International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET218324

Three Factor Authentication Novel Framework through Improve System Privacy and Data Security

Er. Vishal Chauhan, Dr. Chandresh Parekh, Prof. Vivek Joshi
School of Information Technology, Artificial Intelligence, and Cyber Security, Rashtriya Raksha University, Gandhinagar, Gujarat, India

Article Info
Volume 8, Issue 3
Page Number: 183-190

Publication Issue :
May-June-2021

Article History
Accepted : 20 May 2021
Published: 30 May 2021

ABSTRACT

Authentication, Authorization, security and confidential information are number of foremost topics part in the Digital cyber - security Area. There are multiple solutions available in this virtualize cyber world that are presented to user's strength as per digital security. Username and password base are common factor authentication methods. The growing-up popularity with compliance of second factorized methods those driven by the improvement of privacy and security as per the requirement during this digitalization of technological trend. The recognition and success of digital security various measures are big deal to obsessed with simple convenience. Its need more and more implementation for the user privacy, data confidentiality and network security's system. mainly focus on this research Article into dealing with and analysing the implications of security part of 3FA proposal model for additional security in way of systematic manner to improvements of digital security in web-based Application. This paper will be presenting as web-based Application. so, we can create potentially ensure systems are authorized with authentication of user's assurance without loss of convenience between user-system data communication in network.

Keywords: Cyber Security, Authentication, Three-Factor Authentication, Access Control, Web Application, Two Factor Authentication, Single Factor Authentication, Digital Security, Authorization, Privacy

I. INTRODUCTION

In today's the digitalize technological era part is incredible. So, never trusting on the digital system and any human. As per user's system Security and Account information security in Second-factor and First-Factor based Authentication using the various security credential can't adequate to providing a better privacy and security for users or it's system. Hacking script programs code and payload threw simply computerized auto-generated secret key gather by using various tools and programs or many auto password generators that are easily crack it so that it is extremely difficulty to provide system security even If when the First - Factor or the Second Factor base Authentication are commonly used only for digital

security threw securing the remotely access of virtual system but not Real - Time Authorization provided and user system are authenticate using various authentication techniques but we can authenticate real-time user author without any authorization.

The various security malware threats and malicious script, virus, trojan, worms, Ad-ware and key-trackers, etc. are always became harmful & damaging our system and data. Expanded access to account and its critical information upsurges weakness of system and coding and network are used to cracking passwords, Session Hijacking, system and network bypass, various online scams dangerous script and payload, etc. In this regarding, A conventional based login-ID and password or OTP based authentication are insufficiently to provide digital security for several time on various platform providing critical applications like login-form in E-commerce Application, Banking Sector, E-mail, Social Network, Sensitive Financial accounts information, ATM (Automated Teller Machine) E-security, commercial websites or application, official secured network system, online payment gateway, etc. Everything needed system and user authentication with Authorization based Security system that are Considering as third factor-level. And this are having one more independent factor of implementation on second factor authentication that are increasing complexity of provide real-time and better security as third factor Authentication that preventing from attacker, Hacker.

The Multi-factor Authentication Is proposal based assuring multiple level security layer shield type protection threw extending layer of the implementation on one to more than authentication factor that became more and more complex and that irritate at login-time for user that provide improper way for authentication. This paper is mainly concentrating on implementation of third-factor authentication by uses as user's friendly with traditional security methodology threw implement system level and Author/user level and Account level factor authentication with authorization that is novel approach suggested and proposed by this model framework. And meaningful efforts have been made and utilize by using this framework third-factor authentication mechanism. The Research Article Paper into, we are suggesting and proposed this third-factor Authentication framework model and its implementation are briefly described. So, we can tryout extending additional password credential in E-security that are increases for an extra level layered of security.

Today digital e-security concentrate on growing up under IT cyberspace zone. since, everyday corporate zone and business zone and government zone are becoming digitally at global level. Today, all most basic systems dependency on password manager as administrator level. Many User's having new trend to using explicit type password with passphrase, social engineering threw easily guessable of simple and general password with various formats types, password manager etc. further all details with remembering their password into system. Guessable passwords and OTP code break via John-the-Reaper & Rainbow tables attacks. Session Hijacking attack threw direct login access using session-ID. Utilize static passwords and that is storing on IT-administration Systems that present themselves to the ID Thieves, impostors and Hackers.

