Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Sensitive Data Protection Using Bio-Metrics

Namita Chandra[1], Ashwini Taksal[2], Dhanshri Shinde[3],
[1]Department of Computer,
BSIOTR (W), Pune University,
Maharashtra, India

Prof. Archana Lomte[4]
[4]Assistant Professor,
Department of Computer, BSIOTR (W),
Pune University, Maharashtra, India

Abstract— With the developing digital era, the use of internet applications has increased a lot. With the increase in the internet usage, the need of security has increased because of the increase in the hacking and phishing procedures. Moreover, every user has some sensitive and confidential data, which needs more security. One such application where the user needs more security is banking application. In this paper, we provide the security to the confidential data of the user using the OTP and the Biometric Fingerprint scanner. To give a secured application, the fingerprint of the user will be analyzed by the Biometrics device and would be checked if it matches with the database.

Keywords— Authentication, Biometrics, Digital Persona, OTP, QR Code

I. INTRODUCTION

The technology is at its peak. To match with the technology, every application is connected to the internet for a more easy approach. Now-a-days, every application executes on the internet. But with the usage of more and more internet and technology, security concerns have also increased. Moreover, the user's most confidential and sensitive data is at stake. One such application is banking services. Now-a-days the e-banking services have really comforted the users. Now all the transactions can be carried out without any problem in just one go by just moving hands on the computers or the mobiles too. Now there is no need to stand in a long queue. These internet banking have made life so easy. But at the same time, it has made life a little troublesome too[2]. With the increase in the usage of the internet, we are more prone to what is called hacking. This hacking may be of the personal sensitive data or even a key to some of the financial data of the user. For a user, both the data, personal, financial or let it be any data is of great significance. It can't be compromised at any cost. Hence, there is a need to provide the user a high security so that only the legitimate user is given an access. So it is essential that the system should understand who the legitimate user is.

Banking application is one such scenario where all the confidential data and also the financial data needs security. It ensures security, but recently a large number of scams, phishing and hacking on the bank data have really affected the actual user's status. So to protect it, in this paper, we are going to propose a system which will protect the user's confidential data with the use of OTP (One Time Password) and the Biometrics Fingerprint Scanner named, Digital Persona[10][11][15].

This will enable the user to access his data only if he is authenticated for the system and proves himself the legitimate user by scanning of his fingerprint

II. RELATED WORK

A. Based on the mathematical algorithm

Lamport [13] firstly proposed the system of one time password in 1981 by using the one way hash chain. But after the set of old hash chain is exhausted and if an indefinite series of passwords is required, then a new seed value needs to be chosen. This can be very easily hacked, as in this scenario a password file will be maintained to authenticate the user. So the risk of loss of that password file is very high and also it increases the maintenance cost. Because of this, many researchers [1][3][4][6][7][9] came up with the smart card technology to improve the security, cost and efficiency.

B. Based on the smart card

Because of the drawbacks of the mathematical algorithm of password file, the concept of smart card was proposed by the researchers [1][3][4][6][7][9]. But to carry that smart card everywhere was even more burdensome for the user.

C. Based on the time-synchronized token

These time-synchronized one-time passwords which are related to some hardware tokens. These hardware tokens contain the accurate clock that has been synchronized with the authentication server[8]. But because of the session time-outs and the carrying of the token everywhere can be troublesome for the user. Hence this approach also could not gain that much popularity. Moreover the cost of the one-time password hardware and the infrastructure requirements were also a cause for the device failure.

D. Based on the short message service (SMS)

SMSs are the widespread media of communication available on all the mobile handsets. So getting the OTP on the mobile phone is an initial step of the authentication procedure via OTP. But it is not guaranteed whether the message will be delivered, or even if it is to be delivered, how long will it take. Moreover, this SMS based scheme may incur extra charges, making it again problematic for the user.

