IJRRECS/October 2013/Volume-1/Issue-6/941-951 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

ONE TIME PASSWORD APPLICATION BY USING ANDROID MOBILE

K.Sai Ashritha[1], P.Pavan Kumar[2]

[1]M.Tech Student, Dept of CSE, CMR Institute of Technology, Hyderabad, A.P, India

[2]Assistance Professor, Dept of CSE, CMR Institute of Technology, Hyderabad, A.P, India

ABSTRACT:

People have downside memory multiple passwords. This results in reduced security as users utilize the same countersign for varied systems or reveal totally different passwords as they struggle to log in. It can also cause reduced privacy, as users might suppose centralized services to manage their passwords. Currently security concerns unit of measurement on the rise altogether areas like banks, governmental applications, attention business, military organization, tutorial institutions, etc. Government organizations unit of measurement setting standards, passing laws and forcing organizations and agencies to befits these standards with non-compliance being met with wide-ranging consequences. There unit of measurement several issues once it involves security concerns in these varied and locomote industries with one common weak link being passwords. Most systems currently suppose static passwords to verify the user's identity. However, such passwords consort with major management security concerns. Users tend to use easy-to-guess passwords, use the same countersign in multiple accounts, write the passwords or store them on their machines, etc. moreover, hackers have the selection of using many techniques to steal passwords like shoulder surfing, snooping, sniffing, guessing, etc. one altogether these utilizes backward hash chains to come back up with associate OTP for authentication functions. Applying the various from one perform to a particular seed removes the necessity of inflicting SMS-based OTPs to users, and reduces the restrictions caused by the SMS system.In this paper we also use OTP for credit card transactions. when ever the credit card is used by the owner he/she will be receiving an OTP to his mobile(registered phone number) and then the transaction is done only if he/she keyin that received otp manually in the swipe machine.

Keyword: Long term password, online website security, Android application.

1. INTRODUCTION:

Authentication is a Greek word which means the act of conforming an act of truth of a data or an entity. The purpose of the user authentication is to secure their data from thefting by the third party. Authentication is any protocol or process that permits one entity to establish the identity of another entityGenerally authenticated fall into three categories, based on what are known as the factors of authentication: something the user knows (knowledge), something the user has (ownership), and something the user is (inherence).

Basic login authentication process steps as follows:

1. A client requests access to a protected resource.
2. The web server returns a dialog box that requests the user name and password.

3. The client submits the user name and password to the server.

4. The server validates the credentials and, if successful, returns the requested resource.

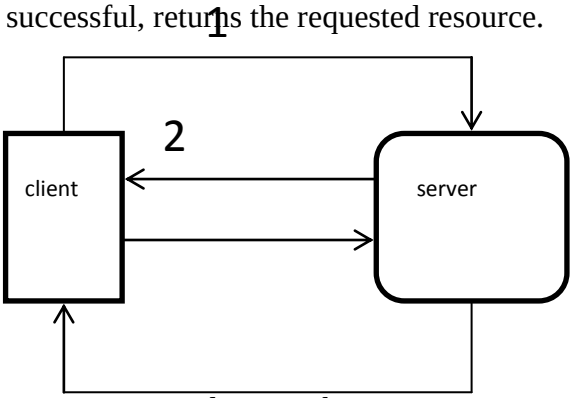

Figure: 1 Basic login authentication process

Authentication is a fundamental aspect of system security. It confirms the identity of any user trying to log on to a domain or access network resources. Text password is the most popular form of user authentication on website due to its convenience and simplicity. Passwords are prone to be stolen under different threats and vulnerabilities. Hence an authentication protocol which protects the user(s) password from various threats has been used. There are two basic authentication types they are non-reputable (proof of origin cannot be denied are biometrics, retinal images) and repudiable.

There are different methods of authentication they are digital signatures, one-time password and public key cryptography etc., and different protocols used by the authentication are secure remote password protocol(SRP),authentication and key agreement(AKA),extensible authentication protocol(EAP),Kerberos.

Day by day the usage of internet is increasing rapidly and also the numbers of threats or attacks are increasing to avoid this Many new techniques for authentication have been introduced one among them is one time password method.

