A Survey on Securing OTP Using Steganography Technique

Mrs A. Sarkunavathi M.Tech[1], S.LingeshKumar[2], L.Muralidharan[3], P.Vasudevan[4]

[1]Assistant Professor, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Pondicherry,
[2] Student, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Pondicherry,
[3] Student, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Pondicherry,
[4] Student, Department of Information Technology, Sri Manakula Vinayagar Engineering College, Pondicherry.

ABSTRACT:

Mobile banking is another plan for bank clients to perform banking exchanges. This paper describes the security shortfalls of the current mobile banking solution and it analyses the possible attacks (both passive and active) on the current SMS banking solution. Another protected SMS informing convention is intended to offer better security for SMS banking. When the OTP messages uses an unencrypted medium to deliver these credentials of authentication ATM fraudsters affects around 100 peoples every day. The client need to give the subtleties during the enrolment procedure and the pictures will be likewise chosen during the hour of enlistment and during the exchange process to be done based on the images selected the admin provides steganography on the given images and the user need to select the original image and if the image that is applied is right scientific articulation and client further proceeds with the accompanying exchange process by producing his one-time password (OTP) and transaction is successful. To improve the security of replacing the traditional security measures by including the concept of internet. These rounds increase security and hence difficult to break the encryption of the image.

Index Terms: **Steganography, Online Banking, OTP, Encryption, Transaction.**

I. INTRODUCTION

A client verification is a procedure to demonstrate that whether a specific client is approved to utilize an objective help or framework. There are different client confirmation techniques, for example, information based verification, proprietorship based confirmation and property based verification. Among them, information based verification is broadly utilized nowadays, for example, ID/PASSWORD in many sites or administrations. However, the password is maybe predictable because it should be easy for users to memorize. In this way, a foe could get the passwords of clients. A Two-Factor Authentication (TFA) can be utilized as a counter measure to this shortcoming. Particularly, OTP (One-Time Password) convention is most generally utilized for TFA with users′ ID/PASSWORD. OTP verifies clients by looking at two OTP values[3].

One of them is generated by authentication server and the other is generated by clients. OTP has a few vulnerabilities against MITM (Man-in-the Middle) assault and MITPC/Phone (Man-in-the-PC/Phone) assault. In the OTP calculation, a server and the customers share some mystery data in an introduction procedure. If an adversary takes some secret information by MITM attack, he also can generate valid OTP value and then may be successfully authenticated. Then again, in the event that a foe embeds a pernicious code in client's gadgets, at that point he can get to authorization to gadget memory and can produce OTP values as in above scenario.

When the algorithm that is secure against these two attacks[6], the proposed algorithm transforms a challenge value to a captcha image file to prevent MITM attack, uses IMSI number in SIM card of mobile device, and limits the accessible time of an assault by sending OTP directly after it is created to forestall MITPC/Phone assault. We examine their proposed calculation is secure against MITM assault and MITPC/Phone assault as contradict to the next OTP calculations. The security level of the secret key is adequate to twofold the security in a record and the login procedure, since every secret key OTP is just substantial once and if you do any mistake, the code generated from the website will change anyway. The timeframe of the secret word's life expectancy is 180 seconds, an opportunity to break the OTP secret key in proportion is 166 = 16,777,216 prospects in a solitary contribution of passwords[4].

II. RELATED WORKS

A. OTP Authentication Methods:

1) Time Synchronization:

The time synchronization is the most general authentication method. At the point when a client needs to be confirmed by the server, every one of them utilizes the common mystery key and the time data to make an OTP esteem. At the point when the customer makes and sends OTP incentive to the server, the server makes OTP esteem by using a similar calculation utilized in the customer side and checks whether two OTP values are the same or not. On the off chance that the two OTP values are the equivalent, at that point the client can be effectively verified. The major strength of time synchronization is that a communicational overhead can be considerably reduced if a client and a server are already synchronized with time and share a secret key[5]. However, it also has weakness that it could not successfully authenticate the user if the synchronized time between two parties is not accurate. Therefore, in time synchronization, the OTP esteem is legitimate for just a brief timeframe. After this period, the OTP worth will be changed.

