International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Survey on Authentication Techniques and User Recognition

Vyanktesh Dorlikar[1], Anjali Chandavale[2]

[1]Department of Information Technology, MIT College of Engineering, Pune, India

[2]SMIEEE, Department of Information Technology, MIT College of Engineering, Pune, India

Abstract: ***Today Mobiles, Computer, Laptops, PDAs are becoming widely popular and largely used. The available authentication techniques are able to secure the device or the area by the use of Knowledge, Possession and Inherence factor. When the use of smart phones for authentication comes into consideration, it becomes a critical task because of complexity, security and the various fluctuations in the wireless medium. The various successful authentication systems in existence are dedicated fingerprint scanner, iris scanner and CCTV, etc. This paper provides the review for various existing authentication methods. Here we have listed authentication methods under the three main categories, first is an Integrated Windows Authentication, where the communication is done with the trusted Kerberos server to obtain a shared secret key. The second is a Basic Authentication system consisting of username/password and trust authentication. The third form of authentication system is a Multifactor Authentication method that is a process of computer access control in which combination of any two from possession, knowledge and Inherence is used to access the system or the area. The methods are discussed in detail throughout the paper.***

Keywords: Authentication Modes, Biometrics, Multifactor Authentication, Face Recognition, Comparing Authentication Modes.

1. Introduction

The mobile technology has many uses such as network administrator set up an alert system, generation of alarms in case of thefts, data wiping if the phone is stolen, push notifications, etc. Thus with application of such mobile technologies most innovative, reliable and secured authentication techniques are developed in the current scenario.

User recognition by using biometrics is a very active research area from the last decades. Numerous techniques are designed to detect and recognize the biometric signature. In this paper, we studied and evaluated various authentication techniques developed till date and presented the methodologies explored so far. Since remarkable shift is observed in considering more than one factor as Face, Voice etc. and other elements in the development of such techniques, understanding existing methods, factors and techniques is considered to be prerequisite for further progress. This paper reveals such techniques, approaches and factors considered for development of authentication systems so far.

Section 2 presents Authentication Techniques. Section 3 Analysis and Application Section 4 Conclusion and section 5 presents Literature referred to the survey.

2. Authentication

Authentication is the process of identifying and verifying an individual, on the basis of username and password. In security systems, authentication and *authorization* are two different terms, authentication is the process of giving persons access to the system or area according to their identity [1]. Authorization is a process of specifying access rights to resources or individuals.

The various types of authentication methods are in existence, such as integrated Windows authentication, Basic authentication and Multifactor authentication.

2.1 Integrated Windows Authentication

An integrated windows authentication technique sometimes called as WindowsNT, NTLM or Challenge/Response authentication. In this authentication technique the user name and password are hashed while sending across the network. The technique uses web browser involving hashing and cryptographic exchange of password.

Windows user information about the client is used for authentication in integrated windows authentication. When authentication exchange fails to authorize the user, Web browser ask for the user windows account user name and password, and then it processes with the use of integrated windows authentication. Then web browser prompts the user for the correct user name and password till three times. As soon as the user is logged on to the local computer as a domain user, authentication is not required when the user accesses a network computer in that domain. [2]

There are two types of Integrated Windows Authentication, Kerberos and Security Support Provider Interface. In the Kerberos system, authentication is done by finding a trusted Kerberos server for obtaining a shared secret key. In Kerberos authentication system only the users having the key can communicate with each other because of key and encryption-decryption of messages sent by the users. The logical part of the Kerberos server is that, Kerberos governs key distributions called the Key Distribution Center (KDC). Once keys are distributed to two users wishing to communicate, Kerberos then issues a ticket through the Ticket Granting Server (TGS). These tickets allow user for the actual communication. [3].