The goal of authentication is to identify and verify that the user has the access to the particular system. In this survey on user authentication we discuss different authentication techniques and how to protect our passwords from stealing to some extent using an authentication method called one time password. The remainder of this paper is organized as follows: Section a pair of discusses the connected work, Section three scientific method, Section four analyzes the protection attributes, Section five assesses our scheme's performance, and at last Section half dozen concludes the paper.

II.RELATED WORK:

B.Ives et al. [1] proposed an alternative security schemes. This is done by both public and private keys In public-key encryption (PKE) the user is authenticated by the private key used to encrypt a message to the server. While similar to a password,

the private key has two structures that increase its security.

1. The private key is stored on a client computer or smart card and can be of considerable length, thus eliminating the need for the user to memorize the code while also avoiding the possibility of the user generating an easy to guess code.
2. The server verifies the code by correctly decrypting certain information sent by the client rather than comparing to a password file thus eliminating any server-side storage of password(s), encrypted or not.

However, a user's private keys must be protected on the client side, thus changing the location of a potential theft.

Public-key infrastructure (PKI) uses PKE to authenticate users across a number of different applications or systems and also it allow a user to have a single private key that can be used across some or all of the user's needs, simplifying key management for the user. In this situation, loss of the user's private key can make several or all of the user's systems vulnerable in a similar way as when a user chooses the same password to enter for multiple systems. However, in this case, greater prominence may be placed on making sure the system is difficult to penetrate with responsibility for the key remaining in the hands of the user. Further, a method of centrally revoking a key can be put in place so that a stolen key can be quickly disabled for all systems. And the significance of this method is it eliminates the need for the user to memorize the code while also avoiding the possibility of the user generating an easy to guess code and the PKI systems are so difficult to use and so poorly implemented, they are usually viewed as vain.

S. Gawandet al. [2] discussed a survey of how users manage passwords for online account(s), password practices, quantifying password reuse and also surveying the contributing factors to this reuse. Technical solutions for online password management can improve practice and without significantly changing user behavior. This is in contrast to alternatives for traditional authentication systems. These alternatives might rely on the user having a particular device such as a cell phone or a physical token such as a smart card. When users access website accounts, they already have their hands on a computer. We can develop systems at the application level or at the browsers especially instead of at the device level. The mainly claim that from a practical point of view is the extent of password reuse and it is likely to become more problematic over time as people accumulate more accounts and having more accounts implies more password reuse.

D. Florencio et al. [3] approach is a better means to address bulk attacks. Here the combined size of the user ID plus password key-space is considered rather than the password key-space alone that protects large institutions against bulk guessing attacks.

It reduces the number of break-ins that an attacker with fixed resources can expect, and reduces the burden on users but there is selection bias: we have data only from users who downloaded the toolbar. These users can be expected to be far more active than the general web using population.

Jermyn et al. [4] proposed evaluate new graphical password scheme that exploit features of graphical input displays to achieve better security than text based passwords. Here we are primarily motivated by devices such as personal digital assistants (PDAs) that offer graphical input capabilities via a stylus, and prototype implementation of one of our password schemes on such a PDA, namely the Palm PilotTM. Therefore, it is more secure compared to text based passwords. But here in this method it requires more space and the

server needs to store the seeds of the portfolio images of each user in plain text. Also, the process of selecting a set of pictures from the picture database can be tedious and time consuming for the user.

S.Chiasson et al. [5] discussed on multiple passwords using text and also click based graphical passwords. However, people generally have difficulty in remembering multiple passwords and also there is a possibility of users reuses the same password for different systems or reveals other passwords as they try to log in. So multiple click based passwords are used in order to avoid the problems of multiple text based passwords which are easy to remember or recall and click-based graphical passwords were significantly less susceptible to multiple password interference in the short-term, while having comparable usability to text passwords in most other respects. Here there is an offset by the graphical passwords' built-in memory cue, which is a more secure memory aid than users.

