us to go into fine details of every aspect of this research.

I will be failing in my duty if I do not express my gratitude to Mr. Ravishanker whose precious suggestions and timely help has enabled me to complete this research proposal in time.

Last but not the least; I owe my gratitude to parents, who have always inspired us during this course of the research.

Date: May 9, 2015

DECLARATION

I hereby declare that the dissertation proposal entitled, Enhanced two-step authentication scheme using TLS for secure seed exchange submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date: May 9, 2015

CONTENTS

Chapter No.	Description	Page No.
1	Introduction	1-8
1.1	Multi-factor Authentication	2
1.2	SSL/TLS Protocol	2-6
1.3	Usernames and passwords	6-7
1.4	One Time password	7
1.5	HOTP and TOTP	7-8
2	Terminology	9-10
3	Review of Literature	11-23
4	Rationale & Scope of Study	24
5	Objective of Study	25-26
6	Research Methodology	27-32
6.1	Registration phase	28-30
6.2	Login and OTP Generation	30-31
6.3	Comparative analysis	31-32
6.4	Tools and equipment's	32
7	Results & Discussions	33-41
7.1	Experimental Works	33-39
7.2	Data Analysis & Interpretation	40
7.3	Performance Evaluation	41
8	Conclusion & Future Scope	42-43
9	References	44-45
10	Appendix	46

FIGURES

Figure No.	Description	Page No.
1	A typical multi factor authentication system using SMS OTP	2
2	TLS Handshake.	3
3	Protocol Nesting	4
4	ICICI Bank's SSL	5
5	Certificate Details	6
6	Renegotiation in TLS	22
7	MITM Attacks on TLS	23
8	Two Step Authentication Illustration	27
9	Flowchart of Proposed system	28
10	TOTP Enrollment	30
11	Signup Form	34
12	Login Form	34
13	2 Step Verification	35
14	Homepage	36
15	Setting Page	36
16	Splash Screen	37
17	Login Screen	38
18	Application Password	38
19	OTP Screen	39
20	Performance Evaluations	41

TABLES

Table No.	Description	Page No.
1	Experimental Results	40

Chapter 1

INTRODUCTION

With the advancement in network technologies everything is going online. From business to government are available online. The data related with business and government organisations is very confidential. So it is highly important to protect the data from unauthorized access. In order to achieve this objective most of the clients and servers use cryptographic techniques so that the data can be encrypted and can be accessed by only authorized people. However, still the online data will not be safe if people do not use a strong password to protect their online accounts. Users often use passwords which are weak and easy to guess. Accounts with such passwords are easy to target because password guessing hardware are getting more advanced. So, only a username and password is not sufficient to protect online accounts. There is a need of more advanced authentication technique.

According to a research by Javelin Strategy and Research, annual number of victims of identity fraud only in US is approximately 12,157,400. The report states that a financial loss of \$13,200,000,000 is happened due to identity fraud in year 2010. According to the report 64% of the victims reported misuse of credit cards and 35% victims reported misuse of existing bank account details [1]. About 6.4 % of the Google account users were reported to be using two-step authentication service [2].

One of the reliable solutions for multi-factor authentication is the use of mobile devices. A SMS (Short Message Service) based two-step authentication system is proposed in [3]. The new generation smartphones are one of the most reliable alternatives for multi-factor authentication. The mobile devices are widely used for security purposes and are quite successful. A location based OTP (One-Time Password) is proposed in [4, 5] which are quite successful in avoiding many attacks. The author of [6] has proposed a two-step authentication system that tries to eliminate vulnerabilities in existing system. A system based on biometrics and graphical passwords has been proposed in [7] and [8] respectively.

1.1 Multi-factor Authentication:

Multi-factor authentication is very successful in providing high security to the online user accounts. In such type of authentication systems instead of asking just username and password, additional information is also asked from the user. These systems can ask for more than 2 identifications of the user. This information can be an OTP which will be sent by the server to the registered mobile of user or there can be some security questions. Also biometric identifications like fingerprints and iris scan can be a part of this authentication scheme. This process makes it very difficult for the attacker to gain the access to online account even if attacker knows username and password of the user. The two step authentication includes password and one more additional password or user ID.

According to a study on 100000 Google accounts only 6.4% of the users are using two-step authentication systems [2].



Figure 1: A typical multi factor authentication system using SMS OTP

1.2 SSL/TLS Protocol

1.2.1 Introduction

SSL/TLS are the cryptographic protocols widely used for providing communication security over the internet. SSL is a standard security technology that establishes a secure and encrypted link between client and server. SSL certificates are provided by Certificate Authority. However SSL protocol in android and web is vulnerable to attacks like Man in Middle Attack (MITM) where the attacker is between the server and client [10]. OpenSSL is the open source versions of SSL and TLS (Transport Layer Security). OpenSSL is also vulnerable to a serious bug named as Heartbleed bug [19, 20]. This bug

allows the attacker to steal the confidential information of the users which is protected by the SSL/TLS. Although Heartbleed bug has been fixed as fixed OpenSSL has been released and it has to be deployed.

SSL/TLS provides multiple configurable security goals, such as:

- Authentication
- Confidentiality
- Integrity
- Non-repudiation
- Replay protection

1.2.2 SSL/TLS Structure

SSL/TLS are multilayered protocols. These protocol suits have two phases for operation

- Negotiation (handshake) phase
- Application phase

The negotiation phase is very crucial phase in terms of security of the protocol. In this phase the secure connection between two parties is established using handshake protocol. This phase is having complex operations and ensures the security of the data. The application phase includes the actual communications and transfer of data. The working of the SSL/TLS is explained in next sections.

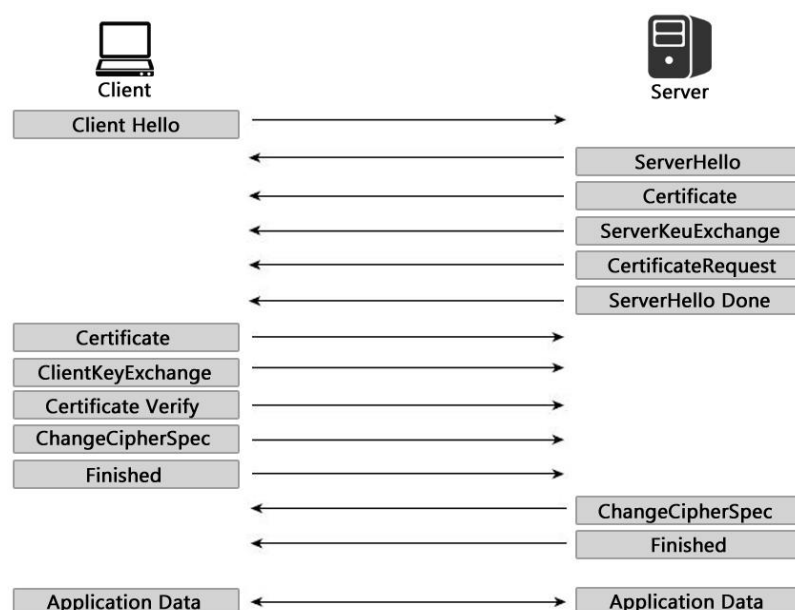


Figure 2: TLS 1.0 Handshake – based on Source: RFC 2246 [9]

The SSL works on the application and transport layers. A secured connection is established between connecting parties with a handshake between them. The client sends “ClientHello” message and ciphersuites to the server. The server responds “ServerHello” and chooses the strongest cipher suit. This cipher suit must be supported by both parties. The server authenticates itself by sending a certificate to the client. The client authenticates the server’s certificate and generate pre-master key which is a random number generated by the client. Using the server’s public key client encrypts the pre-master. Pre-master is decrypted by the server using its private key. The session key is generated by using the pre-master. The server sends a message called ChangeCipherSuit to the server which indicates that all data will be exchanged in encrypted form. After this final step a secured channel is established between connecting parties [12].

1.2.3 Modular Design

TLS protocol has a modular architecture and the design of the protocol is in a layered fashion. There are sub-protocols in the record protocol of the TLS. The protocol supports a wide variety of cryptographic algorithms. The record protocol has following protocols.

Record Protocol

- Handshake Protocol
- Alert Protocol
- ChangeCipherSpec Protocol
- Application Data Protocol

Basically the fundamental functionality of the record layer is communication so it is a communication layer. This layer works on stream of bytes. After accepting byte stream record layer splits them into blocks. These blocks are forwarded to TCP layer [21].

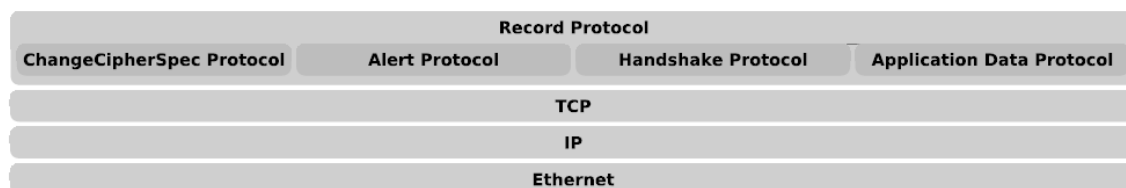


Figure 3: Protocol Nesting

1.2.4 Trust

The user's trust on any website is very important. User trust the websites which have deployed SSL with adequate cryptography and having certificate issued and signed by good Certifying Authority (CA). CA verifies the identity of the websites and signs a certificate only for verified websites. The certificates that are being used are digitally signed. The concept is called PKI (Public Key Infrastructure). User can easily check the trustworthiness of any website from the browser. The trusted websites run on secure HTTP protocol which is displayed as HTTPS in the URL of the website.

