iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** I **Month of publication:** January 2020

DOI: http://doi.org/10.22214/ijraset.2020.1129

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

A Novel Bank Authentication for Secure Transaction

Vaishali Baviskar[1], Koyal Paul[2], Varsha Kumari[3]
[1, 2, 3]*Department of Computer Engineering GH Raisoni Insitute of Engineering and Technology, Pune University, Pune, India*

Abstract: ***Nowadays one-time passwords are used in a lot of areas of information technologies. A few vulnerabilities in authentication protocols based on one-time passwords are widely known [1]. In current work, we analyze authentication protocols based on one-time passwords and their vulnerabilities with Security Access Code (SAC). Both simple and complicated protocols which are implementing cryptographic algorithms are reviewed. At the same time, we examine HOTP protocols, Random forest algorithm (RFA), MD5 algorithm, Blowfish algorithm, linear congruential generator (LCG) [2] which are actively used nowadays. Security is a major issue when using internet services. Double-factor authentication (2FA) is most used at this time to protect user's account. One example of double factor authentication is One Time Password (OTP) [1]. OTP is a password mechanism that is valid for only one login session. In this research. The main result of the work are conclusions about the security of reviewed protocols based on one-time passwords.***

Keywords: Authentication; one-time password, security access code, random forest, md5, blowfish, linear congruential generator

I. INTRODUCTION

To verify its identity, the user can present to a verifier some secret information which is known to both user and verifier. This secret can be something that user has, that user possesses or something that user knows.

A password is a sequence of symbols along with security access numbers with a operator which is kept secret. A password is a thing that user knows and the security access code will be obtained physically to the user by post means. If a password is the only mean of protection, an attacker needs just to find out the password to get access to secret data. One-time password (OTP) is a sequence of symbols which is generated for single use. There is no sense to eavesdrop it. Used OTP is almost worthless to an attacker due to its invalidity. But any third party might access the OTP by different applications. To make system more secure we are bringing in a concept of security access code which is a physically means of password.

First implementations of authentication protocols based on OTP were assuming to store OTPs as a static set of secret passphrases on a data carrier. Nowadays OTPs are dynamically generated on demand with use of cryptographic algorithms.

II. RELATED WORK

A. Literature Survey

Conventional password-based authentication is taken into account inadequate by users as many online services began to affect one another. Online credentials are wont to recover other credentials and sophisticated attacks are directed to the weakest one among many of those online credentials [1]. As researchers are trying to find new authentication techniques, just one occasion passwords, which may be a two-factor authentication scheme, seems like a natural enhancement over conventional username/password schemes. The manuscript places the OTP verifier to the cloud to ease adoption of its usage by cloud service providers [1]. When the OTP verifier is placed on the cloud as a service, other cloud service providers could outsource their OTP deployments also as cloud users could activate their respective account on the OTP provider on several cloud services [1]. This enables them to use several cloud services without the difficulty of managing several OTP accounts for every cloud service. On the opposite hand, OTP service provision saves inexperienced small to medium enterprises from spending extra costs for OTP provisioning hardware, software and employers. The paper outlines architecture to create a secure, privacy friendly and sound OTP provider within the cloud to outsource the second factor of authentication [1]. Cloud user registration to OTP provider, service provider activation and authentication phases are inspected. The security and privacy considerations of the proposed architecture are defined and analyzed. Attacks from outsiders, unlinkability properties of user profiles, attacks from curious service providers or OTP verifiers are mitigated within the given assumptions. The proposed solution, which locates the OTP provider within the cloud, is rendered robust and sound as a result of the analysis.

III. PROPOSED METHODOLOGY

Presently the banks make use of mere OTP mechanism to assure that the final authentication of transactions is done by the authorized user, but the SMS are read by n number of apps such as Truecaller, call recorder etc which are very often found to be installed in everyone's cell phone.
Here comes the loophole in the current approach which ignites us to build the proposed system.
Number of Attacks avoided by OTP access will be used to evaluate the system.

A. OTP

A one-time password (OTP), also referred to as one-time pin or dynamic password, may be a password that's valid for less than one login session or transaction, on a computing system or other digital device for banking purposes or any other transactions. OTPs avoid a number of shortcomings that are associated with traditional 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 as well as something a person knows (such as a PIN).