Perrig et al. [6] proposed a novel method to apply hash visualization to improve the real-world security of root key validation and user authentication. In order to improve the security of the systems is to use hash visualization, a technique which replaces meaningless strings with structured images. Here we analyze two human limitations:
1.Difficulties people have with remembering strong passwords and personal identification numbers (PIN).
2. Secondly with comparing meaningless strings. We use hash visualization to generate images from the strings, and the user can simply compare the images instead of the strings. This is image recognition which is easy compared to exact string recall and all the images generated by Random Art are regular, is firm.

H.Krawczyk et al. [16] discussed how cryptography is used in today(s) internet for implementing a secured channel between two end points and then exchange information over that channel. Typical implementations first call a key-exchange protocol for establishing a shared key between the parties, and then use this key to authenticate and encrypt the transmitted information using (efficient) symmetric-key algorithms. The three most popular protocols that follow this approach are SSL (or TLS), IPsec and SSH. And significances are it is easy and fast to implement but it has too many keys, a new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys and loss of private key is irreparable.

S.Garfinkel et al. [17] proposed a method where people increasingly rely on public computers (e.g., Internet kiosks) to do business over the Internet. But accessing today's web-based email, online auctions, or banking sites invariably requires typing a username and password to prove one's identity to the remote service. This creates significant security vulnerability since the user's password can be captured by the computer and later reused by a hostile party. In order to avoid this we use a mobile phone as a hand-held authentication token, and a security proxy which allows the system to be used with unmodified third-party web services. Firstly, a user (U) that wishes to use an Internet kiosk (K) to access a remote service (R) requiring authentication would instead connect to the trusted security proxy (P). The proxy mediates all aspects of the user(s) communication with the remote service, stores username and password and can use credentials to log in to R. P also stores a mobile phone number for each user.

And it creates a system that is both secure and highly usable.

A. Graphical Passwords:

We study the impact of selected parameters on the scale of the secret house for "Draw-A Secret" (DAS) graphical passwords. we have a tendency to examine the role of and relationships between the amount of composite strokes, grid dimensions, and secret[7] length within the DAS password house. we have a tendency to show that a awfully important proportion of the DAS secret house depends on the belief that users can select long passwords with several composite strokes. If users select [17]passwords having four or fewer strokes, with passwords of length twelve or less on a five × five grid, rather than up to the utmost twelve doable strokes, the scale of the DAS secret house is reduced from fifty eight to forty bits. in addition, we have a tendency to found an analogous reduction once users select no strokes of length one. To strengthen security, we have a tendency to propose a way And describe a representative system that will gain up to sixteen additional bits of security with[8] an expected negligible increase in input time. Our results are often directly applied to work out secure style decisions, graphical secret parameter pointers, and decide that parameters be focus in graphical secret user studies.

B. Purely Automated Attacks

We introduce and appraise varied strategies for strictly automatic attacks against Pass Points vogue graphical passwords. For generating these attacks, we have a tendency to introduce a graph-based rule to with efficiency produce dictionaries supported heuristics like click-order patterns (e.g., five points right along a line). a number of our strategies mix click-order heuristics with focus of- attention scan-paths generated from a process model of visual attention, yielding considerably higher automatic attacks[13][14] than previous work. One ensuing automatic attack finds 7-16% of passwords for 2 representative pictures mistreatment dictionaries of roughly 226 entries. quiet click-order patterns well accrued the attack effectualness albeit with larger dictionaries of roughly 235 entries, permitting attacks that guessed 48-54% of passwords (compared to previous results of a hundred and twenty fifth and Sept. 11 on a similar dataset for 2 pictures with 235 guesses). Our results show that automatic attacks, that area unit easier to rearrange than human-seeded attacks and area unit additional ascendible to systems that use multiple pictures, cause a major threat to basic PassPoints-style graphical passwords.

C. Password Management Strategies

Given the widespread use of watchword authentication in on- line correspondence, subscription services, and looking, there's growing concern regarding fraud. once folks recycle their passwords across multiple accounts, they in- crease their vulnerability; compromising one password[2] will facilitate AN wrongdoer take over many accounts. they often didn't understand that customized passwords like phone numbers are often cracked given an outsized enough wordbook and enough tries. we have a tendency to discuss however current systems support poor watchword practices. we have a tendency to conjointly gift potential changes in web site authentication systems and watchword managers.

