A Security Risk Model for Online Banking System

|  |  |  |
| --- | --- | --- |
| Anshita Dhoot | A. N. Nazarov | Alireza Nik Aein Koupaei |
| Moscow Institute of Physics & | Moscow Institute of Physics & | Moscow Institute of Physics & |
| Technology State University | Technology State University | Technology State University |
| Moscow, Russia | Moscow, Russia | Moscow, Russia |
| anshita.dhoot.23@gmail.com | a.nazarov06@bk.ru | alireza.nik666@gmail.com |

***Abstract* – We are living in an era, where the security of our data has become a huge issue. The services of cyber are the most entertaining and time-saving things in one’s life. Though, people save their data on the cloud, which has been managed by the cyber. Cyber-security plays an important role in this matter. This is the open challenge for the security because many intruders are there who can attack the data and hack the details of the user by the server. If we will see around, then we will find many cases which include cyber-crime. This has become a very genuine concern to secure our datasets which are available on the cloud. Our research includes the security of the datasets which will include intruder detection that can be occurring anywhere on the earth. This has become very important to protect the data from intruders, for this intruder detection should be the most important key to get identified. If we don’t know who is the intruder, then how we will get to know who is stealing the data which has been secured by using much biometric security, fingerprints, passwords, OTPs etc. intruder detection has become very important, especially on mobile objects - airplanes, ships, etc.. As we know the problem then only we are able to find the solution. To prevent this, we are using the methods from machine learning, biometric recognition, data learning or hybrid methods. These are going to be the handle of the system that can help to secure the data from intruders by using best optimization techniques to get precise data. We proposed a model for the banking system, whereby using biometric impressions and digital signatures to make every transaction possible by bank’s customer. This proposes the security for the Smart Online Banking System (SOBS) by using the biometric prints, it can become more secure and reduces a lot of threats can be made by an intruder.**

***Keywords— Intrusion Detection, Model, Security, Smart Banking System, Biometric Imprints, Artificial Intelligence.***

I. INTRODUCTION

In this world of internet, full of cyber-attacks, people demands for the security of their data and expensive things. This era of the cyber world has many intruders which makes internet vulnerable. This is the reason we need to secure cyber-world from various kind of existent attacks can be caused by the intruders. In search of identifying those intruders which can make the security networks vulnerable, we need to find their activities or several kinds of possible attacks on data, and then only we could prevent the data to being stolen.

The basic necessity for the smart banking system is necessary for people to have trust in their account accessibility and security of their privacy. The SOBS works with lots of

978-1-7281-4772-7/20/$31.00 ©2020 IEEE

various ideologies; sometimes it is very huge to secure the large data spaces in the cyber from huge numbers of cyber-attacks. Many intruders are there to attack the user’s account and it is very vulnerable to detect the cyber-crime which is happening to the user’s account. The environment of the online working system includes the One Time Password (OTP) generated by the network, which could be provided to the user for acknowledging the legitimacy of a user’s mobile number.

A biometric system recognizes using a precise physiological or behavioural attribute possessed by a person. This is called a biometric, identification and verification system which depends on the application in which it is used [6]. A verification system measures by comparing the biometric properties of its test with the biometric pattern stored in the database, while an identification system identifies each by probing the whole database to match it.

Physiological biometrics combines fingerprint, face, hand geometry, palm print, etc. whereas behavioural biometrics includes signature, speech, gesture, and so on. A biometric manner must meet properties such as distinctiveness, universality, collectability, and permeability, to be used in a biometric system. Dependency on the internet world and easy access to their debit and credit card details via the online system is becoming a threat for people these days. It has been created many account hackers, unknown transactions from the user's account and many more threats have been generated by these facilities provided by the cyber world [1, 2].

The number of intrusion detections has been cured and abundant types of attacks are there to being secured. Cyber-attacks/cyber-crimes made by an intruder such as phishing, scamming, fraud & identity stealing crimes, virtual crimes, the threat by computer hacker groups/organized crime groups/terrorist groups, money-evasion, and so on [17, 20].

