International Journal of Advanced Research in Engineering and Technology (IJARET)
Volume 10, Issue 5, September-October 2019, pp. 143-153 Article ID: IJARET_10_05_015
Available online at http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=10&IType=5
ISSN Print: 0976-6480 and ISSN Online: 0976-6499

AN EFFECTIVE PASSWORD AUTHENTICATION SYSTEM USING SMART WAY OF PASSWORD RECOVERY IN SUPPORT FOR BANKING SERVICES

R. M. Gomathi
Assistant Professor, Department of IT, School of Computing,
Sathyabama Institute of Science and Technology, Chennai, India

A. Sivasangari
Associate Professor, Department of IT, School of Computing,
Sathyabama Institute of Science and Technology, Chennai, India

K. Indira
Assistant Professor, Department of IT, School of Computing,
Sathyabama Institute of Science and Technology, Chennai, India

E. Brumancia
Assistant Professor, Department of IT, School of Computing,
Sathyabama Institute of Science and Technology, Chennai, India

P. Ajitha
Associate Professor, Department of IT, School of Computing,
Sathyabama Institute of Science and Technology, Chennai, India

ABSTRACT

Banking is one of the most important aspects of everyday routine. Several users are using it for performing numerous transactions and many of them have become online nowadays. With the growth of internet and technology, all the transactions are done online and there is no need for the customer to visit banks frequently. A single click does all the transactions by sitting in one place. Though it is very good to hear even online banking has numerous threats. The users are given their own internet logins wherein they perform their transactions. This has become a critical threat as most of them can be easily hacked and all the transactions are done without their knowledge. In order to preserve their critical information, an efficient authentication based secured framework is designed where in case if the user forgets his password of the login it could be recovered easily. As banking systems ask the user to change the password frequently for security purposes user tends to forget his passwords. By this proposed system it is very easy to recover his forgotten password. The proposed system is evaluated is observed to be efficient than the other existing systems.

Keywords: Banking, Transactions, Security, Authentication, Encryption, Fraud Tolerant, Cipher Text

Cite this Article: R. M. Gomathi, A. Sivasangari, K. Indira, E. Brumancia and P. Ajitha, An Effective Password Authentication System using Smart way of Password Recovery in Support for Banking Services, *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 10 (5), 2019, pp 143-153.
http://www.iaeme.com/IJARET/issues.asp?JType=IJARET&VType=10&IType=5

1. INTRODUCTION

Banking plays a vital role in everyday's life [1]. Without doing any transactions it is very difficult to proceed a life. There are numerous reasons where we do several transactions. In traditional days, we have seen people going and standing in front of the banks and in long queues even for a small transaction. With the growth of the internet has reduced this long waiting queues to a greater extent. People are not visiting banks for their small transactions and when there is a need only then they tend to visit. All the banking services are readily available in banks online services. Let it be fund transfer, applying for a new ATM card or applying for any other services [2]. It is the prime responsibility of a bank to provide a login for every user of their bank in order to access their profile.

The era of internet banking has also tended to numerous security threats [3]. Each user is given a separate password to log in their profile. These passwords are generally very secure and the users are adviced not to share the passwords with anyone [4]. The users are also advised to change their passwords frequently so that they are not compromised to any hackers. While changing the passwords each and every time many users tend to forget their passwords and suffer from not logging into their account. While retrieving their forgotten process it is a huge process wherein several authentication systems play its role. The password reset link is not that easily given to any user, as there might be many security breaches. In this paper, we have proposed a secured and authenticated system which is used for recovering the password with less time. The work is compared with numerous traditional systems and is observed to be working efficiently better than the others. The rest of the paper is organized as follows: In section 2, a summary of related works is given. Section 3 briefs about the proposed model and shows the detailed design of the proposed model. Section 4 presents the experimental results whereas the paper is concluded and future works are pointed out in Section 6.

2. RELATED WORK

There are varied works that are processed and designed by numerous researchers that are built to certify the passwords that are being given to the users from not being victimized. Ramzan and Pervaiz [5] viewed shifted verification arrangements that online banks supply to their clients from every security and convenience point of view; like Two-factor verification approaches to broaden security, that includes 2 essential components: (1) something client knows about, similar to word, PIN, passphrase and so forth.; And (2) one thing client has, such as rotating credit, equipment token and so forth. At that point performed chance investigation upheld the presented confirmation arrangements. Mujinga and Eloff [6] inquired about manners by which to improve the ease of use of web based financial security frameworks. Examined the arranging standards and human capacities regarding the issue required to utilize security frameworks solidly, and examined the improvement of what impacts the conduct of clients of web based financial administrations and appearance at their communication with online security advances, at that point presented a structure for the arranging standards for usable on-line security and tried it abuse the heuristic examination strategy. Hertzum et al [7] assessed and reviewed six Danish online electronic financial frameworks that have genuine