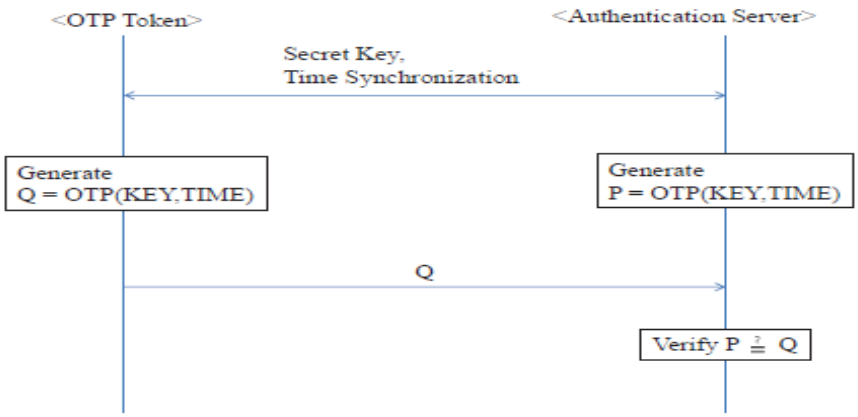

Fig.1. The Authentication Process in Time Synchronization

2) Challenge-Response Authentication:

A challenge response authentication makes a server authenticate users using the challenge values. A server and a customer share a mystery key before confirmation. At the point when a client needs to be verified, the server produces a test esteem and sends it to the customer. The server and the customer at that point produce the OTP esteems simultaneously by using a similar calculation as a contribution of the test esteem and the mutual mystery key[7]. The challenge-response authentication is relatively secure since the server generates a different challenge value each time when the clients attempt to be authenticated. However, it is vulnerable to communication attack when the challenge values are disclosed. Moreover, the server and the clients should more frequently communicate than in time synchronization method.

3) Event Synchronization:

In occasion synchronization, a server and a customer share a mystery key and an include an incentive in an introduction procedure. The check esteem is the quantity of the verification. At the point when a client needs to be validated, the customer builds the check by 1 and creates OTP esteem with the tally esteem and the common mystery key. The customer sends the created OTP incentive to the server from that point. The server builds the tally by 1 and produces an OTP esteem. At that point he checks whether received OTP esteem and created OTP esteem are the equivalent or not. The count values of both server and the client should be same for successful authentication[4]. This method has a problem that if the client generates OTP value but does not pass it to the authentication it will be failed because of different count values of the server and client.

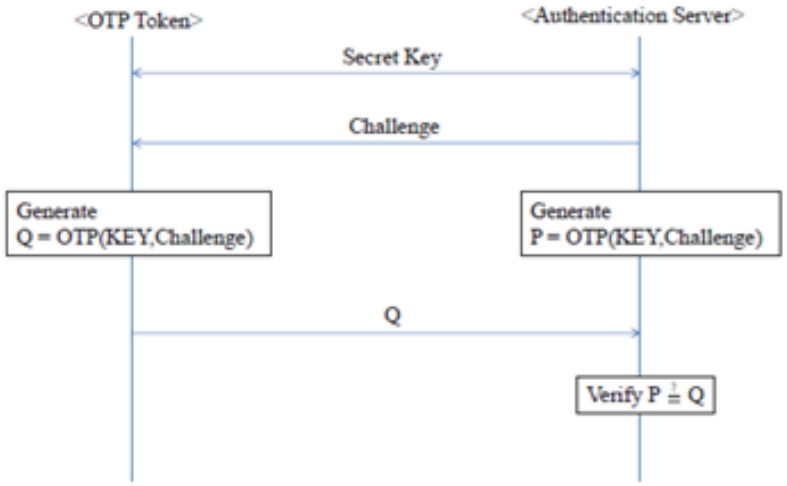

Fig.2. The Authentication Process in Challenge-Response Authentication.