E. OTP (One Time Password)

OTP is a one-time generated password which is valid only once. Using encryption algorithm and cryptographic keys and authentication procedures, system can check validity of password using a mobile phone where it will be sent. Normally used methods of generating OTP are security token, mathematical algorithms, text messaging, mobile phones, and proprietary tokens and other Web based methods[2]. This prevents different forms of identity theft by ensuring that a user name/password combination cannot be used a second time. Typically the user's login name stays the same, and the one time password changes with each login. One-time passwords are a form of strong authentication, and offer more effective protection to online bank accounts, corporate networks and other systems containing sensitive data. The OTP adds an extra level of protection and makes it extremely difficult for fraudsters to access unauthorized information, networks or online accounts.

OTP is very advantageous as it doesn't require the deployment of smart card readers or any drivers on the system of the user. PC and internet service provider doesn't have any mutual authentication so attacker can't identify an OTP using mock-up site.

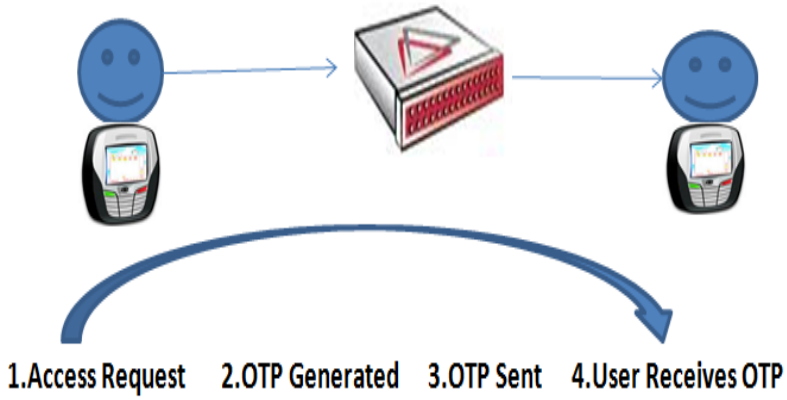


Fig 1. OTP Generation

F. QR-Code (Two-dimensional barcode)

QR or Quick response Codes are a two-dimensional barcode type that can be read using smart phones and dedicated QR reading devices , that are connected directly through link to text, emails, websites, phone numbers and via many ways.

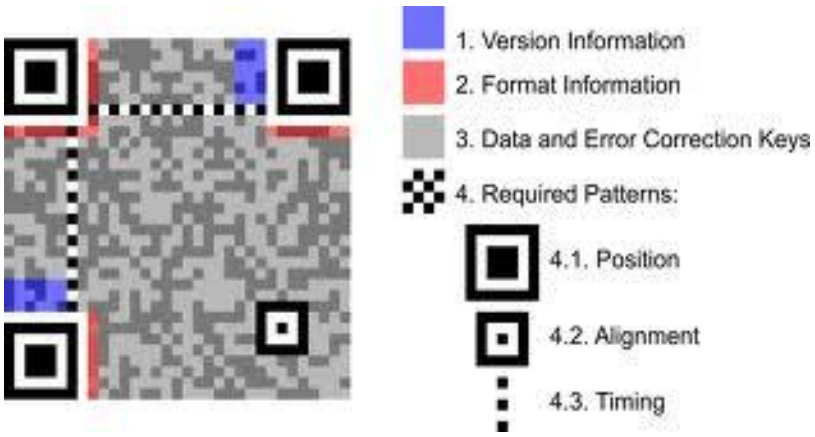


Fig 2. Strcture of QR code

The scope of use for QR codes really is huge, especially for marketing products, brands, services and anything else you can think of [2]. This kind of barcode was initially used for tracking inventory in vehicle parts manufacturing and now-a-days it is widely used in variety of industries. QR stands for "Quick Response" as the creator intended the code.

A QR-code is a matrix included code developed and released primarily to be a symbol that is easily interpreted by scanner equipment. QR-Code is very beneficial in providing the authentication services to the user, but it also has certain limitations:-Users must be equipped with a camera phone and the correct reader software that can scan the image of the QR code. Currently only smart phones are technically equipped with these kind of software. Moreover, many users that have cameras are unable to get QR reading software for their phones.