D. A Large scale Study Of Web Password Habits.

We report the results of an oversized scale study of countersign use and countersign re-use habits. The study concerned 0.5 a mil- lion users over a 3 month amount. A consumer part on users' machines recorded a range of countersign strength,\ usage and frequency metrics. this permits North American country to live or estimate such quantities because the average variety of pass- words and average variety of accounts every user has, what number passwords she varieties per day, however typically passwords[3] area unit shared among sites, and the way typically they're forgotten. we tend to get extraordinarily elaborate knowledge on

countersign strength, the kinds and lengths of passwords chosen, and the way they vary by website. the information is that the giant scale study of its kind, and yields varied different insights into the role the passwords play in users' on-line expertise. We have extended Lamport's plan with some Modifications so as to provide unboundedness and cockiness, avoiding the employment of public key cryptography. The defect of these 2 parameters, unboundedness and cockiness, cause the many vulnerabilities shown with regard to the connected work.

A.Registration Phase:

The aim of this part is to permit a user and a server to barter a shared secret to certify succeeding logins for this user. The user begins by gap the authentication program put in on her cellular phone she enters IDu (account id she prefers) and IDs (usually the web site uniform resource locator or domain name) to the program. The mobile program sends account id and uniform resource locator to the telecommunication service supplier (TSP) through a 3G affiliation to form an invitation of registration. Once the TSP received the account id and also the uniform resource locator, it will trace the user's number supported user's SIM card. The TSP additionally plays the role of third-party to distribute a shared key between the user and also the server. The shared key's accustomed encipher the registration SMS with AES-CBC. The TSP and also the server can establish associate degree SSL tunnel to guard the communication. Then the[6] TSP forwards account id, and to the assigned server. Server can generate the corresponding data for this account and reply a response, together with server's identity ID, a random seed, and server's number. The TSP then forwards id, and a shared key to the user's cellular phone. Once reception of the response is finished, the user continues to setup a long-run arcanum along with her cellular phone.

B.Login phase:

This section can discuss the login and authentication method between the user and repair supplier. The steps below ar shown in Fig. 3. The user logs in to the service provider's web site, e.g., a web bank, requesting access. As a response to the current access request, a secure session is established, i.e., associate SSL session, permitting the user to enter his authentication privileges, i.e., user name and password are the primary issue of authentication, what the user is aware of. additionally the user provides the server together with his OTP's current standing. this standing permits the server to synchronize his seed with the client's current seed to induce identical seed worth on either side before causation a challenge.

The server haphazardly challenges the user with new indexes. The user enters those indexes, in his OTP generator to induce the corresponding OTP. The user responds with this corresponding OTP. The server compares the received OTP with the calculated one.

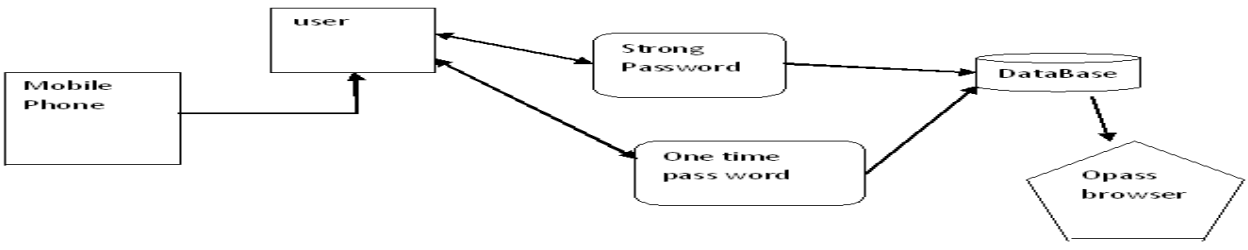

Figure 1. Authentication Protocol Architecture

According to the server check, tired the previous step, the server can transfer associate degree authorization execution or a communication termination.