4) S/Key Authentication:

A S/Key authentication makes OTP values by using a hash function. The authentication process is as follows. First, a server and a client share a secret key. The shared secret key then becomes an input value to the hash function. The server and the client generate first hash value by using this secret key. The first hash value becomes an input value to second hash function. In the client side, the N hash values are stored in the client storage while the server. When the user tries to be authenticated, sends $(N-1)^{th}$ hash value to the server. Then the server generates hash value with the received $(N-1)^{th}$ hash value[3]. The server checks whether the N^{th} hash value which has been stored in the server side is the same as the generated hash value. If the authentication is successful, the server stores $(N-1)^{th}$ hash value and deletes the previous N^{th} hash value. And then he sends to the client a message indicating the client is successfully authenticated.

5) The TOTP Algorithm:

The OTP verification technique can be isolated into two classes in portable condition: SMS-based validation and application-based confirmation. However, the SMS-based authentication cannot guarantee the data confidentiality. So they adopt the application based authentication[10]. The previous OTP authentication is divided into four categories (i.e. time synchronization, challenge-response authentication, and event synchronization). They combine the time synchronization and challenge-response authentication in their proposed scheme. If an initialization process is already done, the other three authentication methods need not send some secret parameters when a user requests an authentication. But in challenge-response authentication, even if the initialization process is done, a server has to send the challenge value which is different at each time, so it can improve security. So it is based on challenge-response authentication to generate random numbers (i.e. challenge value) while using time synchronization. By time synchronization, if a user does not enter the challenge value in 60 seconds, the server sends new challenge value to the user.

6) Image Data Transmission Traffic:

The time synchronization method will not occur any data exchange after the initialization process, until a user requests an authentication. When a user requests an authentication, a client delivers an OTP value to the server. In challenge response authentication method, the challenge value is delivered from a server to a client when a user wants to be authenticated. After that, the client sends generated OTP to the server[3]. In S/Key authentication method, a server and a client share a secret key in an initialization process, and when a user requests an authentication, the client sends a hash value to the server[5]. In the event that the confirmation is finished, the server communicates something specific that advises a fruitful validation to the customer. In occasion synchronization strategy, a server and a customer share a mystery key in an introduction procedure and when a client needs to be verified, the customer conveys the OTP value to the server. A client sends IMSI number of mobile device to a server in an initialization process and then, when a user requests an authentication, the server sends a challenge value as an image file. The client sends generated OTP value to the server. In this authentication method, in contrast to the other methods, because the server sends image files, the communication cost would be larger (e.g. 15KB for an image file). However, considering the request for an authentication is not so frequent, it could be acceptable in practical applications. The data transmission traffic of each authentication scheme is analyzed in Table I.

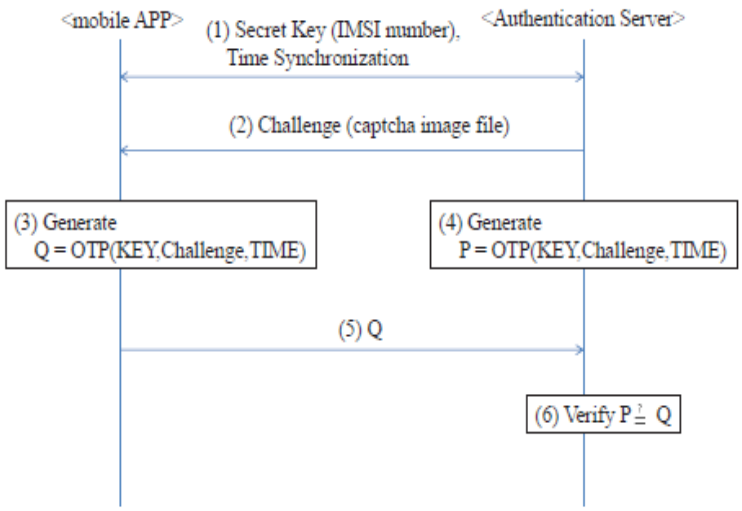

Fig. 3. The Authentication Process in the OTP Algorithm.

