International Journal of Trend in Research and Development, Volume 5(2), ISSN: 2394-9333
www.ijtrd.com

Survey on E-Voting System with Enhanced Security and Privacy

[1]Noorul Shajitha Banu.H ,[2]Murugaraj.R.K. and [2]Prabhu Rajan.S,
[1]Professor, [2]UG students,
[1,2]Department of Computer Science and Engineering, Easwari Engineering College, Chennai, India

Abstract: A security domain is the determining factor in the classification of an enclave of servers/computers. A network with a different security domain is kept separate from other networks.Examples: NIPRnet, SIPRnet, JWICS, NSAnet are all kept separate.A security domain is considered to be an application or collection of applications that all trust a common security token for authentication, authorization or session management. Generally speaking, a security token is issued to a user after the user has actively authenticated with a user ID and password to the security domain. Examples of a security domain include all the Web applications that trust a session cookie issued by a Web Access Management product and all the Windows applications and services that trust a Kerberos ticket issued by Active Directory.In an Identity Federation that spans two different organizations that share a business partner, customer or BPO relation - A partner domain, would be another security domain with which users and applications (from the local security domain) interact.

Keywords: *OTP, security, authentication, authorization, Kerberos.*

I. INTRODUCTION

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password-based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small key ring fob device with the OTP calculator built into it, or a smartcard or specific cell phone) as well as something a person knows (such as a PIN).The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further.

II. LITERATURE SURVEY

According to [1], they have proposed anapproach by using Image Based Password System (IBPS) which generates an OTP based on the image selected by the user. In this work, random numbers are generated from extracted features of image, used as OTP which forms a strong factor for authentication.In this paper images areused to generate OTP based on their features. Finally, a random OTP of variable length is created from an imagewhich is used for successful completion of authentication process. Results could be better if such work is used inreal time systems.In MATLAB platform OTPs are generated using the images. By comparing with other OTP model's theefficiency of this OTP generation technique can further be improved.

In this paper [2] ,we review the noisy password, voiceprint biometric and One-Time-Password. The most common method used for authentication is static passwords. The traditional passwords are vulnerable to dictionary attacks, shoulder surfing and eves dropping. The noisy password attempts to mitigate above mentioned problems. The biometric technique like fingerprints, palm-vein scan can be used for personal recognition. But as compared to other biometric, Voiceprint requires less implementation cost. E-commerce application uses one time password to perform E-transaction. Hence it becomes necessary to provide security while transmitting the OTP. Noisy password is an effective technique to overcome the shoulder surfing attack or peeping attack. For user authentication, if we combine Noisy password with biometric technique then it can produce a more secure system. Among all the biometric procedures, voice biometric is easy to use for normal user. It is less complex as compared to other biometric techniques. Also it requires lower implementation cost.

As proposed by [3], According to [3],a new concept that enhances the overall experience, usability and convenience of the transaction at the ATM is proposed. Features like face recognition and One-Time Password (OTP) are used for the enhancement of security of accounts and privacy of users. Face recognition technology helps the machine to identify each and every user uniquely thus making face as a key. This completely eliminates the chances of fraud due to theft and duplicity of the ATM cards. Moreover, the randomly generated OTP frees the user from remembering PINs as it itself acts as a PIN. The model shows the qualitative analysis of algorithms used based on the metrics of existing algorithms. According to the statistics PCA based face recognition is very accurate, requires less computation time and less storage space as trainee images are stored in the form of their projections on a reduced basis.

According to [4], a new agent-based scheme for secure electronic voting is proposed in the paper. The scheme is universal and can be realized in a network of stationary and mobile electronic devices. The proposed mechanism supports the implementation of a user interface simulating traditional election cards, semi-mechanical voting devices or utilization purely electronic voting booths. The security mechanisms applied in the system are based on verified cryptographic primitives: the secure secret sharing scheme and Merkle's puzzles. Due to pre-computations during the generation of agent, the voter need not to do computations. The proposed distributed trust architecture makes the crucial stage of sending votes elastic, reliable, and effective. One of the main

advantages of the proposed scheme is avoiding users' computations.Therefore it is very flexible and easy to use for all kinds of elections. A user can vote in a traditional way (the votes can be printed) or in electronic booths. The system also provides a user with mobility.The only issue in this proposed system is it requires a lot of computations.

The enhanced security of money transaction in ATM system is carried out by RFID is proposed by [5]. After getting entry, customer has to place ATM smart card in ATM machine. Then ATM machine will automatically generates a 4-digit code i.e. OTP. And that code will be message to the customer's registeredmobile number through GSM modem which is connected to ARM 7. Here customer has to enter this code. After entering OTP, System will check whether entered code is a valid one or not. This whole implementation ensures us a secured and authenticated transaction through RFID and GSM technique with lowest cost and minimum maintenance.

In paper [6],In this paper, we propose TSOTP: a new effective simple OTP method that generates a unique passcode for each use. The calculation uses both time stamps and sequence numbers. A two-factor authentication prototype for mobile phones using this method has been developed and has been used in practice for a year. We also developed atwo-factor authentication prototype for mobile phones using this OTP calculation. The prototype was used in practice for a year and provided complete protection against replay attacks and detection of forced delay attacks. The implementation had the advantage of simple one-pass authentication message exchange, no need for a third party, low computation cost and no cost for proprietary tokens.

