www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 11 Nov. 2016, Page No. 19241-19243

A Survey On Biometrics Authentication For Online Transactions

Neenu Ann Shaji, Soumya Murali, Sumitha Soman, Sandeep Hari, Sanoop Hari
Sree Buddha College Of Engineering, Pattoor, Kerala

Abstract

Authentication represents the process which verifies the identity of a user who has got the rights to make certain actions or changes in an application or on a device. Methods for authenticating users into their devices and online services have to be user-friendly and must uphold privacy.

This paper aims on discussing the different methods adopted for authentication using biometrics rather than using the conventional methods for authentication such as PIN or Password. Biometrics can be used as a very effective method against cyber theft. They are so unique that it is nearly impossible to precisely reproduce a user characteristic.

Keywords: Biometrics, e-commerce, multifactor authentication

Introduction

The followed way of authentication is by providing a security password, username etc. This method of authentication is vulnerable, as anyone having our personal details can easily carry out actions in our name. So, we have to think of an alternate method. Biometric authentication paves its way to the future, as it provides high level of security in a very user friendly manner. No one has to remember lengthy passwords anymore or carry their secret credentials and documents, as the person itself becomes the password for authenticating.

Biometrics can be defined as the physiological or chemical traits of a person. These traits will be unique for each individual and so are used for authentication purpose. They can never be stolen or replicated. And thus avoid dictionary attacks (It is a way of trying hundreds and sometimes even millions of combinations as in a dictionary so as to find the correct one), phishing attacks (fraudulent acts that try to acquire our personal information by gaining faith in us) etc.

Literature Review

The system described here will have two phases **[1]**. Data Acquisition or Learning Phase and Authenticating Phase. In the learning stage, we learn the characteristics by repeating a certain action a predefined number of times. And in the second stage, the actual authentication is done, the stored value gets compared with the read one and the decision regarding success is defined from the level of correlation of the new input with the reference one that was made in step one.

Imposters are those who try to break into our system, the rate of valid users that are passed as

impostors can be termed as FAR (False Alarm Rate) and the vice versa is termed as IPR (Intruder Pass Rate). CER (Correlation Error) determines how precise a system is. The level of accuracy, its speed, storage capacity, cost and easiness of use determine the performance of a biometric system.

In the current scenario ruled by mobile phones and their wide and extensive applications, the prime concern to be addressed is security. The system proposed in **[2]** present an innovative method which uses lip reading for authentication. Lip reading is the tracking of lip movements to identify words. This kind of systems will be safe against key-loggers since the password is not manually entered through the keypad.

Another advantage is that no additional hardware is needed for this system. In this system lip model data set is used in which different characters have been trained and stored. For faster implementation the password recognition is done offline. The password character videos are captured using the mobile phone camera. The password character videos are parsed into different frames and processed. The proposed system has two parts: Frame processing subsystem (FPSS) and classifier part. In the former part user's lip is recognized and segmented. Then feature extraction methods are applied. In the classifier part, the character in the video is recognized from the features extracted from different frames. In this way all the character videos are processed to recognize the password.

Security in online payment systems has been a wide research area since the early days of the Internet and several approaches have been devised by various Organizations.

Security of one-time password (OTP) is essential because nowadays most of the e-commerce transactions are performed with the help of this mechanism. OTP is used to counter replay attack/eavesdropping. Replay attack or eavesdropping is one type of attacks on network-connected computing environment or isolated computing environment. In **[3]**, for achieving 112 bits of security level Elliptic Curve Cryptography (ECC) needs key size of 224-255 bits while others take 2048 key size. Another issue with most of the existing implementation of security models is storage of secret keys. Cryptographic keys are often kept in en-secured way that can either be guessed/social-engineered or obtained through brute force attacks. This becomes a weak link and leads integrity issues of sensitive data in a security model. To overcome the above problem, biometrics is combined with cryptography for developing strong security model. Here gests an enhanced security model of OTP system using ECC with palm vein biometric. The cryptographic keys are also not required to memorize or keep anywhere, these keys are generated as and when needed.

Internet shopping is becoming our new trend. Several online shopping systems serve internet users all around the world and enable people to get the products they need with a small effort. Here **[4]** we propose a new solution that combines finger print recognition with online credit card transactions. The proposed system provides more

security then existing system with finger print recognition. A credit card holder is assigned a virtual credit card that shares the same account as the cardholder's physical credit card. The advantage offered by a virtual credit card is that, even if the credit card number is stolen together with other details, it cannot be used until the user redefines a new temporary limit for a new transaction.

In **[5]**, we aim to shed some light on the benefits and challenges brought about by using biometrics for securing mobile payments. Some potential solutions to address the challenges are also proposed and analyzed. Based on our analysis, it is shown that biometric cryptosystems are the suitable choice for providing security protection to biometric templates and enabling a seamless integration with the existing password-based payment systems. Moreover, the employment of stable feature sets or multimodal biometrics is able to improve the recognition accuracy of biometric-based mobile payment systems. Finally, to provide security for mobile payment systems, we propose a secure mobile payment infrastructure which combines a biometric cryptography modal with a time-synchronized one-time password (TOTP) encryption model.