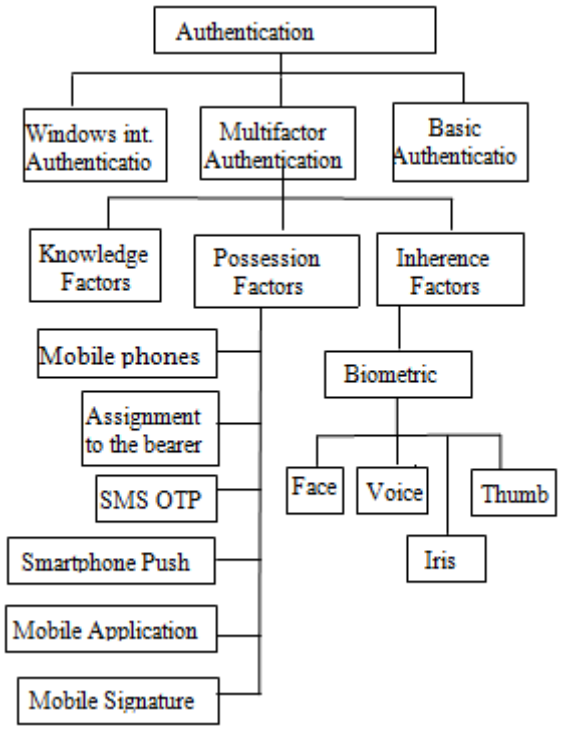

Figure 1: Types of Authentication Techniques

The Security Support Provider Interface authentication depends heavily on Kerberos and is only viable when the server and client are both running in windows. The *security support provider interface* authentication allows mapping amongst its system, the server and the database. [3]

2.2 Basic Authentication

The one of the most common form of authentication system is a username/password system for authenticating the persons and trust authentication for authenticating the communications. In username/password technique, the system relies on the difficulty of guessing the password [4]. There may be some questions about the security about what constitutes a good password which are now a day's used by the banking system i.e. security question followed by the password. In trust authentication, post restructured query language assumes that every user who wants to connect to the server is authorized to gain access to the database regardless of the user name they cite. The trust authentication is a type of authentication is popular with local area networks in which there is a single server and also it is used for multi user machines only if the restrictions of the domain (such as UNIX) are made on the server.

2.3 Multi-Factor Authentication

Multi factor authentication method is a process of computer access control in which present authentication factors from at least two of the three categories to access the system or the area. [5]
1) Knowledge factors - things only the user knows, such as passwords.
2) Possession factors - things only the user has, such as ATM cards.
3) Inherence factors - things only the user is, such as Biometrics.

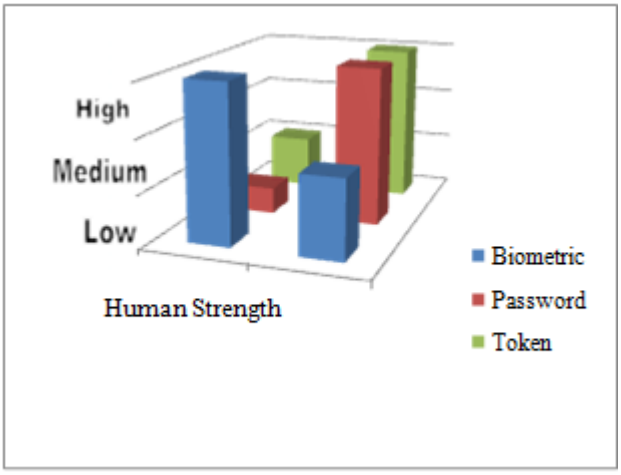

Figure 2: Comparing Authentication Mechanism [6]

1) Knowledge Factors

Knowledge Factors means something only the user knows; this is a common form of authentication such as ID password. In this authentication form, the user is required to enter a secret key in order to authenticate and access the system. A password which should be numeric, alphanumeric or string, including special symbols is used for user authentication. [4]

2) Possession Factors

Possession Factors, something only the user has, this methodology is used for decades for authentication, in the form of a key to lock. The main principle is that the key is a secret and is shared between the granted persons, this same principle created for authentication in computer systems or in the geographic area. [7]

Authentication Method	*Assurance Level*	*Token Type*
Password	Level 1-2	User Selectable
SMS/Token	Level 3-4	SMS, mail, Self Collection
Biometrics	Level 1-4	User him/her self

Figure 3: E-Authentication Method Comparison [10]

(a) Mobile Phones: A newly developing category of two factor authentication tools transforms the PC user's Smartphone into the token device using, text messaging, telephone call, or by the help of some downloadable application to a Smartphone. Since the user communications done over two different channels, the mobile phone now becomes a two-factor authentication device. Such as authentication having ability to scan a QR code by a Smartphone as your two-factor authentication.

(b) SMS one-time password: In Short Message Services (SMS) One Time Password (OTP) method, one time password provided to the user with the help of text message, push notification or voice call. Most of the banks and mobile software use the One Time Password services for the transactions and authentication. [5]

(c) Assignment to the bearer: The basic limitation of mobile phones for secondary authentication is that the respective

user must have the access to a mobile phone during authentication procedure. The user may not use the mobile as office appliances from the home procedure. For converting the mobile phone from a personal appliances to an office appliances for usage inside and outside of the premises must be there. Some circumstances should be undertaken such as mobile phone lost etc.