This paper proposing the security risk model for online banking system introduces inline biometric techniques to prevent the account of a customer. It helps to detect the unexpected trials for the transaction which is occurring to their account without their prior knowledge and prevent their data more securely as it will need techniques from biometric technology, for example, digital signature, face recognition and fingerprints. These techniques help any person to operate a person who is not educated enough to operate any technology, but these techniques help them to prevent their ac them to

Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:05:46 UTC from IEEE Xplore. Restrictions apply.

prevent their account from intruders because it will need the only physical presence of a person who owns the account.

This will help to reduce the paperwork to operate customer’s account, the transaction is hassle-free, and make easily accessible to their data more secure than ever. It prevents from many attacks such as impersonation attack, foreign key attack, man-in-the-middle attack, denial-of-service attack, distributed denial-of-service attack, eavesdropping attack, password attack, phishing attack, spear-phishing attack, cross-site scripting attack, zero-day exploit, and cyber-attack prevention [18, 19].

This paper is designed in a way to explore new details about the cyber-attacks and best possible techniques might be used to secure the account from the customer of any bank. In this paper, seven different sections have been categorized.

II. RELATED WORK

The feature vector introduced by Tico, et al. consists of the standard deviations of the Discrete Wavelet Transform (DWT) coefficients of the whole image at different levels and familiarization. K-Nearest Neighbour classifier employing Euclidean distance is used for matching.

Many intruder attackers are sitting to seek for the leniency of the customer of the bank. The more safe banking system will be there, more customers will feel free to use online banking. Junho Lee, Jungwoon Woo et.al. [3], introduced a technology by providing them with the application by giving the methodology for developing software in terms to create a secure web. It does not have OOAD methodology, UMLsec and Java EE, to maintain the database and to associate it to correlate.

In the malware threats and security solutions Wazid, Zeadally and Das [4] discussed the need for mobile banking and every possible attack which could be occurred while using the mobile banking system. They have shown their work in mobile banking, its limitations and its improvements but there is no model to secure it.

Similarly, R. Bose, S. Chakraborty and S. Roy [5] explained the working principle based on multi-factors of cloud authentication architecture for banking system by using biometric fingerprint authentication by using USB to make sure that data is authentic. Even they have established a secure and safe VPN connectivity but failed to prevent the data from different cyber-attacks.

In this papers [6, 7, 15], proposed an authentic environment for user’s credentials of bank and cloud server but these are not secure enough to prevent customer’s data from the severe cyber –attacks such as phishing and pharming is possible to threaten the data of the customer, whereas this [8], presented the results of several kinds of targeted attack over the online banking system.

Limba, Pleta, et.al. [9], designed a model for cybersecurity management includes six dimensions for better communications within the organization, but it may not able to secure the dynamic plans may change or adapt by various technologies. This assured that it could able to handle the initial and interoperable/moderate level of each dimension of the

cybersecurity model for its management, but it may be vulnerable for dynamic cyber-attacks.

There are various active attacks as well as passive attacks exist which can make and user’s account vulnerable as well as not secure from the attacker. Sundry researchers are working on the smart banking system, but still, there are a number of attacks needed to secure from the attackers [10-14].

III. PROPOSED MECHANISM

Through this paper, we are proposing a multi-factor authentication model developed the throughput with a tolerated area to make the transaction more secure by biometrics section, where the Biometric section acts as a multi-factor gateway as shown in Figure 1. It provides a face recognition authentication (FRA), biometric fingerprint authentication (BFA).