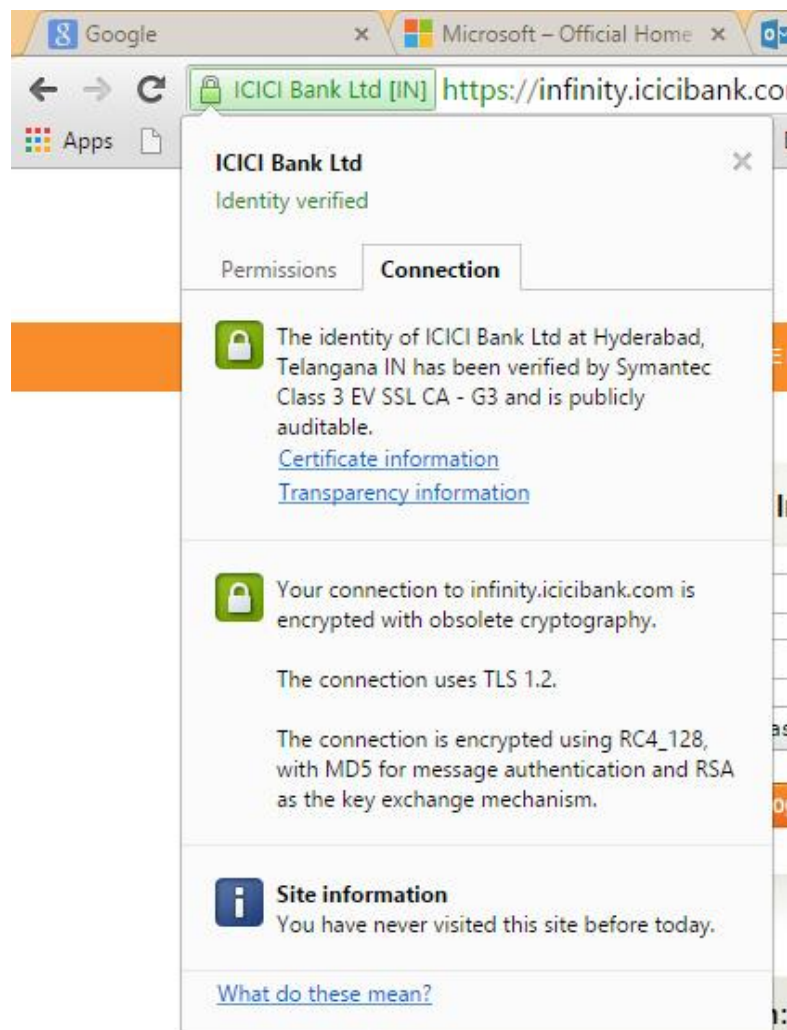


Figure 4: Displaying ICICI Bank's SSL details

Very known banking website ICICBank.com is using TLS 1.2 (Latest Stable) version of SSL protocol. We can check the details of the SSL from the browser. The identity of the website is verified by Symantec Class 3 EV SSL CA – G3 which is one of the most trusted CA available at present.

We can also get details of the certificate by clicking on the certificate information. New popup window will display all of the details of the certificate. Basically the following information is displayed in general detail tab

- Purpose of issuing
- Issued to (to which particular domain of website certificate is issued)
- Issued by (the certifying authority information)
- Valid from (Certificate's validity information)

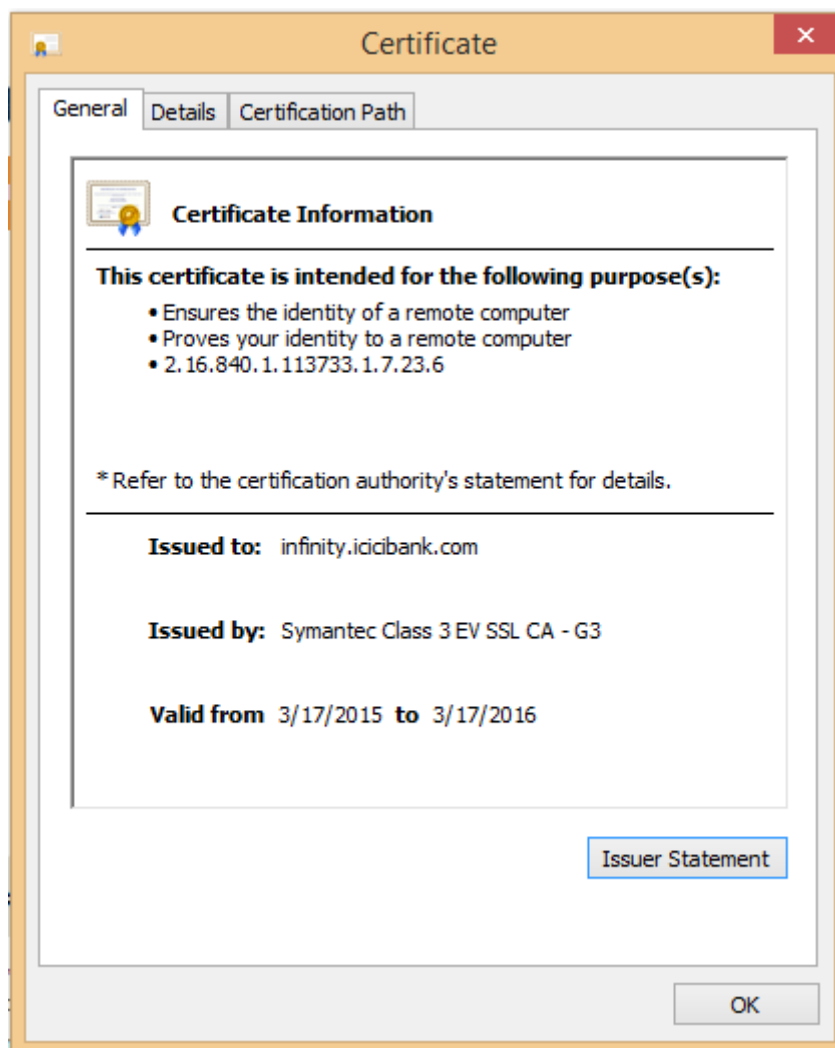


Figure 5: ICICI Bank's certificate information

1.3 Usernames and Passwords:

Usernames and passwords are the most common and most trusted authentication technique used for almost all of the websites. Username may be an email, unique

alphanumeric value, or even a mobile number. Username identify the user who is attempting to access the account. The password authenticates the user and ensure only legitimate user is accessing the account. For better security it is highly important to store the cryptographic hash of the password instead of storing it as plain text. This practice ensures that even if the database is leaked out but the attacker will not able to access the account. The only way to attack will through brute-force.

But the issue with the passwords is that users often use weak and guessable passwords that end up being compromised. Also the password cracking hardware is getting more powerful which makes it easy to crack weak passwords in less time. Weak passwords leads to weak hashes and will result to crack the password in comparatively less time. Users often do not feel comfortable in using long and strong passwords as the feel difficult to memorize the long and strong passwords.

1.4 One Time Password:

It is usually a 4-6 digit numeric value which is generated by the device for every session or transaction. For each session a new code is generated by the system. The user must use this code to authenticate him to successfully login into the system. Most of the OTP algorithms include a secret seed and a counter. The OTP is generated using these two parameters.

$$\text{Password} = \text{OTP} (\text{secret seed}, \text{counter})$$

Every time the system will generate a different OTP because every time the counter is incremented and lead to change in the password even the seed always remains the same. These passwords cannot be used more than once. If an attacker gets the password once it has been used then it will of no use to him. Therefor these passwords are considered secure.

1.5 HOTP and TOTP:

HMAC-based One-Time password [10] and Time-based One-time passwords [11] are most commonly used implementations for generating one time passwords. Most of the time these algorithms outputs a 6 digit numeric value which is treated as one time password. From these two types of the algorithms the Time based one-time passwords is considered as more secure. There are a number of ways to use these algorithms to

generate one time passwords. Following are most common examples:

- **SMS OTP:** The most common method of implementing TOTP is the SMS OTP. When a user attempt to login the system using correct credentials then the server generate and send OTP via registered cellular number of the user as a text message. The user uses that OTP to login the system successfully.
- **Google Authenticator:** Google has tried to eliminate the dependency of the multi-factor authentication system on the cellular network. Google developed an application called Google Authenticator that generates the passwords in offline mode. The offline keystore is generated by using pre-shared secret which is shared during the account registration. The server and the client app will generate same code at any given time so that server can verify the password entered by the user.

The TOTP algorithm: In the proposed system we have used TOTP as a base algorithm to generate required one time passwords. Basically TOTP is based on HTOP but there is a difference between them that is the HTOP is counter based but TOTP is a time based algorithm. TOTP will generate a new value after a defined time. This time is called time step. TOTP supports HMAC-SHA1 and HMAC-SHA2 hash functions. For the implementation the algorithm requires the following important prerequisite.

1. Devices (on which TOTP will be implemented) must able to derive UT (Unix Time). The devices include the token device (e.g. smartphone or personal device) and server which will validate the code generated in token.
2. Both devices must have same seed (shared secret). Also it must be unique.
3. The time-step value is required to be same on both devices.
4. It is mandatory that keys must be generated randomly and using a key derivation algorithm.

Chapter 2

TERMINOLOGY

Authentication: Authentication is confirming the genuinely of an entity. The entity in our case is basically the user who wants to access a website or web service.

Encryption: Encryption is the technique which encodes a message in a way that nobody other than authenticated person can understand it. The message is called plaintext and the encrypted data is called ciphertext. Basically there are two categories of encryption techniques; Symmetric key cryptography and Public key cryptography.

Cipher: Cipher is algorithm used for encrypting and decrypting of data.

GPS: Global Positioning System is navigation system based on satellite. The system provides location services to military, maps and other critical applications.

GSM: Global System for Mobile communication is cellular technology used world widely to operate cellular communication.

IMEI: International Mobile Equipment Identity is a unique number used to identify mobile devices and satellite phones.

MITM: Man In the Middle attack is an attack where the attacker intercepts the conversation of two communicating parties. The attacker can modify the messages coming from one party and send it to the other party on behalf of the first one.

OTP: One time password is usually 4-6 digits or alphanumeric string which is generated using OTP algorithm, valid for one time only and used for multi factor authentication systems.

PKI: In Public Key Infrastructure the identity of the communicating parties are verified by certifying authorities and facilitate users to communicate securely over an unsecure public network

QR Code: Quick Response Code is a two dimensional machine readable code invented in japan. QR code can contain information which can be a numerical value, text, alphanumeric or any characters.

SMS: Short Message Service is a type of communication service which allows text messages of fixed length to send on other mobile device via a cellular network. The service provider may charge for the SMS.

UNIX Time: UNIX time is the number of seconds passed since UTC (Coordinated Universal Time), 1 Jan 1970. UNIX time is a numerical (integer) value which is incremented every second. Therefore the benefit of using UNIX time is that there is not any need to perform calculations on days, months and minutes. Many of the UNIX like operating systems uses UNIX time.

Time Step: Time step in TOTP algorithm is the time duration after which the one time

password will be changed. The default value of time step is 30 seconds. It can be changed according to requirements.

REVIEW OF LITERATURE

Suresh V. Limkar, Rajesh Kumar Jha, Shilpa Pimpalkar, and Santosh Darade proposed a Geo-Encryption based SSL VPN, which is secured with a graphical position based encryption technique. This technique enhances the security of mainstream SSL VPN. This technique enhances security by granting access to confidential information and applications to execute from only a trusted and pre-determined location.

The proposed system uses location parameters obtained by a GPS. The system includes two phases; one is registration phase and other is operation phase. The remote client will be identified by a unique ID which will be allotted during the registration phase. During the SSL handshake phase the location parameters of the client will be compared with the saved trusted location parameters at the server. If the client is in a trusted location then the negotiation will occur successfully and the SSL tunnel will be created. This tunnel will connect the remote user and SSL VPN.

