RESEARCH ON DIFFERENT USER AUTHENTICATION SYSTEM AND THEIR LIMITATIONS

Shruti Lakhara-20BCY10173
Prahasith Polina-20BCY10142
Joel Franko-20BCY10104
Rohan Kolhatkar-20BCY10177

ABSTRACT :

In this report we have included our research on different types of authentication systems and their limitations. This report contains the types of authentication systems which are widely used and there also some systems which are in development or soon to be used widely. Then this report contains the limitations of some authentication systems and then it also contains a survey report on public response about authentication systems . Then we have also concluded with which are some of the secure authentication systems we can use to authenticate. We think that this research paper is really important to understand the importance of authentication systems and their limitations and it will give a basic understanding about the mechanisms of authentication systems.

INDEX TERMS: security , two factor authentication, virtual smart card, security, authentication.

1. INTRODUCTION:

In this paper we have included our research on different types of authentication systems and their limitations. We have explained briefly about different types of authentication systems, their disadvantages and their rate of success. We have also included some working protocols and framework of the authentication systems.The most important factor for concerns with the authentication systems is how secure it is and how easy to use it is. Taking security as the biggest concern we can easily say that a secure and updated authentication system is the need of every organization.

Also the paper presents some new applications of these authentication systems and models which can be brought into use and is more safe.

2. WHAT IS AUTHENTICATION ??

Authentication is a process to know who you are? Every organization wants to have some authentication system so that they may know that the authorized person is only accessing their resources. Authentication is the first step of a good identity and access management process.

Authentication works through passwords, one-time pins, biometric information, token based etc. These are known as authentication systems because they facilitate the authentication process.

Over the past many years, there has been a great development in the field of authentication systems. Many authentication systems overlap or they are used with one another and cannot be classified singly but roughly we can classify them as simple password, image based, token based, QR based approaches. These categories can also be further classified based on security and usability.

3. TYPES OF USERS AUTHENTICATIONS

I. SIMPLE PASSWORD BASED

INTRODUCTION

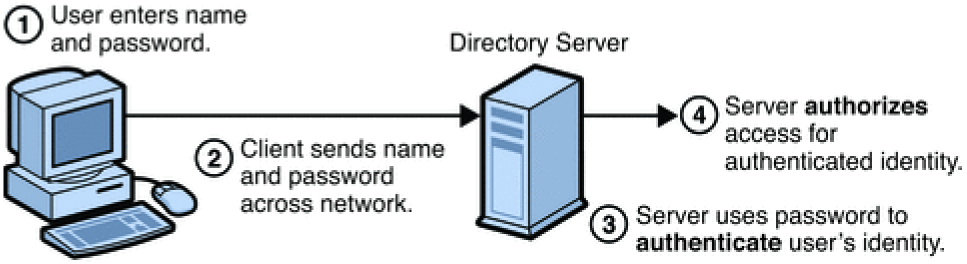
Simple password authentication offers an easy way of authenticating users. In password authentication, the user must supply a password for each server, and the administrator must keep track of the name and password for each user, typically on separate servers.

Steps in Password-Based Authentication

It shows the steps involved in authenticating a client by using a name and N password. The figure assumes the following points.

- **The user has already decided to trust the system, either without authentication, or on the basis of server authentication via SSL.**
- **The user has requested a resource controlled by the server.**

- **The server requires client authentication before permitting access to the requested resource.**



1 User enters name and password.
Directory Server
2 Client sends name and password across network.
4 Server authorizes access for authenticated identity.
3 Server uses password to authenticate user's identity.

1. **The user enters a name and password.**
   For the LDAP bind to Directory Server, the client application must bind with a Distinguished Name. Therefore the client application may use the name entered by the user to retrieve the DN.
2. **The client sends the DN and password across the network.**
3. **The server determines whether the password sent from the client matches the password stored for the entry with the DN sent from the client.**
   If so, the server accepts the credentials as evidence authenticating the user identity.
4. **The server determines whether the identified user is permitted to access the requested resource.**
   If so, the server allows the client to access the resource.