B. SAC

It is the security access code and is the combination of the numeric letters. Along with the numeric code there will a operator such as (+, -, *). The code will be generated by the bank system physically and this code will be given to the individual accordingly.
The code will be secret to the individual using it.
Thus with the combination of otp and sac the password will be generated.
We are going to use the following algorithms:

C. Random Forest Algorithm

Random Forest algorithm is a supervised classification algorithm which has many features of it. We can see it from its name that is to create a forest by some way and make it random. There is a direct relationship between the number of trees in the forest and the results it can get: the larger the number of trees, the more accurate the result. But one thing to note is that creating the forest is not the same as constructing the decision with information gain or gain index approach as shown in fig 1.
For the application in the BANKING domain, Random Forest algorithm used to find out loyal customers for good transactions, which means customers who can do plenty of transactions and fraud customers, which means customers who have bad records like failure to pay back money on time or have dangerous actions.

D. Information Gain for Random Forest

Information Gain which is used with splitting the data using entropy. It is calculated as the decrease in entropy after the dataset is split on an attribute:
Gain (T, X) = Entropy (T) — Entropy (T, X)
T = target variable
X = Feature to be split on
Entropy (T, X) = the entropy calculated after the data is split on feature X

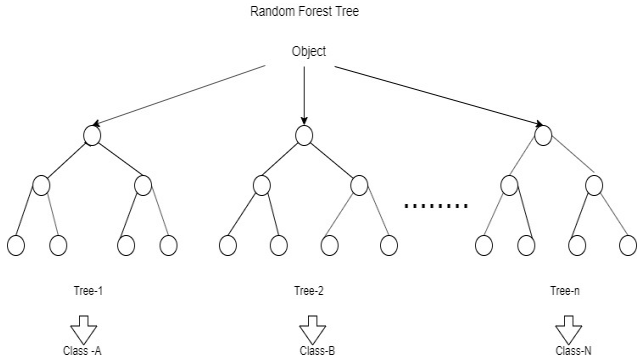


Fig 1. Random forest tree

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

E. Blowfish Algorithm

Blowfish is an encryption technique designed by Bruce Schneier in 1993 as an alternative to DES Encryption Technique. It is significantly faster than DES and provides a good encryption rate with no effective cryptanalysis technique found to date. It is one of the first, secure block cyphers not subject to any patents and hence freely available for anyone to use as shown in fig 2.

1) Block size: 64-bits
2) Key Size: 32-bits to 448-bits variable size
3) Number of subkeys: 18 [P-array]
4) Number of rounds: 16
5) Number of subsitution boxes: 4 [each having 512 entries of 32-bits each

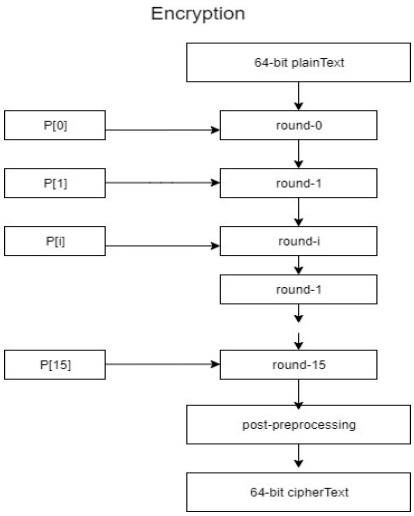


Fig 2. Blowfish pattern

F. MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

G. Abbreviations and Acronyms

1) OTP: One Time Password,
2) SAC: Security Access Code
3) HOTP: HMAC based one time password
4) RFA: Random Forest Algorithm
5) MD5: Message Digest Algorithm
6) LCG: Linear Congruential Generator
7) 2FA: Two Factor Authentication

H. Equations

Linear Congruential Generator (LCG) is a popular and most used method to generate random number. LCG was invented by D.H Lehmer[3]. LCG utilizes a linear model to generate a random number defined as follows:

$$X_{n+1}=(a \times n + c) \bmod m \qquad (1)$$

where a is the multiplier, c is the increment factor and m is the modulus.