The author's vision is to extend this system into other applications which are crucial in terms of security. For example; Location based access control of Employees, operating critical activities from only a trusted location etc. The most obvious advantage of the proposed system is that it uses the location based encryption for providing a better security. But it can be a hard task to implement such system in real time applications. The GPS location is required to be much precise to implement such system in real time application. The other thing that can be done is to make tolerance up to a certain value to avoid errors. The other disadvantage of the system may be requirement of GPS on every device that is willing to connect to the server. Although GPS is a very common module in every mobile device but for the desktop computers and some of the other device does not contain a GPS module. So there will be problems with those devices to connect to the server [12].

Wen-Bin Hsieh, Jenq-Shiou Le proposed a two-step authentication system which is based on the location and login time of mobile which is used as token. A GPS system is must have module in any modern smartphone. The proposed system takes the benefits of the precise location parameters obtained by GPS (Global System for Mobile). The

location and login time both used to enhance the security of the one-time password (OTP's).

The author assumes the clients are registered on server already registered and organised under a PKI (Public Key Infrastructure) system. The other assumption is that the client mobile and server must have synchronised clock .The complete authentication process has two phases. In phase 1 the core authentication scheme is used which is based on the location and time. The phase 2 is used as the supplementary phase or backup phase which will be used in a case where the core authentication fails due to any reason. The server can calculate the velocity of the device by using the following formula:

$$V = \sqrt{\left(\frac{X1-X0}{T1-T0}\right)^2 + \left(\frac{Y1-Y0}{T1-T0}\right)^2}$$

Where V is the velocity of the device X0, Y0 are location coordinates at time T0 and X1, Y1 are location coordinates at time T1.

The author also included the tolerance range in case the device is not at the exact location or location may vary due to GPS limitations. The author stated that the proposed system was protected from many attacks like eaves dropping attack, dictionary attack and lastly MITM [4].

Daesung Lee, Hyun Sook Jang and Ki Chgang Kim have focused on the impact of SSL on the performance of wireless handheld devices such as PDA's. The protocol has a heavy burden on these devices. It takes pretty much time to establish a secure connection while between server and client when a certificate uses PKI (Public Key Infrastructure).

The proposed system includes a lightweight version of SSL which is designed to reduce the client computational load. The client does not need to generate and encrypt the pre_master and it is not required to calculate the master secret. These operations are held by the server itself. Therefore the client which is a lower powerful machine has reduced computational operations and speedup the connection process. Also the mechanism of session reuse helps to reduce the connection establishment time by reusing the previous legitimate sessions. The session reuse makes it easy to reconnect to the server or device to which the device has been connected earlier. The session ID of the communicating parties will be stored and during the reconnect the server will use existing session ID in

ServerHello Message. The client will verify if there is same ID and will connect if it exists.

Author has analysed the proposed protocol against various attacks for security. The original SSL protocol is vulnerable to a number of attacks. In original SSL protocol it is not mandatory to verify the server certificate. But the Light SSL requires verifying the certificate of all communicating parties. Therefore the risk of masquerade attacks becomes very less in case of Light SSL. Verifying server certificate also reduce the risk of man in the middle attacks.

In proposed protocol Pre-master secret is generated on the server side only. The client will not generate any pre-master secret. So there will not any ClientKeyExchange in server and client. This will protect the system from Bichenbacher's selective encrypted text attack.

The performance of the proposed system has been analysed on a computer and a PDA device. The computer which will act as server has Intel Celeron CPU, Ubuntu Operating System and 1 GB of RAM. The PDA device is Sharp Zaurus model SL-C1000. The PDA device is loaded with 64MB RAM and have PXA270 CPU. The experimental results show the improvements in the performance of SSL. The results have been provided against the default SSL protocol. Light SSL connects to sever 45 times faster as shown in the experimental results [13].

Darko Kirovski and Christopher A. Meek have proposed an authentication system which uses tunneled TLS and a trusted personal device. The system was proposed to protect the secrets and passwords from being leaked when user log on to a remote server. The system user trusted personal device to log on to the remote server. There will be a TLS connection between server and terminals browser. The server will check the credentials sent from the terminal browser and allow access to the server if the credentials are correct. The credentials are always protected against attack because of TLS connection secures the data by encrypting before sending it to the other party. The proposed system protects against many attacks like key-loggers, XSS, phishing and many others. The author as assumed a scenario of payment using a credit card. According to the research the major identity theft attacks are phishing and key-loggers. Most of the security tools work by detecting these malicious tools and take appropriate action. But most of the tools for protection available are malware itself. Therefore the trust between

user and service provider servers is collapsing. So, multifactor authentication provides a better security in that case. The author has following 3 crucial objectives.

A: secure login is the first objective which means that the credentials entered from the personal device to distributed terminal via TLS connection. The distributed terminal will never see the plain text of credentials.

B: Second objective is to protect the system from attacks like Cross Site Scripting (XSS).

C: secure logoff is also important objective of the proposed system.

There are 3 components of the proposed system; server which is responsible for managing the user accounts, a personal device which is trusted by the client (usually a mobile device) and finally a terminal machine which is being used by the client and is not trusted [17].

Usman Alhaji Abdurrahman, Mustafa Kaiidli, Jawad Muhammad proposed a graphical location based two-factor authentication technique. The system uses the GPS location of the mobile device and pre-shared key to generate a secret hash. The author named proposed technique pre-shared GPS location and Time stamp (PGT). Author has compared the proposed technique with various other techniques e.g. SecureID. This method is more secure than the secureID because it uses the graphical location as extra security parameter for the authentication. Also PGT use a modifiable pre-shared secret code.

PGT use IMEI or IMSI numbers of the mobile device as seed. The seed is required for generating the OTP by the algorithm. IMEI number of every device is unique so seed is considered to be unique and OTPs generated are random in nature.

For the implement of the PGT a mobile device having GPS capability is used as a token. The token is used as a third factor for the authentication and generates OTPs required. The complete process is performed in 3 stages.

Stage 1 is the normal authentication stage of any web service where the user attempts to login into the server. After providing the registered credentials the stage 2 starts. in stage 2 the token T1 is generated. User need to install PGT app into the mobile device. Also the GPS must be kept on in order to perform PGT technique. The app will generate T1 which is called the security token. Stage 3 includes the verification of the security token

T1. The PGT app will send the security token to the server along with the current GPS location and time stamp. The server will generate security token T2 using the same equation which is used to generate T1. The verification of the security token is performed by comparing T1 and T2. These need to match in order to authenticate the user for accessing the web page or web account.

The author has provided 5 different scenarios for security analysis of the proposed system. In first case if the attacker is having the user credentials then he cannot log in to the web account. Because he need to enter the OTP generated by the PGT app which is only accessible to the registered user.

In case 2 if the attacker also able to capture the communication between the app and the server then read the security token, even then these token are useful for an fixed time interval. These will be expired and will be of no use.

In the case 3 if the attacker also gets the username and password of the user and also finds the registered mobile device for that account then the attacker will be unable to use the device because the PGT app is secured with the PIN.

The proposed system is secure because of many security parameter are being used in the system. But if the attacker is able to spoof the IMEI of the mobile device then the attacker can hack the system and generate the same OTPs which are being generated by the authenticated application [5].

Dimitri DeFigueiredo has discussed about why two step authentication systems can extremely helpful in securing web accounts. His research proves why mobile devices when used as two factor authentication can increase security for our web accounts. Although author has figured out some security problems when using mobile devices e.g. mobile devices are more likely to loss or stolen. Also attacks like phishing are more common when mobile devices are used as compare to desktop computers.

Author has explained why mobile devices are most useful and convenient tools for using in two step authentication systems. Because mobiles are one of the most personal devices of any user so, these devices can be easily accessed by the owner. Also in case the mobile device has been lost or stolen then the user can easily notice this and can take appropriate action. Authentication includes the factors like source of the message, recipient of the

message and why the message was sent. These all factors must be clear while communicating to any second party.

In the discussion about what kind of ID proofs user can use as an added security parameter for multifactor authentication, the explained following there kind of proofs:

- Something that you have
- Something that you know
- Something that you are

The first point is about what you have to show your identity. For example while entering your house you have key to unlock the door. Your key is the identity that lets you to open the door or we can say that you got authenticated. If you have not any physical key then you may need to enter some password or pin. This is something that you know. Your password is not any physical thing; you just remember your password. The third point usually related to the biometric identity of the user like fingerprints, iris scan, voice and face identification systems.

The mobile authentications basically fall in second category that is; something that you have. You can enter one time password or pin that is sent from the authentication server to your mobile. If the username and password of the user are compromised even then it will be hard to access the web account without the OTP. Because, the OTP will be send to the mobile device. Secondly if the mobile device is stolen even then the attacker needs to know the credentials of the users. Users can secure their phone with PIN so that no unauthenticated user can access the mobile device.

The author has recommended using two step authentications when using banking and online transactions. If the banking website is providing this facility then user must use that service [2].

Qiong Pu proposed a smart card and password based two-step authentication system. He extended the research by Yang [18] and resolves the vulnerabilities of the system proposed by Yang. They have suggested techniques to be added to be added in Yang's proposal to remove the vulnerabilities. Using only password based authentication is not very secure because most of the people are using weak and guessable passwords for their accounts. Therefore attacks like dictionary attack and phishing attacks are very easy to perform on such kind of accounts. Multi factor authentication system like smartcard

based authentication systems reduces the risk of such attack to a very large extent. According to the system proposed by the Yang smartcard based 2FA technique must have following properties.

- Server must be sure that the user attempting to login to system is authenticated. The client must be registered on the server previously.
- The client must ensure that the web server he/she is trying to login is authenticated. He must be sure that it is not any phishing website.
- It is mandatory that the server has no information of the password of the registered client. The passwords stored must be encrypted.
- Client must be free to change the password anytime he wants. The server must provide interface to change the password for the client
- The server must provide guidelines to set a strong password

Author proposed a system that meets all of these requirements. The proposed system has two phases as in almost all of the two step authentication systems. The registration phase server S will register the client on the server and issue a smart card to the client A. The client will change the password after receiving the smartcard. In the login phase the smart card will be used as an extra factor for the authentication purpose.

Author has attempted to reduce the risk and improve the security of the protocol proposed by Yang. In the proposed protocol only client will be aware of the long term secret. Server will not know the long term key but only the verifier of the key. The benefit of such will reduce the risk of the brute force. The system overcomes the weakness in the Yang's protocol and fulfills the security requirements as described by the Yang. The author is working on the last requirements [6].

Sonali Patil, Komal Bhagat, Susmita Bhosale, Madhura Deshmukh proposed a two-step authentication system based on biometric identity. In the proposed system they have used iris and fingerprints combined for more accurate and reliable authentication results. They stated that biometric are the safest ID proof of any user and can be used for authentication in many applications. A number of authentication systems have been proposed in past years but authors came up with an idea of using iris and fingerprints combined for the two step authentication system. Most of the systems which are using multiple factors are use of biometric and passwords. So basically they are using 2 factors. The proposed system uses 3 factors that is password along with iris and fingerprints.