In additional part, the system hijacker or hackers having deep knowledge of various number of attacks, tools and techniques like brute force, password guessing, snooping, social engineering, dictionary Attack, shoulder surfing, and session hijack etc. Various attacks are enough to steal and gather information such as ID, Session, passwords and many more critical information. In this vulnerable system on gain entire access to their login accounts or bypass security credential using powerful VPN (virtual

private network) and some powerful malicious script and Payload threw we can't easily catch-up about Hacker footprint.

Second factor validations having some limitations which are integrated the various issuing, and dealing with them that are like tokens and source code and resources. keeping this in our mind, A new scheme will be proposing in future that needed various improvement needed this framework in future, Authentication done by using step by step factors as per we are knowing about user -ID and password based on Alphanumeric with validation of syntax, and various type of graphical password, and user authorized via the biometric security into systematic manner via using concept of Third Factor Authentication framework.

This paper orientations as per following manner: section -1, section -2 both are basically introduced as per above and with literature Review section as Related works portion. section -3 is only explaining about existing various authentication methods And only section -4 part are presenting about the novel proposed third factor authentication framework via figure of Flowchart Diagram., and section -5 explaining about the novel proposed method concept and section -6 about its Advantages and Disadvantages. And last one portion section -7 about my research concept will be use as future work.

II. RELETED WORKS

A. Anderson, Yan, J., Blackwell, R. Grant [1] are discuss about various multiple type of password that are normally chosen by the various user e.g., Some passwords are easily guessable but hard to recall (encryption-Decryption in server cryptography). this author group conducting many experiments threw derive from give us one important advice to the all users as per documentation result. System it self

Gawade, L.S., Rane, Gurav, S.M., Khochare, N.R, P.K., [2] proposed a various authenticate schemes based on graphical password for the cloud technology.

Oberoi, R.K, Kumari, S., [3] proposing one technique are defend against shoulder surfing, by using of recognizable graphical password.

Pankanti, S., Prabhakar, S., Jain, A.K. [4] discussing about comparison on the different type of methods on the biometrics such as fingerprint, Iris and so and so.

Gaikwad, A.N., Soares, J. [5] are introduced about the system are uses iris recognition for authentication using Circular Though Transforming and the fingerprint on using the minutiae matching algorithm on ATM banking system.

Reyzin, L., Smith, A., Dodis, Y. [14] proposing one method used for two-factor based the key generation, where key generating from the biometric as eyes and token are merged and that using mainly concept based on cryptographic application. This proposed technique successfully merges biometric with cryptographic based application. Similarly, Reyzin, L., Dodis, Y., Smith, A. [15] that are explaining how can be using biometric threw generating keys form cryptography-based system, which are secure biometric or not.

III. EXISTING AUTHENTICATION

This propose method are use as third factors authentication to authenticate that approved with the authorized user into the target Android Application & Web Application. The Single Factor authentication as per framework Account base Authentication as usually approach, which is complicated, cheap and secure, in traditional mode of validation form known as Alphabetic-numeric or Alphanumeric Password. Phishing & Social Engineering & DDOS attacks etc.

systemically illegally attack done by Black hat Hacker.