Parameters a, c and m have to be chosen carefully in order to avoid repetition of similar numbers before m .The modulus m should be a large prime integer, while multiplier a must be an integer in the range 2,3,…,m-1.The cycle length of LCG would never exceed the modulus m, but it could be maximized using the three following conditions : 1). c is relatively prime to modulus m; 2). Multiplier a-1 is a multiple of every dividing modulus m; 3). Multiplier a-1 is multiple of four when the modulus m is a multiple of four too[3].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 8 Issue I, Jan 2020- Available at www.ijraset.com

I. System Architecture

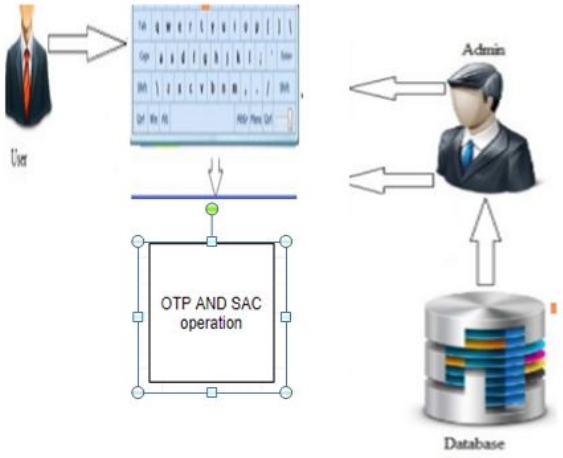


Fig 3.Sytsem architecture

The user will login into his account for transaction then the otp received will be calculated with the sac to make transactions. The server database will check if the calculated value entered as password is correct or not. If correct the transaction will be made as shown in fig 3.

J. Diagrams

As shown in fig 4, the use-case diagram is used to specify the context of the system, used to capture the requirement of a system to validate the system architecture.

The sequence diagrams are the interaction diagrams that detail how operations are carried out accordingly as shown in fig 5.

The fig 6 shows the activity diagram which tells us the dynamic aspect of the system. It is essentially an advanced version form of flow chart which shows the flow from one activity to other.