shortcomings with pertinence simple use. The investigation of the shortcomings asked that security needs are among their causes. Braz and parliamentarian [8] examined the convenience security exchange off of two-factor confirmation ways. They propose 2 rating scales: security and esteem, severally, and use them to coordinate client validation techniques; together with two-factor verification. They all over that two-factor authentification will expand "redundancy," so increasing security, in any case, diminishing ease of use. Subsorn and Limwiriyakul [9] inspected web banking security frameworks in Australian banks by sending a similar examination approach in producing an arranged web banking security list. The outcomes revealed were absence of web banking security everything considered the16 picked Australian banks. higher web banking security data, two-factor validation and more grounded cryptography being used are some of the example suggestions. Casaló et al. [10] considered the impact of apparent security, protection, ease of use and name on the benefactor trust inside the setting of web based banking, likewise, broke down the trust-responsibility relationship inside the setting of monetary web destinations by formalizing a speculation; proceeding with the data collection and live approval forms. At last, correlation the planned model with an opponent one and giving different choices to up the level of customer trust and duty inside the setting of web based financial Weir et al. three looked at 3 very surprising two-factor techniques of e-Banking confirmation as far as by and large quality, security and accommodation as seen by members (50 eBanking clients). The discoveries of this correlation demonstrate that members picked their inclination following ease of use and accommodation frames of mind rather than what they were by all accounts dynamically secure. Al-Somali et al.[11,21] known and analyzed an assortment of things that urge clients to receive and agree to web based banking in Saudi Arabia bolstered an innovation acknowledgment model (TAM) and consolidated some further essential administration factors. The assessment was done to 400 clients. The high pace of unreported wrongdoings could influence the general public in basic leadership and because of this circumstance; half of the violations are not revealed. The users can register to application and can give the detailed report of crimes that happened [12,22]. Data fusion plays a vital role to save energy of the sensors. Different Data fusion models and their working principle are studied, analyzed and surveyed in order to understand the goals of each data fusion model [13]. The classification is made conceivable by structure a learning base against which any information could be sorted. The degree is limited for this situation and henceforth fabricating the information base should be exact else the characterization would be wasteful [14]. This framework is a reasonable structure to prepare the client profile all the more rapidly and productively with the assistance of reranking forms. Adarsh Swaminathan. B et al. proposed a framework which is progressively secure by controlling the measure of client profile's subtleties at the customer side being passed to the server side, along these lines giving protection and keeping up a decent positioning quality. Stemming Algorithm was utilized so as to gather the catchphrases that are much of the time utilized by the client [15,20]. The characterization the clients as spammers, content advertisers and genuine clients by structure a test gathering of genuine YouTube clients utilizing which we can give an order we utilization of substance, individual and social characteristics that help in describing every client class. For compelling order we use SVMKNN which is a functioning learning approach [16,18]. Agricultural developed a system which will automatically monitor the agricultural field as well as performing live video streaming for monitoring the Agriculture field from the server itself, through raspberry pi camera. The agriculture fields are monitored for environmental temperature, humidity and soil moisture. The automatic irrigation will be performed based on the set points of the temperature, humidity and soil moisture sensor. The data collected from the field are monitored in IoT, the data are then processed and necessary information is passed through the field owners for counter measures [17,19].

3. SYSTEM DESIGN OF PROPOSED MODEL

The architecture of the proposed model for banking services is designed as in Fig.1. The data acquisition layer collects user data that is needed for authentication from the data contributors that is the users through online internet banking services. The registration center is used to maintain an online database for various registrations that assigns a unique identity and password for each registered customer. The registration center setups various other parameters such as the signature scheme and cryptosystem. Multiple registration centers are also set up which could be used when a single point of failure occurs in the model. The data trading layer is responsible for maintaining the truthfulness of the raw data collection. It should be free of data collection attacks from external intruders and should properly verify whether the user data provided is through properly registered users. The proposed model is designed to simultaneously guarantee data truthfulness and privacy preservation of the user data obtained from the data contributors. The users register their data with the registration centers and verify that their submitted data is truthful. The data contributors cannot impersonate other contributors data. The baking service provider is enforced to truthfully collect the data and process it for further verification. Both the identities of the data contributors and sensitive information about the data are well protected. The proposed model is extensively evaluated through two real- world datasets and their performance are evaluated. This section will provide a detailed explanation of the various modules used in this model. Fig. 1 shows the complete architecture of the proposed model. The model creates a user with a new mobile number and the account is registered successfully. The proceeding steps in making the password more secure is shown in Figure 1.