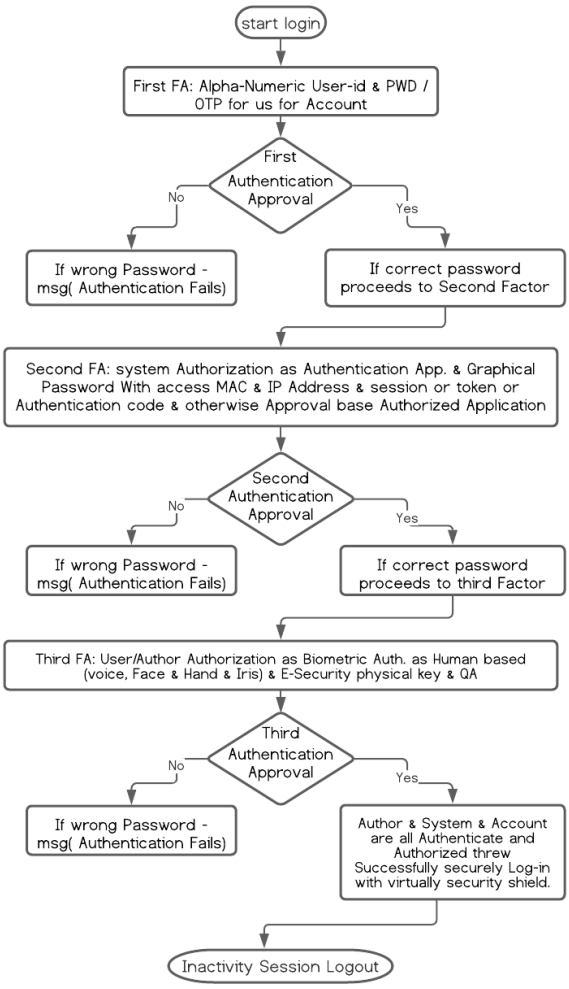
Then after two-time factor use to secure system and Accounts using second factor authentication. This Factor Authentication (2FA) more than secure and reliable to the single factor authentication. As per our framework system Authorization and Authentication based approach.

Today, The Second factor Authentication became general approach that is also easy to use with e-security as Graphical Password such as various types captcha codes, click points, Pass faces, character and picture-based data, etc. After the user provides his/her username and password threw login into their account, the single authentication check will be the Alphanumeric Password which is chosen at the one time of registration for that particular Web Application site/account but in backend we can give system IP-Address and Mac-Address and session and Token etc. primary system identified data store in data-server.

Second Factor Authentication are system and Human combo interaction mode that's for System Bot & Hacker virtually system easily track identified by its digital footprint into logfile of system server. With protection from DOS & phishing attacks. But those are not enough to secure system in today digital world cyber space. Authentication are not much priority and including policy with Authorization matter at login time.

IV. NOVEL PROPOSED THIRD-FACTOR AUTHENTICATION FRAMEWORK

This new framework shall be proposed for third factor authentication method as per follows:



V. NOVEL PROPOSED METHOD CONCEPT

Third Factor Authentication is one part of Multiple Factor Authentication mechanism. And In this Article Paper proposals threw we can build up new methodology threw improvement second factor authentication. This Authentication mechanism threw access a user account basic information and system information, accessing social-engineering accounts and E-mails Accounts, online booking and shopping, etc. type of user accounts are carry out by use of the Alpha-Numeric Password and with the Graphical password.

Alternatively secure and treading authentication method with human authorization come-out into formation of the Bio-metric Authentications uses as face recognition and detection, iris (eyes) recognition, palm (hand) print & finger print, voice (sound) recognizes based on password and heartbeat pulse rate, etc. Human-propensity in creating easily memorable password learns for the password snares. Also Generally Substitute with common-mode as alpha-numeric password are authenticated easily memorable and the graphical password are developing for different purposes by the different developer and different researcher teams.

As per dissertation to end of set hat you're authenticated by user declaration to be onwards. And the unique of the system Machine and Human are identified then confirmed or access is granted for real-time user system. Unanimously, the existing acknowledgment base authenticate via the various common factor as per given below:

(A) Something the user has: Some physical object in the possession of the user, such as a security token, API and security key (USB key), Authentication Application etc.

(B) Something the user knows: Certain knowledge only known to the user, such as a password, PIN, etc.

(C) Something the user is: Some the physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, face lock, typing speed, heart beat pattern in key press intervals, etc.

(D) Somewhere the user is: Some connection to the specific system network or using a GPS signal sets location access for specified server network zone or identify the location on private IP Address.