The implementation includes two modules; one is Enrolment and the other is Authentication. In the enrolment module of the system the eligible users will be registered on the system using their biometric identity. They have to provide their biometric identity to the authentication system. The system admin receives these biometric id proofs that are the fingerprint image and the iris scan image. The system will then process these images and extract the required features of the biometric IDs. The collected information will be saved in the database. The author as provided no proof if this information will be saved as encrypted form or not. The system will use visual cryptography to create the random shares for the images that are enrolled. The two shares will be generated and the user has to use both of the shares for the authentication. There will be no use of any single share.

The next module is the authentication module which will be performed by providing the shares. The system will check the provided images and shares from the database. After verifying the correct share the user will be authenticated to use the system.

Author has implemented the system in MATLAB and used SSIM (Structural Similarity Index Metric) for checking if the images are similar. The provided results prove that the system will produce very less false positive results. But the major issue with the proposed system is to implement in real scenario. The biometric devices are very expensive till date and cannot easily available for each user [7].

S. Indu, T.N. Sathya, Saravana Kumar proposes a 2 Factor Authentication system based on SMS. Author stated that biometric parameters can act as extremely secure tokens but due to high hardware cost these cannot be used everywhere. The author proposed system that uses the mobile based software token. The objective of the system is to replace hardware based software tokens. The system consisting 3 modules: Server Software, Clients mobile software and a GSM modem or any other modem for network connectivity. The proposed system has two modes of operations. One is connectionless approach and other is SMS Based Authentication.

In the connectionless approach the one time password will be generated by the software installed in the client's mobile phone. This password will be generated by without establishing any connection with the server. The client is supposed to use this password for authentication purpose.

The author proposed a scheme in which SMS based authentication will be used as a backup technique for authentication. In the cases where the connectionless approach fails

to perform then SMS based approach will be used. The connectionless approach may fail due to several reasons such as rejection of passwords, Client and servers clock are not synced etc.

The OTP will be sent as an SMS to the client's mobile phone. This OTP will be based OTP algorithm. The SMS password is encrypted with symmetric key encryption using 256 bit key. This will avoid MITM (Man in the middle attack) in the attack. The OTP is alphanumeric and total 4.9×10^{91} unique combinations are possible.

This system of authentication required to maintain a database to handle the information about the identities of the client. This information includes name, username, password and some other information. IMEI (International Mobile Equipment Identity) number, phone number, symmetric key (Use same key for encryption and decryption) is also saved in the database. The password is stored as hash in the database [3].

Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, Sotiris Ioannidis has discussed about various challenges in adopting 2FA (two factor authentication) systems by users. They have also analyzed various websites and user account if they have enabled 2FA. Authors examine about 100000 Google accounts to quantify. To check whether 2FA is enabled on user account the author used password reminder process in their own way. They attempt to perform their analysis without alerting the user so that he/she must not be annoyed. They have used distributed systems to perform the process otherwise their host will be blocked by the server or they must have enter the CAPTCHAs to complete the process. After the completion of their research they come to know that only 6.4% of the existing users were using 2FA.

The author proves that the 2FA significantly increase the security of web based accounts but the issue is adoption of the 2FA techniques. Their research proves that majority of the websites is not providing 2FA and the websites which provides 2FA are not interested in using 2FA. Google was the first service provider which has adopted the two factor authentication system in year 2011. After that Facebook and Yahoo also adopted 2FA in same year. In the year 2012 many of the other websites including Stripe, Bizzard, aTech adopted 2FA.

The researchers used Google password reminder facility to check lakhs of user account to determine whether they are using 2FA or not. Authors face many challenges while

performing the research. One of them was CAPTCHA. Because Google force to enter CAPTCHA in case of more than 3 unsuccessful login attempts.

Authors used a list of millions valid Gmail accounts which was published in Bit-Coin security forum. On 9 Sept 2014 almost 5M Gmail accounts details were leaked and then published in the forum. They believe the users having their account hacked will be using extra security therefore there were more chances that those accounts will having more rate of 2FA adopted. After analysing about 1 lakh accounts they come up with the following results.

91.9% of the accounts were found to be valid. From all those accounts only 6.39% of the users were using two factor authentication systems. This was very less than the expected. The surprising result was that most of the accounts were still not using any kind of verification method for recovering their password in case of forgot or hacked. The recovery method includes mobile verification and recovery email. 68.14% of the users were using their registered mobile phone for the verification purposes.

Their study about 2FA surprisingly gave disappointing facts because only 6.4% users were found to be using two factor authentication systems. Also they illustrated how Google's password reminder facility is being used by the hackers to collect the useful information about the users [14].

A.P. Sabzevar, A. Stavrou proposed an innovative technique for the multi-factor authentication. They have proposed image based passwords for the mobile token which is usually a handheld device. User has to determine various click points on the image and using those click point the user will be authenticated when he wants to login into the website. Authors proposed system to provide protection from various attacks like dictionary attacks and social engineering attacks.

For the implementation of the proposed system they have used the personal mobile device of the user for the second factor for the authentication. Because mobile device is a very convenient way and easily available so it is easy for every user to use the two factor authentication. The server will also act as challengers to provide various challenges of clicks for the user. There will be two images in the system. One is called the password image and other one is called the key image. The password image containing the click point information and is encrypted.

The other image which is the key image is encrypted by the challenger server. It is usually the copy of the password image. This image can be validated on the user's device after decrypting it. The main idea of the system is that the password image is containing some areas which will be clickable. The order of the click points will be defined during the registration phase. More will be click points on the image more will be the complexity of the graphical password. So in order to increase the security user can increase the number of the click points. So the system is flexible in order to increase the security.

Author has also proposed a method for more complicated picture password. The image used as a key will have encrypted with pre specified alpha numeric values. These alphanumeric values are stored behind the image as a grid. The grid is usually predefined. The user has to identify the grid points in order to enter the password from the mobile device.

The proposed system is capable to provide protection from dictionary attack and social engineering attacks. But the system lacks in communication techniques, the system is not using secure connection for the communication purpose. Also the graphical method of the passwords is not very user friendly. So there are very less chances that the end users will adopt the system. Last point is that the proposed system will always relies on the network. So in case of failure of the network the system will not be capable to work [8].

Bruce Schneier has discussed about security of various two-factor authentication schemes. According to author two-factor authentication may be helpful in wide range of applications, but still there is need of improvement of two-factor authentication. These authentication techniques helpful in avoiding old attacks but still vulnerable to many modern attacks such as Trojan attack, Man in the middle attack.

Author stated that people often use easy and guessable passwords. They share passwords to other people in mails, write them in copies or books because they can't memorize it. This is the fundamental reason two factor authentication schemes comes in existence. But the attacker can use techniques like phishing to attack the user where the user will not even realize that he has been attacked.

Another example of such attacks is Trojan attacks where the attacker needs to install a Trojan program in the user's system. Using that Trojan the attacker piggybacks on session. After that the attacker can make fraudulent transactions. The author also talked

about the cost of the hardware involved in these authentication techniques. Two-factor authentication techniques can be more beneficial after some improvements.

The two step authentications are also vulnerable to Man-in-the-Middle Attacks. In such attacks the attacker will intercept the communication between the client and the server (communicating parties). The attacker will get the information from one party A and can change the information before sending to the other party B on behalf of A. Both parties will never know they are having an intermediate person if the attack is performed successfully. Attacker can use the received information in a variety of ways and can use to perform illegal tasks.

According to author the two-factor authentication systems are very important to improve the security. Most of the attacks can be avoided if the user has been using this service. But because not all of the websites are providing this service, not all of the users are aware of this system [15].

Stephen Farrell explained the vulnerability of the renegotiation in the handshake phase of the TLS protocol. In the handshake phase two parties agree on what type of cryptographic algorithms and keys are to be used during data transmission. The TLS protocol allows the clients and server renegotiate if some suitable conditions which isn't cryptographically bound to the first one. The author explained how man in the middle attack can happen on renegotiation. The following images explain how MIITM attack can happen in SSL renegotiation.

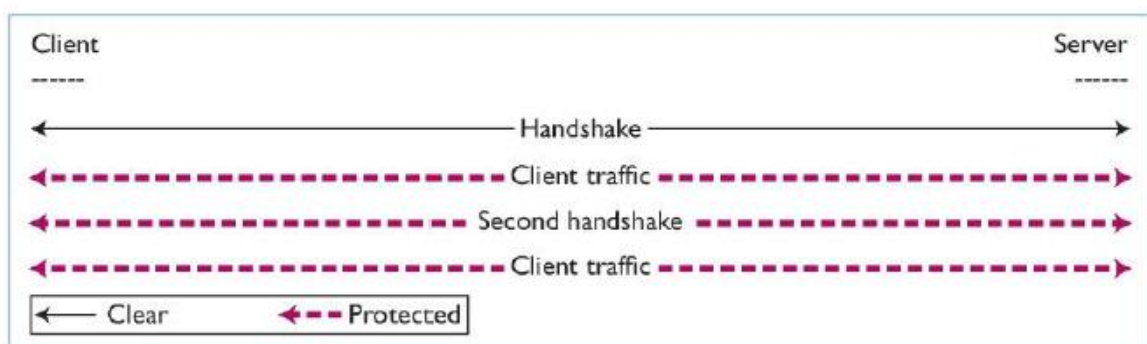


Figure 6: Renegotiation in TLS. The keys established during previous handshake will be used to send client's identity [16].

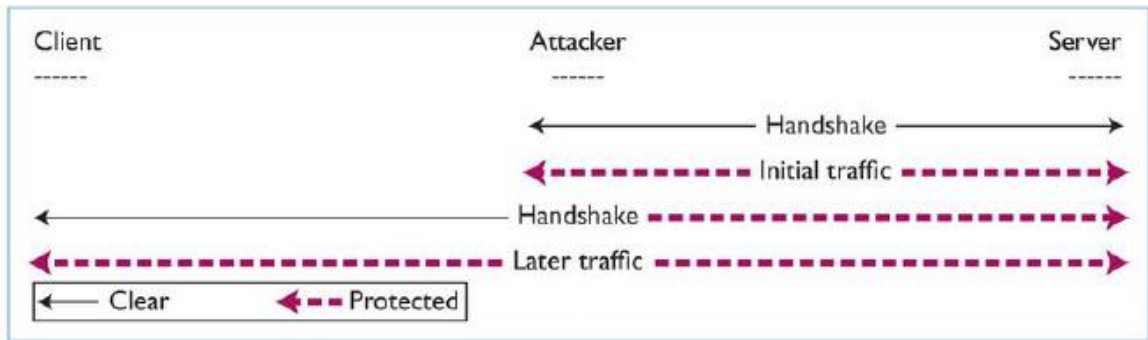


Figure 7: MITM Attack on TLS. The attacker use previous session keys to connect to the server during renegotiation [16].