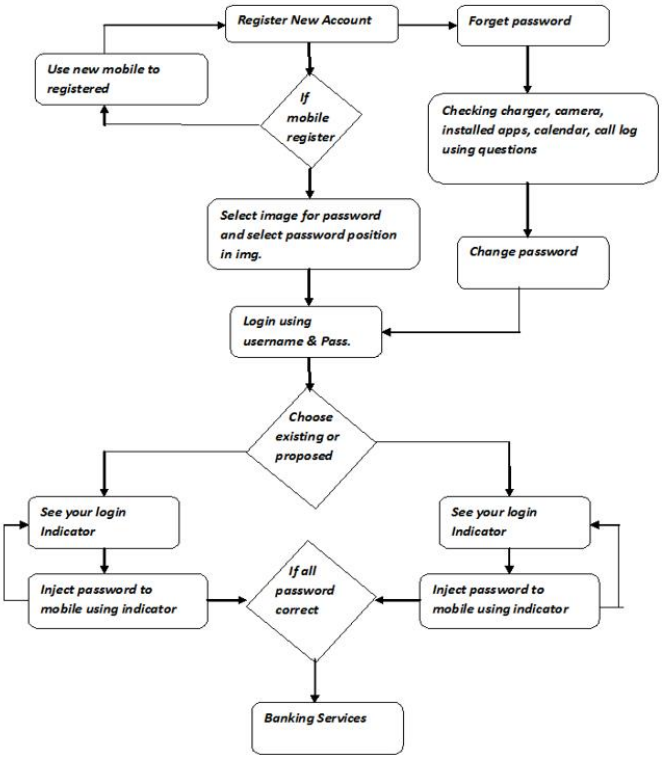

Figure 1 User site Authentication Technology

3.1. Pseudo Identity Generation

All the banking customers undergo the process of registration with the registration center which in turn provides a unique pseudo identity or a Login ID to every registered user. The registration center setups the system parameters well before the beginning of the data trading. The

verification is done at both the ends; the data contributor and the data consumer. Two-layer batch check is finished during information processing and signature total. At the finishing stage, the final verification is done by the data consumer.

3.2. User logs Accumulation

The everyday utilization of banking services by different clients has collected to frame client logs. We expect that there exist some legitimate however inquisitive information patrons, specialist organizations, the information purchasers, and outside aggressors, e.g., busybodies, may assemble touchy data from client information, and perceive the genuine personalities of clients for unlawful purposes, e.g., an assailant can construe an information giver's home area from her financial profile. Henceforth, the passwords given to the client's should be verified in every one of the perspectives. It should likewise be stayed quiet from the framework members, i.e., we should protect information confidentiality. Plus, an outside eyewitness can't uncover an information supporter's genuine character by breaking down datasets sent by the client, i.e., personality safeguarding. The logs dataset will be put away in a database as a vault set. The Third-Party Server needs to register these pertinent logs and produce the procedure.

3.3. Processing of Passwords

By utilizing the wording from the sign-encryption conspire, the proposed model is organized inside in a method for Encrypt-then Sign which uses the system called incomplete homomorphic encryption and personality-based mark. It forces the financial administrations to honestly gather and process the genuine information. The pith is to first synchronize information preparing and signature verification into the equivalent cipher text space, and afterward to firmly incorporate information handling with result verification by means of the homomorphic properties. Such a development is powerless against both the no/fractional information handling assault, as the information purchaser, just knows the cipher texts and neglects to confirm the accuracy and fulfillment of the information administration. Figure 2 shows the throughput of the system when compared with other models.

3.4. Signature-Based Encryption of Passwords

The main responsibility of banking services is to process encrypted passwords. Here the passwords are encrypted and then converted into signatures. To monitor the confidentiality about the baking customer, each unique user ID is processed in the content of the log and is then encrypted and appended to a single signature. To enforce the validation process, service providers have to check the log files periodically. For each processed output their respective signature is compared. Only if the signature is matched the confidentiality of the service providers get upgraded. Thus, we can avoid the fraudulent behavior that has a high possibility of occurrence.

4. EXPERIMENTAL RESULTS

The system model was designed using JDK 1.7 and Tomcat 7.0. The application is designed as shown in Figure 2.