Second-factor authentication best way solution providing for users and customers with a cost-effective, very flexible with custom base GUI interface and very strong authentication. But sometime Hacker can bypass and broke that security using malicious scripts and tools. However, since, cyber frauds are still being convenient with Second-Factor authentication, it is understood that are not totally security provided but the fraud-rate is reduced as compared to associated with single-Factor authentication. The main goal of computer security as system security to uphold by the availability, integrity and privacy policy furthers the critical data, files and information entrusted manner to the system can be attained by using various Second-factor authentication technique. As per protectors, Second-factor Authentication could undeniably decrease existence of new e-security trend in cyber space by multiple online frauds, and other online various extortion. The serves as an extra layer of security that protects and enhances the existing second factor authentication system implementation, that proposed by this novel third-factor authentication (3FA) framework is briefly described in this article.

3FA having informative security policy and processes that means of credit are credential base combining to the probability for entity system, and the general user, that is legal way to catch out real-holder identification and its system information. In this Article only highlighted on implementation security on proposed authentication method including Authorization as third factor authentication are enhanced by Digitalize Cyber security. that is requires the use of reliable factor for the third factor authentication like:

(i) Account base Factor Authentication:

Something users knowing about, e.g., an alpha-numeric, general textual password (E-mail ID, User ID, Password & OTP etc.)

(ii) System base Factor Authentication:

Something users knowing and clicking, e.g., various Graphical password (Captcha code, Graphical Text, Graphical Sum, Authentication Code, OTP, Approval code etc.)

(iii)User (Author) Human base Factor Authentication:

Something user can prove for authorization e.g., Biometric Identity (Face, Iris & Finger print and palm print & voice password) or personalized self QA.

VI. DISCUSS ABOUT ADVANTAGES AND DISADVANTAGES OF THE PROPOSED MODEL

+ On the proposed model of benefits [Advantages]

(i) in features needed improvement to this securely privacy preservation system based

(ii) there will be Authenticable Login mechanism with authorization as real time user to securing web portals, admin panel and web applications

(iii) Since there are third level of protection, it is better way to providing depth Digital security.

(iv) it is very easy to implement & Maintain by IT-Security Audit & MNC company.

+ On the proposed model of weakness [Disadvantages]

(i) not for some disability & blind people for not available or not working bio security features.

(ii) it's required more and more memory space or virtual memory as cloud memory space to store & Load necessary information & metadata

(iii) That is taking out small amount of the additional time with additional security layer features for login mechanism can reset time generate problem.

(iv) if we having selected authorized authentication system Application and that system is lost and crash then after we can't access through our account by any unauthenticated system.

VII. FUTURE WORK

Third Factor Authentication are giving us authorized security threw this proposed model framework are used in future helping-out web-based application like Facebook, twitter, g-mail, Instagram, telegram, snapchat, etc. and any other E-Commerce and Business Sites.

VIII. CONCLUSION

we comparing 2FA & 3FA in web Application comparing. As on Result 3FA are providing better security & privacy to the system and data comparing 2-FA. Progression with in the systematic manner validation type various technique threw checking out tomorrow authentication problem solution necessity but not today problem solution. We are mainly focus to improve authentication mechanism systematic manner with system has Authorized or Authenticated then check Real-time user having as Authorized via authentication on web-based application. At the ending out point. Sometime need to improvement into coding and security system layer that aren't easier to get critical data information such as password from database but we authenticate with real-time owner are authorized or not. Some challenges are biggest tuff to forecast, different types vulnerabilities in the software-based security testing. Integrating of third-factor authentication give us the better higher-level security solution with authorization. As per the confirmation mechanism are used to authentication and to authorization merging improvement one step ahead for e-security, By the way proposed framework model can be suitable using in many e-security and critical applications and its virtual security area in the web based oriented applications on various Operating System like Android, Windows, iOS, etc. My ultimate goal thought that are proposed third-factor authentication shall be incite more digitalize vital e-security.