III. IMPLEMENTATION

Basically the paper is based on the application of web and a Biometric Device Fingerprint Scanner. This includes the two types of user of the system, one is the administrator and the other is the legitimate user.

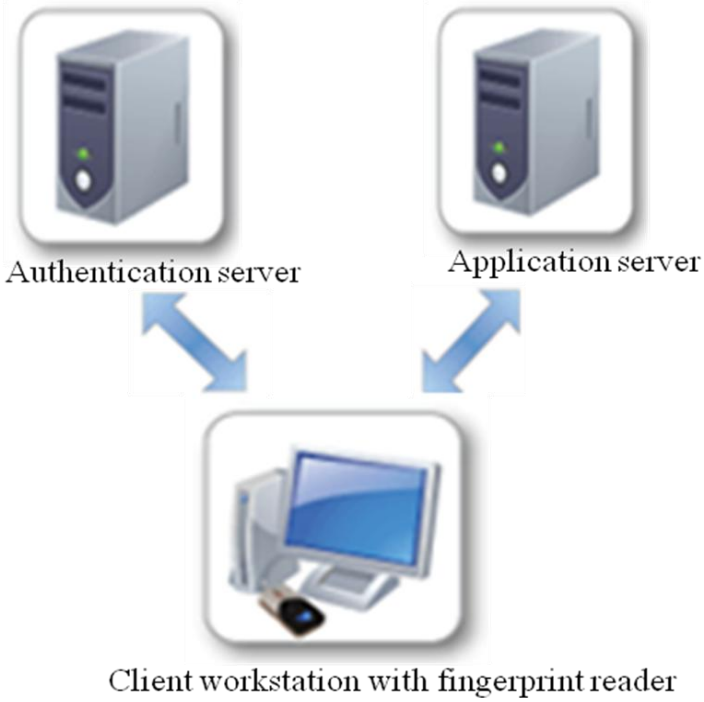


Fig 4. Actual Demonstration Of the Working Of the System

The administrator will be able to create account according to the user after the user has registered himself. Moreover he can allow or disallow user profile. For example, when the user loses his registered mobile, the administrator only can modify the details of that user. Moreover, he has the access to the details of the user, but in encrypted form. In this way, we are protecting the user's data by the administrator of the system too.

