A Survey on Knowledge-Based Authentication

[1]Manjunath D, [2]Nagesh A S,[3]Sathyajeeth M P, [4]Naveen Kumar J R, [5]Syed Akram

[1,2,3]Student, Department of CSE,B M S College of Engineering,Bangalore
[4,5]Assistant Professor, Department of CSE,B M S College of Engineering,Bangalore

Abstract : Traditionally text based passwords are the most popular user authentication method, but have security and usability problems. Alternatives such as biometric systems and tokens have their own drawbacks. This survey paper will focus on the existing graphical password system's security and usability. Also how the graphical passwords improves authentication. Graphical password system not only minimizes the security attacks and also avoids the user tendency towards selecting the weak passwords.

***Keywords*— Knowledge Based, Authentication,Cued Click Points, Persuasive, One-Time Password.**

I. INTRODUCTION

Common knowledge based authentication methods include alphanumeric passwords and graphical passwords. Alphanumeric passwords have a few drawbacks, for example users tend to set passwords that are easy to guess. On the other hand, passwords generated by system that are difficult to guess are hard to remember. To overcome these drawbacks graphical passwords were introduced.

One of the methods of graphical passwords is one in which a user clicks on an image in sequence, for a fixed number of times to authenticate himself. The drawback of this method was the tendency of users to click on certain points on an image, called hotspots. hotspots are those points on an image where the tendency of clicking is maximum. These hotspots can be easily guessed by attackers. To overcome this drawback [9], Sonia et.al proposed a system in which the user is persuaded to click on a point other than the hotspots and also include multiple images in the password to make it less vulnerable.

This survey paper is structured as follows. the existing categories of authentication and comparison. A detailed survey on graphical passwords and design and implementation issues of graphical passwords is discussed.

OVERVIEW OF AUTHENTICATION METHODS

Presently, Authentication methods can be divided into three main categories.

1. Token based authentication
2. Biometric based authentication
3. Knowledge based authentication

Token based authentication method includes bank cards, smart cards etc. Token based techniques uses Knowledge based as second factor to strengthen the security such as ATM with PIN. Token based techniques have passwords usability problem and card can be stolen by third party. Biometric system [14] includes fingerprints, iris recognition etc. This technique provides highest level of security but expansive and slow. Knowledge based authentication requires the knowledge of users on something they know. These types of passwords are currently having widespread uses.

KNOWLEDGE BASED AUTHENTICATON

Knowledge-Based Authentication is commonly referred to as KBA [16], which is a method used to authenticate that seeks to prove the identity of someone accessing a service, such as a website. KBA requires the knowledge of personal information before logging in to grant access to the protected material to the individual.

In this authentication scheme the user is asked to answer at least one "secret" question. KBA is often used as a component in multifactor authentication and for self-service password retrieval.

There are two types of Knowledge-Based Authentication:

Static KBA: Static KBA, also referred to as "shared secrets" or "shared secret questions", is commonly used by banks, financial services companies and e-mail providers to prove the identity of the customer before allowing account access, or as a fall-back if the user forgets their password.

Dynamic KBA: Dynamic KBA is a high level of authentication that also uses knowledge questions to verify each individual identity, but requires no previous contact. This is because the questions are generated on the fly and based on information in a consumer's personal aggregated data file (public records), complied marketing data, or credit report.

TEXT-BASED AUTHENTICATION

Text-Based Authentication involves authentication of a person in order to provide access to the protected material by asking the person to enter a text-based password which he had already provided during the registration phase.

Text-Based Password has very good usability features but less security features as the password can be easily guessed when it is provided by the user. There is another type where the password is generated by the system which has good security features as it is difficult to guess but it is also difficult to the user to remember the password as it contains the characters jumbled which has no dictionary meaning.