III. SECURITY EVALUATION AND ANALYSIS

A. Security Analysis for MITPhone Attack:

The MITPhone attack is very powerful attack in that an adversary can access to any memory space of target devices and can read, write or transmit the data from the memory. If any malicious code is installed in user′s mobile device, the OTP generation algorithm and a secret key would be disclosed, then it can be possible that an adversary is successfully authenticated by generating a valid OTP value himself. They use two methods to defense this attack, the primary technique is to utilize IMSI number as a mutual mystery key. The IMSI is a number that put away in SIM card of cell phone[2]. It is interesting an incentive for every cell phone and put away in SIM card so a foe who needs to peruse information from memory cannot realize this IMSI number. A client can use this IMSI number as a shared secret key of OTP algorithm by sending it to the server in the initialization process. The subsequent technique is to constrain the accessible time of MIT Phone assault. When a user requests an authentication, the server sends challenge value as a form of image file to the client. Even though an adversary has control over the memory of user′s mobile device, they cannot know the challenge value before the user enters it from the QR image. When the user enters the challenge value and clicks ′Send′ button, the client generates an OTP value with the time stamp value, challenge value and IMSI number and at the same time sends the generated OTP value to the server. This can considerably limit the available time of MITPhone attack[9] . The attack must be complete within the time to generate an OTP value in user′s mobile device and the time to transmit the OTP value to the server. However, the adversary should also have time to generate the OTP value and time to transmit it to the server. For this reason, the available time of an attack will considerably be limited.

B. Security Analysis for MITM Attack:

They use a captcha image file as a counter measure to MITM attack. The captcha is an image that only human can read. It has some visually distorted characters such as alphabet or number. It prevents any program from reading the contents of image automatically by ′image processing.′ An adversary who uses MITM attack can read transmitted data between a server and a client. However, if an important data are transmitted as a form of a captcha image file, the adversary could not read the data automatically by using his program. The main idea of this scheme is that a server delivers a challenge value to the client as a captcha image file. The server stores the captcha images generated using digit numbers of from 0 to 9 in the servers database[3] . When the server generates a challenge value, it transforms the each digit to the captcha image files, and then the server combines them to one integrated image file and passes it to the client. The server stores many different captcha images of each digit. It randomly chooses one of the captcha images when it transforms one digit to a captcha image file. So, although an adversary gets a challenge value, so cannot automatically read it by image processing.

TABLE II. THE SECURITY ANALYSIS

	Security against MITM attack	Security against MITPhone attack
OTP Algorithm	O	△
Time Synchronization	△	X
Challenge-Response Authentication	X	X
S/Key Authentication	△	X
Event Synchronization	△	X

The **Table II** represents the security analysis of the attack.

The **Table I** represents the computational analysis of the authentication technique in secret key.

TABLE I. THE ANALYSIS ABOUT COMPUTATIONAL OVERHEAD

Authentication method	**Data transmitted from client to server**	**Data transmitted from client to server**	**Total data transmission traffic**
OTP Algorithm	IMSI number (initialization process),OTP(authentication process)	Challenge (authentication process, image file)	15KB
Time Synchronization	OTP (authentication process)	Secret Key (initialization process) Time Stamp (initialization process)	1 KB
Challenge-Response Authentication	OTP (authentication process)	Secret Key (initialization process) Challenge (authentication process)	1 KB
S/Key Authentication	OTP (authentication process)	Secret Key (initialization process) Data of successful authentication (authentication process)	1 KB
Event Synchronization	OTP (authentication process)	Secret Key (initialization process)	1 KB

Advantages of Steganography Technique:

- Puzzle redirecting and login process are the top of Puzzle technology, using mathematical problems. Image Puzzle Solving with AES Algorithm the most helpful in preventing the users from cybercrime by providing authorized access.
- Hiding Information is used to protect identities and valuable data from theft or unauthorized viewing by concealing the message within an unsuspicious image.