C.Recovery Phase:

Recovery part is selected for a few specific conditions; as an example, a user could lose her mobile phone. The protocol is ready to recover authentication setting on her new mobile phone presumptuous she still uses constant number (apply a replacement SIM card with previous phone number). Once user installs this authentication program on her new mobile phone, she will be able to launch the program to send a recoveryrequest together with her account ID and requested server ID to predefined TSP through a 3G association. This message Procedure of recovery part. Includes all necessary components for generating future one-time passwords to the user . once the mobile program receives the message, like registration, it forces the user to enter her semipermanent parole to breed the proper one-time parole. throughout the last step, the user's mobile phone encrypts the key document and server present to a cipher text. The recovery SMS message is delivered back to the server for checking. Similarly, the server computers and decrypts this message to make sure that user is already recovered. At now, her new mobile phone is recovered and prepared to perform any logins. For future login, one-time parole are used for user authentication.

D.GSM Modem Implementation

GSM electronic equipment could be a specialised form of electronic equipment that accepts a SIM card, and operates over a subscription to a mobile operator, a bit like a portable. From the mobile operator perspective, a GSM electronic equipment appearance a bit like a portable. importation the comm Driver and connecting the electronic equipment to the computer with port.

F.Numerical Illustration:

Through the registration method, the user gets 2 totally different hash functions, e.g., hA , that might be SHA-1, and hB , that might be MD5 , together with Associate in Nursing initial seed, "sint ," because the concatenation of the IMEI, IMSI, and registration time, that might be "123456789123456123456789123450701201020025 9" forward IMEI is "123456789123456," IMSI is "12345678912345," and also the registration time is "1/1/2013 20:02:59." subsequently the server sends a random challenge worth of recent indexes, e.g., x, y = 3, 4 , which implies the user needs to calculate his session OTP victimisation this formula: 6860606117791918852336381360201633315 8 . chain by hour angle. conjointly as indicated in it's not admittable for x nor y to beuptozero.

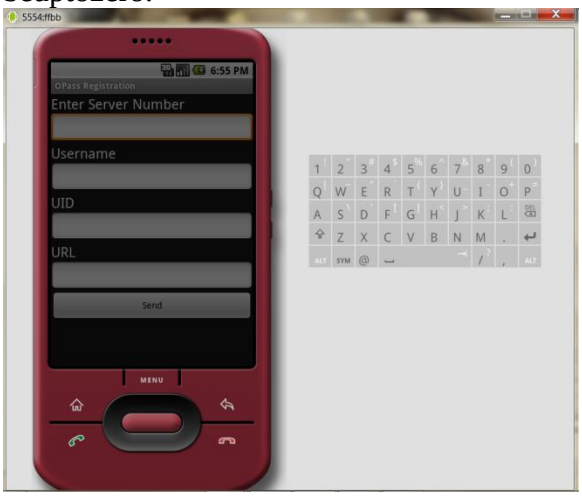

Figure 2. Login Phase

a.One Time Password:

One-time Passwords ofter well understood security enhancements over existing word systems. Our projected theme gets the

superb protection enjoyed by users of existing OTP systems to all or any users. we have a tendency to want to be clear that we are going to have constant security and usefulness queries that arise with alternative OTP systems. not like standard registration, the server requests for the user's account id and signal, rather than word. once filling out the registration type, the program asks the user to setup a long-term password. This long-term password is used to generate a chain of one-time passwords for further logins on the target server.

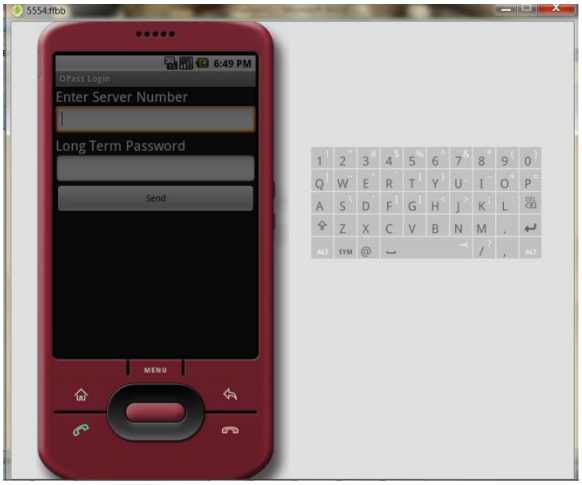

Fig-2(a) Ont Time Password.