RATIONALE AND SCOPE OF STUDY

Multi-factor authentication is getting popular because of its security. But many aspects of multi-factor authentication can be further improved and simplified. The SMS based two-step authentication systems are dependent on network. Therefore this is only workable if the mobile has a network to revive the SMS. Our implementation is more beneficial in providing a high end security. Firstly, the onetime passwords generated within the client app therefore the passwords are not dependable on any cellular network. Once the registration is complete, the client app generates six digit one time password (OTP) that can be used for the authentication purpose. Unlike Google authenticator TOAST shares secret via a secure channel (using TLS connection). This ensures the secret is not compromised or spoofed.

The mobile devices without camera can also get the benefits from these techniques because in these techniques instead of scanning QR code (Quick Response Code) users can simply switch to username and password for registration purpose. The app will create secure connection with server to share the secret if the credentials are correct. After that the app will generate offline key store.

This system can be embedded in many other applications where high end security is required, e.g. online banking applications, cloud storage applications and etc. Our methodology can be easily implemented in any type of applications and supports variety of operating systems. This system can be implemented on Android, iOS and Windows app.

OBJECTIVE OF STUDY

The existing systems of multi-factor authentication either rely on the cellular network to send an OTP. The main objective of this research is to use cryptographic techniques to provide a better multi-factor authentication system. The aim is to build a smartphone app which will provide offline time based onetime passwords to provide authentication to web based accounts.

The main objective of the research is to build a system to generate offline keystore on client app without sharing any sensitive data (shared secret) publically For this purpose secure TLS connection between client app and server is established .The transmitted data will not be spoofed or tempered in between .In this way only legitimate user will gain access to the online account. The complete system will be able to operate without any network expects the registration phase. The objectives of the research can be summarized as follows;

- 1. Develop a two-step authentication system for enhanced security:** The fundamental focus of the research is to build a cryptographically strong two step authentication system. To protect web accounts two step authentication system can be helpful and provide enhanced security.
- 2. The system must work in offline mode expect from setup phase (offline keystore):** Most of the two step authentication systems are network dependent. Network dependent systems works on the condition that the device and authentication server has reliable network connectivity. For example SMS based system will need to send one time password via an SMS on the user's device. But in the proposed system the application can generate one time passwords on the offline mode. If there is not any connectivity between the server and application even then the system will work fine and generate required one time passwords.
- 3. The system will work without any cost to user:** As in SMS based two-step authentication systems the server will send an SMS to the user's device, the user may have to pay for the cost of SMS. In our system there is no SMS and no cost for the SMS will be charged.
- 4. The keystore must be encrypted:** The data in the device will be encrypted and

protected from any misuse.

5. **Seed will be transmitted to client app by using a TLS connection:** One of the most important objects of the research is to transmit the seed to the mobile device in a secure way. The TLS connection is the best way to achieve this objective. The seed will be shared using a TLS connection
6. **Password Protected Application:** The authentication application is password protected. After the setup of the user account on the application, the user need to set a password for the application. Whenever user open the application the user will enter the password to enter into the application.

RESEARCH METHODOLOGY

OTPs are very important to enhance the security. To break the dependency of OTP to network based system, an offline application can provide the OTP when required. A smartphone is required for this purpose to install the app which will provide the offline keystore facility. Although this system can be implemented in almost all type of operating systems running today.

The system will use TLS connection between the mobile device and web to share the seed to the generate offline keystore. This is one time process where the device will need network connectivity. Once offline keystore is generated on the device offline passwords can be generated as per requirement. The following figure explains the overall working of the two step authentication system.



Figure 8: Illustration of series of operations involved in two step authentication

The mobile device will act as a token for verifier device for the authentication system. The TOTP application will be installed on the mobile. The flow chart of the methodology has been depicted in figure.

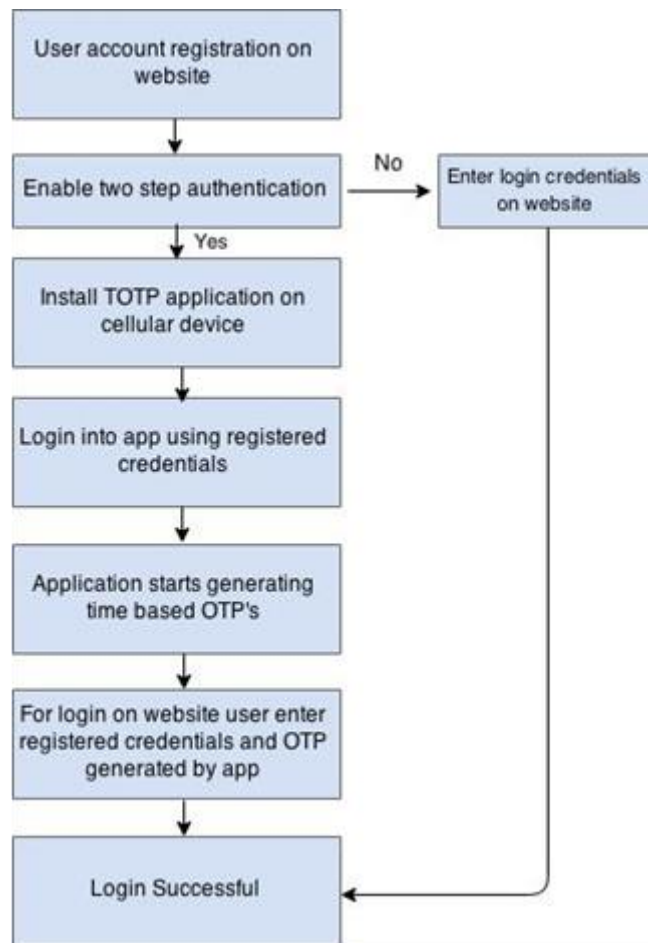


Figure 9: Flow chart explaining proposed authentication system

To achieve all the objectives of the research a smartphone application will be developed which will generate the offline keystore. This app can be developed in any kind of mobile operating systems. For our research android app will be developed that will work for the client authentication. This system of authentication includes three entities. First is the user itself who attempt to login, second is the server who will respond to the users authentication request and the third is the smartphone application which will generate one time passwords.

6.1 Registration phase

The complete system starts with the registration /signup of the user account on the website. The website must provide username and password to the user for authentication purposes. There must be secure connection provided by the server for the registration. It is mandatory that passwords must be stored as hash code by using a computationally slow

hash function. After registering web account if the user want to enable two step authentication then user must have TOTP app installed on his personal mobile device.

On the mobile device following steps are need to be followed.

Step 1: Mobile application will request to enter registered credentials of user. User will login using registered credentials into application.

Step 2: The application will establish a secure (TLS) connection with web server. The server will send confirm TLS connection and send session key to application

Step 3: App generates TOTP request and send to server. The request has following parameters.

Encrypt [data = username, password; cipher = AES256CBC, key = session key]

Step 4: The server will decrypt the request

Decrypt [AES256CBC, data = TOTP request, key = session key]

Step 5: Server will check the credentials in database. If correct then server will generate a unique 32 bit string (seed) for that user account.

Step 6: Server will encrypt the seed and send it to application using same TLS connection

Encrypt [data = seed; cipher = AES256CBC, key = session key]

Step 7: Application will decrypt the seed

Decrypt [AES256CBC, data = seed, key = session key]

Step 8: The TOTP algorithm in app will use seed to generate OTP's

Step 9: User need to provide PIN as a password to protect the application to prevent unauthorized use.

The app will securely receive the seed send by the server via TLS connection. The app will securely store the seed in the keystore. The application will generate the one time password using the seed provided by the server SHA1 & Two fish symmetric key cipher is used to encrypt the key store. The cipher block chaining (CBC) mode is used for the encryption. The application will be protected for avoiding any un-authorized access.

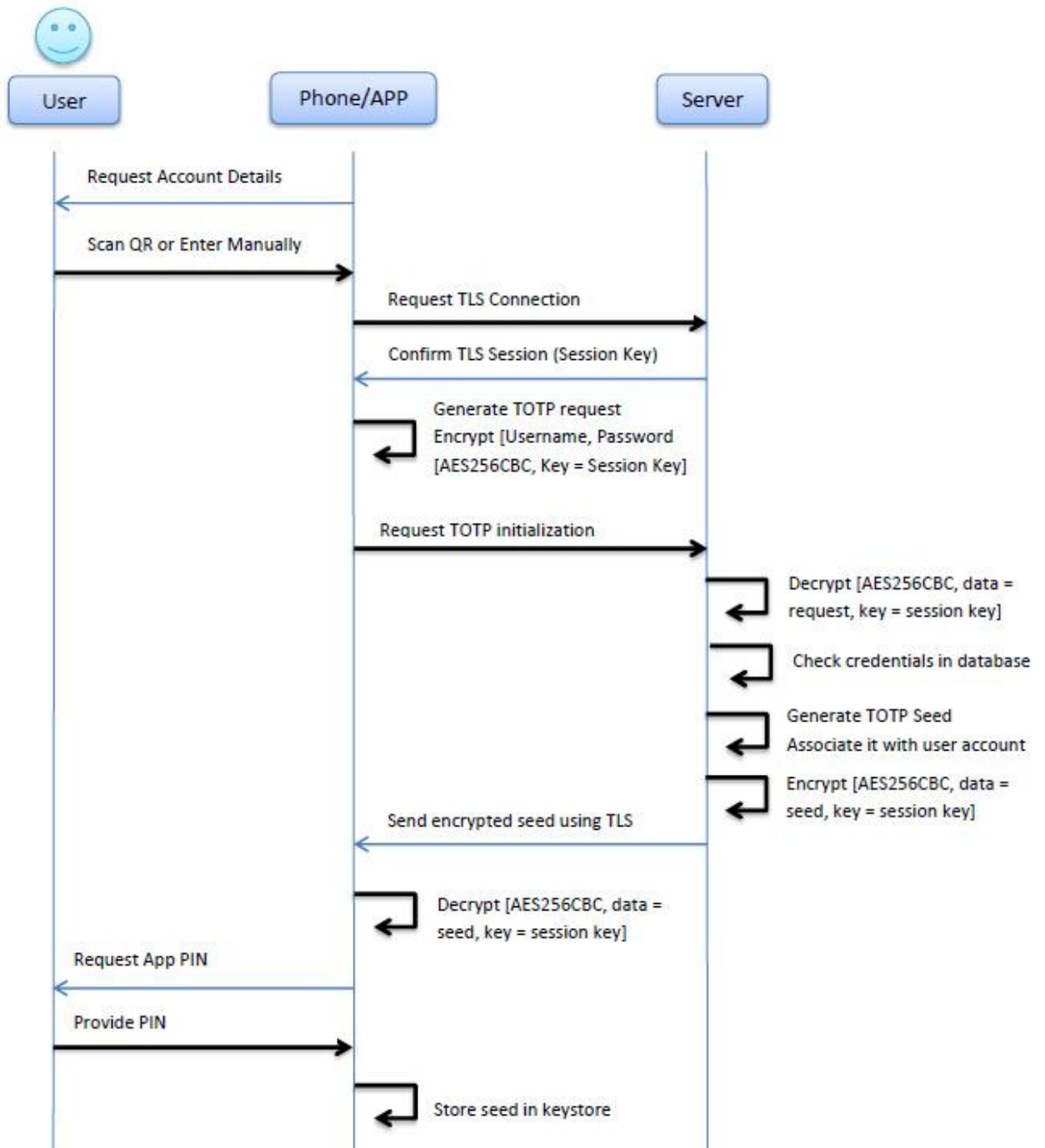


Figure 10: TOTP Enrolment

6.2 Login and OTP Generation

After successful registration of account and device the application will be capable of generating one time passwords for authentication purpose. The application will be

password protected and this password will be 4 digits PIN. The application use TOTP algorithm and this algorithm use HMAC-SHA1 for generating passwords. HMAC stands for Hash based message authentication code. The algorithm takes 32 bit character stream (seed) as input and provide 6 bit alphanumeric stream as one time password.