Figure 2 Graphical Authentication Application

The system was evaluated on various parameters proposes the user site authentication technologies that are used for the two-factor authentication login where transaction verification is available. Various login requirements and Password recovery methods are also discussed. Before creating a login in this module, the user is asked to enter his IP Address to make the application even more secure. Once the user creates it, it could be changed only when the user uses his graphical authentication password to change it. Hence this could avoid the use of using the application of the user in other devices. The screen prompting for the IP Address of the user is depicted in Figure 3.

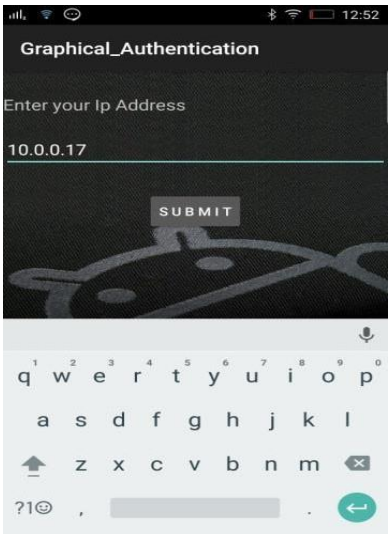

Figure 3 The input of IP Address

Figure 4 shows the graphical view of user authentication. New user registration page and user login page is depicted. The user is allowed to register for the first time using his mobile number.

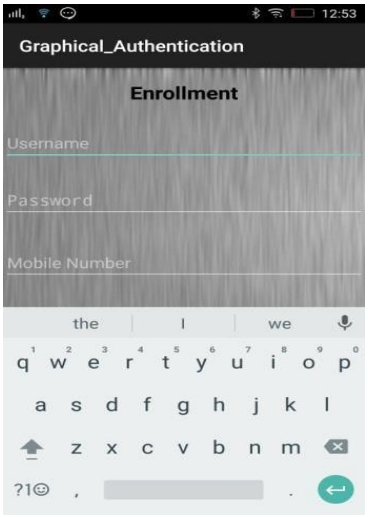

Figure 4 User Registration Page

The user can then set his password as shown in Figure 5. The password could be used for his subsequent logins.

Figure 5 User Registration Page

When the user attempts to forget his password a new dialog prompts as invalid passcode where the user gets an option of recovering his old password through the registered mobile number. The page is depicted in Figure 6.

Figure 6 Password Recovery

Figure 7 Selecting Graphical input Authentication

While password recovery, there could be a chance of any malpractice. In order to avoid it, the user has to select a graphical image that he has used while registering. When the graphical input given now matches the older one then the user is able to successfully recover his password. The panel showing the user to select the image is shown in Figure 7.

Figure 8 Graphical Authentication

Once the graphical image is chosen by the user, the decoding of the input takes place by each and every pixel. In Figure 8 we can observe that the given input is segregated into numerous columns and the decoding takes place to match it with the previously given authentication password.

Figure 9 Navigation Pane

The navigation pane of the graphical authentication panel is given in Figure 9. By using this pane the user is able to move and select the input from is device effectively.

Figure 10 Selecting Graphical input Authentication

The proposed model has two services that are provided to the user. One is the Graphical authentical and another one is the Improved Graphical authentication. The user can select any one of the above two mentioned methods to authenticate the passwords that they are using for their banking applications. The panel of the proposed model is depicted in Figure 10.

5. CONCLUSION

Banking plays a critical role in everyone's life. All the transactions done on for banking purposes are numerously used via internet banking. Passwords are generally given to the users for protecting their own data and sharing of it might cause a great security threat to the user. In order to protect the passwords, they need to be authenticated. As there are several attempts to change the passwords regularly, many users tend to forget them. Password recovery is a great research work and numerous researchers are working on it to make it more secure. In this paper, we have proposed a method that is used to securely authenticate the password while recovering it. The evaluation results have shown the efficiency of the model when large datasets are used. Future works may include the use of various machine learning techniques to make the model more feasible to complex datasets and handle the growing privacy threats.

REFERENCES

[1] Freixas, X., & Rochet, J. C. (2008). *Microeconomics of banking*. MIT press.

[2] Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International journal of bank marketing*, *21*(1), 5-15.

[3] Hole, K. J., Moen, V., & Tjostheim, T. (2006). Case study: Online banking security. *IEEE Security & Privacy*, *4*(2), 14-20.

[4] Herley, C., van Oorschot, P. C., & Patrick, A. S. (2009, February). Passwords: If we're so smart, why are we still using them? In *International*

[5] Conference on Financial Cryptography and Data Security (pp. 230- 237). Springer, Berlin, Heidelberg.

[6] F.Ramzan, T.Pervaiz, " Online Banking Security," Linköpings Uni versity, Sweden. 10.