Then, the program mechanically sends a registration SMS message to the server for finishing the registration procedure. The context of the registration SMS is encrypted to supply information confidentiality. User authentication conjointly designed a recovery section to mend issues in some conditions, like losing one's mobile phone.

IV. Security Analysis

Security Schemes: It is often aforesaid that whereas planning the GSM system, it had all security measures in mind, however as time passed and algorithms were cracked by the hackers, SMS-OTP based mostly systems weren't unbroken secure. Despite the apparent high prices and therefore the given limitations of word security systems in phone (Fig 1), we have a tendency to believe it's imperative that e-commerce security systems move efficiently to either increased word security systems or various security schemes like sensible cards or biometry. whereas there ar varied alternatives to word security systems, every involve tradeoffs. Among the issues ar the price to implement, the time needed to use, any special issues relating to place of use (for example, should it's from a specific computer), ability to[10] amendment the theme if it's compromised, physical limitations, health issues (for example, a fingerprint reader on a public site), non-interchangeableness, time sealed, and so on. it's on the far side the scope of this text to totally explore every of those alternatives and their limitations. However, the most categories of other technology ar mentioned to demonstrate their potential.

Pre-Play Attack

Unless the challenge is protected, a kind of "suppress replay attack," called a "pre-play attack," becomes potential. take into account that Associate in Nursing unwelcome person, United Nations agency is ready to predict[11] subsequent challenge, desires to impersonate the user to the service supplier. The unwelcome person takes the service provider role, by impersonating it to the user, and asks the user to certify itself(Fig 3). The interloper chooses future challenge which will be chosen by the service supplier once authenticating the user. The challenge's response sent by the user is memorized by the interloper**.**

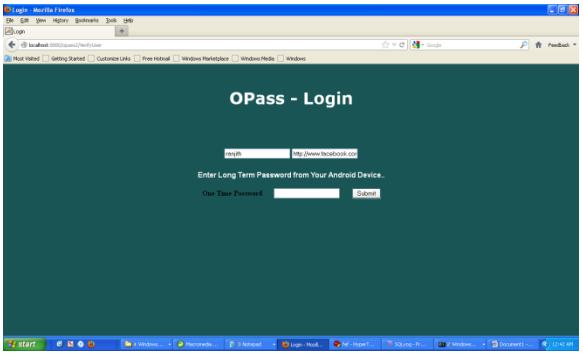

Figure 3. Verification Application for any webapp.

Then, at some future time, the unwelcome person will impersonate the user to the service supplier, victimization this memorized response. Our proposal permits the service supplier to challenge the user with unpredictable uniformly distributed values of x and y . If we have a tendency to suppose that x and y will take one price of forward m values, the likelihood of with success estimation a challenge are the chance of x and y , that is adequate to one money supply. we will see this property because the ability to resist.

V. Performance Assessment

The performance analysis considers the machine price from the user aspect. Considering the t th authentication login time, the use of the S/KEY™ can price the user variety of N − t hash operations, wherever N is that the outlined chain length. Bicakci's theme [8] has rock bottom variety of steps, utilizing only 1 chain step; the worth of this profit is that the use of public key cryptography to supply the signature chain. but time based mostly algorithms ought to guarantee a main server synchronised internal clock. Our approach prices the user x + y hash operations, that is extremely low cost compared with the amount of N − t hashes. Our approach doesn't involve public key techniques, and has no would like of utilizing time synchronization. All participants felt that the registration and login processes within the user authentication system were straightforward. what is more, they united that user authentication using otp was safer than the initial login system. it's quite vital to create users feel secure. It conjointly demonstrates that our planned system was like minded to users not withstanding background. a number of the participants like user authentication using otp to the initial login system. Meanwhile, several participants recommended that the user authentication using otp was higher suited to money websites, for instance on-line banking or on-line looking and credit card transactions. They believed that general websites don't would like such high security level.