As proposed by [7],an OTP(One Time Password) is an authentication method using a randomly generated nonce. Its purpose is to overcome security vulnerabilities that occur from using the same password for every transaction. When using a nonce as an encryption key for an encryption algorithm, for every data exchange a new random number is generated, thus creating an enhanced security process. Through utilizing this, authorization and data between Energy IoT(Internet of Things), Gateway, and User Device that exist in the same WPAN(Wireless Personal Area Network) can be protected.Through the comparison between the existing Energy IOT Mesh Network`s security to the two-factor security method, we confirm that the third party cannot threaten the low Energy IOT Mesh Network due to this two-factor security. In the near future, there is a need to recognize the importance of Energy IOT Mesh Network which is an essential element of Big Data collection and accordingly enhance security methods. The proposed security process in this paper will aid the improvement of security.

Tabulation

S.NO	Paper	Technique	Result	Issues
1	A Novel Approach For Generation Of OTP'S Using Image's	Image Based Password system	Generates an image based on OTP.	Incorrect prediction in computation can occur.
2	A Review on noisy password,Voice Biometric and one time password	Noisy password with biometric technique	Secure user authentication	Higher implementation cost
3	Enhanced security for ATM machine with OTP and Facial recognition features	Face recognition Technology	Security using OTP and Face recognition	Have to filter images which becomes complex
4	A Light-Weight e-Voting System with Distributed Trust	secure secret sharing scheme and Merkle's puzzles	Electronic voting system	Involves a lot of computations.
5	Smart ATM Access and Security System using RFID and GSM Technology	RFID and GSM technique	Secured and authenticated transaction	Investment cost is higher initially
6	A new One-time Password Method	Computation based on time stamp and sequence numbers.	Unique passcode generated	Vulnerabilities to keyboard monitor attacks, memory scan attacks and software clone attacks.
7	Design and Implementation for Data Protection of Energy IOT utilizing OTP in wireless mesh network.	One Time Password(OTP)	Secure data transmission between energy IoT gateway and user device	Inefficient topology(Mesh topology)
8	A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords	challenge/response mechanisms.	mutual authentication scheme	Lot of permutations

According to [8]the paper proposes a novel one-time password (OTP) mutual authentication scheme based on challenge/response mechanisms. In the scheme, random sub-passwords and corresponding hashes are shared between a user and a server, respectively. By performing modular algebraic operations on two or more randomly chosen sub-passwords, relatively independent OTPs can be produced in the scheme. The used sub-passwords are renewed according to random permutation functions. With tens of random sub-passwords, we can get enough OTPs that can meet the practical needs. The stores and calculations can be implemented with a microcomputer in the user's terminal. At the same time, the

scheme can provide sufficient security in ordinary applications.

CONCLUSION

From the review of various journals, it is concluded that the use of security features has been profound and made advanced by quite a lot of improved applications.OneTime Passwords are a leading technology in today's world of ttwo way aunthentication systems for more secure applications. The System can be extended and can include a user study with larger and more participants to validate the collected results and analysis of the schemes.

Reference

[1] Kalyanapu Srinivasa, Dr.V.Janaki, "A Novel Approach For Generation Of OTP'S Using Image's", International Conference on Computational Modeling and Security (CMS 2016).

[2] R. Gnana Praveen, Roy P Paily,IConDM 2013, "A Review on noisy password, Voice Biometric and one time password"International Conference on Information Security and Privacy, Nagpur, India.

[3] Mohsin Karovaliyaa, SaifaliKarediab, SharadOzac, Dr.D.R.Kalbanded,"Enhanced security for ATM machine with OTP and Facial recognition features",International Conference on Advanced Computing Technologies and Applications (ICACTA2015).

[4] AnetaZwierkoa, ZbigniewKotulskia ," A Light-Weight e-Voting System with Distributed Trust", Electronic Notes in Theoretical Computer Science 168 (2007) 109–126.

[5] Arjun K, Kalaiselvan R, ArunaJayashree R, "Smart ATM Access and Security System using RFID and GSM Technology ", International Conference on Explorations and Innovations in Engineering and Technology(ICEIET-2016).

[6] Yun Huang, Zheng Huang, Haoran Zhao, Xuejia Lai,"A new One-time Password Method",2013 International Conference on Electronic Engineering and Computer Science.

[7] Anuj Parikh,Dhvani Shah, Krupa Popat, Prof. Harish Narula "Design and Implementation for Data Protection of Energy IOT utilizing OTP in wireless mesh network"4th International Conference on Power and Energy Systems Engineering, CPESE 2017, 25-29september on Power and Energy Systems Engineering.

[8] António, Daniel Vieiraa, Hugo Fernandesc, Nelson Nunesa Nuno Costaa, , JoãoBarrosoc" A novel one-time password mutual authentication scheme on sharing renewed finite random sub-passwords" Journal on Computer and System Sciences.