(d) Smartphone push: The push notification services are developed in modern mobile platforms, such as the iPhone and Android phones, which are used for providing a challenge/response mechanism on a mobile. While performing a sensitive transaction or login, the mobile will instantly arise a notification, which pushed to mobile phone containing full details of user's transaction and the user responds to deny or approve the transaction by simply pressing a button on their mobile phone [8].

(e) Mobile applications: Smart phones and tablets now a day's having capability of downloading applications which are highly secured. This method allows a cryptographic key to be used to authenticate the user, which protects from a man-in-the-middle attack. Examples of this type of services are Mahasecure, star token etc.

(f) Mobile signature: Mobile signatures are digital signatures usually created by using a Subscriber Identity Module (SIM) card, on the mobile device with a private key of the user. In this system text is signed and securely sent to the SIM card of a mobile phone. The text message of the user is displayed by the SIM. User checks it before putting a PIN code to form a signature, which then sent back to the service provider of SIM. [9]

The authentication methods are compared according to assurance level. Above table established registration requirement specific to each level. There is no specific requirement for level 1. Both remote registration and in-person registration required for level 2 and 3. Explicit requirement is required for every scenario in level 2 and 3. Finally, only in-person registration required for level 4. [10]

3) Inherence Factors

Inherence factors are something only the user is; the definition of true multi-factor authentication is satisfied by Biometric authentication. Users are biometrically authenticated by their fingerprint, voice print, and iris and face scan using provided dedicated hardware and then enter a password in order to get access to system or area [11]. Biometric authentication is the most secure way of authentication till date.

(a) Biometrics and Smart Phones: The development of an authentication system for smart phones using finger photos and the research of finger photo recognition under daily circumstances has very recently raised a lot of attention. Due to the inability of most cameras to focus on the finger, only one of the five evaluated smart phones was able to capture suitable finger photos [12]. The work of Dreamiest is concerned with finger photo recognition with two different smart phones. The results are not comparable with this work because the photos were taken only in one session and under different conditions and processing was done offline on a PC. Moreover, one Smartphone was placed on a fixed hanger to capture the finger photos. The achieved Equal Error Rate(EER) was 4.66%. The other one was held by a (third) human operator. The result was an EER with 14.65%. Both conditions do not correspond to a realistic scenario. Finger photo recognition with a lower resolution camera in a fixed position under laboratory conditions was tested in 2010. A continuous shooting mode for the camera was used to capture multiple photos at once from test subjects in one session. A low EER up to 1.23% with preprocessing of the captured photos was achieved under the mentioned circumstances. The work of Muller and Sanchez-Refloat shows that finger photo recognition is even possible with web cams. Web cams without auto-focus have the ability to focus on very close objects. A lower resolution of 640x480 pixel of the finger photos is sufficient. A False Acceptance Rate (FAR) of 0.18% and a False Rejection Rate (FRR) of 10.29% were achieved. [13].

(b) Facial recognition system: A facial recognition system is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source [14]. A simple ways to do this is by using facial database and comparing the selected face from the image. Some face recognition algorithms identify face features by extracting landmarks, and features, from an image. For example, an algorithm may analyze the size of face, position of facial features, and/or shape of the eyes, jaw, cheekbones, and nose. This image features are then used to search for other images of matching features. Some other algorithms normalization of facial images and then compresses the face data and saves the data in the image which is useful for face recognition. A probe image is compared with the face data [15]. Recognition algorithms are divided into two main approaches, photometric, the statistical approach where extraction of an image values and a comparison of that values with templates to eliminate variances or geometric, which look at distinguishing features [16].

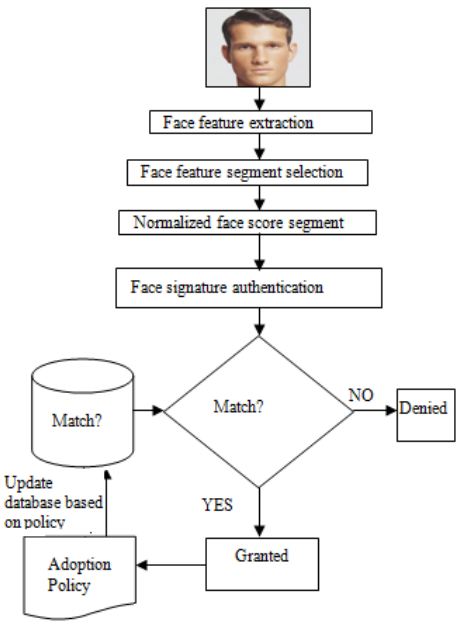

Figure 4: Flow of face recognition systems [13]

Popular face recognition algorithms include Elastic Bunch Graph Matching using the Fisher-face algorithm, Principal Component Analysis using Eigen-faces, Linear Discriminate Analysis, the Multi-linear Subspace Learning using tensor representation, and the neuronal motivated dynamic link matching [17].