In order to solve security problems facing the mobile e-commerce, a new security model in mobile e-commerce based on voice recognition is proposed in **[6]**. Voice recognition mainly consists of four steps: receiving the user voice signal, using wavelet analysis to de-noise, extracting feature and comparing the voice features. Specifically, the user's voice signal de-noising and feature extraction of voice are completed by the third party. Next, the third party sends the new voice features to the mobile e-commerce company. Mobile e-commerce company finds the latest voice features in its database for the user and compares them with the voice features which send from the third party. If it's found that the voice features consistent with each other, it also indicates that the voice recognition is passed by the system and the user is legal.

The human finger nails have a high degree of distinctiveness, even in the case of identical twins or even between different finger nails of an individual. In **[7]**, this is used as a key to develop a new biometric authentication system using a single nail plate. The nail authentication system developed is based on the high individuality of the dermal structure underneath the fingernail plate, known as nail bed. Because of inconsistent properties of growing nail plate the nail bed alone is considered. Semantic points mediation technique is used to form a pentagon structure on the nail bed and texture properties inside the structure is masked and used as Region of Interest (ROI). Principal Component Analysis (PCA), Independent Component Analysis (ICA), Haar Wavelet and Scale Invariant Feature Transform (SIFT) are used for feature extraction.

A multimodal biometric system is proposed in **[8]**. Here the multimodal biometric authentication solution is based on three identifiers: iris, voice and faces. A mel-cepstral voice recognition is described first. Then, face authentication is

approached by using SIFT-based features. Next, LAB-based iris recognition approach is proposed. The biometric fusion is performed at the level of the decision module.

Personal identification numbers (PIN) and unlock patterns are highly popular authentication mechanisms on smart mobile devices but they are not sufficiently secure. PIN or pattern mechanisms enhanced by additional, implicit behavioral biometric authentication can offer stronger authentication assurance while preserving usability, therefore becoming very attractive. In this work **[9]**, we present a comparison study on the authentication accuracy between PIN-based and pattern- based behavioral biometric authentication using both smartphone and tablet. We developed a uniform framework for both PIN-based and pattern-based schemes and used two representative methods—Histogram and DTW—for user verification.

In [10], We propose a secure, robust, and low-cost biometric authentication system on the mobile personal device for the personal network. The system consists of the following five key modules: 1) face detection 2) face registration 3) illumination normalization 4) face verification and 5) information fusion. For the complicated face authentication task on the devices with limited resources, the emphasis is largely on the reliability and applicability of the system. Both theoretical and practical considerations are taken. The low hardware and software cost makes the system well adaptable to a large range of security applications.

Conclusion

In the current scenario ruled by mobile phones and their wide and extensive applications, the prime concern to be addressed is security. As technologies for implementing a secure mobile environment is getting flourished, so is the emergence of newer and advanced security threats. This necessitates the introduction of advanced authentication systems. Biometrics can be thought of as the most important among them. Biometric features are unique to a person and they can never be forged. Even though accurate calculations are quite not possible, they can be widely used since it is the most secure way. The limitation found was that, even the same user using different hands (left and right) for authentication was identified as intruders.

References

[1] **Touch Based Biometric Authentication for Android Devices**, Alexandru-Cosmin Grivei, **ECAI 2015 - International Conference – 7th Edition**, Electronics, Computers and Artificial Intelligence, June 2015, Bucharest, ROMANIA

[2]

Mobile phone security using automatic lip read ing, Fatemeh Sadat Lesani; Faranak Fotouhi Ghazvini; Rouhollah Dianat**,** e-Commerce in Developing Countries: With focus on e-Business (ECDC), 2015 9th International Conference.

[3] **Enhancing Security of One-Time Password using Elliptic Curve Cryptography with Biometrics for E-Commerce Applications**, Dindayal Mahto, Dilip Kumar Yadav

[4] **Online Credit Card Transaction Using Finger Print Recognition**; Dr.M.Umamaheswari, S.Sivasubramanian , B.Harish Kumar , International Journal of Engineering and Technology, 2010

[5] Yang, W., Hu, J., Yang, J., Wang, S. and Shu, L., **Biometrics for Securing Mobile Payments: Benefits,Challenges and Solutions**, 2013 6th international Congress on image and Signal Processing.

[6] **Application of Voice Recognition for Mobile E-Commerce Security**, Wujian Yang; Yangkai Wu; Guanlin Chen. Circuits, Communications and System (PACCS), 2011 Third Pacific-Asia Conference on 2011

[7] **Biometric Authentication using finger nails : Emerging Trends in Engineering**, **Technology and Science,** Sathishkumar Easwaramoorthy, International Conference, 2016

[8] **Multimodal Biometric Authentication based on Voice, Face and Iris** ; E-Health and Bioengineering Conference (EHB), 2015, Tudor Barbu,Adrian Ciobanu,Mihaela Luca

[9] **Comparison of PIN- and Pattern-based Behavioral Biometric Authentication on Mobile Devices**; Military Communications Conference, MILCOM 2015, Yanyan Li, Junshuang Yang, Mengjun Xie, Dylan Carlson, Han Gil Jang, Jiang Bian

[10] **Biometric Authentication System on Mobile Personal Devices**; IEEE Transactions on Instrumentation and Measurement, 2010, Qian Tao,Raymond Veldhuis