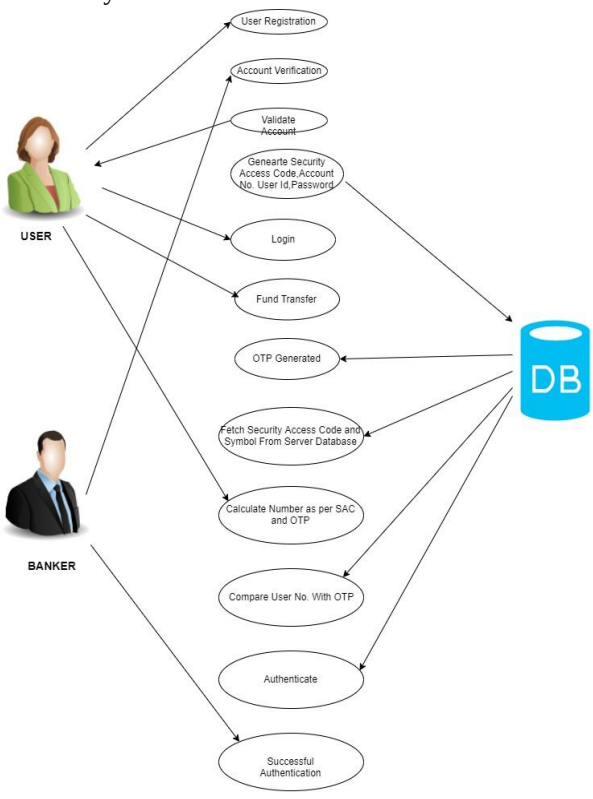


Fig 4. Use-Case Diagram

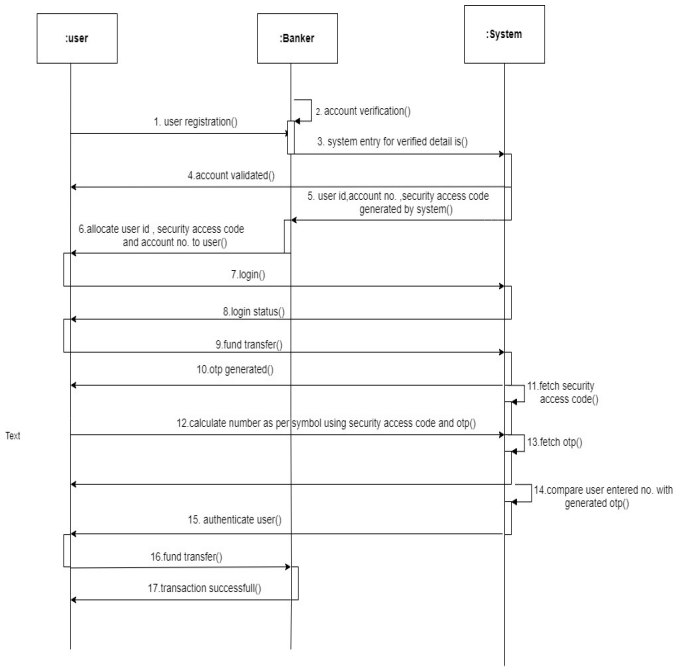


Fig 5. Sequence diagram

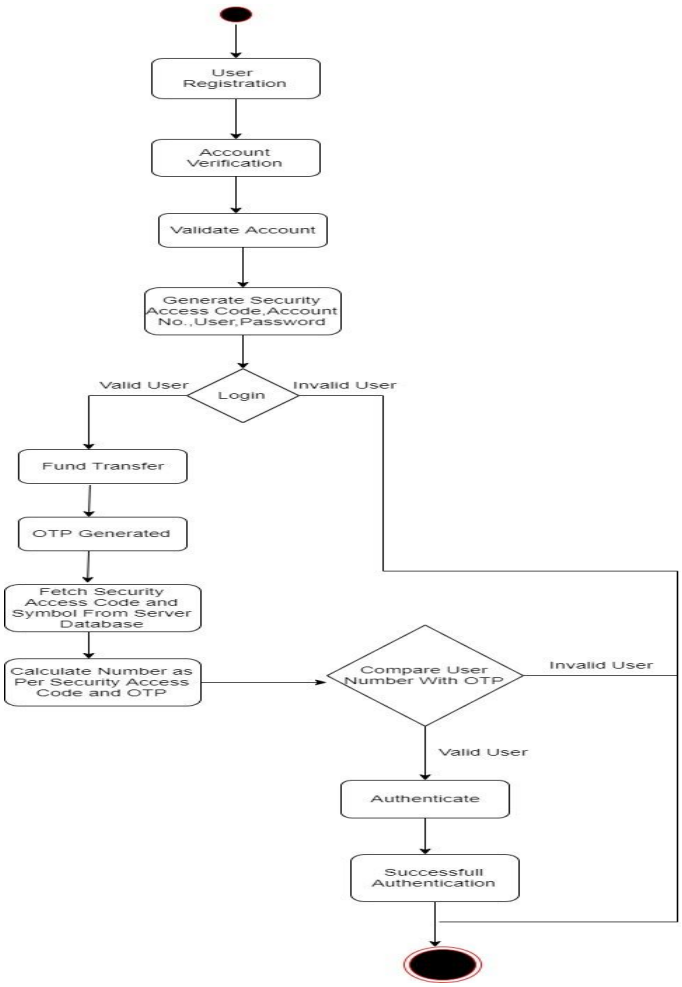


Fig 6. Activity diagram

IV. RESULTS AND CONCLUSIONS

This study introduces a blueprint, important security tips as well as required protocols for OTP services to help banking system and individuals to shift their conventional username/password based authentication schemes to a more secure OTP-based TFA scheme. Security and privacy problems of migrating the OTP service with the SAC is considered carefully. It should be mentioned that the proposed architecture does not aim to solve the flaws of conventional username/password usage such as memorizing problem or vulnerability against guessing attacks. In contrast, adding a second factor to conventional authentication is the result of the afore mentioned problems. This is a common approach since problems arising from human nature are hard to prevent. A realistic usage scenario is identified together with its attack model. The conceptual design's security analysis shows that the architecture and the protocols are robust and sound. The proposed approach is effective as a two factor authentication security mechanism and provides many configurable options by design. User profiles are open to future development at user devices, such as regular password management, credential management, and so on. The design lets companies spend less on OTP-based TFA transition both in the perspectives of experience, employers, hardware and software. Additionally, it lets the users to manage many of their accounts easily at one place, yet via unlinkable profiles.. Given the aforementioned advantages, it is believed that the proposed architecture is an initial step for realization of such services..

