ISSN No:-2456-2165

Biometric Based User Authentication from Mobile Phones Using User Centric Protocol

Jitty Merin Mathew
P G Student, Department of Computer Science and Engineering
Mount Zion College of Engineering
Pathanamthitta, India

Ajeesh S
Assistant Professor, Department of Computer Science and Engineering
Mount Zion College of Engineering
Pathanamthitta, India

Smita C Thomas
Research Scholar, Department of Computer Science and Engineering
Vels University,
Chennai, India

Abstract:- The main purpose of this paper is to introduce a solution for vouching user's from the security issues while using mobile phones for online resources, using a user centric solution without the involvement of provider of the identity in the execution. This is a three factor authentication mechanism. In order to generate a biometric identifier from user's biometric image, which is distinctive, changeable and replicable, a classification technique is used which involves the features extracted from the user's biometric image.

Keywords:- *Biometrics, vouching, privacy, security.*

I. INTRODUCTION

Nowadays biometrics is used as one of the main authentication solution. Because it has many advantages like distinctive, unchangeable, etc., But it has disadvantages such as non-revocability, non redundancy etc., The main aim of this paper is to generate a distinct biometric id from user's biometric images. Since biometric authentication has gained popularity most of the service providers are made use of this endorsement solution. The existing biometric endorsement solution have security and seclusion issues. The authentication mechanism uses face as the biometric characteristics. The mechanism needs the user to register their biometric characteristics with the service providers. During the time of registration, the endorsement system records data's of the registered user and is called as biometric template. The data's extracted are the stored into a database. This data's are then matched with the newly generated one. Seclusion of the generated template is an important concern. If the template containing the data's are hacked, user's may lose their seclusion for ever unless an appropriate mechanism is used. It may include mechanisms like cancelable biometrics [1].

This risk can be managed by an identity provide (IdP) based mechanism for endorsement. This mechanism allows the user to register with the identity provider. When the user needs to endorse, the service provider communicate with the provider of the identity to perform endorsement. So the user does not have to be registered and disclosed their biometric features at the third party for endorsement. Thus it better providing protection for the user's identity. But this solution has other seclusion issues. Because the IdP is participating in each activity, it can deduce the susceptible information like transaction patterns of the user.

In order to solve the above mentioned seclusion issues user based identity solution is used. It does not require the identity provider to perform endorsement. In this solution, during the registration process, the service provider can perform endorsement without the help of identity provider. For example,[2] during the registration using identities like email address, passwords etc., the user's get a token which helps them to endorse directly with service provider without disclosing their identities with the IdP. The implementation of such solution is challenging due to the reasons such as: the real owner of the identity needs to regenerate the exact feature during the registration and endorsement, it should be able to avoid identity stealing in the case of mobile phone robbery, It is vulnerable to Man in the Middle attack [9].

The main purpose of this paper is to introduce a solution for vouching user's from the security issues while using mobile phones for online resources, using a user centric solution without the involvement of provider of the identity in the execution. The proposed solution does not have the limitations that are mentioned such as: it does not require the storage of user's identity with the service provider, it does not need to store id at identity provider (IdP), it does not require the participation of identity provider,IdP in the endorsement process.

It also solves the issues in biometric endorsement solution by generating a biometric identifier from user's biometric image, which is distinctive, changeable and replicable, a classification technique is used which involves the features extracted from the user's biometric image. The proposed solution includes a key agreement mechanism to alleviate Man in the Middle attacks.

II. RELATED WORK

M. Scott [9] proposed an M-Pin protocol which displaces the existing password based authentication system which is less secured. The main issue while using the password based solution is the possibility of password robbery. The concept of M-Pin is that, it issues large encrypted secret to the enrolled user. It then verifies the

authenticity of the user by using this key. It does not need the users to store their data's on the database. M-Pin involves the usage of a third party, who is called the Trusted force. This approach mainly performs two factor endorsement. During enrollment, the user directly enrolls with the server, which maintains an encrypted password. So the server is not only responsible for daily operations, it is also responsible for user enrollment.

D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain proposed a continuous endorsement mechanism based on face. This approach uses a mechanism to fuse users mobile phones with their biometric images. It provides accuracy of the face identification. This mechanism thoroughly observing and authenticating the users activity and usage of the device. It includes a mechanism for discerning the real user.

