Abstract: In this paper we describe the methods for implementing connectionless approach for stronger authentication. This connectionless approach includes the two factor authentication using mobile phone (Android). The main purpose of this method is to provide the stronger authentication in online transaction. Mobile phone is used for the purpose of generation of OTP. It improves the security of Internet payments by providing an additional password to the user. Using the password the user can successfully make his payment. Online card transactions over Internet need enhanced security. Secure processing system facilitates additional security by way of a cardholder-chosen password, which is known only to the cardholder. Dynamic password authentication is one solution that uses the added security of credit cards to offer better protection against online fraud. The primary benefit of this system is the reduction in disputed transactions and the resultant exception handling expense and losses. Thus the proposed system is adding an extra layer of security at the point where you enter information online. The service helps to prevent unauthorized online use before it happens by confirming your identity with an additional password.

Keywords: One Time Password (OTP); Connectionless,; Authentication; Security; Transaction; Random String; Two factor Authentication, Personal Identification Number(PIN).
1. Introduction:
In these days most of systems are rely on the Static password, such passwords are vulnerable for attack. Users tend to use easy-to-guess passwords, use the same password in multiple accounts, write the passwords or store them on their machines, etc.[1] Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, snooping, sniffing, guessing, etc. Today use of mobile phones is increased beyond just calling or texting. Mobile connectivity options have also increased. After standard GSM connections, mobile phones now have infra-red, Bluetooth, 3G, and WLAN connectivity. We are using the mobile phone for generating the One Time Password (OTP) [2][4]. OTP generating application is developed for Android based mobile phones. We developed two factor authentication system using mobile phone(android) it consist of two modes connection oriented and connectionless. Connection oriented is e-mail and SMS based, it is more expensive. Connectionless approach for android based mobile phones which is easy to use, secure and cheap. In the next section we described background about authentication factor, existing system. Section III described proposed system. Section IV described algorithm of system. In Section V described about system analysis. Section V concludes the paper.

1.1. How OTP is generated at client side?
We are using android based mobile phone for the generation of OTP. Where user has to enter the predefined attributes value such as user id, date of birth and ATM pin no. mobiles IMSI no. and current date and time is automatically retrieved by the inbuilt function of application. And using this parameter an OTP is generated.
Time is one the main factor in this process where it gets changed regularly.

1.2. How Secure is our generated OTP?
We are using SHA1 algorithm to generate the one time password. SHA1 is basically a secure hash algorithm that works with input less than 2^64 bits in length. Output generated by SHA1 algorithm is 160 bits. It is more secure than MD5 algorithm. It gives a fix length of output. Here we get 20 bytes of string i.e. 160 bits. 20 bytes gives 40 characters. It is very hectic task to enter those 40 characters for that we divide that 20 bytes into 4 chunks each of 5 bytes & perform XOR operation on that chunks. Which gives us output of 5 bytes i.e. 10 characters. These 10 characters are final secrete key known as generated One Time Password (OTP).
2. Background:

Authentication is done to identify whether person is genuine or not if she/he is genuine then grant the access of system otherwise denied it. There are three universally recognized factors for authentication exist today are: what you know (e.g. passwords, PIN’s), what you have (e.g. debit card or credit card), and what you are (e.g. figure prints, face recognition, biometrics, etc.). —Two factor authentications [1][2][4]. is a mechanism which implements two of the above mentioned factors and is therefore considered stronger and more secure than the traditionally implemented one factor authentication system. One of the examples of two factor authentication includes withdrawing money from an ATM machine. When someone wants to draw money from the ATM, first he/she has to input his/her ATM card i.e. what you have and again he/she has to enter the pin number i.e. what you know in order to access his/her account. Dynamic password authentication is one solution that uses the added security to offer better protection against online fraud [7]. The primary benefit of this system is the reduction in disputed transactions and the resultant exception handling expense and losses. The substantial proportion of customer complaints could be eliminated with the use of Authenticated Payment. This will have a positive impact on user profitability. To make online transaction even simpler and safer, a secure processing system is being introduced. Passwords are known to be an easiest target for hackers. For that banks are using tokens as a mean for two factor authentication. Tokens come in two formats: Hardware and Software. Hardware nothing but small device which are small and can be conveniently carried. E.g. ATM, Debit cards etc. Software tokens are PIN that changes with time. When user wants to authenticate to system at that time she/he uses that PIN. Such programs implement one time
passwords (OTP) algorithm [1][2]. OTP algorithms are difficult to break, since unauthorized user should not able to guess next password in sequence. Factors that are used in OTP algorithms which include the unique information of user such as user id, DOB, time etc.