IV. LITERATURE SURVEY

I. Shaik Arshiya, B. Aruna, P. Guru Prasad, Ravi Kumar Tenali, "Steganography Security On Bank System" ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

They developing an application based on security as the rate of internet users are increasing and most of the users either use internet for money transaction and social media the rate of cybercrime is increasing rapidly and there is a need to secure bank system to prevent customer from cybercrime [1]. we have developed a three-tier architecture in which the concept of image steganography is inspired from google which checks whether it's a human or robot and all the data is applied with encryption and decryption. The customer need to provide the details during the registration process and the images will be also selected during the time of registration and during the transaction process to be done based on the images selected the admin provides steganography[5] on the given images and the user need to select the original image and if the image that is applied is correct then the puzzle is set up with mathematical expression and user further continues with the following transaction process by generating his one time password (OTP) and transaction is successful.

II. Hoyul Choi, Hyunsoo Kwon, Junbeom Hur Department of Computer Science and Engineering Korea University "A Secure OTP Algorithm Using a Smartphone Application" in 2015.

Several authentication protocols are being used in mobile applications. OTP is one of the most powerful authentication methods among them. Be that as it may, it has some security vulnerabilities, especially to MITM (Man-in the-Middle) assault and MITPC/Phone (Man-in-the PC/Phone) assault. An enemy could know a substantial OTP esteem and be validated with this mystery data within the sight of those assaults[8] . To take care of these issues, we propose a novel OTP calculation and contrast it and existing calculations. The proposed plot is secure against MITM assault and MITPC/Phone assault by utilizing a captcha picture, IMSI number implanted in SIM card and constraining accessible time of an assault.

III. Shally & Gagangeet singh aujla, "A Review of one-time password mobile verification" Vol. 4, Issue 3, Jun 2014.

Use of mobile phone is quite common in the modern day environment. With the increase in the facilities for the users of different sectors, data theft has also increased. To prevent the authentication process from the data theft, one-time password system is applied to various sector of the industry like if you are logging in into an account, you need a OTPK password to get verified that you are the authenticated user. In such a case the user must be registered to the network to get the OTPK password[5]. This paper focuses on the different aspects of OTPK and the ways of creation of this system. With all the made survey over here, it is concluded that the One-time password is a very important part in every sector of the industry. This paper concludes about the methods of creation of the one-time password generation system and effect of Trojans in the system.

IV. Havard Raddum, Lars Hopland Nestas, and Kjell Jørgen Hole, Security Analysis of Mobile Phones Used as OTP Generators" in 2015.

The Norwegian organization Encap has created conventions empowering people to utilize their cell phones as one-time secret word (OTP) generators. An underlying examination of the conventions uncovers minor security defects. Framework level testing of an online bank using Encap's answer at that point shows that few assaults permit a vindictive individual to transform his own cell phone into an OTP generator for another person's financial balance. Some of the suggested countermeasures to thwart the attacks are already incorporated in an updated version of the online banking system. A third party was responsible for integrating Encap's product into the evaluated online bank. The integration enables several practical attacks[4]. The described client-side malware and phishing attacks on the customer authentication in the online bank are possible because the defense against replay of old activation requests is insufficient, and because the link between the previously used OTP generator and the new phone-based OTP generator is too weak. Encap received an early version of this paper with recommendations to implement the suggested counter measures to thwart possible future attacks. The authors have since been informed that Encap and the third party have implemented some of the described countermeasures.

V. Dr.Ananthi Shesashaayee, D. Sumathy, "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security" Vol. 2, Issue 10, October 2014.

The improvement and headway in innovation makes the advanced PDAs and PDAs More complex. It has radically changed the manner by which we play out our m-banking exchanges. At the point when a customer starts a bank exchange, he is furnished with an OTP which is sent to his enrolled versatile number by means of SMS. The customer sends back the OTP inside a brief period to finish the exchange. The OTP SMS is produced by the bank server and is given over to the customer's portable administrator. To keep away from any potential assaults like phishing, man-in-the centre assault, malware Trojans, the OTP must be made sure about. So as to give a solid and secure method of online exchanges with no trade off to accommodation, a dependable m-banking validation conspire that joins the mystery PIN with encryption of the one-time secret word (OTP) has been created right now. The mystery PIN known distinctly between the customer and the bank is utilized for encoding the OTP. After the scrambled OTP SMS arrives at the customer's versatile, the PIN is utilized again utilized for decoding. The plain OTP content ought to be sent back to the bank will confirmed at the server to finish the exchange started. The mix of PIN with OTP gives verification and security[11]. The proposed plot gives security regardless of whether any questions emerge due any potential assaults like web hacking or versatile robberies.