(1) 3 Dimensional Recognition: The main advantage of 3D face recognition is that it is not affected by changes in lighting. This technique also identifies facial features from a various range of viewing angles. 3D data points from a face vastly improve the precision of facial recognition. 3 dimensional researches are enhanced by the development of sensors that do a better job of capturing 3D facial image. These sensors work by projecting the structured light upon the face. A dozen or more number of image sensors placed on one CMOS chip. Each sensor captures a different part of the spectrum. For that goal a group at the Technion on applied tools from metric geometry to treat expressions as an isometrics. A company called Vision Access created a firm solution for 3D face recognition [18].

(2) Skin Texture Analysis: Skin texture analysis is one more emerging trend where the visual details of the skin are used. This technique called skin texture analysis, turns the unique lines, spots apparent, and patterns in a person's skin into a mathematical space [13]. The result of tests has shown that with the addition of skin texture analysis and performance in recognizing faces is increasing 20 to 25 percent.

Secure Socket Layer:

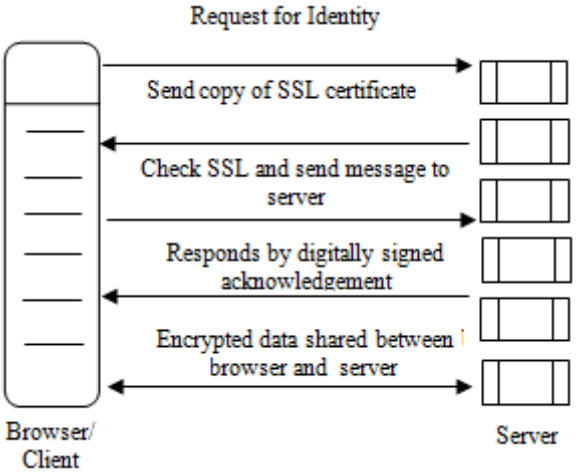

Figure 5: SSL Communication

The Secure Sockets Layer (SSL) and Indent-based types of authentication provide an excellent mode of communication, especially when the Transmission Control Protocol connection is using a Hypertext Transfer Protocol connection. When the Hypertext Transfer Protocol connection is made, a "hello" message is sent by the user to the server; then server side responds with another "hello" message. [19]

One way authentication allows an SSL client to confirm an identity of SSL server where as SSL server cannot perform an identity of SSL client. Two ways SSL Authentication is also known as mutual SSL authentication also SSL client to confirm identity of SSL server also confirm Identity of SSL client. [11]

3. Application and Analysis

The authentication techniques are developed remarkably in the last decades. A variety of techniques have emerged, influenced by developments in related fields as discussed in this paper. This paper provides comprehensive discussion and provides insight into the concepts involved and perhaps provoke further advances in the area. Most of the authentication technologies which are in existence are developed further to provide more secured authentication. Out of above discussed techniques multifactor authentication techniques are more reliable and useful. Considering the current scenario and as the use of Smart Phone is pervasive and become a necessity of life, more advanced authentication techniques is a need of time and thus more secured and reliable techniques are on the way of development.

These techniques are used in various sectors such as Security, Defense, Research Centers, IT Companies and offices.The biometric is most secure authentication technique. This technique is not reliable as the scalability increases because of the dedicated scanners. Now days after authorization user get access to the area, but no technique is available to monitor the user activity. For monitoring user's activity and to reduce the effect of scalability, smart phone can be used as the authentication device using the biometric signature captured by mobile phone camera.

4. Conclusion

The Authentication applications are developed with the use of various techniques. In this paper three techniques were discussed. The techniques began with Basic Authentication, which considers user name and password system to Multifactor Authentication which considers knowledge factors, possession factors and inherence factors. The Multifactor Authentication technique is most secured among discussed authentication modes. Other secured techniques such as Windows Authentication and Secured Socket Layer are developed and used in the internet or the system usage authentication. If we are focusing on authorization of the restricted area, most of the authentication must be done with the help of biometric signature. Various dedicated scanners are required to scan the biometric sign and unavailability of technique to monitor user's activity raised problem to some extent. With the advancement in technology and widespread use of smart phones, it is found that various techniques are developed for authentications, as it has provided ease of modes for authentication and clubbing of two or more techniques provided more secured and reliable framework. The authentication techniques in smart phones such as Biometrics, Facial Recognition, Voice Control access and location tracking are also developed and widely used in individual capacity along with organizational level. Consistent development is on the way including 3-Dimensional authentication techniques. Skin Texture Analysis in facial recognition provides more ease of use and reliable approach for authentication. We have included a list

of references sufficient to provide a more detailed understanding of the approaches described. We apologize to researchers whose important contributions may have been overlooked.