We have created the Login and Registration page as shown below in fig 7 and fig 8.

The HTML user login page displays one text filed, password, push button and submit button. We have used JavaScript validation in Login page. We have used push button that resets all fields to blank. We have set username and password value. If an individual enters a wrong username or password or both wrong ,then a "Error: Incorrect username or password" message is displayed till the person enters the correct one, it will not login.

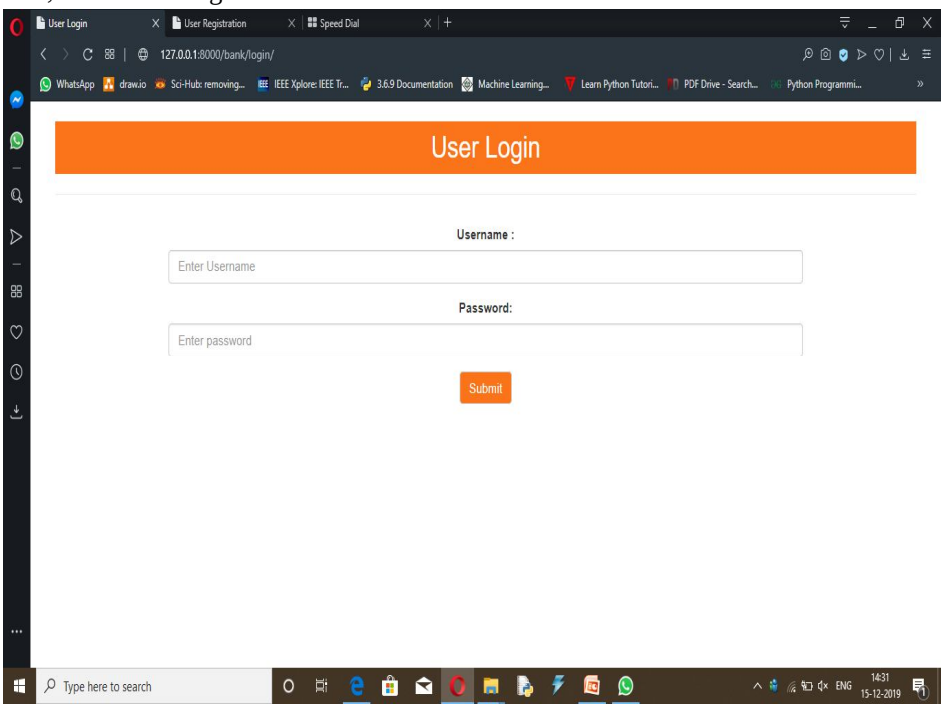


Fig 7. Login Page

At present the concept of online registration is a must form that has emerged a great relief to both the user and the banking firm. It saves lot of time, reduces risk of losing data, which was an excellent concern with manual registration forms.

Here in our registration form, you will find several text fields required to fill. Registration form is developed using the HTML tags and it includes form and text elements .The push button used here will reset the shape to blank. These elements are using form created and eventually JavaScript is added for validation of the screen.

Moreover, if you do not enter any value in the text fields, an "Error " message will appear. It is mandatory to fill all the fields and cannot be left blank.

Once the fields are filled correctly, submit form now adds the information .