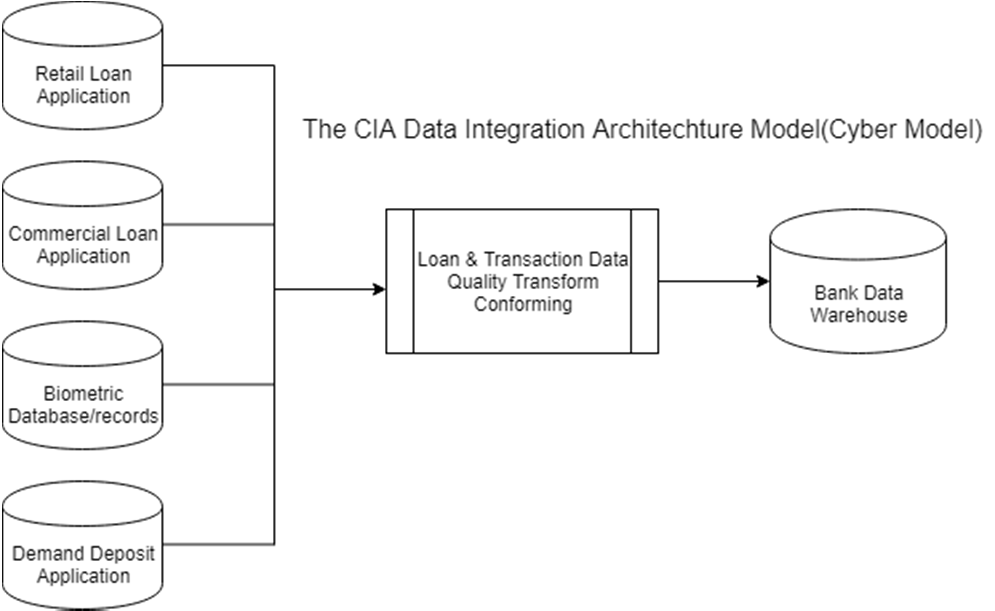


Fig. 1.The proposed Mechanism

These two techniques are working perfectly and providing extreme authenticity for verification of the valid user, it makes not a single transaction transferred from one account to the other, without any prior knowledge of the user. This proposed model, not only making transaction secure enough as well as reliable system for the user, but it also provides mobile operability for the user, it doesn’t matter where the user is, he/she can operate their account by verifying their transaction either from BFA or FRA, as shown in Figure 2.

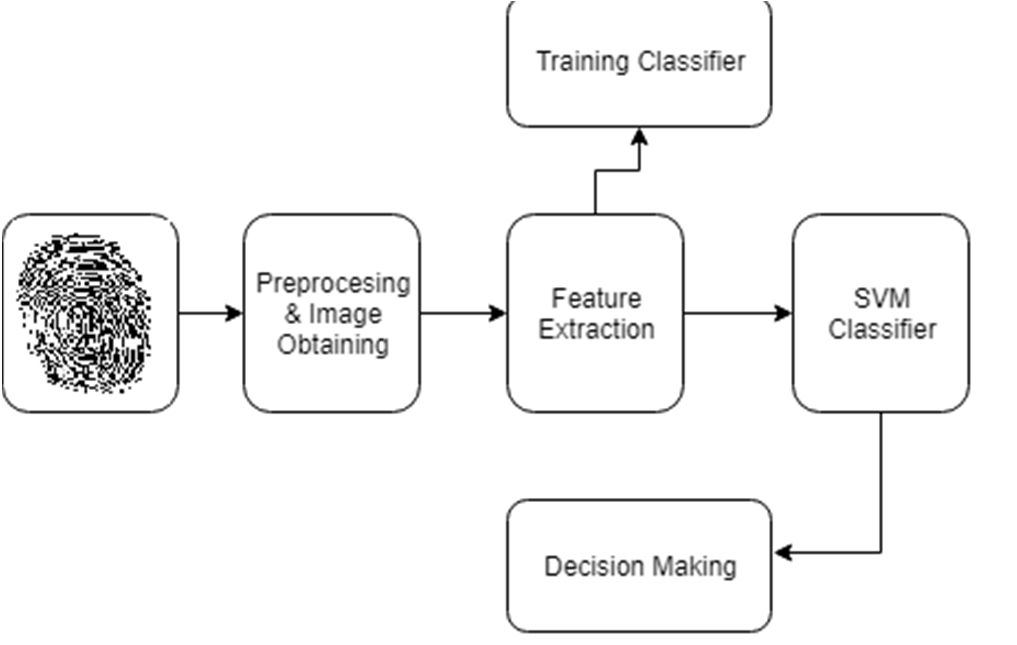


Fig. 2.Block diagram of Proposed Biometric BFA and FRA

Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:05:46 UTC from IEEE Xplore. Restrictions apply.