SIGN IN with email

User ID abc@gmail.com

Password •••••••••

GRAPHICAL PASSWORDS

Image based or Graphical based passwords are the best alternatives to traditional text based passwords. Graphical passwords were originally described by Blonder in 1996. Based on his description we can define graphical based authentication is a mechanism where an image would appear on screen, and the user would click on a few regions of it as password.
Graphical Passwords provide both usability and security for user. Psychological studies say that Human can remember pictures better than text, hence usability is achieved. Research is going on to improve better security than text passwords by improving password space and resistance to dictionary and guessing attacks.
Typically, we can view Graphical passwords as two Categories

- Recall Based Techniques

In this technique, user is asked to reproduce something he created or selected during registration process. Draw-a-secret scheme, Pass-points scheme and Signature scheme are examples for this technique.

- Recognition Based Techniques

In this technique, user passes authentication by recognizing and identifying the images he selected during registration stage. Pass face scheme, Dhamija and Perrig scheme, Sobrado and Birget scheme are examples for this technique.

Many schemes have proposed based on recall and recognition techniques [5] [6]. Those are,

- Draw-A-Secret (DAS) [1], this technique is purely recall based technique where user has to reproduce the secret drawn during registration phase in order to login to the resource.
- Dunphy and Yan proposed the BDAS technique where they added background images to DAS to encourage powerful passwords.
- Pass shapes technique is proposed by Weiss and De-Luca. In this technique passwords are converted into alphanumeric based on 8 stroke directions and 45 degree intervals.
- In variation to DAS, Tao and Adams designed Pass-Go technique where user has to select the intersection points on grid in the same sequence as selected during registration improving the usability.
- Pass faces, a recognition based technique in this user pre-select a set of human faces during registration as password. During login time a panel of candidate face is presented user has to select the face belonging to their set among decoys.
- In Deja-Vu technique [15] user has to select the subset of random art from the larger sample for their portfolio. During login user has to select the random art belong to his subset among decoys.
- Pass points (PP) [9], a cued recall based technique where user has to select the sequence of click points in an image provided.
- Cued click points, a variation of pass points in the sense that user has to select each click points in different images.

Author compared the all techniques using usability and security attacks as parameters to measure the strength and weakness of the technique. Author finished is writing by giving advises about how should be a future graphical password technique. Advisee includes theoretical password space meeting the security policy of intended domain, avoidance of selection of weak passwords by user, mild resistance to capture attacks and cues for memorability.

PASS POINTS

In Pass points, passwords consist of a sequence of five click points on a given image. User has to select those click points in correct order during login time to successfully login into his account. Here user can use either system provided images or their own images. Android pattern lock is an example for this method.

CUED CLICK POINTS

Cued click points [4] [9] are variant of pass points where passwords consist of five click points on five different images instead of five points on one image. It is made as such to reduce the usefulness of hotspot to attackers. For user, only one image on a screen is displayed on which he has to select a click point to get next image.

The next image displayed is based on the location of the previously entered click point. Different click points results in different image sequence so we can achieve more password space. User get access to their source only when they entered five click points correctly. Selection of wrong click point on an image results in displaying wrong image next. No alerts are given in between entering click points if any wrong, so that can avoid guessing attacks.

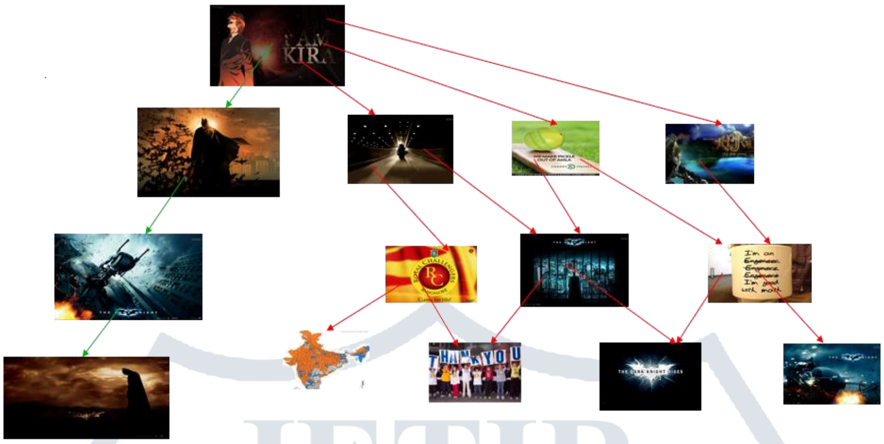

Fig. 1. A user navigates through images to form a CCP password. Each click determines the next image (ref. from [9]).