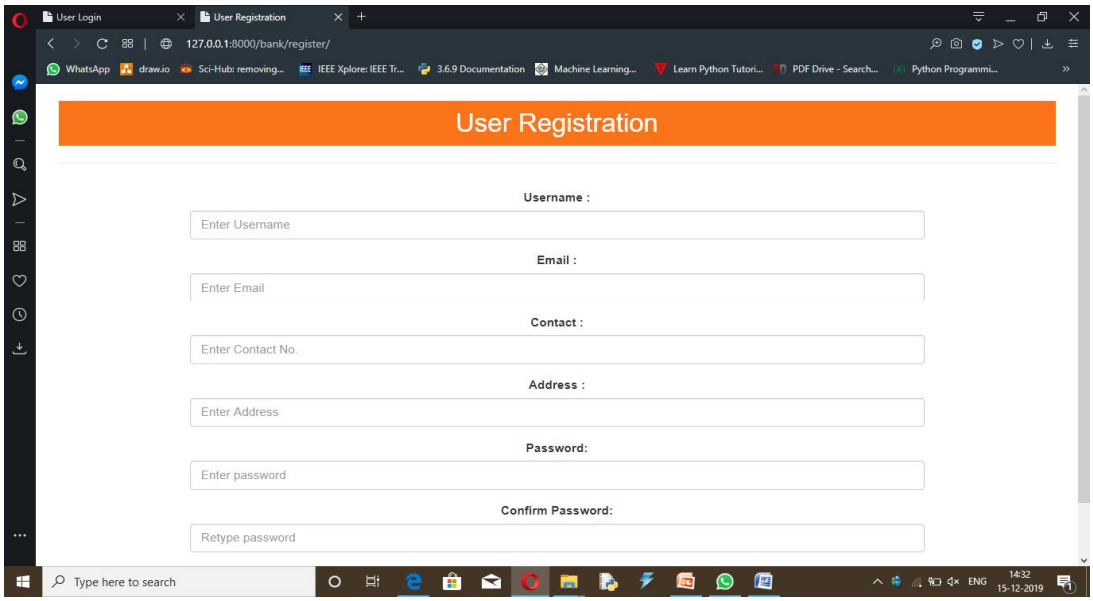
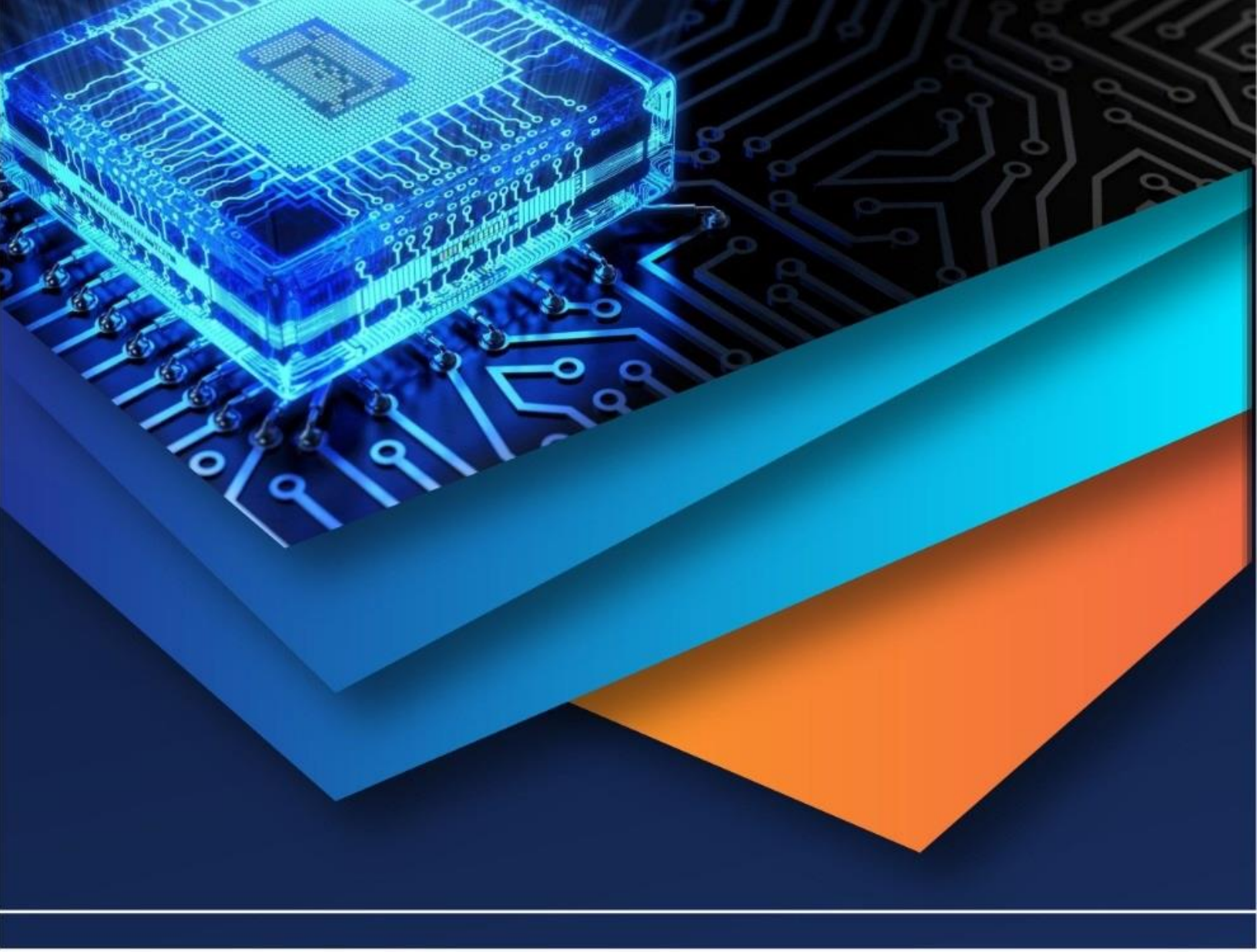