In this model of the smart online banking system, FRA or BFA will be used to take input to authenticate system’s model. It helps to obtain an image for preprocessing through the fingerprints/face recognition/digital signature. The next step will be the feature extraction, in this whatever the image has been captured by the machine as input via preprocessing & image obtaining gateway. The received image will be processed to SVM classifier or training classifier, which will help to generate to make a decision, either to validate the user or reject it. The rejected input will as again to give input to the machine and accepted input will allow the user to handle the transaction of their account.

This is how the proposed model will work and provide an authenticated user to transact into the banking system. Anything can be done smartly, there is no validation can deny BFA or FRA. These are the most renowned technologies which enhance the security of the transaction. This also helps the existing banking system more secure than the existing online banking system.

The act of CNN as the extractor of feature and the dense layer which consisted output from the image extractor, which helps to provide input to the SVM that classify the object presence, within the proposal of candidate region. Additionally, to predict the object's presence, this proposed algorithm will increase the bounding box’s prediction that helps to produce offset value to extract the precise data of the user.

The benefits of CNN, comparatively, to its antecedents that robotically to detect the vital features without taking any help of human expertise or human’s supervision. The major steps have been explained by Figure 2, diagrammatically. It includes Preprocessing & Image Obtaining, Feature Extraction with the help of Neural Networking or features of Region-Based with Convolution Neural Networking (R-CNNs) helps to detect object which could be applicable to the deep models, Features Extraction, and Verification.

The R-CNNs model, select various existed regions from the image for e.g. Anchor box, bounding box, their categories of labelling such as offsets, etc. after selecting from the image, they use CNN for forwarding computation that helps to extract features from the given area. Later, the feature of each proposed region predicts the category of labelling as well as the bounding box. Explicitly, R-CNNs composed four major parts which have been mentioned below:   
 i)Selective Search: it is performed on the received input image. It helps to select the multiple high-quality from the proposed regions, which help to select the image on multiple scales includes variants of sizes and shapes.

This makes to the label on proposed-region of the category as well as a ground-truth bounding box.

ii)Pre-trained CNN: it selects and places the in-truncated form before the proposed region’s output layer. It helps to transform it into the required input dimensions by the network. It uses the forward computation to provide the output of feature extraction from each proposed region.

iii)Featured & Labeled Category: it combines the each proposed regions to set an example that helps to train

the multiple Support Vector Machines. It helps to determine the example is belonged to a certain category or not.

iv)Featured & Labeled Bounding Box: it combines the each proposed regions to set an example that helps to train a Linear Regression Model for granted-truth for predicting Bounding Box.

IV. BASIC MATHEMATICAL MODEL

This proposed mathematical model as per CNN’s major parts, as mentioned below:

a)Fast R-CNN Model: this uses the complete image of CNN input for the process of feature extraction, rather than the proposed region. Furthermore, the network trains to update parameters of the model as the input of the whole image, then CNN output will generate the output of CNN as shape (1\*c\*h1\*w11\*c\*h1\*w1).

b)Assuming Selective Search: it generates the n proposed regions, which have a different shape to indicate particular Regions of Interests (ROIs). Its different shapes and sizes will have differed from similar shapes and similar shapes must be extracted from the existed ROIs. (Let us assume the height = h2 and the width = w2).

c)Completely Connected Layer: it is used to change the shape of the output to n\*dn\*d (d= model design will determine this d).

d)Category Prediction: during this process, the shape will be the completely connected layer to its output which is transformed again into n\*qn\*q. we use soft-max regression for this, where q is the number of the category. During the time of this bounding box prediction, the entire connected layer’s shape of the output will be transformed again into n\*4n\*4. It means that it helps us to predict the category as well as the bounding box for existed proposed region.

V. VERIFICATION

The function of Support Vector Machine is an extensively used tool, especially in the technique for pattern recognition area. It also makes to use the principle of Structural Risk Minimization (SRM), which provides a good performance in the field of non-linear patterns, especially in the concept to transform the input vectors converted into the space of high dimensional feature with the help of kernel.

It will be located to the optimal hyperplane for its linearly separable data as well as it extends to its no-linearly separable data with the help of mapping to the space of high dimensional feature space. SVM has several applications such as authentication based on biometric-based data, text categorization, information management, bioinformatics, digital signature, and so on.

The principle on which SVMs is based i.e. Structural Risk Minimization (SRM), which is based on the Statistical Learning Theory (SRT). If you wish to know more about SVM, then it is available in Vapnik20, Byun21 & Lee. LIBSVM22 has been used for the process of verification. We

Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:05:46 UTC from IEEE Xplore. Restrictions apply.

have four built-in kernels at our removal, those are linear, radial basis function, sigmoid and radial basis function. These parameters require SVM to turn such as another learning algorithm to find out optimal parameters, which provides the enhanced precision of the result on test data. Remaining three kernels are used for this process. In this, each kernel will have the five-fold-cross-validation process to perform on the existed training set. Algorithmic ‘Grid Search’ is used to receive parameters such as γ and c. The values of γ and c are giving the best optimal average of the cross-validation for its precision, which are employed at the place of testing this process.

VI. EXPERIMENTAL RESULT

DATASET

Those databases which have benchmark FVC2002DB1B [16], has been used for our experiments, which consist of ten users with eight impressions for each of it. These databases are divided into the testing set as well as the training set, where the training set has seven images of fingerprints and testing set has one image of fingerprints. Those images have been taken with a size of 388\*374, at 500 dpi resolution.

EXPERIMENTS

The several fingerprints have been selected to train, to test and to repeat the entire process for four times. This makes the experiments repetition for trials then it considered as its final performance. Each and every set has features set, aside from the verifying them through SVM process. The various window size (w), has experimented on ROI, that makes it best to acquire the superlative result for a 5\*5 window size of fuzzy features, after of all this, on the invariant moments for a 16\*16 of window size. The entire features have been normalized before the process to provide input to the SVM.

Each set of features is set aside for verification using SVM.

Different window sizes (W) have experimented on ROIs. The best results are obtained on fuzzy features for a window size of 5x5 and on invariant moments for a window size of 16x16. The features are normalised before inputting to SVM

|  |  |
| --- | --- |
| TABLE I. ***FVC2002*** | ACCURACY OF THE PROPOSED METHOD  ***Accuracy*** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *Fuzzy features*  *Invariant moment features* | |  |  |  | | --- | --- | --- | | Linear | BFA and FRA | Polynomial | | 74.8 | 87.6 | 77.6 | | 92.4 | 95.1 | 90.1 | |

VII.CONCLUSION

Thus, the models and methods proposed in the work allow to construct effective mechanisms for the protection of cyber-security in banking system at the canonical, logical and physical levels of their representation, providing access and admission to the content of their data to only with the appropriate user authority and establishing rules for user interaction with information resources according to the criteria of optimal, consistent with the requirements. This gives the

best possible architecture to access with ease and most secure way to save their data from different intruders. Future research includes to secure this model from different unknown attacks and to make it more feasible to the users.

REFERENCES

[1]Taylor, Robert W., et al. "Cybercrime and cyber terrorism." 2019.

[2]Umanailo, M. Chairul Basrun, et al. "Cybercrime Case as Impact

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Development | of | Communication | Technology | That | Troubling |
| Society." *Int. J. Sci. Technol. Res* 8.9. 2019, pp. 1224-1228. | | | | |

[3]Lee, Junho, et al. "A Software Development Methodology for Secure Web Application." *International Journal on Advanced Science, Engineering and Information Technology* 9.1. 2019, pp. 336-341.

[4]Wazid, Mohammad, Sherali Zeadally, and Ashok Kumar Das. "Mobile banking: evolution and threats: malware threats and security solutions." *IEEE Consumer Electronics Magazine* 8.2. 2019, pp. 56-60.

[5]Bose, Rajesh, Srabanti Chakraborty, and Sandip Roy. "Explaining the Workings Principle of Cloud-based Multi-factor Authentication Architecture on Banking Sectors." *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE, 2019.

[6]Ronchi, Corrado, et al. "Security, privacy and efficiency of internet banking transactions." *2011 World Congress on Internet Security (WorldCIS-2011)*. IEEE, 2011.

[7]Hole, Kjell Jørgen, Vebjørn Moen, and Thomas Tjostheim. "Case study: Online banking security." *IEEE Security & Privacy* 4.2. 2006, pp. 14-20.

[8]Correia, Márcio AS, et al. "Segurança em internet banking." XIII Simposio Brasileiro em Seguranca da Informacao e Sistemas Computacionais (SBseg), Gramado-RS. 2008.

[9]Limba, Tadas, et al. "Cybersecurity management model for critical infrastructure", 2019.

[10]Nami, M. R. "E-banking Issues and challenges: ACIS International Conference on Software Engineering, Artificial Intelligences, Networking and Parallel." *Distributed Computing (SNPD),* 2009.

[11]Dandash, Osama, Phu Dung Le, and Bala Srinivasan. "Security analysis for internet banking models." Eighth ACIS International Conference on

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Software | Engineering, | Artificial | Intelligence, | Networking, | and |
| Parallel/Distributed Computing (SNPD 2007). Vol. 3. IEEE, 2007. | | | | |

[12]Peotta, Laerte, et al. "A formal classification of internet banking attacks and vulnerabilities." *International Journal of Computer Science & Information Technology* 3.1. 2011, pp. 186-197.

[13]Nor, Fazli Bin Mat, and Kamarularifin Abd Jalil. "An enhanced remote

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| authentication | scheme | to | mitigate | man-in-the-browser |

attacks." *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*. IEEE, 2012.

[14]Nagaraju, Sabout, and Latha Parthiban. "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway." *Journal of Cloud Computing* 4.1. 2015. P. 22.

[15]Taylor, Robert W., et al. "Cybercrime and cyber terrorism." (2019).

[16]Kour, Jaspreet, M. Hanmandlu, and A. Q. Ansari. "Biometrics in Cyber Security." *Defence Science Journal* 66.6, 2016.

[17]Nazarov, Aleksei Nikolaevich. "Estimation of the information safety level of modern info-communication networks on the basis of the logic-probability approach. "*Automation and Remote Control* 68.7. 2007, pp. 1165-1176.

[18]Nazarov, Alexey Nikolaevich, Xuan Tien Nguyen, and Minh Hai Tran. "MODELING OF INFORMATION ATTACKS, AND SECURITY RISK ASSESSMENT OBJECTS. Conference "*Information Society Technologies*". Moscow, 2016.

[19]Kizza, Joseph Migga. *Guide to computer network security*. London: Springer, 2009.

[20]Wang, Huaqun, Debiao He, and Shaohua Tang. "Identity-based proxy-oriented data uploading and remote data integrity checking in public cloud." *IEEE Transactions on Information Forensics and Security* 11.6. 2016, pp. 1165-1176.

Authorized licensed use limited to: Marathwada Mitra Mandal's College of Engg. Downloaded on August 07,2023 at 09:05:46 UTC from IEEE Xplore. Restrictions apply.