STRENGTHNING SECUIRITY USING ONE TIME PASSWORD

Textual Passwords and Graphical Passwords are the most widely used type of authentication methods. Both have their own drawbacks. Textual passwords are easy to remember and easy to guess by the attackers when they are created by the user. If the textual passwords are created by the system then they are hard to remember and difficult to guess. The key-logger attack also affects the textual password authentication. Graphical Passwords are prone to shoulder-surfing attack. Hence this paper presents about OTP (One Time Password) [8] which we are going to use in android phones.

The user need to create a Long-Term Password (LTP) which secures the information on his mobile. Then the user will be sent an OTP to his mobile using which the user can access the information on the server through the mobile.

One-time password protocol

The OTP **[8]** is generated using a one-way hash function. An input c is given, if we want to create N one-time passwords, the first OTP is produced by performing the hash function N times on the given c. The second OTP is produced by performing N-1 times the hash function on the given input c and so on.

$\mu0 =HN(c)$ ……………….(1)

$\mu1=HN-1(c)$……………….(2)

Hence the general formula is given by,

$\mu i=HN-i(c)$ ……………….(3)

While using these onetime passwords they can be shuffled while generating.

Threat Model

An OPASS model[8] is created to check the threats which are possible on user side as well as server side. The attacker can steal the LTP from the user and if he gains access to the user's mobile then the attacker will have access to the user's information. The attacker can get the LTP from the user by using phishing websites and key loggers. On the server side the attackers can exploit vulnerabilities of OPASS to pass the authentication phase without being detected by the website.

There are four phases in OPASS model. The first phase is the Registration Phase where the user enters the details like username and email-id which will be stored in the database. In the next phase that is Confirmation Phase the user details are uploaded to the server and checked if the account is unique or not. The Login phase is used to direct to the server to identify the user by launching an application in the user's Mobile phone. There is no problem of Man in the Middle Attack as there is no password to be entered to go to the website. There is another phase called Recovery Phase which is used when the user loses his Mobile Phone and want to connect the new Mobile to the account.

In Registration Phase, the user is asked to enter the LTP, this cannot be accessed by the attacker because the mobile is checked if it is malware-free before entering the LTP. In Login Phase, the attacker cannot get the OTP because it will encrypted and will be sent to the registered mobile number. The Man in the Middle attack is also not possible as the server once learns that an attacker is intruding it stops the process. Hence the OPASS model is built to overcome all these attacks by making use of LTP and OTP generated by using one way hash function.

KNOWLEDGE BASED AUTHENTICATION ATTACKS

The possible attacks on knowledge based authentication according to Common Attack Pattern Enumeration Classification (CAPEC) [3] format are,

1. Password Brute Force: It uses "Probabilistic Techniques" as a method of attack. Probabilistic technique shows that when one object is selected randomly from a class of objects, the probability that the result would be the same as the desired result is more than zero, so password brute forcing works by an attacker who uses trial and error method to explore all possible passwords of the user. There are two versions of brute force attacks which are:
Dictionary based password: It is a type of brute force attack in which the attacker creates a dictionary of textual or graphical possible password, and then tries to find an account with one user name and the passwords in the created dictionary
Rainbow table password attack: Normally administrator saves the passwords of user in hash form. In this type of attack the attacker pre computes Hash of billions of passwords and store them in a Rainbow table in order to find the correct password. The main idea of the rainbow table is using chain of hashing and reduction function. A hash function maps the plaintexts to hashes, and the reduction function reduces the length of hash function to a fix value.

2. Sniffing attack: When user enters textual password it is transferred as sequence of packets. The packets go up and down through network along with the packet's destination address to show which computer is permitted to accept it. Using sniffer software attacker modifies the configuration of network interface card promiscuous mode to collect all these packets. To protect from sniffing attacks the sensitive information must be properly encrypted.

3. Spoofing attack: It consists of various techniques like action spoofing, content spoofing and identity spoofing. In "Action Spoofing" the attacker changes the mechanism of actions to lead victim to a wrong way. In "Content Spoofing", the attacker changes the contents of one page to show his messages rather than the original one. In the "Identity Spoofing", the attacker impersonates a legitimate user. Identity spoofing has several types like "Man in the middle attack" and "Phishing attack". In Man in the middle attack the intruder uses spoofing method by sitting somewhere between the client and the server and starts sniffing packets or even alter message from first party and send the changed message to the second. In phishing attack the attacker steals the user's confidential information by pretending to be a legitimate entity. For example, an attacker design a fake website exactly like a bank's portal, then starts to send out a spam e-mails to a large random number of users trying to convinces the user to visit the cracked website and enter their account number and password.

4. Social engineering attack: It is one of the oldest attack in which attacker uses psychological and technical methods of tricking the user into believing that he needs to provide his confidential information. The preventive measure for this type of attack is very hard because it does not include any kinds of bugs and weakness in the system.

5. Physical security attack: When an attacker has physical access to the computer there is a chance of bypassing authentication and easily get access to resources even without authenticating.

6. Shoulder surfing attack: The attacker tries to use direct observation like looking over the user's shoulder, using binoculars or even closed circuit television cameras for capturing user's credential

DESIGN AND IMPLEMENTATION ISSUES OF GRAPHICAL PASSWORDS

Security: As discussed in the above discussion [3], care should be taken to avoid knowledge based attacks while designing graphical passwords.
Usability: The main advantage of the graphical passwords is that pictures can be remembered easily than the alphanumeric passwords. Some preliminary user studies presented in some research paper support this [9] [6]. We cannot judge it is happened in real world because still users of graphical passwords are less. The main complaint of graphical passwords is the login time. Login process may take too long because retrieving images from large collection is slow [5].
Reliability: The major design issue of graphical passwords is maintaining reliability and accuracy of the system. The more error tolerant the program, the more vulnerable it is to attacks [5].
Storage and communication: Graphical password system needs more space to store images. Text passwords are best in this view because graphical passwords need to store thousands of images. Some compression techniques can be used to reduce the storage size and network transfer delay.

GRAPHICAL AUTHENTICATION METHOD USING A SINGLE IMAGE

A method of authentication mechanism using images, pictures, colors and other graphical elements to gain access to a secure platform, section of a platform, specific content, website, computer, mobile device or other electronic device. This method [13] includes three modules namely user registration, authentication and maintenance of graphical password. User registration is initiated through user selection of system or user provided images, colors or other graphical elements for authentication process. The graphical elements may be photos, pictures or images that are memorable to the user and are from within one or more relevant categories, e.g. colors, playing cards, animals. A graphical user interface (GUI) having virtual dials, wheels, reels or keypads to display images is used to implement the login/authentication process. Graphical password creation is confirmed within the application or other secure communication link once the graphical password is created as part of user registration. The user to authenticate himself to the secured content after user registration, launches the application and selects the secret graphical elements from a menu of similar graphical elements from the same graphical categories generated by the system. In the authentication phase, the system compares the user chosen elements from the set of graphical elements to the secret graphical elements defined and stored from user during registration. If the selected graphical elements are same as stored elements then the user is granted access. The user can increase or decrease the strength of the graphical password by increasing or decreasing the total number of graphical elements established in the registration process that must match during the authentication session. Thus the present invention relates to authentication methods and systems that leverage human's abilities to recognize and use graphical images to provide access to content within a secure platform, network, website, computer, mobile device or other electronic device.

AUTHENTICATION SYSTEM USING AN ARRANGEMENT OF DYNAMIC GRAPHICAL IMAGES

Method of providing an authentication system using an arrangement of dynamic graphical images [12]. The graphical images are arranged as a grid or matrix for presentation on a device display for user authentication. The graphical images are derived from a designated authentication category and non-authenticating category. The selects a series of one or more password elements corresponding to graphical images from the authentication category which form the password entry. In the registration phase, a user selects a series of one or more image categories, which will serve as the user's authentication sequence. The user inputs a username during login phase, which was created during registration phase. After validating the username, a grid of images corresponding to the pre-defined categories will be displayed. One image from each category will appear at a random location within the grid. Each image will have a corresponding character associated with it called image identifier. These image identifiers are displayed on each image in the login phase. The user enters the image identifiers of the images which correspond to the category of images selected during the registration phase. These image identifiers are matched with the identifiers for corresponding category of images. The identifiers are generated randomly and are mapped to the images during pre-authentication phase. This provides protection against attacks which track keystrokes.

GRAPHICAL AUTHENTICATION SYSTEM USING ATTRIBUTES ASSOCIATED TO IMAGES

In this method [11] of graphical password authentication, a number of graphical images are presented on a display screen of an access device, such as a handheld smart phone. Each graphical image is associated with one or more attributes. The user sequentially selects graphical images and a password is generated based on the combination of attributes of the selected images. The generated password is compared with a stored password to authenticate the user and grant access to the device. The graphical passwords also include time, motion, and/or keyboard input attributes such that the passwords are multidimensional. In another approach, the access device is used to connect with a remote computer system and the generated password is transmitted to the remote computer system to authenticate the user and allow access to the remote computer system.

GRAPHICAL AUTHENTICATION SYSTEM USING SUB IMAGES INSTEAD OF A SINGLE IMAGE

In this method [10] of authentication a graphical password composed of various identifier images that are clearly distinguishable from each other, is produced for an electronic system, such as a database, a computer program or Internet pages. Various partial images representing certain subareas of a whole identifier image have been saved in electronic form called as an image archive, from which passwords are produced. The subarea of an identifier image is represented by partial images which are divided into subgroups. The identifier images of graphical password are composed by selecting partial images from different subgroups and by combining the selected partial images into one complete identifier image. The identifier images may be facial images of people, and the partial images are images showing different subareas of a human face. One advantage of this authentication system is that the number of images stored in the archive is less compared to other graphical image based password authentication systems. Instead of storing a large number of complete identifier images, partial images of few complete images are stored in the archive, thereby reducing the system’s memory consumption.

REQUIREMENTS FOR KNOWLEDGE BASED AUTHENTICATION

This paper presents a set of requirements to create a secure user authentication method which uses user’s knowledge. The first issue refers to eavesdropping an authentication session and using the stolen data in the next session. The second issue involves predicting the authentication challenge by analyzing the previous challenges. The third issue involves guessing the correct responses to the authentication challenges. The fourth issue is the authentication server’s vulnerability. If the authentication server is hacked then the security of the data stored in the server is compromised.

There are three ways of authenticating a user, using something the user has, something the user knows and something the is. Research has been done on the fourth factor which involves user’s location to authenticate him.

The existing evaluation criteria includes Fact based authentication methods, which are used more often which are also called “personal verification questions”. Fact based authentication methods will be using the personal information relating to the user which can be from any sources. Fact based authentication methods are divided into two types. Static KBA uses the predetermined facts like user’s birth date or user’s mother’s maiden name etc. to authenticate the user. Dynamic KBA, which involves the information which is not shared by the user beforehand, the data can be collected from user’s banking, shopping etc. activities. Dynamic KBA is rarely used because it is difficult to create algorithms which creates the different questions dynamically for every user.

The properties are separated into three categories. The first category questions usability benefits. These benefits evaluate how easy it is for users to authenticate themselves to the system. The second focuses on deploy ability. This requirement is very important since many authentication methods have been discarded because of the difficulty of deploying them on large scale. The last category focuses on security benefits.

The proposed system deals about one time challenges, challenge predictability, response guess ability and Independence of the authentication server security. The security of an authentication method depends on how it secures the data which is really important. Even it is more secure, there will be some flaws. The attacker can intercept the data. The attacker can easily insert himself in a secure communication channel if the end user accepts the attacker's forged certificate. The data can also be intercepted in a non-technical way by using social engineering techniques which may be "Dumpster Diving". The attacker can also eavesdrop by using the sound made by keyboard. To overcome all this the user proposes one time password to authenticate the users. The "Challenge predictability" says that the attacker should not be able to predict the next challenge by making use of previous challenge. In the first way the attacker can reverse engineer the algorithm by using a set of recorded challenges which should be avoided. The second way is "Chosen message attack" which adaptively queries the authentication server to gain information. The "Response Guess ability" means the attacker can manage to guess the answer or password with the help of information collected about the user. But sometimes it is difficult for the attacker to guess the correct response the second time also in one time challenge. To avoid response guess ability the authentication server must use the data which user does not share with friends and acquaintances. The "Independence of the authentication server security" says that the authentication server and the database used to store the user data must be separated. If the data is stored in the same server then the security of the data may be compromised. In cryptography, the passwords are salted and hashed before storing into the database. If the attacker manages to get the data from the server, he can reverse engineer and find the salted value and so that he can decrypt all the data stored in the server.

ZERO KNOWLEDGE PROTOCOLS USING DIFFIE-HELLMAN KEY EXCHANGE

A method to provide authentication and confidentiality using Zero Knowledge Protocol (ZKP) and key exchange. ZKP is used for authenticating identity of users and exchange of secret is done using Diffie-Hellman key exchange protocol. The authentication process takes place between a Prover P and a Verifier V, where P proves his identity to V using a protocol called interactive proof. The interactive proof transmits only the output of a statement (true/false) but does not transmit any further information. There are two types of interactive proofs, mathematical statement and proofs of knowledge. The Verifier authenticates the Prover by asking him questions repeatedly and successful authentication takes place only when the verifier gets the expected answer each time. The characteristics of ZKP are completeness, rationality and zero-knowledge. Once the identity is established secret information is exchanged using Diffie-Hellman key exchange protocol which allows two users to exchange secret key over open communication channel without meeting in advance. The key is then used to encrypt subsequent communications using symmetric key cipher.

SECURE AND USABLE AUTHENTICATION IN ONLINE EXAMINATIONS

In traditional online examination environments, physical interaction is often replaced with authentication mechanisms. The absence of face-to-face interaction increases the number of authentication challenges. The "challenge questions" is a widely used authentication approach, which utilizes personal information as authentication token. It is believed that students can exploit the absence of face-to-face invigilation and identification to their benefit and turn to academic dishonesty. Impersonation in the absence of physical invigilation is also reported in online examinations. The authors developed the PBAF authentication approach, which implements challenge questions for security of online examinations, due to usability challenges reported in a number of studies, recall and recognition image-based questions were implemented in this empirical study. The PBAF is a multi-modal authentication approach, which utilizes login-identifier and password and challenge questions for authentication purposes. Students are required to supply answers to profile questions on each visit to be able to access learning resources. The PBAF generates and presents random challenge questions before any online examinations can be accessed. Students' answers to challenge questions are verified against their profile answers using authentication mechanism. Users are presented with previously chosen image to recall and identify their selection in order to authenticate. The recall image- based authentication was implemented as recall image-based multiple choice questions in the PBAF approach. The correct image is presented with a set of distraction images and user is challenged to recognize a previously viewed or selected image.

SNIPPET: GENUINE KNOWLEDGE BASED AUTHENTICATION

This paper presents the past, present and future of the knowledge based authentication. Passwords are the most commonly used method to authenticate the user from very old days. Even Now-a-days passwords are widely used by all the people to authenticate themselves while doing the activities like online shopping, banking etc. According to National Institute of standards and Technology there are three types of authentication, something you know, something you have and something you are. The most popular are password, smart card and fingerprint respectively.

"Something you know" is the most used authentication method. The concept of the passwords is centuries old which is easily understood by the users and developers. The keyboard is also very old which is used to enter the password. These are the two reasons why the passwords are widely used method of authentication from many years. But care has to be taken so that the password is not weak enough to be guessed by the attacker. There is difference between data, information and knowledge. Data is simply data which is of no use to anyone until some context is added to it. If context is added to the data then it is called as information. Knowledge is the theoretical or practical explanation of the subject. The cognitive processing of the brain happens is three phases remember, understand and apply. Remember is the ability to retrieve the relevant facts from the memory. If the context is added to the remembered data then it means that the user has understood the data. Apply is third level of cognitive domain where the user uses the information correctively in a given situation.

The "what you know" authentication method can be tested by using recall, cued-recall and recognition methods. Passwords use recall method, Cueblot mechanism uses cued-recall method and graphical password uses recognition method. The quiz-based approach can be used which involves two types, fact based and opinion based questions.

Knowledge is the best way for the users to get authenticated. Recognition based techniques are much more easier for the user to use. The user can be asked to write something with his own hands and a number of PIN numbers can be created which also includes the handwriting of the user and can be shown to the user to identify his own handwriting. The same method can be used in other way, the user can be asked to draw some images and while authenticating those images can be shown to him and can be asked to recognize them which is easier for the user to remember. "Fact Finding" involves a survey which was conducted on programmers. The programmers were asked to recognize the code which they have written. 42% programmers were able to recognize their own code with another 39% being unsure. This experiment was based on recognition methods. The other programmers were asked to recognize their friend's code which they some were able to recognize and some were not able to recognize.

ZERO KNOWLEDGE BASED AUTHENTICATION TECHNIQUE IN CONTEXT-AWARE SYSTEM

The system uses a zero knowledge-based protocol for user identification and context-aware system for verifying and protecting the user's identity and location. The protocol uses two basic principles first, it uses a physical token used for active gesturing and as the cryptographic basis for authentication. Second, it uses a context-aware system to verify the location of the user, and to log out when the user leaves the computer in a certain place. If the context-aware infrastructure is unreachable for any reason, the user is requested to enter his password when trying to log in. If the token cannot be accessed for any reason, the user is requested to enter both his username and password as usual. Hence, in case of system failure, security is not compromised, and the system is still usable.

The server used in this protocol is called context server which contains the data structure that stores the information about users, places or things. Each user is connected to leaf level routers called mist routers and forms the mist circuits. These routers conceal the identities of communicating parties. The authentication program is running on the java card. Each client is associated with a card reader and the program is executed every time a user inserts his card into the reader on the client. The card contains user's id, password and a pair of secret key and public key. When the card is inserted the applet creates RSA key-pair. The secret key is stored on the card and the public key is stored in a central server along with the id of the user.

ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1]. P. R. Devale Shrikala M. Deshmukh, Anil B. Pawar, "Persuasive Cued Click Points with Click Draw Based Graphical Password Scheme" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013.

[2]. Navgire Priyanka D, Prof. Jayapal PC, "Graphically Secured Password" International Journal of Advance Research in Computer Science and Management Studies, Volume 2, Issue 11, November 2014.

[3]. Farnaz Towhidi, Azizah Abdul Manaf, Salwani Mohd Daud, Arash Habibi Lashkari, "The Knowledge Based Authentication Attacks" supported by project UTM-J-13- 01/25.10/3/02H07(1) from Research University Grant (RUG) of University Technology Malaysia (UTM).

[4]. Prof. Anil Kulkarni, Sangameshwar, "Design, Implementation and Evaluation of Knowledge-Based Authentication Mechanism Using Persuasive Cued Click-Points" International Journal of Advance Research in Computer Science and Software Engineering, Volume 3, Issue 8, August 2013 ISSN: 2277 128X.

[5]. Mr. A. A. Shinde*, Ms. S.R. Chokhandre, Mrs. R.C. Roychaudhary, Mrs. S. S. Telrandhe Mrs. C. N. Rokde, "A Survey: Login with Image Based Password Authentication" International Journal of Advance Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014, ISSN: 2277 128X.

[6]. Robert Biddle, Sonia Chiasson, P.C. van Oorschot, "Graphical Passwords: Learning from the First Twelve Years" School of Computer Science Carleton University, Ottawa, Canada.

[7]. Moulisai Rachagundla, Syed Gulam Gouse, "A Graphical Password Scheme using Persuasive Cued Click Points" International Journal of Modern Engineering Research (IJMER) ,www.ijmer.com, Vol. 3, Issue. 5, Sep - Oct. 2013 pp-3005-3007 ISSN: 2249- 6645.

[8]. R.Selva Bhuvaneshwari, P.Anuja, "Secured Password Management Technique Using One-Time Password Protocol In Smartphone" International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 3, March 2014, pg.976 – 981, ISSN 2320–088X.

[9]. Sonia Chiasson, Member, IEEE, Elizabeth Stobert, Alain Forget, Robert Biddle, Member,IEEE, and P. C. van Oorschot, Member, IEEE "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism" A version of this paper has been accepted (Oct 2011) for publication in IEEE Transactions on Dependable and Secure Computing (TDSC).

[10]. "METHOD AND SYSTEM FOR PRODUCING A GRAPHICAL PASSWORD, AND A TERMINAL DEVICE" Patent no: 7,376,899 Issue date: May 20, 2008 Assignee: Nokia Corporation (Espoo, FI) Inventors: Mantyla; Janne (Espoo, FI).

[11]. " SYSTEM AND METHOD FOR AUTHENTICATING A USER USING GRAPHICAL PASSWORD" Patent no: 8,347,103 Issue date: January 1, 2013 Assignee: NIC, Inc. (Olathe, KS) Inventors: Jones; Nolan (Overland Park, KS), Sherry; J. D. (Olathe, KS).

[12]. "METHODS AND SYSTEMS FOR GRAPHICAL IMAGE AUTHENTICATION" Patent no: 8,850,519 Issue date: September 30, 2014 Assignee: Confident Technologies, Inc. (Solana Beach, CA) Inventors: Osborn; Steven L. (Sand Springs, OK), Davis; Nicholas A. (Tulsa, OK), Sontag; James L. (Portland, OR), Norvell; Joel (Tulsa, OK).

[13]. "ELECTRONIC AUTHENTICATION USING PICTURES AND IMAGES" Patent no: 8,881,251 Issue date: November 4, 2014 Assignee: RememberIN, Inc. (Hopkinton, MA) Inventors: Hilger; Stuart (Hopkinton, MA).

[14]. K. Gilhooly, "Biometrics: Getting Back to Business," in Computerworld, May 09, 2005.

[15]. R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in Proceedings of 9th USENIX Security Symposium, 2000.

[16]. K. Skrai, P. Pale, B. Jeren "Knowledge based authentication requirements" MIPRO 2013, May 20-24, 2013, Opatija, Croatia.

[17]. P Lalitha Surya Kumari, Prof. Avula Damodaram "An Alternative Methodology For Authentication And Confidentiality Based On Zero Knowledge Protocols Using Diffie-Hellman Key Exchange" in 2014 13th International Conference on Information Technology.

[18]. Abrar Ullah, Hannan Xiao, Trevor Barker , Mariana Lilley "Graphical and Text Based Challenge Questions for Secure and Usable Authentication in Online Examinations" The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014).

[19]. Karen Renaud1, Demetris Kennes, Johan van Niekerk and Joe Maguire "SNIPPET: Genuine Knowledge-Based Authentication" 2013 IEEE

[20]. Chun-Dong WANG, Li-Chun FENG, Qiang WANG "Zero-Knowledge-Based User Authentication Technique in Context-aware System" 2007 International Conference on Multimedia and Ubiquitous Engineering(MUE'07)

[21]. www.wikipidea.org.