The password will change every 30 seconds which will be beneficial to avoid sniffing attack. The service provider website which will enroll 2-step verification required to ask one time password after successful login using clients' username and password. The client will authenticate himself by using the current OTP from the mobile app. After successful verification the client will be able to login into service provider website.

6.3 Comparative Analysis against other 2 factor authentication system

The proposed system is designed to achieve 3 goals. First the seed must never expose second the system will generate OTP in offline mode and last the secret seed will be transmitted via a secure tunnel. The other authentication schemes are different from our proposed system in many aspects.

When comparing our system with SMS OTP our proposed system provides benefits of offline generation of one time passwords (OTP's). Most of the websites including banking and others used this approach for 2 step authentications. Since this scheme relies on the cellular network, this scheme may fail in some cases when the network is not available. In other words the system will fail in the absence of the cellular networks. Also if the user needs to switch between multiple mobile numbers then this can be an issue for the SMS based authentication scheme. This means the user needs to update the mobile number on the respective server to use 2 step authentications. The proposed system overcomes these all issues by providing an offline password generation method. The user can switch between different mobile numbers as the number is not associated with the client app. The main benefit of the SMS based authentication is that it is compatible all the mobile devices. Only future needed is the SMS capability. Overall the proposed system will perform reliability because it is independent of the network.

The interface of our proposed system is quite similar with Google authenticator but the core functionality is totally different. The both systems generate one time password (OTP) offline. But the major difference lies in seed exchange and seed storage

techniques. Google authenticator use QR code for transmitting the seed to the app. But the proposed system use QR code as well as TLS (Transport Layer Security) connection for securely exchange the seed from the server to the app. the proposed system also enables the mobile phones without camera to use this authentication system by adding the feature of login in app using username and password.

6.4 Tools & Equipment's for Implementation

The 2 step authentication system includes server–client app and the user. The client application can be implemented in various available Operating systems. The prioritised environment for mobile app is Android OS. The Android app is developed in Android SDK (Software Development Kit) which is freely available to use [22]. The proposed system can also be implemented in .Net Application. The tools use for .Net Application is Visual Studio 2012 with .Net framework 4.5. The server use for our proposed model will have configuration Intel Core i7 3740 QM 2.7 GHz, 16 GB RAM, Gigabit Ethernet.

RESULTS AND DISCUSSIONS

7.1 Experimental works

The proposed system has been implemented in ASP.NET platform using Visual Studio 2012. An android mobile application has been developed using Android development kit. Basically, in any two step authentication system there are 3 entities.

- User
- Authentication Server
- Authentication Token (Mobile device/app)

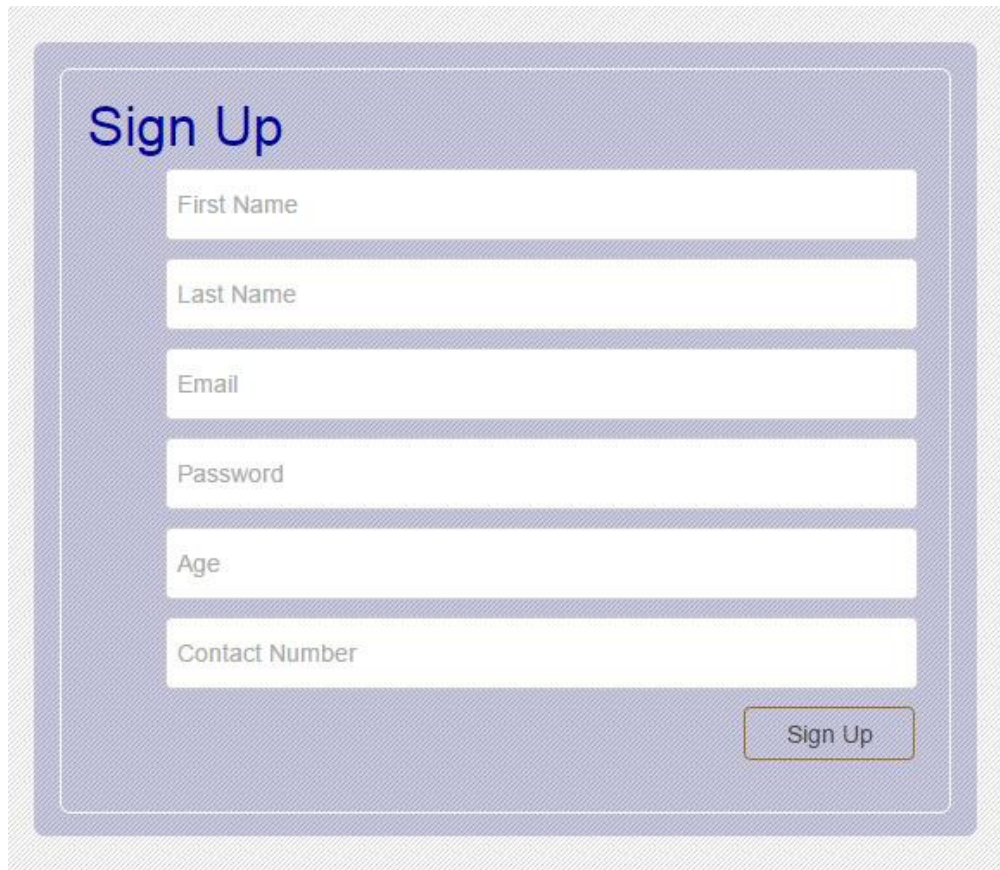
7.1.1 Website / Authentication server

The authentication server can be any website which provides any type of the server to users (e.g. Banking websites, ecommerce websites etc.). We have developed a dummy website for implementing the proposed system. The website will be having following pages.

- Sign Up/Registration (For creating new user accounts)
- Login
- Interface to enter One Time Password
- Settings (Provides option to user if they want to enable 2 step authentication)

7.1.1.1 Signup/Registration:

User need to register in order to any website like banking and ecommerce websites. The signup page will let the user to enter basic details of him and create an account on the server. The registration page is illustrated in figure 11.



The image shows a 'Sign Up' registration form with a light blue background. At the top left, the title 'Sign Up' is written in a large, dark blue font. Below the title are six white input fields stacked vertically, each with a light blue border and a label: 'First Name', 'Last Name', 'Email', 'Password', 'Age', and 'Contact Number'. At the bottom right of the form is a rectangular button with a light blue border and the text 'Sign Up' in a dark blue font.

Figure 11: Signup/Registration Form

7.1.1.2 Login

The registered users can login into the website. User needs to use the registered credentials to login into the website. Figure 12 illustrates the login page.



The image shows a 'Login' form with a light blue background. At the top left, the title 'Login' is written in a large, dark blue font. Below the title are two white input fields stacked vertically, each with a light blue border and a label: 'Username' and 'Password'. At the bottom right of the form is a rectangular button with a light blue border and the text 'Login' in a dark blue font. At the bottom left, there is a checkbox with the text 'Remember me' next to it. At the bottom right, there is a blue hyperlink that says 'Sign Up'.

Figure 12: Login Form

7.1.1.3 Two-Step Verification Page

If the entered credentials of the user found to be authenticated by the signup page, the user will be asked to enter the One Time Password. The one time password will be generated by mobile application installed in the mobile device of the user. Figure 12 illustrates the 2-step verification page.

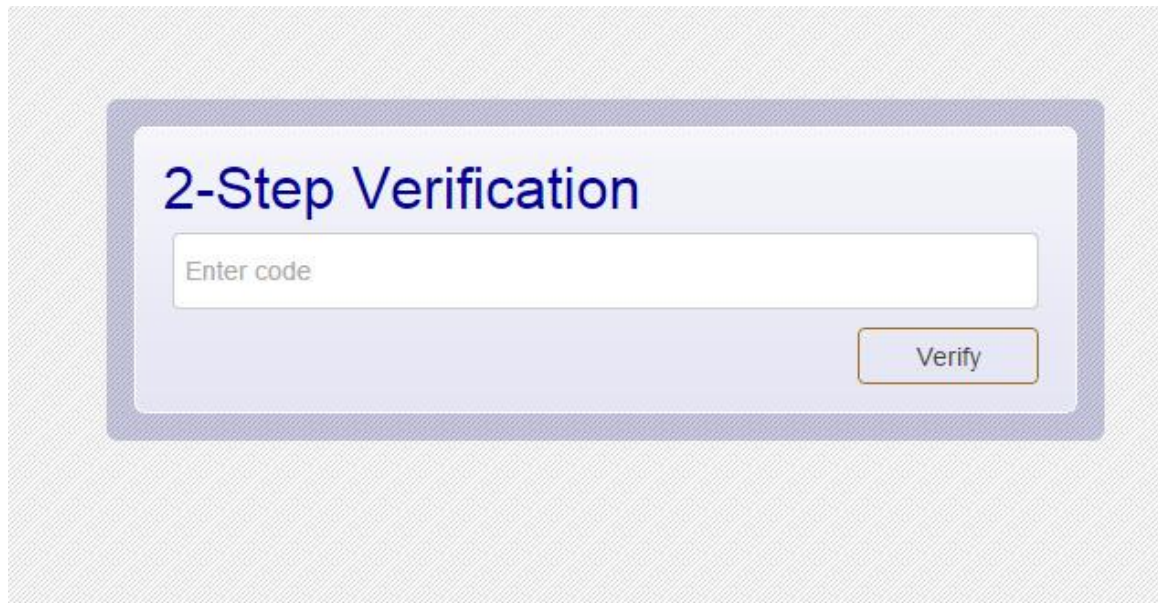


Figure 12: 2-Step Verification page

7.1.1.4 Homepage/Default Page

After the successful verification the user will be redirected to the homepage of the website. Actually, this will be decided by the server that user will be redirected to which page. Figure 13 shows the interface of the homepage which is a dummy website to implement the proposed system.