MD5 Algorithm

MD5 is associate algorithmic program that's wont to verify knowledge integrity through the creation of a 128-bit message digest from knowledge input (which is also a message of any length) that's claimed to be as distinctive thereto specific knowledge as a fingerprint is to the precise individual. MD5, that was developed by academician Ronald L. Rivest of MIT, is meant to be used with digital signature applications, that need that enormous files should be compressed by a secure technique before being encrypted with a secret key, below a public key cryptosystem. MD5 is presently a typical, net Engineering Task Force (IETF) Request for Comments (RFC) 1321. in step with the quality, it's "computationally infeasible" that any 2 messages that are input to the MD5 algorithmic program may have because the output a similar message digest, or that a false message may be created through apprehension of the message digest.

MD5 is that the third message digest algorithmic program created by Rivest. All 3 (the others ar MD2 and MD4) have similar structures, however MD2 was optimized for 8-bit machines, as compared with the 2 later formulas, that ar optimized for 32-bit machines. The MD5 algorithmic program is associate extension of MD4, that the critique found to be quick, however probably conditionally secure. as compared, MD5 isn't quite as quick because the MD4 algorithmic program, however offers rather more assurance of knowledge security.

VI. Conclusion

In future we've got a bent to implement project supported the GPRS techniques. With facilitate of the GPRS technique we are going to supply faster authentication.A epitome of user authentication using otp is in addition enforced to measure its performance. The standard time spent on registration and login is twenty one.8 and 21.6 s, severally. per the result, SMS delay occupies quite ordinal of total execution time. The delay is shorter by exploitation advanced devices. Consequently, all of them in agreement authentication is safer than the primary login system in websites and in credit card transactions.

VII. References

[1] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.

[2] S. Gawand E. W. Felten, "Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy . Security, New York, 2006, pp. 44–55, ACM.

[3] D. Florencio and C. Herley, "A large scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., NewYork, 2007, pp. 657–666, ACM.

[4] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle,"Multiple password interference in text passwords and click-based graphical passwords," in CCS '09: Proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp.

[5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *SSYM'99: Proc. 8th Conf. USENIX Security*

[6] A. Perrig and D. Song, "Hash visualization: A new technique to improve real-world security," in Proc. Int.Workshop Cryptographic Techniques E-Commerce, Citeseer, 1999, pp. 131–138.

[7] J. Thorpe and P. van Oorschot, "Towards secure design choices for implementing graphical passwords," presented at the 20th. Annu. Computer Security Applicat. Conf., 2004.

[8] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," Int. J. Human-Computer Studies, vol. 63, no. 1–2, pp. 102–127, 2005.

[9] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in AVI '06: Proc. Working Conf. Advanced Visual Interfaces, New York, 2006, pp. 177–184, ACM.

[10] B. Pinkas and T. Sander, "Securing passwords against dictionary attacks," in CCS '02: Proc. 9th ACM Conf. Computer Communications Security, New York, 2002, pp. 161–170, ACM.

[11] J. A. Halderman, B. Waters, and E. W. Felten, "A convenient method for securely managing passwords," in WWW '05: Proc. 14th Int. Conf. World Wide Web, New York, 2005, pp. 471–479, ACM.

[12] K.-P. Yee and K. Sitaker, "Passpet: Convenient password management and phishing protection," in SOUPS '06: Proc. 2nd Symp. Usable Privacy Security, New York, 2006, pp. 32–43, ACM.
[13] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," in SOUPS '07: Proc. 3rd Symp. Usable Privacy Security, New York, 2007, pp. 1–12, ACM.
[14] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in CHI '09: Proc. 27th Int. Conf. Human Factors Computing Systems, New York, 2009, pp. 889–898, ACM.
[15] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords," in SSYM'04: Proc. 13th Conf. USENIX Security Symp., Berkeley, CA, 2004, pp. 10–10, USENIX Association.
association.
[16].H.karwczyk "The older of encryption and authentication of protecting communications (or:how secure is ssl?)," in advances cryptology—CRYPTO 2001,2001,PP.310-331.
[17].M.wu,S.Garfinkel,andR.Miller "secure web authentication with mobile phones," in DIMACS workshop usable privacy security software ,citeseer,2004.