IX. ACKNOWLEDGEMENT

We are gratefully thanks to my Research Guide Dr. Chandresh Parekh (Head of Department SITAICS – School of Information and Technology & Artificial Intelligence & Cyber Security at Rashtriya Raksha University, Gandhinagar, Gujarat, INDIA). We are gratefully thanks to my Research Co-Guide Prof. Vivek Joshi (Assistant Professor at SITAICS – School of Information and Technology & Artificial Intelligence & Cyber Security at Rashtriya Raksha University, Gandhinagar, Gujarat, INDIA).

IX. REFERENCES

[1]. Blackwell, A., Anderson, R., Yan, J., Grant, A., "Password memorability and security: Empirical results." IEEE - Institute of Electrical and Electronics Engineers on privacy and security,2007, vol. 2 (no. 5), p.25-31.

[2]. Gawade, L.S., Gurav, S.M., Rane, P.K., Khochare, N.R., "Graphical password authentication: Cloud securing scheme.", January 2014, In Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014 International Conference on IEEE - Institute of Electrical and Electronics Engineers (p. 479-483).

[3]. Oberoi, R.K., Kumari, S., "Defense against Shoulder Surfing Attack for Recognition Based Graphical Password." IJECS - International Journal of Engineering and Computer Science, 2014 vol. 3(no. 07).

[4]. Pankanti, S., Jain, A.K., Prabhakar, S., "Biometric recognition: Security and privacy concerns." IEEE - Institute of Electrical and Electronics Engineers privacy and security, 2003 vol. 99(no. 2), (p.33- 42).

[5]. Gaikwad, A.N., Soares, J., "Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP" IEEE - Institute of Electrical and Electronics Engineers Xplore conference International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), 2016

[6]. Dodis, Y., Reyzin, L. and Smith, A., "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data" Advances in Cryptology Springer Link - Annual International Conference on the Theory and Applications of Cryptographic Techniques - EUROCRYPT 2004, (p 523-540)

[7]. Van Oorschot, P.C., Bonneau J, Herley, Stajano, F., "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." IEEE - Institute of Electrical and Electronics Engineers Symposium in Privacy and Security, May-2012 (p. 553-567).

[8]. xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou., "A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy" in Distributed Systems. IEEE – Institute of Electrical and Electronics Engineers, 2010.

[9]. Rajesh Karman Megalingam, Binitha Ann Scaria "Enhanced E-commerce Application Security using Three-Factor Authentication", Second International Conference on intelligent Computing and Control Systems – ICICCS, 2018

[10]. C. Lakshmi Devasena "Three-Factor Authentication for Fortified Login to Ensure Privacy Preservation and Improved Security" International Journal of Applied Engineering Research ISSN 0973-4562 Vol.13, (p. 7576-7579) Nov.- 2018

[11]. Aspen Olmsted, William Kennedy "Three Factor Authentication" 12th International Conference for Internet Technology and Secured Transaction – ICITST, 2017.

[12]. Edward F. Gehringer "Choosing passwords: Security and Human factors" IEEE - Institute of Electrical and Electronics Engineers, (ISTAS'02) - international symposium on Technology and Society, ISBN 0-7803-7284-0, (p. 369 – 373), 2002.

[13]. Alireza Pirayesh Sabzevar, Angelos Stavrou, "Universal Multi-Factor Authentication Using Graphical Passwords", Proceedings of the IEEE - International Conference on Signal Image Technology and Internet Based Systems, (p. 625-632), 2008.

[14]. Manav Singhal and Shashikala Tapaswi "Software Tokens Based Two Factor Authentication Scheme" International Journal of Information and Electronics Engineering, Vol.2(No. 3), (p. 383 – 386), May - 2012.

[15]. Sharifah Mumtazah Syed Ahmad, et al "Technical Issues and Challenges of Biometric

Applications as access control tools of Information Security" International Journal of Innovative Computing, Information and Control Vol.8(No. 11), (p. 7983 – 7999), Nov. - 2012.

Cite this article as :

Er. Vishal Chauhan, Dr. Chandresh Parekh, Prof. Vivek Joshi, "Three Factor Authentication Novel Framework through Improve System Privacy and Data Security", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 183-190, May-June 2021. Available at
doi : https://doi.org/10.32628/IJSRSET218324
Journal URL : https://ijsrset.com/IJSRSET218324