7.1.1.5 Settings

We have provided the option to the users that they can enable or disable the two step authentication according to their choice. If the user has selected to disable to two step authentication, the user will no longer need to enter the one time passwords. But this is not recommended because it leads to degrade the security of the user account. The interface has been illustrated in figure 14.

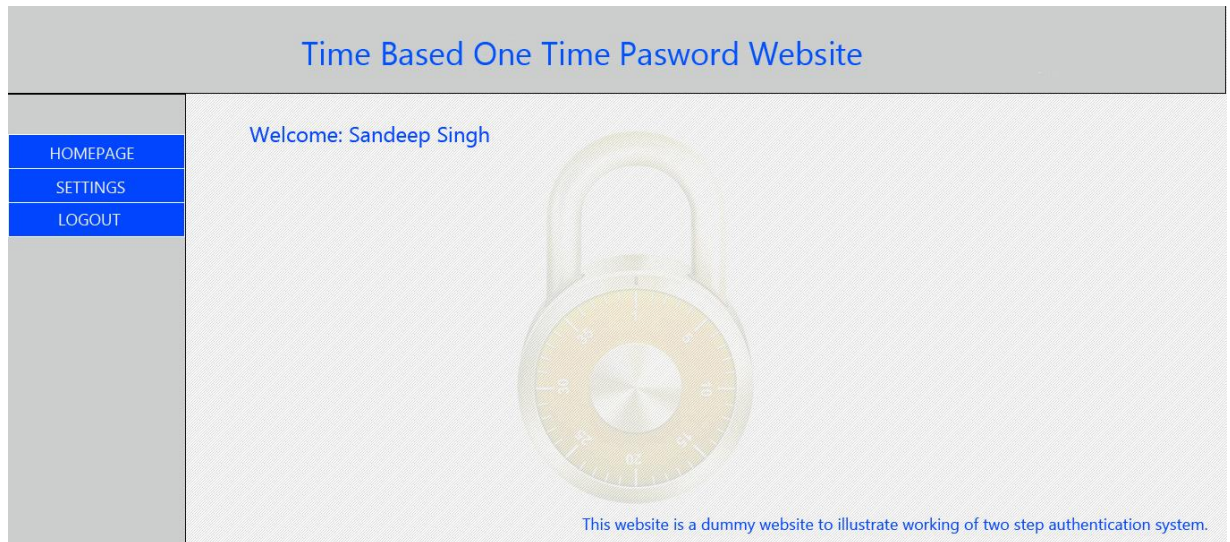


Figure 14: Homepage

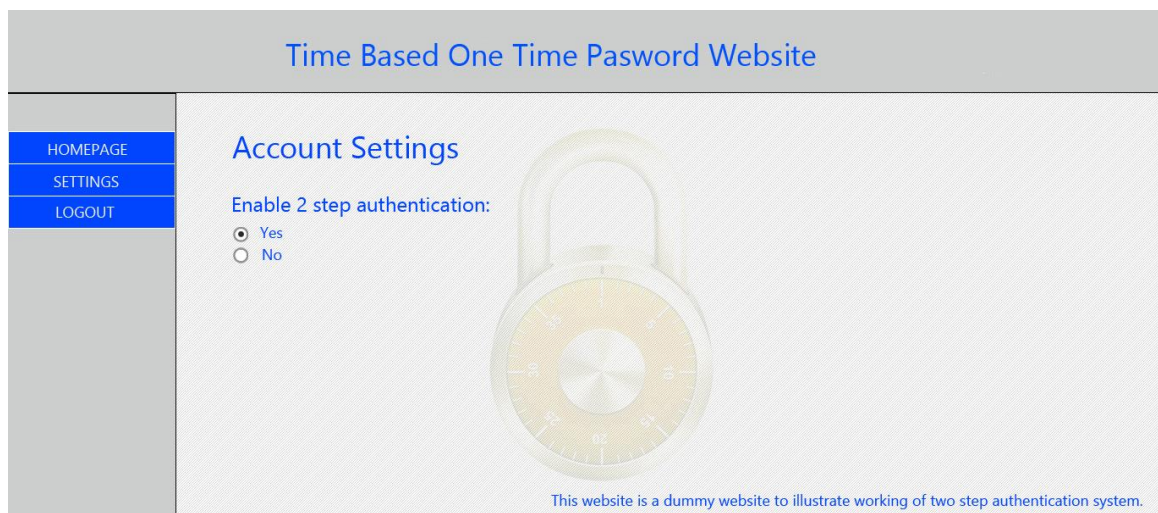


Figure 15: Settings page to enable/disable two step authentications

7.1.2 The mobile application

The third entity of the system is the mobile application which will generate one time passwords on the user's device. We have developed an android application for this purpose. User will need to install the mobile application. The application has following screens.

7.1.2.1 Splash Screen

When user opens the application for the first time, the splash screen appears for 5 seconds. After the setup the splash screen will never appear. Figure 16 illustrates the design of splash screen.

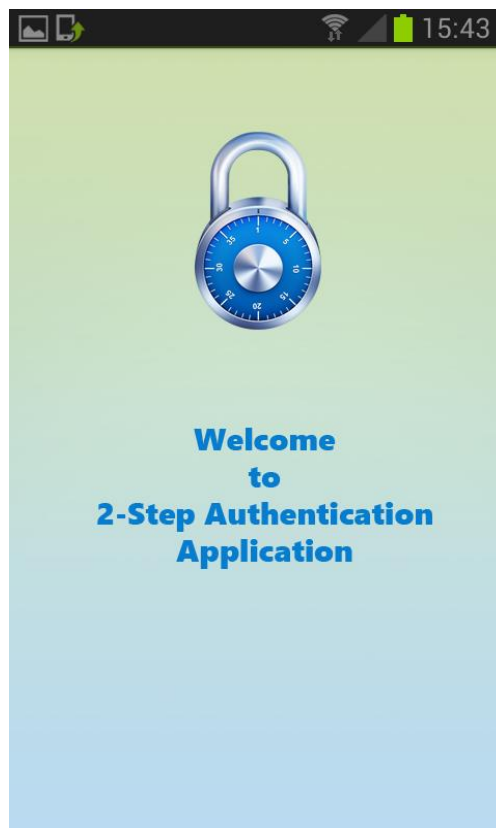


Figure 16: Splash Screen

7.1.2.2 Login Screen

The login screen will appear after splash screen. The user will need to enter the registered login credentials. Therefore only registered users can use application. Application will connect to the server using a secure connection. This is the first step for the setup of the two step authentication. Login screen has been illustrated in figure 17.

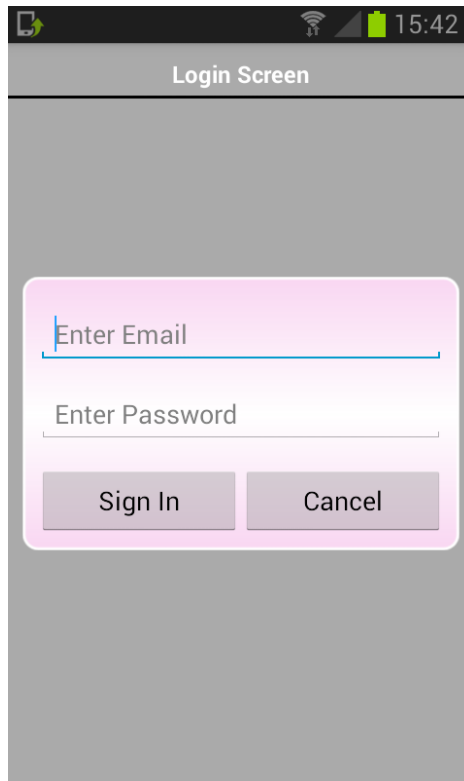


Figure 17: Login Screen

7.1.2.3 Application Password Interface

To protect the application from unauthorised use in case that the device has been stolen, user will need to enter the password to enter the application after the setup. The user will enter the password used to login into the server. Illustration is given in figure 18.

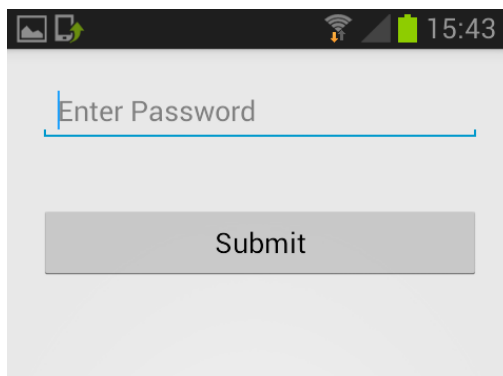


Figure 18: Application Password

7.1.2.4 One Time Password Screen

This screen will provide the one time password which will be used to login into the web account. The password will be generated by application in offline mode. No network connectivity is needed to generate the passwords. The application will be showing the registered account information in addition to one time password. The screen has been illustrated in figure 19.

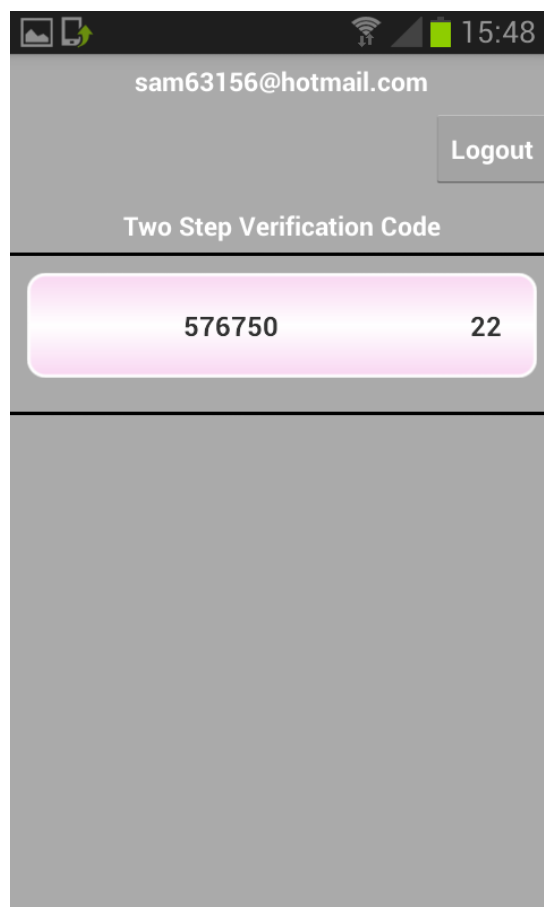


Figure 19: One time password screen

7.2 Data analysis and interpretation

For testing the proposed system user defined values of UNIX time (timestamp) and shared secret has been used. Same values have been tested using 3 different modes and results have been given in table 1. Time step is 30 second.