[7] M. Mujinga and M.M. Eloff, "Towards Usable Online Banking Security", School of Computing University of South Africa, South Africa.

[8] M. Hertzum, N. Jørgensen, M. Nørgaard,(2004) "Usable Security and E- Banking: Ease of Use vis-à-vis Security," Roskilde University, Denmark.

[9] C.Braz and K.-M.Robert, (2006) "Security and usability: the case of user authentication methods," in the 18th International Conference of the Association Francophone.

[10] P. Subsorn and S. Limwiriyakul, (2011) “A Comparative Analysis of The Security of Internet Banking in Australia,” in The 2nd International Cyber Resilience Conference.

[11] L. V. Casaló, C. Flavián, and M. Guinalíu, (2007) “The role of security, privacy, usability and reputation in the development of online banking,” Economics and Business Studies, University of Zaragoza, Zaragoza, Spain.

[12] S. Al-Somali, R. Gholami, B. Clegg, (2009) “An investigation into the acceptance of online banking in Saudi Arabia,” Operations & Information Management Group, Aston Business School, UK.

[13] Infanta Amirtha Mary N., Dharshini J. and Sivasangari A. (2016), “Crime reporting integration of crime & complaint reporting and effective data sharing with multi user access”, International Journal of Pharmacy and Technology, ISSN: 0975-766X, Vol. 8, Issue. 2, pp. 11916-11924.

[14] E. Brumancia, S. Justin Samuel, R. M. Gomathi and Y. Mistica Dhas, (2018)"An Effective Study on Data Fusion Models in Wireless Sensor Networks ", Vol. 13, NO. 2, January 2018.

[15] P. Ajitha, Dr. G. Gunasekaran, (2014) “Semantic Based Intuitive Topic Search Engine”, International Review of Computers and Software, Praise Worthy Prize, PP 1964-1970, Vol.9, No.12 Nov 2014. ISSN: 1828-6003 e-ISSN: 1828-6011.

[16] B. Adarsh Swaminathan, Vinod Kumar, G., Gomathi R. M., (2016) “Personalized mobile web search engine”,International Journal of Pharmacy and Technology, 8(2), pp. 11925-11931,

[17] Indira K., Christal Joy E., (2014) “Prevention of Spammers and Promoters in Video Social Networks using SVM-KNN”, International Journal of Engineering and Technology, Vol.6, No.5, Oct – Nov 2014, Pp. 2024-2030.

[18] Ramya Venkatesan ,Anandhi Tamilvanan, (2017) "A Sustainable Agricultural System Using IoT" IEEE International Conference on Communication and Signal Processing, April 6-8, 2017.

[19] A.Sivasangari, P.Ajitha, K.Indira, “Air Pollution Monitoring and Prediction using Multi View Hybrid Model", International Journal of Engineering and Advanced Technology (IJEAT)ISSN: 2249 –8958,Volume-8, Issue-2S,pp.1370-1372.

[20] Brumancia E., Gomathi R.M., Naidu, D.A., Srikanth, D., “Contention based forwarding message in vanet after an emergency event”, Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019.

[21] Anandhi, T., Kishore Kumaar, V.S., Maha Ganesh, S., Gomathi, R.M, “A sustainable vehicle parking using IoT”, Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019.

[22] Indira, K., Ajitha, P., Reshma, V., Tamizhselvi, A. , "An efficient secured routing protocol for software defined internet of vehicles",2nd International Conference on Computational Intelligence in Data Science, Proceedings, oct 2019 .

[23] P. Ajitha, Dr. G. Gunasekaran., Semantic Based Fuzzy Inference System (SBFIS) Prediction of Patient Emotion and Prescription using support vector machine” in the Journal of Medical Imaging and Health Informatics, PP 769-773, ISSN: 2156-7018, Vol.6, No.3, June2016.

[24] S. Senthil Kumar and Dr. P. Abirami. Customer Usage Patterns and Satisfaction of E-Banking Services. International Journal of Advanced Research in Management, 8(1), 2017, pp. 12–20.

[25] Dr. M. Raja, Dr. M. Muthu Gopalakrishnan, Dr. R. Venkatamuni Reddy, Prof. A. Nagaraj Subbarao, Customer‟s Satisfaction on Online Banking Services Offered by Selected Private and Public Sector Banks in Chennai City, Journal of Management, 6 (2), 2019, pp. 310–319.

[26] B. Al Mannai, S. Suliman and Y. Al Alawai, Implementation Effect on Bahrain Industrial Performance, International Journal of Industrial Engineering Research and Development, 8(1), 2017, pp. 27–48.