- **Password Policy**

A password policy is a set of rules that govern how passwords are administered in a system. Directory Server supports multiple password policies. The password policy can be configured to suit the security requirements of your deployment.Of Directory Server are created with a default password policy.

- **Types of Password Policy**

Directory Server provInstances ides the following password policies.

1. **Default password policy**

The default password policy is defined in the configuration entry cn=PasswordPolicy,cn=config. The default password policy applies to all accounts in the directory except for the directory manager.

The parameters of the default policy can be modified to override the default settings. However, because the default password policy is part of the configuration for the instance, modifications to the default password policy cannot be replicated.

2. **Specialized password policy**

A password policy can be configured for an individual user or for set of users by using the CoS and roles features. However, specialized password policies can not be applied to static groups.

A specialized password policy is defined in a subentry in the directory tree. Like the default password policy, the specialized password policy uses the pwdPolicy object class.

A specialized password policy can be assigned to a single user account or can be assigned to a set of users by using roles. When referenced by a user entry, a specialized password policy overrides the default password policy.

II. GRAPHICAL OR IMAGE BASED

INTRODUCTION:

Naturally for the human mind it is hard to remember text based passwords. Text-based passwords are easy to guess because of the use of a general set of numbers, character and special symbol. For that purpose we implemented the Graphical Password Authentication System. In that we used Image based & Pair based authentication system.

- **Firstly in Imaged based password user can choose pixels on that image as password. For each image only one pixel is selected. After selection one pixel change the image select second pixel from second image similarly users select three pixels. In pair based password, user chooses characters from columns and rows simultaneously from the grid then getting that intersection point as a password.**

- **We have provided shuffling option for interchanging character sequence it helps to prevent the shoulder suffering attack. So we have improved security by using PCCP and Imaged based password system which having ability of protect from the attacker, crackers etc**

- **Graphical passwords offer another alternative, and are the focus of this paper. Graphical password systems are a type of Image-based authentication that attempt to understand the human memory for visual information. A comprehensive review In Pass Points, passwords consist of sequence pixel click-points on a given image. Users may choose one pixels in that image as click-points for their password. To log in process, they repeat the sequence of clicks in the same order**

I. PERSUASIVE CUED CLICK POINTS (PCCP):

In persuasive cued click point algorithm, image divided in small grid or small parts of view, after that user choos

1. **User Registration: User chooses user name and set of image pixels as password for first time.**
2. **Login: At the time of login user enters same user name and pixel images as password which was stored in database at time of registration to get log-in.**
3. **Verification: After submitting set of image pixels choosed they are matched with database for checking whether they are valid or not.**
4. **Confirmation:After verification is done on the basis of that it is confirmed whether to give access to user or not**

II. PAIR-BASED PASSWORD:

At the time of registration, user needs to enter user name and secret pass. When user enters a user name grid consist of set of character get grid displayed. User has to choose secret pairs of characters, in this pair first character belongs to column and second character belongs to row. After on completion of registration data is store in database. At the time of login user needs to follow same procedure as like registration phase. Password should be consisting of minimum five characters. At the login time when user enter password and submit it goes to verification phase in which enter password is match with password entered at registration phase which is stored in database. We can use pair based password in web login application, ATM Machine, banking application, mobiles and many more.

