Journal of Engineering Sciences
Vol 11, Issue 6,June/2020
ISSN NO:0377-9254

USER AUTHENTICATION USING g-RAT AND FINGER-PRINT

Nirmal M.D.[1], Saurabh D. Gadekar[2], Pawan R. Ghogare[3], Shailesh U. Ghogare[4], Jagruti M. Ghorpade[5]

[1]PREC, Loni Computer, SPPU, India
[2]PREC, Loni Computer, SPPU, India
[3]PREC, Loni Computer, SPPU, India
[4]PREC, Loni Computer, SPPU, India
[5]PREC, Loni Computer, SPPU, India

Abstract—Individual Banks store Brobdingnagian amounts of user sensitive information on their non-public server or cloud server. The most challenge in any on-line industry is to secure data that keep in internet server, additionally providing additional degree of privacy to individual bank consumer throughout each dealing. The foremost secured system is user authentication to log in and out of the account by a consumer. User authentication is that the method that's exercised immeasurable times round the globe by victimization completely different techniques and ways. The foremost distinguished manner of authentication is alphanumeric watchword forms that are used for many years. Licensed access is turning into a difficult issue owing to the introduction of contemporary technologies. Additionally, ancient alphanumeric passwords have vital security problems, as an example, humans forget the mix of keys thanks to the choice of a troublesome key combination. Moreover, after they opt for a straightforward key combination, this helps hackers to crack their passwords simply. Therefore we tend to thought of planning a secured authentication system which is able to have 2 layers initial the user has got to demonstrate victimization gRAT technique wherever a pattern of pictures has got to be elect so once productive gRAT there comes second layer as identity verification. Once success of each techniques the banking App are going to be opened wherever the user will do banking operations. The industry and authentication system can use Cloud as communication medium. The information on the cloud are going to be secured victimization AES formula.

Keywords—Authentication System, gRAT, Biometric Authentication, Mobile Computing, Cloud Computing, Banking System and AES.

1. INTRODUCTION

In today's digital era, each organization wants to store their customer information in a secure and safe manner. The stored information not only meets the demand of the organization itself but can also meet the demands of other organizations, if stored on a global platform. In a banking organization the data comprises of its customer's private information. If this data is compromised by a hacker it will make a huge loss to the customer. So we thought of designing a security project for banking application. Data security is one of the prerequisites of any digital data transaction storage system. Web servers are the place where all the information of a system being stored. To provide secure data we can utilize a lot of processes but a single authentication system does not tends to be reliable and secure. In order to solve this problem, we create a multi layered authentication system using gRAT and Biometric authentication systems together as one.

2. LITERATURE SURVEY

1. G-RAT: a completely unique Graphical irregular Authentication Technique for shopper good Devices:- In 2018 Mudassar Ali Khan, Ikram Ud Din and Muhammad Khurram Khan authored this paper that explains user authentication is that the method that's exercised a lot of times round the globe by victimization completely different techniques and ways. The foremost distinguished means of authentication is alphabetical watchword forms that are used for many years. Approved access is changing into a difficult issue owing to the introduction of recent technologies.

Additionally, ancient alphabetical passwords have vital security problems, for instance, humans forget the mixture of keys thanks to the choice of a tough key combination. Moreover, after they select a simple key combination this helps hackers to crack their passwords simply. Ancient passwords also are at risk of many forms of attacks, for instance, lexicon attack, brute force attack, and malware. To supply a simple and safer authentication technique, a graphical watchword has been introduced during this paper for shopper electronic devices that uses a picture or a group of pictures for authentication. We've got classified the present graphical watchword ways into recognition based mostly, cued-recall based mostly, pure-recall based mostly, and hybrid techniques. Thanks to the constraints of the present graphical passwords, we've got introduced a brand new technique, named Graphical Random Authentication Technique (gRAT), that generates an irregular set of pictures when a user tries to certify him/herself by maintaining the protection and value at constant time. The gRAT technique is additionally tested by user-centric analysis in terms of security, usability, usefulness, and utility, and therefore the experimental results show that the projected technique is safer and helpful within the real-life authentication applications.

2. Robot based mostly Mobile Application: Development for Web Login Authentication victimization Fingerprint Recognition Feature: - This technique was projected in 2017 by Nilay Ylldmm and Asif Varol that explains several mobile device manufacturers currently incorporate biometric safety features into their merchandise. And, some device makers currently permit application developers to use these options via their code development kits (SDKs). During this study, we tend to utilize fingerprint scanning and recognition technology, a well-liked biometric security feature, to develop an internet login authentication mobile app. Our application uses the Samsung Galaxy S5 fingerprint recognition feature and International Mobile instrumentality Identity (IMEI) variety to get single time passwords. inside a restricted timeframe, the secure passwords are often accustomed sign in/log in to on-line user accounts associated with government, banking, education, etc. because the production of mobile devices with fingerprint recognition continues to extend, finger print user authentication apps, just like the one we tend to introduce during this study, can become a current security live.