VI. Mohsin karovaliyaa, Saifali karediab, Sharad ozac, Dr.D.R. Kalbande, "Enhanced security for ATM machine with OTP and Facial recognition features" in 2015.

The reason for this paper is to fortify security of the ordinary ATM model. They have placed another idea that improves the general understanding, ease of use and accommodation of the exchange at the ATM. Highlights like face acknowledgment and One-Time Password (OTP) are utilized for the upgrade of security of records and protection of clients. Face acknowledgment innovation encourages the machine to distinguish every single client interestingly in this manner making

face as a key. This totally dispenses with the odds of misrepresentation because of burglary and guile of the ATM cards Moreover, the arbitrarily produced OTP liberates the client from recollecting PINs as it itself goes about as a PIN.

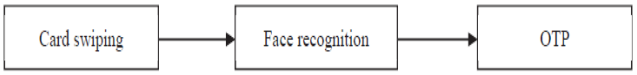

Fig.4. Flow of Model

VII. Manikandan, Kishore, Saran Kumar, Suriya, Vivek, "Enhanced Security for ATM Machine with OTP and Facial Recognition Features" in 2019.

They built up another idea that upgrades the general understanding, ease of use and accommodation of the exchange at the ATM. Highlights like face acknowledgment and One-Time Password (OTP) are utilized for the upgrade of security of records and protection of clients. Face acknowledgment innovation causes the machine to recognize every single client exceptionally consequently making face as a key[3]. This totally wipes out the odds of extortion because of burglary and guile of the ATM cards. This calculation. As per the measurements PCA based face acknowledgment is exact, requires less calculation time and less extra room. After the completion of the project we will collect the quantitative aspects of the model and compare it with the qualitative results for further proof.

VIII. Reshma Begum, Dr. Basavaraj Gadgay, Veeresh Pujari, Pallvi B.V, "Security of ATM System Using Biometric and OTP" Vol.5, Special Issue 4, June 2017.

The ATM card is increasing, in the present system pin number is used for ATM transaction security. which can be easily stolen, guessed or misused by many ways with this one can lose his money. This roused us to build client security by adding the biometric and OTP to the current framework. It likewise set forward certain issues which incorporate sensor solidness and time utilization. And some queries like user lose how much if his card is misused and to withdraw a low amount is it really admirable to go through the entire biometric process. As an answer we present a requirement on exchanges by ATM including biometric (unique finger impression) to improve the framework execution and to tackle[13]. They are including a cut-off measure of money, if the entered sum is more than the breaking point, it is important to introduce biometric. On the off chance that one has to pull back the base money, biometric examining isn't obligatory just will enter the OTP for client validation. It helps clients to spare time and keep up sensor execution by not outfitting their biometric for not many hundred separated from looking after security[13]. Here they are even maintaining the sensors performance along with saving user time when smaller transaction is performed by setting the limit on maximum cash withdrawal. When more cash is being debited only then we will check authentication using biometric. Along with this ATM system is also secured from the fraud attacks by using the tilt sensor and buzzer, if anybody try to move the ATM machine there will be buzzer alert.