References

[1] A. Jameer Basha, V. Palanisamy, T. Purusothaman.*"Multimodal Person Authentication using Qualitative SVM with Fingerprint, Face and Teeth Modalities"* International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-1, Issue-4, April 2012

[2] G. Andrew Duthie, Matthew MacDonald , "*ASP.NET in a Nutshell"* pp 191-200.

[3] Shengli Liu, Wenbing Wang and Yuefei Zhu, *"A New-Style Domain Integrating Management of Window sand UNIX "* WAIM '08. International Conference, 2008, Page(s): 619 – 624.

[4] Chaudhari, S., Tomar, S.S. ; Rawat, A., "*Design, implementation and analysis of multi layer, Multi Factor Authentication (MFA) setup for webmail access in multi trust networks* ", Emerging Trends in Networks and Computer Communications (ETNCC), 2011 International Conference, IEEE, April 2011, pp 27 – 32.

[5] Mohammed and M.M., "*A multi-layer of multi factors authentication model for online banking services" Elsadig, M.Computing,* Electrical and Electronics Engineering (ICCEEE), 2013, Page(s): 220 – 224

[6] Philip Statham, "*Threat analysis*", Boimetric Consortium Conference, September 19 - 21, 2005.

[7] Jae-Jung Kim and Seng-Phil Hong, "*A Method of Risk Assessment for Multi-Factor Authentication*", Journal of Information Processing Systems, Vol.7, No.1, March 2011.

[8] Dmitry Namiot and Lomonosov Moscow State University, Faculty of Computational Math and Cybernetics Moscow, Russia *"Geo-fence and Network Proximity",* International Conference, NEW2AN, Springer, 2013 pp 117-127.

[9] Hans Graux, and Jarkko Majava," *Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*", European Communities, 2007.

[10] William E. Burr, Donna F. Dodson W. Timothy Polk, " Registration and Identity Proofing", Information Decurity, NIST Publication, April 2006, Ch.7, Sec 7.2.1, pp 21-25.

[11] Dinesha, H. A. and Agrawal, V.K., *"Multi-Level Authentication Technique For Accessing Cloud Services* ", Computing, Communication and Applications (ICCCA), IEEE, Feb. 2012, pp 1-4.

[12] Machha Narendar, M.Mohan Rao and M.Y.Babu, " *Multi-Layer User Authentication Approach For Electronic Business Using Biometrics"* Global Journal of Computer Science and Technology,Vol.10, July 2010, pp.63-67.

[13] Muhammad Faysal Islam, DCM. Nazrul Islam.**"***Biometrics-Based Secure Architecture for Mobile Computing",* Systems, Applications and Technology Conference (LISAT), IEEE Long Island, 2012 , Page(s): 1 – 5,

[14] Rajesh Kumar Gupta and Umesh Kumar Sahu "*Real Time Face Recognition under Different Conditions*" International Journal of Advanced Research in Computer Science and Software Engineering", IEEE journal of selected topics in signal processing, vol. 3, no. 5, October 2009.

[15] Gunjan Mehta and Sonia Vatta "*An Introduction to Face Recognition System Using PCA, FLDA and Artificial Neural Network"* International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 5, May 2013.

[16] Aldrian, O, Smith, *"*Inverse Rendering Of Faces With A 3d Morphable Model *",* Pattern Analysis and Machine Intelligence, IEEE Transactions on Biometrics Compendium, Volume:35 , Issue: 5 , September 2012, pp 1080 – 1093.

[17] Yoon Young Park and Yong Keum Choi and KyungOh Lee " *A Study on the Design and Implementation of Facial Recognition Application System"* International Journal of Bio-Science and Bio-Technology. Vol.6, No.2 , 2014, pp.1-10.

[18] S. Elaiwat, M. Bennamoun, F. Boussaid, and A. El-Sallam*"3-D Face Recognition Using Curvelet Local Features"*IEEE Signal Processing Letters, Vol. 21, No. 2, February 2014

[19] *Suresh,V.M., Karthikeswaran,D. ;* Sudha,V.M. , "Web server load balancing using SSL back-end forwarding method" D.M. Advances in Engineering, Science and Management (ICAESM), International Conference, IEEE Conference Publications , Publication Year: 2012 , Page(s): 822 – 827