3. Group action System on robot Smartphone: In 2015 Benfano Soewito, Ford Lumban Goal, Echo Simanjuntak and Fergyanto E. Gunawan printed the work that in the main explains group action system Which is presently exist still has weaknesses. The primary is that the long queues ahead of the group action machine at the time to come back to figure and leave work. The second is cheating, staff will raise her/his friend to try and do group action method. The third is generally group action system has not been connected with the payment system in human resources code or within the finance department. The fourth, staff World Health Organization work outside the workplace can't do group action method. during this paper, we tend to introduced Associate in Nursing group action system based mostly finger print technology and GPS employing a smartphone integrated with payment system that may eliminate all the issues higher than. Our analysis conjointly supported prediction that within the next few year all the sensible phone can have a fingerprint scanner.

4. Cloud Based Secure Banking Application: In 2017 Neha Raghoba Parab, LouellaMMesquita Colaco and Fiona Coutinho published a work which mainly studies: individual Banks store vast amounts of user sensitive data on their private server. Sharing this data with other banks will provide an efficient way of offering their customers with personalized services and will deliver value-added data services to the entire banking sector. This data is highly sensitive and requires a secure sharing medium. However, secure data sharing is a taxing and troublesome job. This paper proposes a framework for sharing Secure Sensitive Data between banks which includes Secure Data Transfer, Secure Data Storage, Secure Data Delivery and Usage & Destruction of Data which uses Variable AES in place of Normal AES for securely storing the data as Variable AES is an enhancement to Normal AES since it uses new sub key for each block of data. This framework provides security of the user's sensitive data and shares this data safely. To allow banks to share their data we have implemented this framework using the cloud application where we provide user authentication, data integrity and access control using the Proxy Re-Encryption mechanism.

3. METHODOLOGIES

The proposed work is a combination of gRAT Authentication, Biometric Authentication, Cloud computing, Mobile computing and desktop computing together.

4. WORKING OF GRAT

• The gRAT system is a graphical password technique that uses images which are presented on the screen in a 3x3 grid.

• In other words, in the gRAT system the place of pictures changes every time a user wants to be authenticated.

• The proposed system has three steps of registration and authentication:

a) Step 1: In the first step, a user selects a category of images that is provided by the gRAT application.

b) Step 2: In the second step, the user chooses a password from a 3x3 grid picture, which is provided on the screen, and then draws a pattern by swiping on images.

c) Step 3: This step is about the authentication, where users draw the same pattern that has already been selected during step 2 to validate their profile.

5. WORKING OF FINGERPRINT

• It's pretty obvious why we have fingerprints—the tiny friction ridges on the ends of our fingers and thumbs make it easier to grip things.

• By making our fingers rougher, these ridges increase the force of friction between our hands and the objects we hold, making it harder to drop things.

• There are two separate stages involved in using system like this:

a) Enrollment: Where the system learns about all the peoples, it will have to recognize each day.

b) Verification: Anyone who wants to gain access has to put there on scanner, this scanner takes there fingerprint check it against all the prints in the database stored during enrollments.

6. DESIGN

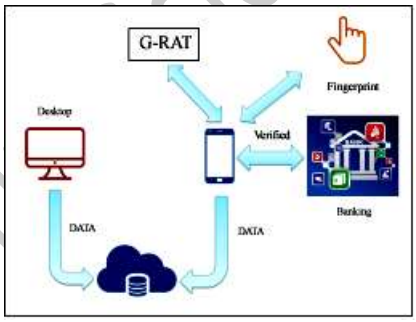

Figure1: Relevant Mathematics Associated With the Project

7. MATHEMATICAL MODULES

Set theory applied to the project:

1. Register Authentication:-

Set(R) =fR0, R1, R2, R3, R4g
R0 2 R = Register gRAT with Image Pattern.
R1 2 R = Register Biometric fingerprint.
R2 2 R = View results.
R3 2 R = Save Authentication info on Cloud.
R4 2 R = Secure info using AES.

2. Verify Authentication:-

Set (U) =fV0, V1, R2, V2, V3, V4g
V0 2 V = Verify gRAT with Image Pattern.
V1 2 V = Verify Biometric fingerprint.
R2 2 V = View results.
V2 2 V = Verify Authentication using Cloud.
V3 2 V = Start Banking Application.

V4 2 V = Perform Banking Operations.

