I J C T A, 9(26) 2016, pp. 363-369

Analysis of Authentication Techniques in Information Security Systems

Esther Rani. D[1], J. John Raybin Jose[2]

ABSTRACT

Authentication is crucial to preserve security during information exchange in the modern world. Unauthenticated intruders can cause havoc to the security systems by blocking resources, corrupting or stealing information, and exploit the data. Varieties of Authentication techniques are available today and they are employed in different instances for identifying and allowing the valid users and thereby preventing the invalid ones. Token based techniques are used to secure personal details. Knowledge-based authentication is used to prevent the person accessing the websites unofficially. Biometric based authentication can be used for variety of identification purposes. Text based authentication uses a password for validating individuals. Graphical based authentication uses image based passwords to access information. This paper analyses several authentication mechanisms available today and their usefulness in maintaining different aspects of security.

Keywords: Authentication, security, password, token, bio-metric, textua, graphical, knowledge.

1. INTRODUCTION

Authentication validates a user. It establishes communication between the sender and the receiver to access data through a secret path. The purpose of an authentication scheme is to allow access to information by the valid users. Authentication techniques employed for security systems are of five types namely

(i) Token-based
(ii) Knowledge-Based
(iii) Biometric Based
(iv) Text Based and
(v) Graphical Based.

Token based technique is an authentication method in which tokens such as key cards, bankcards, smart cards are used to provide security[13] .Token based techniques use password which can be easily stolen by an unknown party. In token based authentication, user can either forget the password or lose the card.

Knowledge-based authentication methods include [12] two types of passwords. They are alphanumeric passwords and graphical passwords. Alphanumeric passwords have few demerits. Graphical passwords are difficult to guess. To overcome the vulnerability of alphanumeric passwords, graphical passwords introduced. The biometric based authentication is more secure than knowledge based authentication. The biometric-based authentication involves fingerprints, iris recognition and face recognition. Biometric system scrutinizes the individual person uniqueness by using one of these means for recognizing and it is profitable to the users. Biometrics system offers several advantages over the conventional security measures. Biometric systems are more convenient to use when compared with traditional authentication systems such as knowledge based and token based authentication [5].

[1] Research Scholar, Department of Computer Science, Bishop Heber College, Tiruchirappalli. *E-mail: jesuschristtruegod@gmail.com*.

[2] Assistant Professor & Head, Department of Information Technology, Bishop Heber College, Tiruchirappalli.
E-mail: raybinjose@yahoo.com.

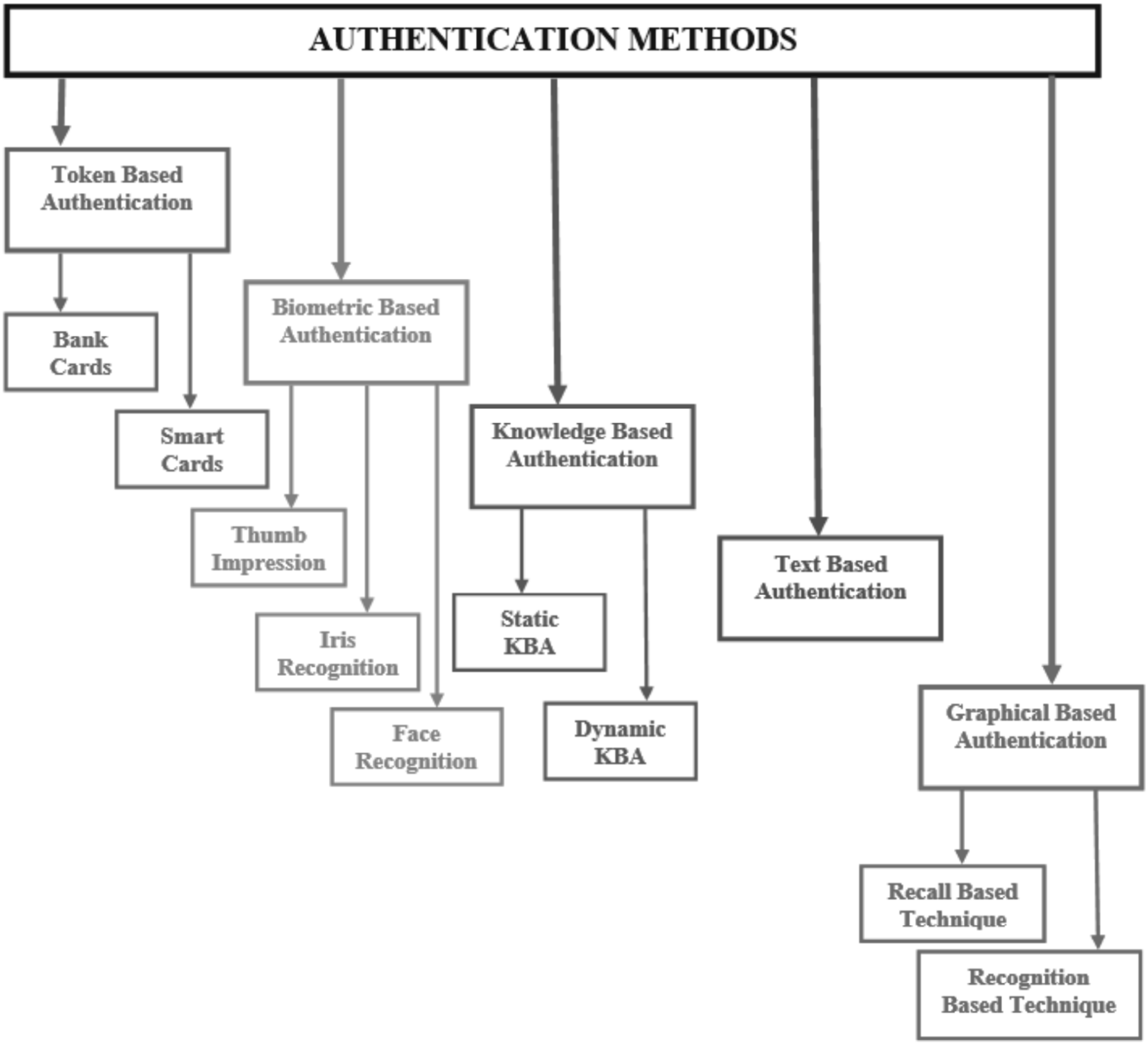
AUTHENTICATION METHODS
Token Based Authentication
Bank Cards
Smart Cards
Biometric Based Authentication
Thumb Impression
Iris Recognition
Face Recognition
Knowledge Based Authentication
Static KBA
Dynamic KBA
Text Based Authentication
Graphical Based Authentication
Recall Based Technique
Recognition Based Technique

Figure 1: Classification of Authentication Methods

Text based authentication involves authenticates a person [12] to avail the system in protected manner. It allows only the person who has provided the user details in the registration phase. It does not allow any person who has not entered the details in the registration phase. Text based authentication provides low security features but high usability features. Graphical based authentication is mainly graphical image oriented. Graphical based authentication provides both the security and usability for user [12]. Using graphical based authentication, we can send the data in a hidden way. It cannot be easily captured by an intruder.

2. ANALYSIS OF AUTHENTICATION METHODS

There are five types of authentication techniques, they are,

1. Token based authentication
2. Biometric based authentication
3. Knowledge-based authentication
4. Text based authentication
5. Graphical based authentication

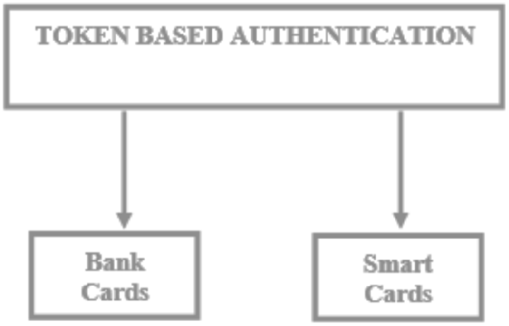

Figure 2: Categories of Token Based Authentication

2.1 Token Based Authentication

Token Based authentication methods are used popularly in smart cards.

2.1.1 Bank card

Bank cards are used to accomplish bank transactions. To protect the user details, bank cards, have the unique identification number. The bank cards are helpful in maintaining the user details in secured manner.

2.1.2 Smart cards

Smart cards used mainly in the shops to show the identity of the user and protect from misuse by another person. Token Based have the problem in the password. So, it is easily theft by the other members. To avoid this method to use the biometric-based authentication.

Celestine Lyn Paul [1] gave the perceptions of the 24 participants in 10 weeks about the smart card authentication. The drawback in this work is that the smart card supported applications are less in number. Vaibhav Kale [2] proposed the mobile based authentication scheme in which a QR code is using for the bank security. The AES algorithm is used for the mobile based authentication. This gives security to the data. Min-Shiang Hwang [3] explained the remote user authentication used for smart cards. This scheme is divided into the three phases. They are

(a) Registration Phase
(b) Login Phase
(c) Authentication Phase.

It is mainly used in with a password file or a verification table.

2.2 Biometric Based Authentication

Biometric Based Authentication is used nowadays. Biometric gives more security. Presently several new types of biometric devices are used. Biometric authentication provides authorization to the valid users. Thefts can be controlled by biometric-based authentication. Different Biometric Authentication practices are given below,

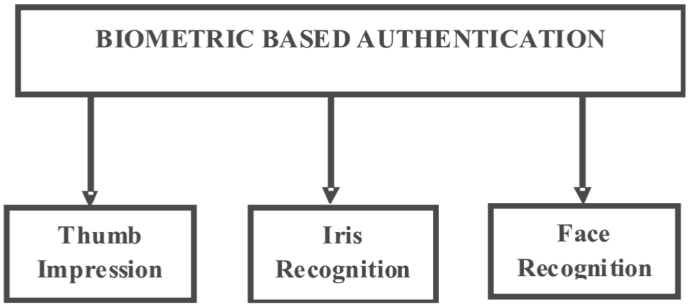

Figure 3: Types of Biometric Based Authentication

2.2.1 Thumb impression

The thumb impression is an important personal identity. Every person in the world has a unique thumb impression. It is prominently used in authentication.

2.2.2 Iris Scanning

The iris scanning is also used in biometric-based authentication. This technique is used in aadhar cards as a proof for the personal identity. In the aadhar card process there are three stages are follow,

1. Design the iris recognition code in the MATLAB
2. Obtain the output in the form of string and send it to the COM port of PC.
3. Receive the COM port data from the microcontroller and display in the LCD screen.

2.2.3 Face recognition

The face recognition is also used in biometric authentication. This is used to find the person accurately. It used in the attendance system in companies.

Anita Rana [4] explained that in upcoming days biometric will play a major role in everybody's life. The biometric devices are used in the Military, Wildlife, and used in many other applications. The biometric devices are in different sizes. The security scheme is used in trust management. In this the trust management system it checks the sender node with another node. After receiving feedback, it finds and erases the unwanted packets. Rubal Jain [5] explained a biometrics system that has various attacks on the biometric templates and it utilizes techniques to protect from the attacks on biometrics. Quratulain *et. al.* [6] proposed the biometric system is the emerging field technology. This paper gives the different reviews on the biometric systems. This survey tells that 95% to 100% results in biometric systems are accurate. Biometric provides better security. Bhanu Priya Taneja [7] tells about a system to find the signature is the real or fake. This paper explains the ways to find the real signature of a person. This job was done on the different stages of testing. Mukesh D. Rinwa [8] explained that face recognition is the growing fast technology in the research field. It used to check individual's identification. In this paper, different techniques are used to represent the face. The commonly used techniques in the face recognition are LBP, ELBP, LTP, LDP, LTrP, and, LDN. Pooja Chugh [9] proposed a voting system with biometric techniques.

In order to reduce the voting time and manual work, a biometric system is developed and used. By using the aadhaar number the government system database attaches to the aadhaar number database. This biometric system helps in reducing the fake votes. Sunny Shahdadpuri [10] explained about the face and the hand gesture recognition for personal identity. A new model of the Hidden Markov Model (HMM) proposed and it yielded about 99% of success in the rate of recognition. SVD (Singular Values Decomposition) coefficients feature are also used for hand gesture system and skin segmentation. Neyire Deniz Sarier [11] proposed a biometric based verification system. The remote authentication based on the server-side functionality is used to store the data in the biometric system. This paper tells the different storage mechanisms using biometric techniques. This system is used to save time and the storage cost of the database.

2.3 Knowledge Based Authentication

Knowledge-based authentication is commonly known as KBA, this technique authenticates a person who is accessing the website unofficially and gives usage details. The two types of knowledge-based authentication are Static KBA and Dynamic KBA.

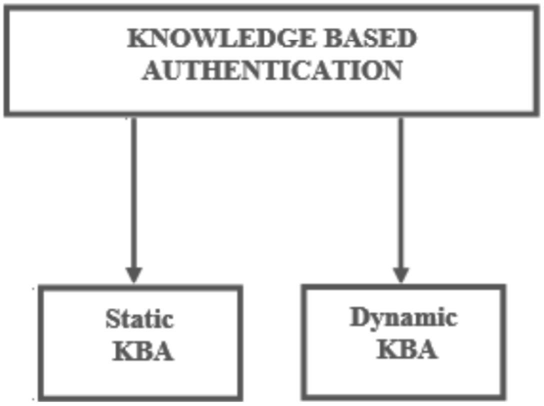

Figure 4: Types of Knowledege Based Authentication

3.1 Static KBA

Static Knowledge Based Authentication shares the secrets. It used in the banks, IT companies etc. The email subscriber is to show authentication of the user before the user performs the function or they give the password to the user if they forget the password.

3.2 Dynamic KBA

The dynamic knowledge is the top-level of authentication. Knowledge based questions are used to check each single authorization.

According to Manjunath D [12] in the olden days the text-based passwords are used, but now a day’s biometric systems are used. This paper promotes graphically oriented passwords because they improve the security as well as the authentication. It avoids the weak passwords. Nikhil Tarkeshwar Ambade [13] explains that the text-based passwords are used often, but they are easily attacked by the hackers, and this leads to loopholes in security. Nikhil Tarkeshwar Ambade [14] also proposed that alphanumeric passwords are easy to remember therefore, hackers easily find out these passwords. But, strongly coined passwords are tough to find out and therefore these type of passwords can be used by the user. Persuasive cued click point technique is a better technique, which can be adapted in such situations.

3.4 Text Based Authentication

The text-based authentication authorizes the user and gives the permission to the user on entering a valid text-based password to do the intended function. The usage features of text-based passwords are high, but they are low in the security features, these passwords can be easily tracked by the intruders.

3.5 Graphical Based Authentication

Graphical based authentication is the form of text-based authentication. In Graphical based authentication a picture is shown, when the user clicks on the regions that are the passwords access is permitted, otherwise the user is denied access.

There are two types of graphical passwords. They are

(i) Recall Based and (ii) Recognition based Authentication techniques.

3.5.1 Recall Based Technique

Recall based technique uses graphics that are created or selected during the registration process. The three types of recall based techniques include

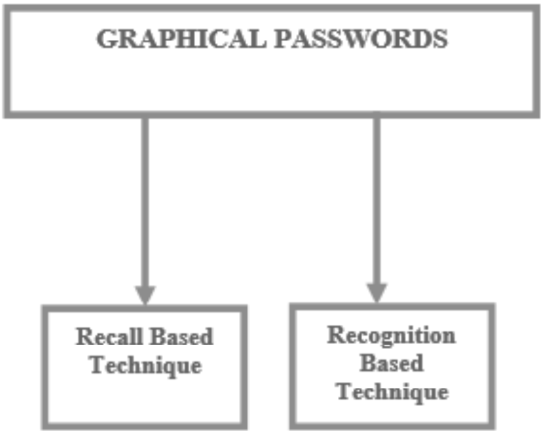

Figure 5: Techniques of Graphical Based Authentication

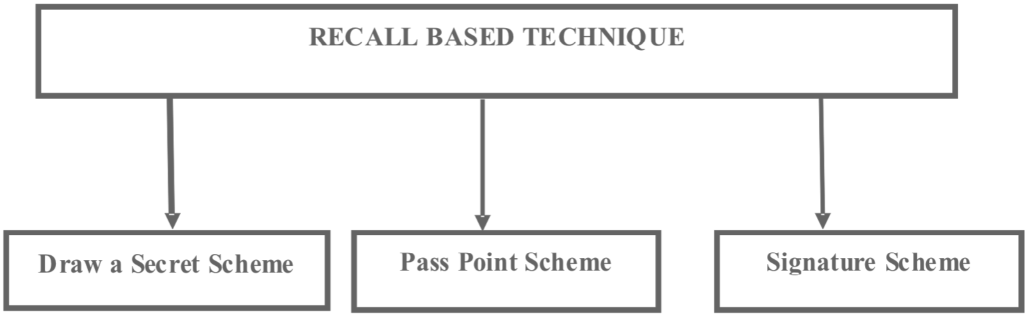

Figure 6: Types of Recall Based Techniques

(i) Draw a Secret Scheme, (ii) Pass Point Scheme,
(iii) Signature Scheme

3.5.1 (a) Draw a – Secret Scheme

Draw-a-Secret Scheme (DAS), is a technique which is purely a recall based technique, where the user has to secretly draw an image during the registration phase [1] In order to login the secret image must be selected.

Pass shapes technique is proposed by Weiss and De-Luca. In this method, the graphical passwords are turned into alphanumeric. It is based on 8 stroke angles and 45-degree intervals. In a different scheme to DAS, Tao and Adams structured Pass-Go technique where the user has to choose the intersecting points on the grid in the same order selected during the registration phase to access the system. Pass faces scheme is a recognition based technique, the user pre-selects a set of people faces during the registration as a password. During the login process user faces are shown and the user has to select the correct face to enter into the system.