II. TOKEN BASED

A Secure Token-Based Communication for Authentication and Authorization Servers

- This **article provides** a way to ensure **that you can ensure** secure **connections** between **certifications and authorization** and resource servers without relying on **the** correct server **configuration. To do this,** this **document enters** additional encryption of the **transferred token and protects** the transmission independently **in** the server **configuration.**
- This **article presents CaaS (central approval and** authentication **systems)** that implements the **OpenID** platform and **OUTT2.0 frames.**
- **He** showed the importance of the **safety of the transport layer** (TLS) **of the OAUTT2.0 system and has shown the main case of use.**
- This **is** the **incorrect configuration** server **opens important safety.**
- **Both** the user **and** the security **infrastructure could not** determine the missing security **level at runtime.** Therefore, token encryption **is** introduced that **protects** tokens and **system** resources even **when** the TLS protocol is not **enabled.**
- This mechanism prevents OAuth2.0 based **systems** from being **used** due to deployment **failures.**

III. BIOMETRICS BASED:

BioTouchPass2: Touchscreen Password Biometrics Using Time-Aligned Recurrent Neural Networks:

- **This research paper enhances password scenarios through two-factor authentication approaches asking the users to draw each character of the password instead of typing them as usual.**
- **The main contributions of this study are as follows:**
    - **i) they have presented the novel MobileTouchDB public database, acquired in an unsupervised mobile scenario with no restrictions in terms of position, posture, and devices.**
    - **This database contains more than 64K online character samples performed by 217 users, with 94 different smartphone models, and up to 6 acquisition sessions.**
    - **ii) They have performed a complete analysis of the proposed approach considering both traditional authentication systems such as DTW and novel approaches based on RNNs. In addition, they have also presented a novel approach named TimeAligned Recurrent Neural Networks (TARNNs).**
    - **This approach combines the potential of DTW and RNNs to train more robust systems against attacks.**

- **In this research paper they have performed a complete analysis of the proposed approach using both MobileTouchDB and eBioDigitDB.**
- **Their proposed TARNN system has outperformed the state of the art, achieving a final 2.38% EER, using just a 4digit password and one training sample per character. These results encourage the deployment of their approach in comparison with traditional systems where the attack would have 100% success rate under the same impostor scenario.**
- **In addition, They have also demonstrated the application of our proposed TARNNs for another time sequence recognition task, i.e., online handwritten signature verification.**
- **Their proposed TARNN system has achieved 1.66% and 0.87% EERs for skilled and random forgery scenarios respectively, outperforming in large margin the state of the art.**
- **This research can evaluate the usability and performance improvement of the proposed TARNN approach for different behavioral biometrics and identification scenarios, such as keystroke biometrics.**

A STUDY ON MACHINE LEARNING APPROACH FOR FINGERPRINT RECOGNITION SYSTEM:

Fingerprint method of identification is the oldest and widely used method of authentication used in biometrics. The result and accuracy of fingerprint recognition depends on the presence of valid minutiae. This paper reviews the fingerprint classification including feature extraction methods and learning models for proper classification to label different fingerprints.Basically there are two types of fingerprint Recognition System AFAS (Automatic Fingerprint Authentication System), AFIS (Automatic Fingerprint Identification/Verification System) The main parameters characterizing a digital fingerprint image are such as Resolution, Area, No. of pixels, Depth, Geometric accuracy, etc.Images are acquired from crime scene using methods ranging from precision photography to complex physical and chemical processing techniques and saved as the database. Experimental results show that the method based on adaptive median filter for fingerprint image enhancement outperforms the traditional median filtering method in filtering impulse noise performance. A fingerprint is characterized by abundant and strong textural information. The textural properties of a live fingertip surface are dependent upon skin elasticity, pore distribution and perspiration phenomenon. As a result, the pixels along and around the ridges of a live fingerprint exhibit wide and random variations in gray-level

values.Fingerprints in the crime scene plays an important role to identify the criminal involved in the crime. Crime scene images (CSI) are images taken from the crime spot. When crime is occurred, the investigator takes both latent and patent sample of fingerprints left behind. These mentioned methods conclude that the fingerprint is fast and accurate for more reliable and secure system. Future research work can be carried out to improve the quality of the image by improving the image enhancement technique and develop a better matching technique.

IV. QR BASED

Utilizing QR codes to verify the visual fidelity of image datasets for machine learning:

This paper focuses on methods of protecting image-based datasets by verifying the visual fidelity of the data. The Quick Response (QR) code is a two-dimensional (2D) barcode, which was invented by the company Denso Wave (Denso Wave Incorporated).

A QR code is made up of light and dark modules, which are organized into function patterns and an encoding region. The size and data capacity of a QR code is determined by its version and error correction level. The higher the error correction level, the greater the capacity for data recovery. QR codes with higher error correction levels have lower capacity for encoding actual data as compared with the same QR code version with a low error correction level. Two methods are being discussed to verify the fidelity of the data.

1. Method 1 - Linear Verification String (LVS) method

The notion behind this method is to generate a verification string for each image in a dataset. Hence, it is called the Linear Verification String (LVS) method. The purpose of a verification string is to be able to ascertain whether an image has been altered from the original image. An advantage of generating a verification string is so that respective images in a dataset do not have to be compared with their original image. Moreover, the verification strings will require much less storage space when compared with the size of an entire image dataset. This is due to the fact that the size of a verification string, which is a bit string consisting of 0s and 1s, is much smaller than the size of an image.

2. Method 2 - Aggregate Verification String (AVS) method

The main drawback of the previously described LVS method, is its requirement to have to store the verification strings of all images in a dataset. Storage requirements are proportional to the number of images in a dataset. While the LVS method may seem impractical, it can be used to independently identify any alteration in an individual image Ii, because the verification string Vi must be stored. Hence, when storage space is not an issue (such as the use of cloud storage), this method is feasible and attractive.

In this paper, the problem of protecting image-based machine learning datasets against alteration by an adversary was examined. Two methods were presented, namely, the Linear Verification String (LVS) method and the Aggregate Verification String (AVS) method. The purpose of these methods is to provide mechanisms for verifying the visual fidelity of images in a dataset without the need to store and use the original dataset for verification. In both the LVS and AVS methods, verification strings were generated from the important visual content of the images and associated with QR codes. Nonetheless, in the AVS method, one can only ascertain whether the dataset has been altered, but cannot determine the visual fidelity of individual images.

V. TWO FACTOR AUTHENTICATION

Two factor authentication is a subtype of multifactor authentication. In the two factor authentication two authentication systems are used. For example when we login in any gmail account it sends the notification to the phone or main device. So here two factors are used, one is the password and other one is notification on the device. Other examples can be of various transaction mobile applications when we first open them it asks for a pin and for transaction you have to use OTPs. So here also two factors: simple password and OTPs are used.The most use of two factor authentication comes in forgot passwords steps in websites.

Two-factor authentication (2FA) is crucial for protecting the security of users authenticating to online servers. Despite its importance, users hesitate to use 2FA, due to usability issues.

USAGE OF TWO FACTOR AUTHENTICATION OFFLOADING FOR MOBILE CLOUD COMPUTING:

Security analysts have shown that it is possible to compromise the mobile two-factor authentication applications that employ SMS-based authentication. In sms based two factor authentication users are requested to provide something like a password they know like password and then OTP is sent to mobile devices. However,it has been shown that it is possible to bypass this security mechanism.

When a user launches the legitimate mobile banking application, a fake login interface is triggered by the malware to cover the original banking application. The login credentials, which are filled by the user in the fake application, are sent to the attacker. The malware can also capture the SMS verification code sent to the user, and then it can send it to the attacker. This attack succeeds in tricking the user by employing a visual phishing technique, i.e., creating a fake screen that is visually similar to the legitimate application.

To deal with the above two issues, we consider that offloading mobile applications to the cloud, which is resource-rich and can provide a more secure environment, presents a good
solution when energy limitation and security constraints are raised.