This paper introduces our work on a face-based continuous au-thentication system that operates in an unobtrusive manner. We present a methodology for fusing mobile device (uncon-strained) face capture with gyroscope, accelerometer, and magnetometer data to correct for camera orientation and, by extension, the orientation of the face image. Experiments demonstrate (i) improvement of face recognition accuracy from face orientation correction, and (ii) efficacy of the pro-totype continuous authentication system

This paper introduces our work on a face-based continuous au-thentication system that operates in an unobtrusive manner. We present a methodology for fusing mobile device (uncon-strained) face capture with gyroscope, accelerometer, and magnetometer data to correct for camera orientation and, by extension, the orientation of the face image. Experiments demonstrate (i) improvement of face recognition accuracy from face orientation correction, and (ii) efficacy of the pro-totype continuous authentication system

This paper introduces our work on a face-based continuous au-thentication system that operates in an unobtrusive manner. We present a methodology for fusing mobile device (uncon-strained) face capture with gyroscope, accelerometer, and magnetometer data to correct for camera orientation and, by extension, the orientation of the face image. Experiments demonstrate (i) improvement of face recognition accuracy from face orientation correction, and (ii) efficacy of the pro-totype continuous authentication system

III. EXISTING SYSTEM

The existing biometric endorsement solution have security and seclusion issues. The authentication mechanism uses face as the biometric characteristics. The mechanism needs the user to register their biometric characteristics with the service providers. During the time of registration, the endorsement system records data's of the registered user and is called as biometric template. The data's extracted are the stored into a database. This data's are then matched with the newly generated one. Seclusion of the generated template is an important concern. If the template containing the data's are hacked, user's may lose their seclusion forever. It also makes use of a user centric identity based solution.

The use of this solution leads to many security issues for the user's identity while performing endorsement through user's mobile device. The implementation of such solution is challenging due to the reasons such as: the real owner of the identity needs to regenerate the exact feature during the registration and endorsement, it should be able to avoid identity stealing in the case of mobile phone robbery, it is vulnerable to Man in the Middle attack. This solution is not useful for performing authentication since it does not provide security against attacks such as Mafia Fraud attack also called as Man in the Middle attack. In order to overcome the disadvantages of the existing system, the proposed system is implemented which uses a user centric endorsement solution.

IV. PROPOSED SYSTEM

The proposed approach involves three components: User, Service Providers-an organization which provides services for using internet, Identity Provider-provides user endorsement services. The proposed system includes two phases: Enrollment phase and Authentication phase.

A. Enrollment Phase

During the enrollment phase, a user is enrolled with the service provider to perform endorsement.

- *Generating Biometric Identifier (BID)*

The mechanism used to generate a biometric identifier is to train the biometric features of the user in a machine learning based classification technique. The main reason for using this mechanism is to met the requirement of creating distinct label of the class which is to be associated with the user. This need would not be met by a binary classifier which results only 0 and 1. The biometric identifier is generated by adding the class label with a key, K1 of 128 bits long, which is generated using a key derivation function. The result obtained is a distinct, changeable and replicable biometric identifier.

- *Training Biometric Features*

The main thing that take in to account while considering the selection of mechanism needed to train the data is that the selected mechanism must be secure and usable. This approach uses a support vector machine based classification approach to train the data. Because it protect the privacy and security of the training data. It provides the assurance for the data stored in the user's system. The data selected for training should be selective to make the artifact strong.

B. Enrollment Protocol

Certain rules are implemented for the user registration process. The protocol used is an enrollment protocol which is executed between the user and the identity provider. When the user makes a request to get enrolled in the system with identity provider, the identity provider initially performs the feature

ISSN No:-2456-2165

extraction from the user's biometric images. Then a training data is built by reserving a class label with the user's biometric features. The identity provider then generates a random value which is used as the input of the key derivation function. In the next step, a biometric identifier is constructed. Then an encrypted commitment is created by taking two values such as the biometric identifier and the next key generated from the user's password. At last the identifier is created by adding commitment, Meta data and signature of the identity provider.

C. Authentication Phase

During this phase the user's needs to endorse their identity with the service provider. In order to perform endorsement (authentication), an extended endorsement protocol is used instead of basic authentication mechanism. Because this protocol has a key agreement mechanism which helps to prevent Man in the Middle attack. This protocol overcomes the limitations of the basic authentication mechanism such as: stealing of biometric identifier ie; Man in the Middle attack. It is accomplished by the service provider in which the user needs to authenticate. This type of attack is possible because the basic endorsement solution does not make sure that the attack is not taken place since it does not perform verification before the transaction is carried out.

D. Extended Endorsement Mechanism

This is the backbone of the proposed approach. It includes a key agreement mechanism which has two main purposes such as: it helps to prevent Mafia Fraud attack or Man in the Middle attack, it generates a key to initiate safe communication.The extended authentication protocol has two separate phases such as identity validation phase and key agreement phase.

This protocol is same as that of authentication protocol except, during validating identity, the service provider sends two parameters along with the challenge created. In the second phase ie; in the key agreement phase, the user creates secret using the parameters and service provider creates a secret key using a random secret, the data in the interrupt dispatch table (IDT) and the helper data. The derived key is then used to perform a handshake to verify that the Man in the Middle attack has not taken place and perform safe communication

V. ARCHITECTURE

This portion describes the architectural implementation of the authentication solution used in the proposed approach. Fig.1 shows the constituents in the authentication solution and it also represents its flow of the execution. It has three main factors. They are: the software in our device, software of the identity provider and software of the service provider. The software present in the user's device has two sub factors: client of identity provider and client of the service provider. The software is fragmented into two because it provides reusability and confidentiality of the user data.The numbering on the arrow in the Fig.1 represents the flow of execution between the user and identity provider. The arrows that numbered 1 and 2 represents the user's registration process which is done between the user and the provider of the identity.

During the endorsement through client of the service provider, it then first make a request to identity provider (IdP) in the 3rd step which produces an identity and data. It is then provided as input to the service provider's client. In the next step, the clients then forward it to the provider. In the 7th step, the service provider then forwards two parameters back to the client. Then identity provider allows the user to perform endorsement by entering user's biometric identity and to create a key called as proof to perform handshaking in the next step. In the 9th step, the derived key is then forwarded to the service provider. If the proof created is successful, then a secure communication is established.

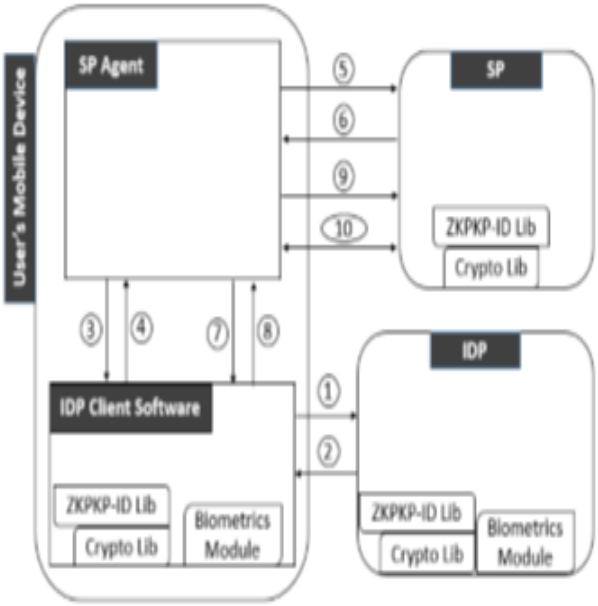

Fig 1:- Architecture of Authentication solution

VI. CONCLUSION

The proposed scheme introduces a solution for vouching user's from the security issues while using mobile phones for online resources, using a user centric solution without the involvement of provider of the identity in the execution. This approach focuses on the seclusion of user's biometric identities. The main concept behind using this approach is that it includes a key agreement mechanism which helps the user's from the Man in the Middle attack. It also generates a biometric identifier from user's biometric image, which is distinctive, changeable and replicable, a classification technique is used which involves the features extracted from the user's biometric image.

The proposed schemes provide highly feasible and strong endorsement mechanism and performs execution efficiently. This scheme uses a user centric solution to perform authentication.

REFERENCES

[1]. V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review,"IEEE Signal Process." Mag., vol. 32, no. 5, pp. 54–65,Sep. 2015.
[2]. F. Paci, E. Bertino, S. Kerr, A. Lint, A. Squicciarini, and J. Woo, "VeryIDX—A digital identity management system for pervasive computing environments," in Proc. 6th IFIP, , pp. 268–279, 2008.
[3]. M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cognit. Neurosci, vol. 3, pp. 71–86, Aug. 1991.
[4]. U. Feige, A. Fiat, and A. Shamir, "Zero-knowledge proofs of identity," J. Cryptol, vol. 1, no. 2, pp. 77–94, 1988.
[5]. Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Privacy Enhancing Technologies , vol. 5672, 2009.
[6]. Y. Huang, L. Malka, D. Evans, and J. Katz "Efficient privacy-preserving biometric identification," in Proc. IEEE NDSS, pp. 1–14, Feb. 2011.
[7]. D. Crouse, H. Han, D. Chandra, B. Barbello, and A. K. Jain, "Continuous authentication of mobile user: Fusion of face image and inertial measurement unit data," in Proc, pp. 135–142, May 2015.
[8]. T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in Proc. CRYPTO, pp. 129–140, 1991.
[9]. M. Scott. M-Pin: A Multi-Factor Zero Knowledge Authentication Protocol. Accessed: Nov. 14, 2017.
[10]. Mikhail I. Gofman, Sinjini Mitra, T.-H.K.Cheng, and N. T. Smith, "Multimodal biometrics for enhanced mobile device security.
[11]. D. Chaum, J.H. Evertse, and J. van de Graaf, "An improved protocol for demonstrating possession of discrete logarithms and some generalizations," in Proc. pp. 127–141 1987.
[12]. N. Asokan, J. E. Ekberg, and K. Kostiainen, "The untapped potential of trusted execution environments on mobile devices," in Financial Cryptography and Data Security (Lecture Notes in Computer Science), vol. 7859, A. R. Sadeghi, Ed. Berlin, Germany: Springer, 2013.
[13]. C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," EURASIP J. Inf. Secur., vol. 2011, p. 3, Dec. 2011.