IX. Mohammed Hamid Khan Shah and Anchor Kutchhi, "Securing ATM with OTP and Biometric" in 2015.

The need of cash must be fulfilled when you are conveying cash with you. That likewise builds the danger of getting robed. Bank is a most secure spot to keep cash. Bank gives Automated teller machine (ATM) which can give cash anyplace you need. ATM is a simple method to get cash, you simply need to embed card and secret phrase and you just got the cash. Be that as it may, consider the possibility that somebody will take your card and by one way or another he/she will know your secret phrase, it will give him/her full access to your cash[14]. That bring up issue on present security and requests something new in the framework that can give second degree of security. Once secret phrase (OTP) is secret key that approves a legitimate client for only one login to the separate framework. In the event that client is unapproved, framework won't permit further access. OTP can be created by utilizing distinctive cryptographic hash works that gives a fixed string which can be utilized as second level security at ATM. In age of OTP there are numerous components that can make OTP novel each time it is produced. Components that can be considered are time at when the client is getting to the machine, account number of the client, portable number of the client, Location of the client, International Mobile Station Equipment Identity (IMEI) number which is one of a kind for each cell phone. By thinking about elements like day by day life issue (general issues) that is telephone got turned off, battery is down; less inclusion of system can influence the OTP arrangement and so forth. To keep away from application based issue this report likewise propose an answer for example biometric security; by utilizing biometric security the elective security will be as same as OTP.

V. CONCLUSION

From the above survey work, it is concluded that by using the above algorithms and the steganography encryption technique for hiding the OTP message in order to provide more security. The designed protocol provides an end-to-end security communication from the client and server side. An OTP is the major threats for user so providing more security to protect it through encryption by steganography method to ensures more security.

REFERENCES

[1] Dr. AnanthiShesashaayee, D. Sumathy "OTP Encryption Techniques in Mobiles for Authentication and Transaction Security", Vol. 2, Issue 10, October 2014.

[2] Havard Raddum, Lars Hopland Nestas, and Kjell Jørgen Hole "Security Analysis of Mobile Phones Used as OTP Generators", Department of Informatics, University of Bergen in 2010.

[3] Hoyul Choi, Hyunsoo Kwon, Junbeom Hur "A Secure OTP Algorithm Using a Smartphone Application", 978-1-4799-8993-5/15/ 2015.

[4] Manikandan, Kishore, Saran Kumar, Suriya, Vivek "Enhanced Security for ATM Machine with OTP and Facial Recognition Features" in 2019.

[5] Mohammed Hamid Khan Shah and Anchor Kutchhi "Securing ATM with OTP and Biometric", ISSN: 2321-8169 -2041 - 2044, Volume: 3 Issue: 4 ,2015.

[6] Mohsin Karovaliyaa, Saifali Karediab, Sharad Ozac, Dr.D.R. Kalbanded "Enhanced security for ATM machine with OTP and Facial recognition features", ICACTA-2015.

[7] Reshma Begum, Dr. Basavaraj Gadgay, Veeresh, Pujari, Pallvi B.V "Security of ATM System Using Biometric and OTP", Vol.5, Special Issue 4, June 2017.

[8] Shaik Arshiya, B. Aruna, P. Guru Prasad, Ravi Kumar Tenali "Steganography Security On Bank System" ISSN: 2277-3878, Volume-8, Issue-1, May 2019.

[9] Shally & Gagangeet Singh Aujla "A Review of One Time Password Mobile Verification", ISSN(P): 2249-6831; ISSN(E): 2249-7943, Vol. 4, Issue 3, Jun 2014, 113-118.

[10] S. Chiasson, "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Computer Security, 2007, pp. 359–374.

[11] Secure internet banking authentication,"A.Hiltgen, The IEEE Security and Privacy, vol. 4, no. 2, pp. 21–29, 2006.

[12] Chang-Lung Tsai, Chun-Jung Chen." Trusted M-banking Verification Scheme based on a combination of OTP and Biometrics ", Journal of Convergence Vol 3, No. 3,23-30, September 2012.

[13] K. Rieck, P. Stewin, and J.-P. Seifert ,"SMS-Based One-Time Passwords: Attacks and Defense" DIMVA 2013, LNCS 7967, Springer-Verlag Berlin Heidelberg 2013,pp. 150–159, 2013.

[14] RupinderSaini, Narinder Rana,Rayat 'Comparison of various biometric methods', Institute of Engineering and IT, International Journal of Advances in Science and Technology (IJAST) Vol 2 Issue I.

[15] Dr.D.S. Rao et. al.," One Time Password Security through Cryptography for Mobile Banking", International Journal of Computer Technology and Applications, Sept-Oct 2011