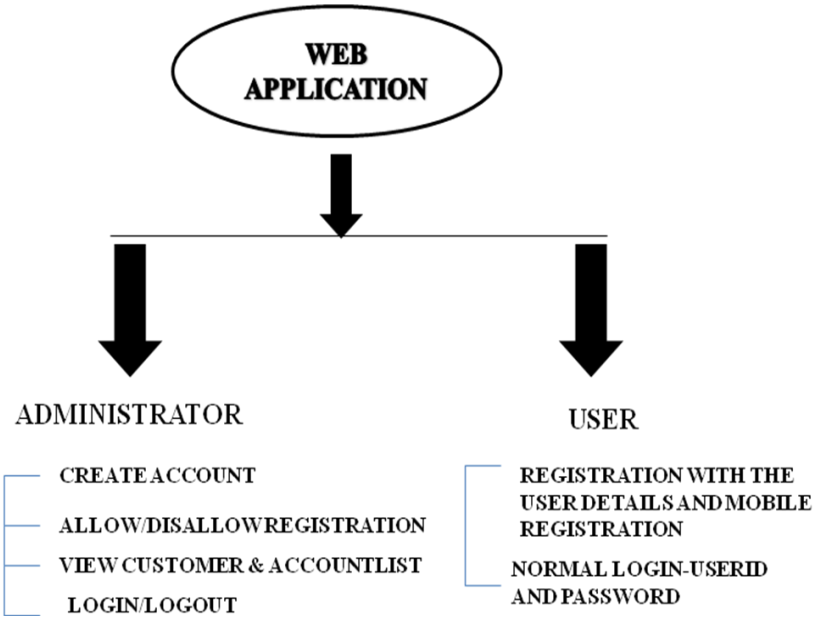


Fig 3. Actual Demonstration of the user of the system

The user firstly will register himself with his personal details and would provide his contact number for the mobile registration. Then the system would send a One Time Password (OTP) on the registered mobile. Now the user gives the OTP as specified in the initial steps of the authentication of the legitimate user. Moreover, the Biometric Device Digital Persona would scan the fingerprint of the user. Now this fingerprint sample will be validated against the saved fingerprint in the database of the bank system. If the system founds the fingerprint matching, then the database can be accessed by the user, else the system denies the access.

Moreover, the administrator is the only person who can somehow get to the details of the user as he is responsible for carrying out the various procedures like creating the account. But even if the administrator gets an access somehow to the user details, the data will be visible to the administrator but in an encrypted format.

How digital persona – the fingerprint scanner works?

Fig 5. Digital Persona – Device used for Fingerprint Scanning

Digital Persona Online is the device used in the authentication of the legitimate user[15]. This is a modular client/server software development kit which allows the user and the business to add strong authentication services to the web applications they provide with a little or no changes. It basically manages the fingerprint authentication and runs on the client side[10][11]. After downloading and installing the device and the software, the user can register their fingerprints to be saved for further authentication of the web application. After registering, the user can again and again authenticate himself for the database and can get an easy access for the database.

Moreover, this Digital Persona device supports all Digital Persona fingerprint readers and also most of the fingerprint readers built into notebooks by major computer manufacturers.

IV. ALGORITHM

I. OTP code generator algorithm

This OTP Generation algorithm is a hashing algorithm rather than being an encryption or authentication algorithm.[5]. The general approach of this algorithm is to transform a set of bytes into another set of bytes. Moreover, this is an irreversible algorithm, which means that the result can't be used to get the source.

This algorithm uses a key to transform one array of bytes into another. This secret key must be 20 bytes at least, which infers that the algorithm takes the 20 bytes secret key along with 8 bytes counter to create an 8 digit number. Moreover, this OTP will be valid for a couple of minutes.

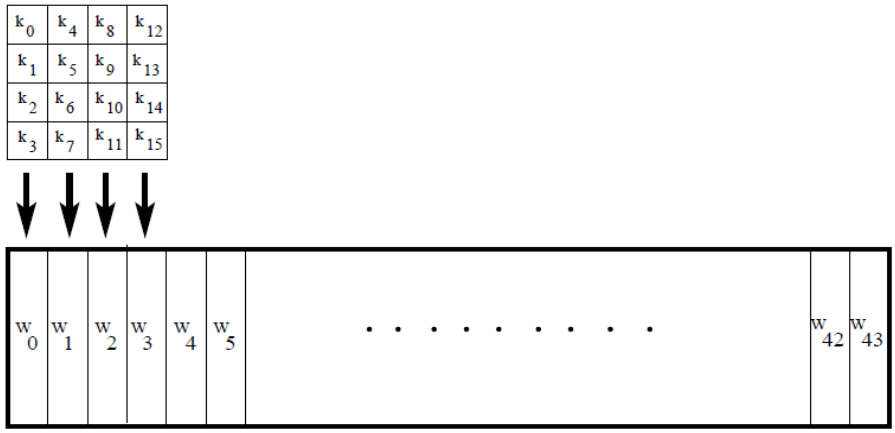
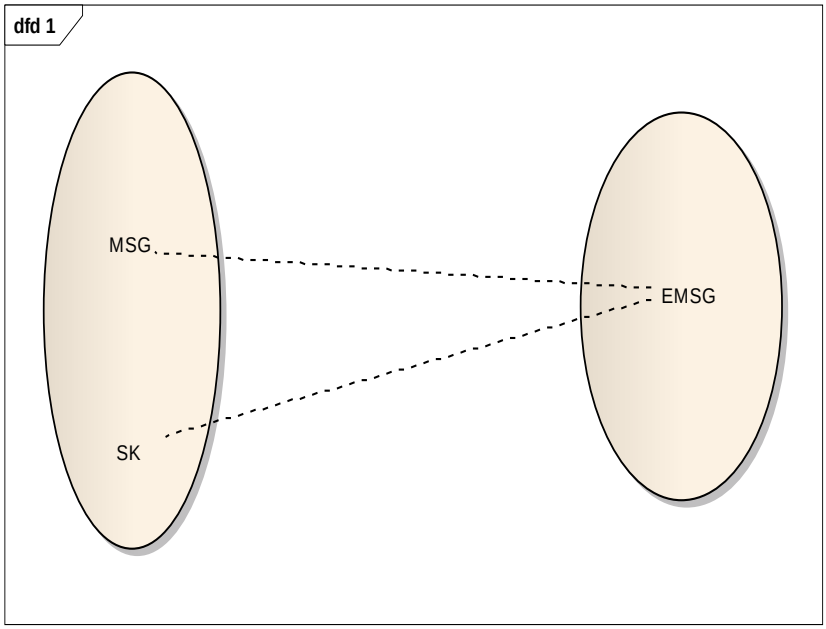
II. AES Algorithm (Advanced Encryption Standard)

Basically AES Algorithm is a symmetric key algorithm, which means that the same key is used at both encrypting and decrypting the data. Moreover, it is based on the design principle known as substitution-permutation network.

In this paper, we are applying AES Algorithm for the protection of the sensitive and the confidential data of the user. In our paper, we have implemented a system where the hacker, even if hacks the the user's data somehow, he will get an access to the user's data but in an encrypted form. Moreover, the administrator of the system, can have an access to the whole system. But even if he tries to access the user's data, he will get the data in the encrypted form only, which can only be decrypted by following the procedure of the OTP generation and the fingerprint scanning. This algorithm uses 4*4 column-major order matrix of bytes.

TABLE I
AES ALGORITHM MATHEMATICAL MODULE

Sr. No	Algorithm Strategy
1	User(U) this is actor handles system functionality. SET OF U={1.....N}
2	Enter Message for Encryption(E) and Decryption(D). For example "hello" and "$!~v^gdj".
	Enter the Password key for data Encryption and Decryption. For example "xxxxxxxx".
	String str=E{"hello"}; String str1=D{"$!~v^gdj".};
	Output of E="$!~v^gdj"; Output of D="hello";
3	Check input string is provided or not.
	Check key password is provided or not.
	Check provided input is valid or not.
4	If User call E function and provided input for E function is invalid then system will get Exception.

	If User call D function and provided input for D function is invalid then system will get Exception.
	If user provide all input rights then system will get success message else system will get failure message.
5	Let S be a closed Intrusion Detection system such that S = {MSG,K | d , A} where MSG represents the data to be encrypted ,K is secret key , A is Encrypted Data ..... Let be a rule of K,MSG into A such that for given AES; it returns . Encrypt(K,MSG) |® A. . Decrypt(K,A) |® MSG. **.....** Encryption / Decryption Assuming a 128-bit key, the key is also arranged in the form of a matrix of 4 × 4 bytes. As with the input block, the first word from the key fills the first column of the matrix, and so on. The four column words of the key matrix are expanded into a schedule of 44 words. (As to how exactly this is done, we will explain that later.) Each round consumes four words from the key schedule. The figure below depicts the arrangement of the encryption key in the form of 4-byte words and the expansion of the key into a key schedule consisting of 44 4-byte words.  The overall structure of AES encryption/decryption is shown in Figure .
6	

7	K ∈ NP Set The required Time : $O(2^n)$ This problem are : NP-Hard K ∈ {x,y} X ∈ P Is require time : O(n log n) Y ∈ NP The required Time : $O(2^n)$ **So that we can solve this problem by** NP-Complete. P∈ NP and P~=NP

V. CONCLUSION

This paper provides the security and Authentication for online application system by using OTP and Biometrics System of Fingerprint Scanning In daily life, use of banking applications is increased gradually. The security of such type of online applications is more important. Current online applications provide the security like security card, passwords for authenticating the user but do not provide more security for the users and are also not available for any emergency situations. In order to overcome the disadvantages of security cards, we will use OTP and Biometrics for Authentication of online application system.

The Bank generates the OTP using permutations and combinations and random password generation and then user reads the OTP using their mobile phone, which is validated against the registered mobile number. Also the password and the username are validated. In the last stage of verification, the finger scanning is also done and the user is finally authenticated

ACKNOWLEDGMENT

The authors are sincerely grateful to Prof. A.C.Lomte, our Project guide and mentor for her valuable guidance and encouragement. Also the authors are thankful to the Computer Engineering Department of JSPM's Bhivarabai Sawant Institute of Technology & Research (For Women) for their support in providing a good environment and facilities like books, internet and the other resources to complete this research.

REFERENCES

[1] H.Y.Chien, J.K.Jan, and Y.M.Tseng"*An efficient and practical solution to remote authentication: smart card*," Computers & Security. Vol. 21, No. 4,pp, 372-375,2002.

[2] Young Sil Lee, Nack Hyun Kim,Hyotek Lim, HeungKuk Jo, Hoon Jae Lee, "*Online Banking Authentication System using Mobile-OTP with QR-code*", Page(s):644-648,Nov. 30 2010-Dec.2 2010, E-ISBN :978-89-88678-30-5.

[3] H.C.hsiang, W.K.shih. "*Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards*", Computer Communications, Vol. 32, Issue4, pp. 649-652, 2009.

[4] M.S.Hwang and L.H.Li, "*A new remote user authentication scheme using smart cards*",IEEE Transactions on Consumer electronics, Vol.46,No.1,pp.28-30,2000.

[5] D.M'Raihi,M.Bellare,F.Hoornaert,D.Navvache, O.Ranen,"*HOTP:An HMAC-Based In-Time Password algorithm*",RFC4226,December2005.

[6] M.Peyravian and C. Jefferies, "*Secure remote user access over insecure networks*",Computer Communications,Vol.29,Issue 1,pp.660-667,2006.

[7] H.M.Sun, "*An efficient remote user authentication scheme using smart cards*", IEEE Transactions on Consumer electronics, Vol. 46, No.4, pp, 958-961, 2000.

[8] Sang-2 Cho,Hoonjae Lee,Hyo-Taek Lim, Sang-Gon Lee, "*OTP Authentication Protocol using Stream Cipher With Clock-Counter*",October, 2009.

[9] J.Xu, W.T.Zhu, and D.G.Feng, "*An improved smart card based password authentication scheme with provable security,*" Computer Standards & Interfaces, Volume 31, Issue 4, pp. 723-728, June-2009.

[10] P.reid, "*Biometric for network Security*", 1st Indian Reprint, Pearson Education, New Delhi, 2004.

[11] E.Spinella, "*Boiometrics Scanning technologies:Finger, Facial and Retinal Scanning*", SANS technology Institute, San Francisco, dec.,2002.

[12] Reily,D.,Smolyn,g. and Chen,H., "*Towards fluid,mobile and ubiquitous interaction with paper using recursive 2D barcodes*", Pervasive Mobile Interaction Device 2007(PerMID2007),workshop at Pervasive 2007,Toronto,Canada,2007.

[13] L.Lamport, "*Password Authentication with insecure communication*", Communications of ACM, Vol.24,No.11,pp. 770-772,1981.

[14] DeFigueiredo, Dimitri: "*The case for mobile Two-Factor Authentication*". Security & Privacy, IEEE, Sept.-Oct. 2011.

[15] Jinwei gu, jie Zhou and Chunyu Yang," *Fingerprint Recognition by Combining Global Structure and Local Cues*", IEEE TRANSACTIONS ON IMAGE PROCESSING, pp.1952, Vol.15,No. 7, July 2006.