Unix Time	UTC Time	Value of Seed/Shared Secret	Mode	OTP
946728000	01/01/2000 12:00pm	00000000-0000-0000-0000-000000000001	SHA1	822628
946728000	01/01/2000 12:00pm	00000000-0000-0000-0000-000000000001	SHA256	084939
946728000	01/01/2000 12:00pm	00000000-0000-0000-0000-000000000001	SHA512	015143
1123481162	08/08/2005 6:06am	88c6ab9d-c259-4e7b-9edd-b8ca494e6ea5	SHA1	286889
1123481162	08/08/2005 6:06am	88c6ab9d-c259-4e7b-9edd-b8ca494e6ea5	SHA256	456877
1123481162	08/08/2005 6:06am	88c6ab9d-c259-4e7b-9edd-b8ca494e6ea5	SHA512	362298
1183182907	06/30/2007 5:55am	91dfd7fa-3afb-4fa1-89b6-1b8006d13d95	SHA1	207710
1183182907	06/30/2007 5:55am	91dfd7fa-3afb-4fa1-89b6-1b8006d13d95	SHA256	817920
1183182907	06/30/2007 5:55am	91dfd7fa-3afb-4fa1-89b6-1b8006d13d95	SHA512	883097
1430976297	05/07/2015 5:24am	15010b37-0bfe-4074-9841-7ac27c756c17	SHA1	874770
1430976297	05/07/2015 5:24am	15010b37-0bfe-4074-9841-7ac27c756c17	SHA256	557471
1430976297	05/07/2015 5:24am	15010b37-0bfe-4074-9841-7ac27c756c17	SHA512	326678

Table 1: Experimental results using user defined values

7.3 Performance evaluation

We have evaluated the system using different algorithms (SHA1, SHA256, and SHA512) and find out the execution time (elapsed ticks). The execution time of SHA1 is found to be least as compare to other algorithms.

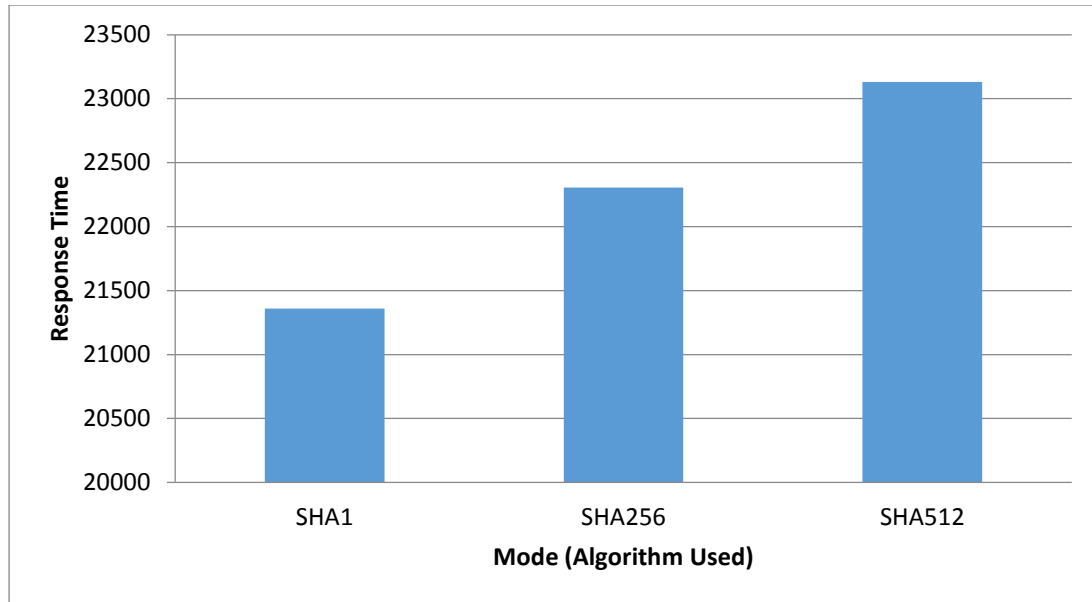


Figure 20: Response time evaluation using different algorithms

CONCLUSION & FUTURE SCOPE

In this research, the multi-factor authentication system is aimed to be improved by using TLS connection between server and client app. Because the seed is shared using secure connection so it is never exposed. The system will generate offline passwords and eliminate the dependency on the network. The proposed system is free of cost. The service providing website can use this system to enhance the security of their system without charging any additional cost. Because there are no SMS services related to system so there will be no cost of SMS to server and client. The offline keystore is encrypted and password protected to avoid any unauthorized use. Unlike Google authenticator the proposed system can be used in the mobile phones without camera. This system can be embedded in wide range of applications to provide multi-factor authentication.

The system has a great future scope and we are working on the following improvements.

1. The proposed system can run reliably on android mobile phones. We are working to develop applications for other operating systems like iOS and Windows Phone Applications
2. An SMS based OTP can be developed in case there is any issue with application. The server will send an SMS to the registered mobile phone if the device fails to generate one time password due to any unexpected problem
3. There are chances that the device can be lost or stolen. In such a case we want to add a new feature of “Trusted Devices”. User need to add any two trusted phone numbers in his/her account. In case the device is lost the server will send different recovery code to both of the registered numbers. The user will have to enter the both recovery codes in order to recover the account. This feature will ensure the recovery of the account and will increase the security of the system.
4. Biometrics can be a part of our two step authentication system. There are many mobile devices which has fingerprint readers (e.g. iPhone 6, Note 4 etc). This feature can be used for two step authentication system. The user will registered the device

and touch id on the server. Whenever user want to login into a web account, the website will as user to use his touch id on the registered device. After successful scan the device will send a message to the server. The server will allow the user to login to the account if the user is authenticated.

I. Research Papers:

- [1] Strategy, Javelin. "Research. 2011 Identity Fraud Survey Report: Consumer Version." *Pleasanton, CA* (2011).
- [2] Arkin, Brad. "The case for mobile two-factor authentication." *IEEE Security & Privacy* (2011).
- [3] Indu, S., T. N. Sathya, and V. Saravana Kumar. "A stand-alone and SMS-based approach for authentication using mobile phone." In *Information Communication and Embedded Systems (ICICES), 2013 International Conference on*, pp. 140-145. IEEE, 2013.
- [4] Hsieh, Wen-Bin, and Jenq-Shiou Leu. "Design of a time and location based One-Time Password authentication scheme." In *Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International*, pp. 201-206. IEEE, 2011.
- [5] Abdurrahman, Usman Alhaji, Mustafa Kaiiali, and Jawad Muhammad. "A new mobile-based multi-factor authentication scheme using pre-shared number, GPS location and time stamp." In *Electronics, Computer and Computation (ICECCO), 2013 International Conference on*, pp. 293-296. IEEE, 2013.
- [6] Pu, Qiong. "An improved two-factor authentication protocol." In *Multimedia and Information Technology (MMIT), 2010 Second International Conference on*, vol. 2, pp. 223-226. IEEE, 2010.
- [7] Patil, Sonali, Komal Bhagat, Susmita Bhosale, and Madhura Deshmukh. "Intensification of security in 2-factor biometric authentication system." In *Pervasive Computing (ICPC), 2015 International Conference on*, pp. 1-4. IEEE, 2015.
- [8] Sabzevar, Alireza Pirayesh, and Angelos Stavrou. "Universal multi-factor authentication using graphical passwords." In *Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on*, pp. 625-632. IEEE, 2008.
- [9] Dierks, Tim, and Christopher Allen. "Rfc 2246: The tls protocol." *IETF, January*(1999).
- [10] M'Raihi, D., M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen. "Hotp: An hmac-based one-time password algorithm." *The Internet Society, Network Working Group. RFC4226* (2005).

- [11] M'Raihi, D., S. Machani, M. Pei, and J. Rydell. "Totp: Time-based one-time password algorithm." *Internet Requests for Comments, Internet Engineering Task Force (IETF), RFC 6238* (2011).
- [12] Limkar, Suresh V., Rakesh Kumar Jha, Shilpa Pimpalkar, and Santosh Darade. "Geo-Encryption-A New Direction to Secure Traditional SSL VPN." In *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, pp. 1070-1071. IEEE, 2011.
- [13] Lee, Daesung, Hyun Sook Jang, and Ki Chang Kim. "A Lightweight Protocol Based on the SSL Protocol for Handheld Devices." In *Information Science and Applications (ICISA), 2011 International Conference on*, pp. 1-4. IEEE, 2011.
- [14] Petsas, Thanasis, Giorgos Tsirantonakis, Elias Athanasopoulos, and Sotiris Ioannidis. "Two-factor Authentication: Is the World Ready? Quantifying 2FA Adoption." In *Proceedings of the Eighth European Workshop on System Security*, p. 4. ACM, 2015.
- [15] Schneier, Bruce. "Two-factor authentication: too little, too late." *Communications of the ACM* 48, no. 4 (2005): 136.
- [16] Farrell, Stephen. "Why didn't we spot that?[Practical Security]." *Internet Computing, IEEE* 14, no. 1 (2010): 84-87.
- [17] Kirovski, Darko, and Christopher A. Meek. "Tunneled TLS for multi-factor authentication." In *Proceedings of the 11th annual ACM workshop on Digital rights management*, pp. 31-40. ACM, 2011.
- [18] Yang, Guomin, Duncan S. Wong, Huaxiong Wang, and Xiaotie Deng. "Two-factor mutual authentication based on smart cards and passwords." *Journal of Computer and System Sciences* 74, no. 7 (2008): 1160-1172.

II. Websites:

- [19] "SSL Vulnerabilities: Who listens when Android applications talk?", Available: <https://www.fireeye.com/blog/threat-research/2014/08/ssl-vulnerabilities-who-listens-when-android-applications-talk.html>
- [20] "The Heartbleed Bug", Available: <http://heartbleed.com/>
- [21] Microsoft. *How SSL/TLS Works*. Available: [http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa374757(v=vs.85).aspx)
- [22] "Android SDK", Available: <https://developer.android.com/sdk/index.html>

Chapter 9

Appendix

Glossary	Page No.
Authentication	1
Cipher	3
CBC	14
GPS	6
GSM	8
HMAC	14
IMEI	8
Keystore	11
MITM	1
OTP	1
PKI	6
QR Code	10
SMS	1
Symmetric key	8
Seed	4
TOTP	4
TLS	1