3.5.1 (b) Pass points scheme

In the pass points scheme, the password consists of an order of five click points on the given image. The user has to chose the click points in the proper order to login into the account successfully. Here, the user can use the built-in images or the other images. The example for this is the android pattern lock model.

3.5.1 (c) Signature scheme

In the signature scheme the user writes the signature and it is matched with the signature with that of the person stored in the memory. During authentication signature is verified, if it does not match with the available signature, it eliminates the signature.

3.5.2 Recognition Based Technique

Recognition based technique is the easiest technique and the user can effortlessly use this technique to gain access to the system. The user is asked to write something on his or her own hands and a PIN number is allotted to the user for authentication. After submitting the proper pin number the user is asked to find the drawn image. If the user selects the correct image drawn during the registration process the authentication process will be completed positively. The pass face scheme is an example of the recognition based technique.

CONCLUSION

The different types of authentication techniques used currently are analyzed in this work. The biometric authentication is the latest and it is more reliable than other techniques. Knowledge based Authentication is helpful in tracking unofficial users of websites and providing their usage details. Token based authentication techniques are very much helpful in handling smart card authentications. Graphics based authentications techniques are reliable and makes the authentication process simple for the users. Even though text based authentication techniques are not too strong they are widely accepted and used because of their popularity and simplicity.

REFERENCES

[1] Celestine Lyn Paul, Emile Morse, Aiping Zhang, Yee-Yin Choong, Mary Theofanos., “A Field of User Behavior and Perceptions in Smartcard Authentication,” *National Institute of Standards and Technology*, 1-17, 2011.

[2] Vaibhav Kale, Yogesh Nakat, Sameer Bhosale, Abhijeet Bandal, Ramesh G.Patole., “A Mobile Based Authentication Scheme Using QR Code for Bank Security,” *International Journal of Advance Research in Computer Science and Management Studies*, **3**, 2015.

[3] Min-Shiang Hwang, Li-Hua Li.,”A NEW REMOTE USER AUTHENTICATION SCHEME USING SMART CARDS,” *IEEE Transactions on Consumer Electronics*, **2**, 2016 .

[4] Ankita Rana, Er. Ankita Mittal., “A REVIEW ON VARIOUS SECURITY FLAWS AND THEIR POSSIBLE COUNTER MEASURES OVER WIRELESS SENSOR NETWORK,” *International Journal of Advance Research and Innovative Ideas IN education*, 2, 2016.

[5] Rubal Jain, Chander Kant., “Attacks on Biometric Systems: An Overview,” *International Journal of Advances in Scientific Research*, 283-288,2015.

[6] Quratulain, Hadeeqa ayat, Iraq Arshad, Aliya Ashraf Khan.,”Biometric Security through Multimodal Systems,” *International Journal of Advanced Research in Computer and Communication System Engineering*, **2(3)**, 510-517, 2015.

[7] Bhanu Priya Taneja, Navdeep Karur, “Biometric System Based on Off-Line Signatures,” *International Journal of Advanced Research in Computer and Communication Engineering*, **4**, 2319-5940, 2015.

[8] Mukesh Rinwa D, B.S. Borkar., “Face Recognition System using Local Feature Descriptors: A Survey,” International *Journal of Advanced Research in Computer Engineering & Technology*, **4**, 2015.

[9] Pooja Chugh, Pradeep Dimri., “Review of existing Indian Voting System and hybrid design using Biometric Security in Voting Authentication Process,” *International Journal of Electronics and Computational System*, **4**, 2015.

[10] Sunny Shahdadpuri, Bhagwat Kakde., “Face Recognition and Hand Gesture Analysis System,” *International Journal of Science and Research*, **5**, 2016.

[11] Neyire Deniz Sarier, “A Survey of Distributed Biometric Authentication Systems,” **155**, 43-44, 2009.

[12] Manjunath D, Nagesh A S, Sathyajeeth M P, Naveen Kumar J R., “A Survey on Knowledge-Based Authentication,” *Journal of Emerging Technologies and Innovative Research*, 2, 2015.

[13] Nikhil Tarkeshwar Ambade, Prof. Dr. Arati Dixit., “Graphical Passwords Authentication: A Survey,” *International Journal of Computer Science and Mobile Computing*, **4**, 247-254, 2015.

[14] Nikhil Tarkeshwar Ambade, Prof. Dr. Arati Dixit., “Robust Authentication Based Graphical Passwords Mechanism,” *International Journal of Computer Science and Mobile Computing*, **4**, 1049-1056, 2015.