3. System Analysis:
When the user transacts online, the existing system does not contain any additional password security. She/he does not provide any additional information for online payment. Proposed system involves the users to authenticate themselves using their personal mobile phones. The Two factor authentication using mobile phone system could not replace the existing authentication system, but instead serves as an added layer of security that protects and enriches the existing authentication system.

4. Proposed System:
The proposed system allows user or customer to use a personal password to confirm his identity and providing greater reassurance and security. The proposed method guarantees that authenticating to systems, such as online banking. The proposed system involves a mobile phone for generating One Time Password. The generated password is valid for only short period of time and is generated by factors that are unique for both, server and mobile device itself. We proposed a secure, convenient and user friendly two factor authentication using mobile phone scheme and discusses its application to online banking.

To meet the user requirements, the proposed system incorporates the following features:

--In this proposed system specifically the example of online banking is taken to represent the online transaction. After the entering the details of transaction he user can select the mode of transaction connection oriented or connectionless.

--After selecting connectionless mode of transaction, user will generate OTP on his/her android mobile phone. And providing that OTP to system to complete transaction.

--When OTP is CORRECT i.e. generated on mobile phone and generated at server side are both match then transaction will be succeed otherwise it will be denied.

--If user doesn’t have android mobile phone then user will select the connection oriented system. Where OTP is directly send to user mobile phone by server. This OTP is any random string generated by server.
5. System Design:

![Proposed System Flow](image)

**Figure 2**

1. Here first client visits to banks website to make transaction. Login using username and password.
2. If username and password are correct then bank grant the permission to client and user able to access his/her account.
3. Client fills all the transaction detail and proceeds to next page.
4. Here client choose the mode of transaction. i.e. Connectionless to generate own OTP or Connection oriented to ask server to send OTP on his/her mobile phone.
5. After selecting connectionless mode user generates his/her own OTP on their android based mobile phones. Using unique parameters such as User ID provided by bank, DOB, Your mobiles ISMI number, and ATM pin number and most important factor i.e. Date and Time.
6. Client use this OTP to complete their transaction.
7. As soon as OTP reach to the server, server starts generating OTP using same parameters available at server. If both OTP gets match then transaction will be completed otherwise it will be denied.
6. **Features:**
   - It is not depends upon users mobile network.
   - It is easy to use, secure and cheap
   - It could not replace the existing authentication system, but instead serves as an added layer of security that protects and enriches the existing authentication system.

7. **Requirement Specification:**

   7.1. **Software Requirements:**
   - Operating System : Windows 7
   - Language : JAVA
   - Front End : Servlet/Swing
   - Back End : MySQL
   - Web server : Glassfish/Apache Tomcat
   - Builder Tool : MyEclipse

   7.2. **Hardware Requirements:**
   - Main Processor : Intel Core 2 Duo
   - Ram : 512 Mb Ram
   - Mother Board : 945gvm Intel Chipset
   - Hard Disk : 80GB
   - Monitor : 17” Color Monitor
   - Keyboard : Standard 102 Keys
   - Mouse : Optical mouse

8. **Conclusion:**
Two factor authentication systems is a user-friendly package and requires little prior knowledge of software. The system is highly flexible and is well efficient to make easy interactions with the database. The proposed system has two option of running, either using a free and fast connection-less method or a more expensive SMS-based method. Both methods have been successfully implemented and tested, and shown to be robust and secure. The goal of computer security to maintain the integrity, availability and privacy of information entrusted to the system was successfully obtained.
References:

1. Fadi Aloul, Syed Zahidi, Wassim El-Hajj, "Two Factor Authentication Using Mobile Phones"
3. Anders Moen Hagalisletto, Arne Riiber, "Using the mobile phone in two-factor authentication".
5. Qinghua Li, Student Member, IEEE, and Guohong Cao, Fellow, IEEE "Multicast Authentication in the Smart Grid With One-Time Signature"IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011.
6. DATA SHEET Two-Factor Authentication Made Easy"www.duosecurity.com"
7. Tomáš Rosa "The Decline and Dawn of Two-Factor Authentication on Smart Phones", INFORMATION SECURITY SUMMIT 2012