Fig 8. Registration page

REFERENCES

[1] Emir Erdem and Mehmet Tahir Sandikkya, 'OTPaaS- One Time Password as a Service', Member of IEEE, 2018.
[2] Sergey Babkin, Anna Epishkina ,'Authentication Protocols Based on One- Time Passwords', Cryptology and Cybersecurity department, Moscow, Russia, 978-1-7281-0339-6/19, 2019.
[3] Imamah, 'OTP based on Advanced Encrypted Standard(AES) and Linear Congruential Generator(LCG)', Faculty Of Engineering, Bangkalan, Indonesia, 978-1-5386-5251-0/18, 2018.
[4] Siva Janakiraman , Kalavagunta Sowmya Sree, V. Leela manasa, Sundararaman Rajagopalan, K. Thenmozhi and Rengarajan Amirtharajan, 'OTP on Demand-An Embedded System For User Authentication', Department of Electronics and Communication Engineering, 978-1-5386-2238-4, 2018
[5] H. Tanaka, O. Takizawa, and A. Yamamura, "A trial of the interception of display image using emanation of electromagnetic wave," Journal of the National Institute of Information and Communications Technology Vol, vol. 52, no. 1/2, 2005.
[6] L. Cai and H. Chen, "Touchlogger: Inferring keystrokes on touch screen from smartphone motion." HotSec, vol. 11, pp. 9–9, 2011.
[7] R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," Pattern Recognition, vol. 35, no. 12, pp. 2727–2738, 2002.
[8] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," Pattern Recognition, vol. 37, no. 11, pp. 2245–2255, 2004.
[9] S. H. Khan, M. A. Akbar, F. Shahzad, M. Farooq, and Z. Khan, "Secure biometric template generation for multi-factor authentication," Pattern Recognition, vol. 48, no. 2, pp. 458–472, 2015.
[10] N. Haller, C. Metz, P. J. Nesser, and M. Straw, "A One-Time Password System," Internet Engineering Task Force, Request For Comments 2289, 2 1998, https://www.ietf.org/rfc/rfc2289.txt.
[11] D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, and O. Ranen, "HOTP: An HMAC-Based One-Time Password Algorithm," Internet Engineering Task Force, Request For Comments 4226, 12 2005, https://www.ietf.org/rfc/rfc4226.txt.
[12] D. M'Raihi, S. Machani, M. Pei, and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm," Internet Engineering Task Force, Request For Comments 6238, 5 2011, https://www.ietf.org/rfc/rfc6238.txt.
[13] I. Ion, R. Reeder, and S. Consolvo, ""...no one can hack my mind": Comparing expert and non-expert security practices," in Eleventh Symposium On Usable Privacy and Security (SOUPS 2015). Ottawa: USENIX Association, 2015, pp. 327–346. [Online]. Available: https://www.usenix.org/conference/soups2015/proceedings/presentation/ion
[14] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, vol. 24, no. 11, pp. 770–772, 1981.
[15] N. Haller, "The S/KEY One-Time Password System," Internet Engineering Task Force, 5177 Brandin Court, Fremont, CA 94538, USA, Request For Comments 1760, 2 1995, https://www.ietf.org/rfc/rfc1760.txt.
[16] B. Groza and D. Petrica, "One time passwords for uncertain number of authentications," in Proceedings of 15th International Conference on Control Systems and Computer Science CSCS15, 2005, pp. 669–674.
[17] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, T.-H. Kim, and H. Elkamchouchi, "Mobile one-time passwords: two-factor authentication using mobile phones," Security and Communication Networks, vol. 5, no. 5, pp. 508–516, 2012.
[18] L. Gong, J. Pan, B. Liu, and S. Zhao, "A novel one-time password mutual authentication scheme on sharing renewed finite random subpasswords," Journal of Computer and System Sciences, vol. 79, no. 1, pp. 122–130, 2013.
[19] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Cloud authentication based on anonymous one-time password," in Ubiquitous Information Technologies and Applications. Springer, 2013, pp. 423– 431.
[20] F. Cheng, "Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm," Mobile Networks and Applications, vol. 16, no. 3, pp. 304–336, 2011.