Vein diagram of intersection of two sets:

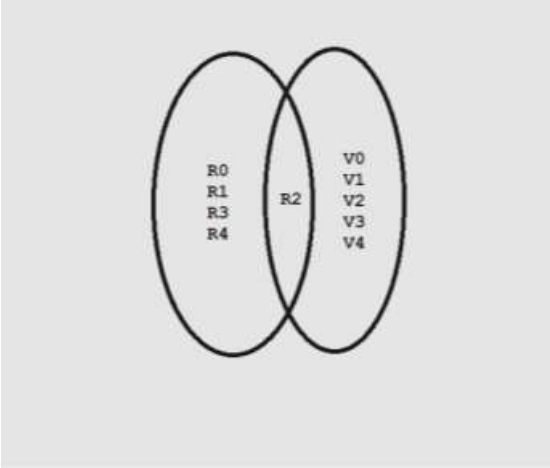

Figure 2: Vein Diagram Figure

Probability of our Project Modules:

1. in Register Module:-

We have two possibilities for successful registration i.e. whether internet is present to save data on cloud or not.

P (present) =1/2
P (not) =1/2
Hence, P (Internet) = P (present) + P (not)
=1/2 + 1/2
= 1

2. In Verify Module:-

We have two possibilities for successful verification i.e. whether proper authentication process of gRAT and Biometric is followed or not.

P (present) =1/2
P (not) =1/2
Hence, P (Authentication) = P (present) + P (not)
=1/2 + 1/2
= 1

Conditions:

1. Success Conditions: The system will take an input from user create a secured Authentication technique using gRAT and Biometric Authentication techniques.

2. Failure Conditions: For real-time information gathering internet is must.

8. CONCLUSION

The general aim of this project is to increase the usability, security, and memorability of the graphical passwords for consumer electronic devices, thus, we focus on pure recall based graphical passwords. We were successful at designing an innovative scheme that improves memorability as well as provides security and usability. It is deduced from the obtained results that the proposed system is more secure than the existing graphical scheme and shoulder-surfing resistant. In this project, we are developing a novel approach to provide a secured environment for a banking system using gRAT and Biometric authentication system together. We have assembled cloud computing and desktop application together to build a whole new system which is secured and reliable. It is more intelligent in minimizing the risks of hacker attacks on the banking system.

9. REFERENCES

[1] D. Lin, N. Hilbert, C. Storer,W. Jiang, and J. Fan, "Uface: Your universal pass- word that no one can see," Computers & Security, vol. 77, pp. 627– 641, 2018.

[2] R. Amin, R. S. Sherratt, D. Giri, S. Islam, and M. K. Khan, "A software agent enabled biometric security algorithm for secure file access in consumer storage devices," IEEE Trans. Consum. Electron. vol. 63, no. 1, pp. 53–61, 2017.

[3] D. Giri, R. S. Sherratt, T. Maitra, and R. Amin, "Efficient biometric and pass- word based mutual authentication for consumer usb mass storage devices," IEEE Trans. Consum. Electron. vol. 61, no. 4, pp. 491–499, 2015.

[4] F. Tari, A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. 2nd ACM symposium on Usable privacy and security, 2006, pp. 56–66.

[5] K. Gilhooly, "Biometrics: Getting back to business," Computerworld, May, vol. 9, p. 2005, 2005.

[6] G. Blonder and P. GRAPHICAL, "United states patent 5559961," Graphical Passwords, 1996.

[7] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in USENIX Security Symposium, vol. 13, 2004, pp. 11–11.

[8] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentica- tion," in USENIX Security Symposium, vol. 9, 2000, pp. 4–4.

[9] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem," in IEEE 33rd Int. Computer Software and Applications Conf. (COMPSAC'09), vol. 2, 2009, pp. 318–323.

[10] D. Weinshall, "Cognitive authentication schemes safe against spyware," in IEEE Symp. Security and Privacy, 2006, pp. 6–pp.

[11] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," Int. jour. human-computer studies, vol. 63, no. 1, pp. 128–152, 2005.

AUTHORS PROFILE

Mr. Nirmal M.D. Completed B.E., Information Technology in the Year 2007. M.Tech. in the Discipline of Computer Science and Engineering... Currently Working As Assistant Professor In Pravara Rural Engineering College, Loni And Pursuing Ph.D., In The Area Of Image Processing And Internet Of Things. Having 10 Years of Experience in Teaching Field. Published Research Papers In Image Processing Area. Currently Working On Smart Precision Farming to Improve Green House Agriculture.

Saurabh D. Gadekar BE Computer (Student)

Pawan R. Ghogare BE Computer (Student)

Shailesh U. Ghogare BE Computer (Student)

Jagruti M. Ghorpade BE Computer (Student)