4. COMPARISON TABLE OF ALL METHODS

FEATURES	SIMPLE PASSWORD	GRAPHICAL	TOKEN	BIOMETRICS	QR	TWO FACTOR
contain images for processing	no	yes	no	yes	yes	maybe
Multiple authentication processes	no	no	no	no	no	yes
types:-	Numerical Alphabetical or both	Image or pattern based	---	Facial and fingerprint	----	Different combinations of two authentication systems.
Usage in real life.	Almost used everywhere.	Pattern based logins systems in phones	In online cloud application like Mega	Mostly used for recording physical presence/ data.	Mostly in online transactions.	Can be used anywhere using two systems.
features/issues	If the password is not set strong using lowercase,uppercase,symbols it can be easily broken. Also a simple social engineering attack can destroy it security.	It is mostly used in pattern locks in phones. It is also prone to shoulder surfing. Also it takes generally more storage to store image than text passwords.	It is the new advance system. But token relies on just one key.Also if someone has already breahed your email he may know your auth token as well	It cant be used anywhere it require a device that needs to be present which have stored	It is mostly used in verification purpose than as a single system. Another disadvantage it requires phones with camera to verify it.	Implementing it is the bit complex is.it can be turned against users. In token based two factor authentication if you miss the token it will lead to further wastage of time. So we can say usability wise it is more complex but it provides more security comparing to other ones.

5. CONCLUSION

Upon evaluating various authentication systems on number of parameters and security features we came to conclusion that single authentication system always have more security issues than the multifactor/two factor authentication is. So to increase the security we can implement two factor authentication it can be SMS base otp one or a notification on your phone to verify it you or not etc etc. Also the deployment of the system depends upon the nature o user for example for verifying the presence biometrics one is the best. So nature of user also enables them to pick the authentication system according to their need. But in general we can say that in the present scenario Two factor authentication system is the best one out of all the systems present in todays time.

6. REFERENCES

- 1. Mushtaq Ali , Amanullah Baloch, Abdul Waheed , Mahdi Zareei , Rimsha Manzoor1, Assam Sajid, And Faisal Alanazi “A Simple And Secure Reformation-based Password Scheme”
- 2. Nizamani, Shah, Hassan, Raheel, Shaikh, Riaz, Abozinadah, Ehab Mehmood, Rashid “A Novel Hybrid Textual-graphical Authentication Scheme With Better Security, Memorability, And Usability “
- 3. Takayuki Kawamura , Tadashi Ebihara , Naoto Wakatsuki , And Keiichi Zempo , “Eyedi: Graphical Authentication Scheme Of Estimating Your Encodable Distorted Images To Prevent Screenshot Attacks”
- 4.Syed Shabih Ul Hasan; anwar Ghani; muhammad Bilal; alireza Jolfae “Multifactor Pattern Implicit Authentication”
- 5.Ruben Tolosana; Ruben Vera-rodriguez; Julian Fierrez; Javier Ortega-garcia : Touchscreen Password Biometrics Using Time-aligned Recurrent Neural Networks
- 6.Ba Ajeethra; Sv Gautham Prasath; R Arun Balaji; Kakelli Anil Kumara” Cryptography Based Face Authentication System For Secured Communication”
- 7.N.R. Pradeep; J Ravi “An Efficient Machine Learning Approach For Fingerprint Authentication Using Artificial Neural Networks”
- 8. Yang-waichow ,Willysusilo, Jianfengwang, Richardbuckland, Joonsangbaek, Jongkilkim, Nanli” Https://Www.Sciencedirect.Com/Science/Article/Pii/S1084804520303040”
- 9. Chow, Yang-wai,susilo, Willy, Yang, Guomin,au, Man Ho, Wang, Cong “Authentication And Transaction Verification Using Qr Codes With A Mobile Device”
- 10. Abdelouahid Derhab; Mohamed Belaoued; Mohamed Guerroumi; Farrukh Aslam Khan”two-factor Mutual Authentication Offloading For Mobile Cloud Computing”
- 11. Yossi Oren; Dan Arad “Toward Usable And Accessible Two-factor Authentication Based On The Piezo-gyro Channel”
- 12. Petrova, K. Romaniello, Beatriz, Medlin, B.Vannoy, Sandra “Https://Www.Researchgate.Net/Publication/307879267_qr_codes_advantages_and_dangers”