[21] D. Florˆencio and C. Herley, “One-time password access to any server without changing the server,” in Proceedings of 11th Information Security Conference (ISC), vol. 8. Springer, 2008, pp. 401–420.
[22] B. Vaidya, J. H. Park, S.-S. Yeo, and J. J. Rodrigues, “Robust onetime password authentication scheme using smart card for home network environment,” Computer Communications, vol. 34, no. 3, pp. 326–336, 2011.
[23] K.-C. Liao, W.-H. Lee, M.-H. Sung, and T.-C. Lin, “A one-time password scheme with qr-code based on mobile phone,” in Fifth International Joint Conference on INC, IMS and IDC. IEEE, 2009, pp. 2069–2071.
[24] “Yubikey,” https://www.yubico.com, accessed: 2017-03-20. “Googleauthenticator,” https://github.com/google/googleauthenticator/wiki, accessed: 2017-03-20.
[25] D. Wang and P. Wang, “Two birds with one stone: Two-factor authentication with security beyond conventional bound,” IEEE transactions on dependable and secure computing, 2016.
[26] D. Wang, D. He, P. Wang, and C.-H. Chu, “Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 4, pp. 428–442, 2015.
[27] Q. Xie, D. S. Wong, G. Wang, X. Tan, K. Chen, and L. Fang, “Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1382–1392, 2017.
[28] T. Dierks and E. Rescorla, “The transport layer security (tls) protocol version 1.2,” Internet Requests for Comments, RFC 6238, August 2008. [Online]. Available: https://www.ietf.org/rfc/rfc5246.txt
[29] R. Dingledine, N. Mathewson, and P. Syverson, “Tor: The secondgeneration onion router,” in 13th USENIX Security Symposium, 2004, pp. 303–320.
[30] E. Bresson, O. Chevassut, and D. Pointcheval, “Security proofs for an efficient password-based key exchange,” in Proceedings of the 10th ACM conference on Computer and communications security. ACM, 2003, pp. 241–250.
[31] Available“http://www.edgeverve.com/finacle/resources/thoughtpapers/Documents/what-the-future-online-banking.pdf
[32] Sheena S, Sheena Mathew,“ A STUDY OF MULTIMODAL BIOMETRIC SYSTEM”, IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 — pISSN: 2321-7308
[33] S.R.Soruba Sree , Dr. N.Radha,”A Survey on Fusion Techniques for Multimodal Biomet- ric Identification, International Journal of Innovative Research in Computer and Com- munication Engineering, Vol. 2, Issue 12, December 2014.
[34] Mary Lourde R, and Dushyant Khosla, ”Fingerprint Identification in Biometric Security Systems”, International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010 1793-8163
[35] K.Saranya,K.Baskar,”Multibiometric Secure Index Value Code Generation for Authentication and Retrieval”,Iternational Journal for Scientific Research & Development— Vol. 1, Issue 5, 2013 — ISSN (online): 23210613
[36] Sui, Yan, Xukai Zou, Eliza Y. Du, and Feng Li,”Design and Analysis of a Highly User-Friendly, Secure,Privacy-Preserving, and Revocable Authentication Method”,IEEE Transactions on Computers, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY