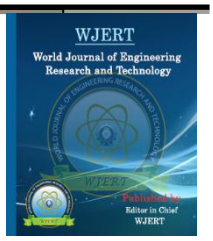
wjert, 2022, Vol. 8, Issue 4, 373-386. Review Article ISSN 2454-695X

World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924



A FRAMEWORK TO IMPROVE SECURITY AND QOS IN BANKING SECTOR

[1]Gaurav Sharma and *[2]Anil Kumar Kapil

[1]Faculty of Mathematics and Computer Sciences, Motherhood University, Roorkee, Uttarakhand, India.

[2]Faculty of Mathematics and Computer Sciences, Motherhood University, Roorkee, Uttarakhand, India.

Article Received on 16/02/2022 **Article Revised on 08/03/2022** **Article Accepted on 28/03/2022**

***Corresponding Author**
Anil Kumar Kapil
Faculty of Mathematics and Computer Sciences, Motherhood University, Roorkee,Uttarakhand, India.

ABSTRACT

With the rapidly growing banking industry, frauds in banks are also increasing very fast, and fraudsters have started using innovative phishing methods. With the technological advancements, intrusion attack activities are being seen very frequently in our wired/wireless communication networks used for e-services like online banking, digital payments, and E- commerce. Nevertheless, technological advancements have developed new ways for detecting and preventing those fraudulent activities. Such activities enforce severe threats to financial systems at the level of operations and damage hardware. This paper investigates the issues in banking services security with Quality of Service (QoS) and proposed solutions thereof.

KEYWORDS: Security, QoS, intrusion, banking sector, E-Commerce

1. INTRODUCTION

The popularity of a system or a software solution depends upon its user-friendliness, reliability, and security. The user-friendliness is concerned with user interface design which is highly related to user-centered design. All these implementations are under human-computer interaction (Kumar, 2011). The reliability of a software system is concerned with the quality of service (QoS) (Aloufi et al., 2021) and quality assurance (Lata and Kumar, 2010). The security methods are broadly two types: network-protected and device-protected. Different

firewall solutions are in use for this purpose. For separate devices, a genuine antivirus is also an additional protection layer toward security threats. The majority of electronic payments are done using mobile phones and laptops. Therefore, the security of those devices cannot be compromised. Nowadays, most mobile phones are having fingerprint or face recognition modules to keep safe the device from any unauthorized access. Many ATMs are also having fingerprint recognition sensors for cardless banking. Several template-based algorithms (Kumar and Sharma, 2009; Kumar et al., 2019) and training-based biometric approaches (Gupta and Kumar, 2010; Kumar et al., 2020; Kumar et al., 2021) are existing as security solutions for devices to protect. Kumar et al. 2021 presented a prototype for a touchless and cardless system for ATM cash withdrawal (Kumar et al., 2021).

2. LITERATURE REVIEW

In the banking system, a large number of users or customers are there to avail themselves the online services. To manage a large amount of data of customers, finance records, log files, etc., the use of data mining techniques is widespread. The log file of every transaction is recorded in banking servers to deal with any fail and successful transactions. Nami (2009) presented a survey of e-banking barriers and benefits from the point of view of customers and banks along with major issues and challenges like risk management and factors associated with e-banking establishment. Musleh et al. (2012) discussed the use of biometric fingerprint technology for the identification and authentication of bank customers for online services. They also discussed how biometric fingerprints can improve banking security to protect assets. Manthoulis et al. (2020), Carmona et al. 2019, Jing and Fang (2018) presented various predictions and ways to identify the bank customer for authentication (Keramati et al., 2016), detecting fraud transactions (Lv et al., 2019), segmenting the customers (Marinakos and Daskalaki, 2017; Smeureanu eta l., 2013; Ogwueleka et al., 2015), predicting bank customer interest using digital marketing (Ilham et al., 2019; Farooqi and Iqbal, 2019; Lahmiri, 2017; Moro et al., 2014), and analyzing sentiments of bank customers to offer the required services (Krishna et al., 2019). Table 1 shows a classification of observations in the banking sector. This comparative study is conducted from research published from 2013 to 2020 concluding the use of algorithms and collective learning methods used by some of the researchers.

Table 1: Algorithms and techniques used in the banking and financial sectors (2013-2020).

Contribution	Algorithm used						Ensembl elearning used		Area	Accuracy (Acc)/Area under the curve (AUC)
	Decision Tree	Neural Network	Support Vector Machine	K-Nearest Neighbour	Naive Bayes	Linear regression	Bagging	Boosting		
(Manthoulis et al.,2020)			Yes			Yes		Yes	Predicting bankfailure	AUC = 0.98
(Ilham et al., 2019)	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Predicting long-term deposit	Acc. = 97.08%
(Krishna et al., 2019)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Analysing sentiments of bank customers	AUC = 0.83
(Lv et al., 2019)		Yes							Detecting fraud in bank accounts	Acc. = 97.40%
(Farooqi and Iqbal, 2019)	Yes	Yes	Yes	Yes	Yes				Predicting bank marketing outcomes	Acc. = 91.20%
(Carmona et al., 2019)						Yes	Yes	Yes	Predicting banking failure	Acc. = 94.75%
(Jing and Fang, 2018)		Yes	Yes			Yes			Predicting banking failure	AUC = 0.92
(Lahmiri 2017)		Yes							Predicting bank marketing outcomes	Acc. = 71.00%
(Marinakos and Daskalaki, 2017)	Yes	Yes	Yes	Yes		Yes			Bank customer classification by telemarketing	AUC = 0.90
(Wan et al., 2016)	Yes		Yes	Yes			Yes	Yes	Predicting outstanding loans	AUC = 0.97
(Keramati et al.,2016)	Yes								Predicting bankcustomer churn	AUC = 0.93

(Ogwueleka et al.,2015)		Yes				Yes			Identification ofbank customers' behaviour	AUC = 0.94
(Moro et al., 2014)	Yes	Yes	Yes			Yes			Predicting bank marketing outcomes	AUC = 0.80
(Smeureanu et al.,2013)		Yes	Yes						Segmenting bank customer	Acc. = 97.13%

3. Security Issues in Banking Sector

Some of the most plentiful e-Services security issues being faced including online banking and other transactions in the financial sector are identity theft, banking account takeovers, credential stuffing, automated malware threats, cloud breaches, remote working, phishing attacks, and spoofing. Table 2 shows those major issues and their possible solutions.

Table 2: Security issues and available solutions.

Security issue	Description	Possible solution
Identity theft	The intruders can spy on the user's account even without stealing the card.	• Multi-factor authentication • Enable real-time alerts
Banking account Takeovers	Many times, the real account user does not even know that account-related communication is redirected to the intruder's details.	• Multi-factor authentication • End-to-End Encryption • Secure code andarchitecture • Enable real-time alerts
Credential stuffing	Credential stuffing is a kind of security issue in online banking, which is often targeted to have access to the personal details of the bank customer. With that stolen account details and programmed large-scale login requests, the intruders can get unauthorized access to the bank accounts of the customer.	• Multi-factor authentication • Enable real-time alerts • Educate customers about security
Automated malware threats	Another issue in online banking is automated malware attacks. The intruders send malicious code to the bank's server through automated tools to complete repetitive tasks to earn a significant amount of money against a very little associated cost.	• End-to-End Encryption • Secure code andarchitecture • Enable real-time alerts
Identity theft	The intruders can spy on the user's account even without stealing the card.	• Multi-factor authentication • Enable real-time alerts
Banking account Takeovers	Many times, the real account user does not even know that account-related communication is redirected to the intruder's details.	• Multi-factor authentication • End-to-End Encryption • Secure code andarchitecture • Enable real-time alerts

Credential stuffing	Credential stuffing is a kind of security issue in online banking, which is often targeted to have access to the personal details of the bank customer. With that stolen account details and programmed large-scale login requests, the intruders can get unauthorized access to the bank accounts of the customer.	• Multi-factor authentication • Enable real-time alerts • Educate customers about security
Automated malware threats	Another issue in online banking is automated malware attacks. The intruders send malicious code to the bank's server through automated tools to complete repetitive tasks to earn a significant amount of money against a very little associated cost.	• End-to-End Encryption • Secure code andarchitecture • Enable real-time alerts
Cloud breaches	The majority of banks use cloud services to minimize IT infrastructure ensuring data storage/backup and easy availability. But thisalso involves a risk of security breaches. The recent studies exposed that the major corporate cloud hacking activities are done by China.	• Multi-factor authentication • End-to-End Encryption • Secure code andarchitecture • Enable real-time alerts
Remote working	A lot of challenges are there with remote working over a secured network, especially in the Covid-19 pandemic. The challenge raisedhere is that every bank employee is not using a secure network to work from home. This might be very attractive for hackers looking for stealing sensitive data from those employees.	• End-to-End Encryption • Secure code andarchitecture • Secure VPN
Phishing Attacks	Phishing attacks are very common intrusion activities nowadays to get unauthorized access to users' data like credit/debit card numbers, personal identification number (PIN), OTP, and username/passwords as well. Recently, it is observed that most phishing attacks are being targeted at bank staff.	• Enable real-time alerts • Educate bank employees about phishing and security • Using secure VPN
Spoofing	Spoofing is a new way of cyber-attacks where intruders copy the URL of a bank's trusted website with a new website that looks almost similar to its genuine website. The customereven does not know that he/she is not using the bank's original website and becomes the victim by providing login credentials.	• Multi-factor authentication • Enable real-time alerts • Educate customers about security • Change PIN and password frequently

4. QOS Issues in Banking

QoS is concerned with the use of methods and tools working on a network for controlling the traffic and ensuring the performance of crucial applications with limited network capacity. QoS

enables the businesses setup for adjusting their overall network traffic by prioritizing the necessary applications. A few years ago, traditional business networks were being managed as separate entities. For example, the phone and conference calls were operated on one network, while computers, servers, and other shared devices operated on another network. They rarely shared the common bandwidth, unless a computer was used over a telephone line to access the internet. That was the time when networks were supposed to carry data with limited speed. But nowadays, so many interactive applications are there to carry audio and video contents that need to be transmitted at high speed, by ensuring lossless packet delivery. QoS is especially crucial to ensure the high performance of important applications requiring high bandwidth in real-time network traffic.

Some recent developments are seen in sensitive metrics, which are aimed to accompany the existing calculation of bandwidth and ping latency. Such sensitive metrics can be as simple as looking at the passive collection of transport headers from transmission control protocol sessions and calculating the time taken by transmission control protocol for a round trip between transmitter and receiver. QoS is a mechanism able to control the network traffic and regulate overall network activities by prioritizing the applications. With QoS, the applications can run over significantly enhanced over the network, specifically in terms of speed, latency, packet lossless transmission. QoS functions by creating separate virtual queues for different services, as per the predefined priorities. By QoS, the network administrator has the right to stipulate the order of execution of events in which packets are processed to determine the priority of the applications. QoS can improve the type of performance of AODV (Rana and Kumar, 2019) network traffic like bandwidth, latency, loss, jitter, etc. Figure 1 illustrates how QoS regularises the bandwidth for the smooth execution of network traffic.

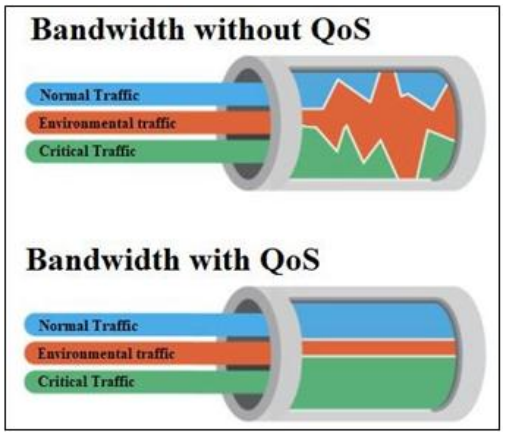


Figure 1: Bandwidth performance without and with QoS.

With the speedy progress in information and communication technologies, the daily life of citizens is becoming easier as most of the things can be controlled with mobile phones and computers connected with the Internet. But a lot of challenges are arising to prevent the personal and financial data from intruders to be attacked. One of the common threats is phishing, which is a kind of social engineering intrusion by designing users' authentication data to spoof the login page of a trusted website (Karlof, 2009). However, the authentication cannot be completed without a one-time password (OTP) or type allocation code (TAC) (Lahmiri, 2017) on the user's registered mobile number. Almost all banks in India are using OTP authentication (4 to 8 digits) and some banks in Malaysia use TAC number which is an 8-digit number for 3GPP GSMA devices by sending it to the customer's mobile to authenticate the user when to complete the transaction. Furthermore, the passwords do not provide nonrepudiation security, and the passwords are supposed to be broken easily with the scripts that are easily available on the web and may be the users choose easily remembered and easily guessed password like their pet and vehicle number, date of birth or mobile number (Mulesh, 2012; Ayoub and Rodriquez, 2011).

Figure 2 shows the major aspects regarding customer satisfaction with the security of the data to avail the services. The satisfaction level of customers includes cloud services in a user-friendly way with flexible cost, security for digital authentication along with confidentiality and integration, maintenance support for genuine quality of service.

Figure 2: Aspects of customer satisfaction with services.

Quality of service is deployed with the Security Gateway to secure the banking system. The integration of QoS with other technologies provides QoS for both the virtual private network

(VPN) and unencrypted network traffic to extend the advantages of a secure, consistent and low-cost VPN. QoS enables to development of basic policies specific to the local area network requirements. QoS optimizes the network performance and records the performance of the system through log files. The integrated authenticated QoS provides QoS for end-users in dynamic IP environments, like remote access. Figure 3 shows the QoS implementation of security servers, QoS policies, and modules, security gateways to connect two networks in a secured way.

QoS-optimal should be used as a way to increase the security of IoT devices as nowadays many IoT devices are in trend for banking like mobile phones, ATMs, kiosks for money deposit, and passbook entry. When some device is connected with the Internet it is obvious to have pretty good security against various threats by intruders. While configuring the network infrastructure for QoS, the express mode permits the definition of the basic policies promptly and enables easy running.

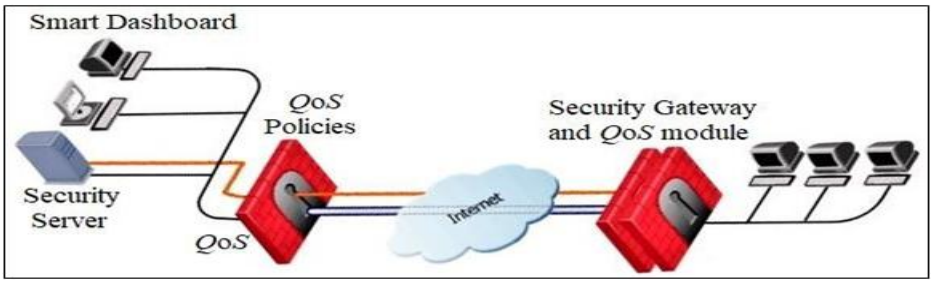


Figure 3: QoS enabled security server.

The traditional way of QoS integrates the advanced features. It can be specified as "traditional" or "express" each time for the installation of a new policy. Many Security Challenges are there with the banking system regarding security. As so many IoT devices are also there in the flexible banking systems like ATMs, mobile apps, passbook entry kiosks, money deposit kiosks, etc. so the security becomes the main concern to deal with intrusions. To operate the IoT devices, the time factor needs to be thoroughly studied. The time response of IoT devices or sensors needs to be fast and consistent for ease of use and for satisfying the users' requirements. Therefore, to meet the requirements the users use lossless and secure data transmission provided by architectures like fog and edge computing.

5. QoS Optimization

QoS is mainly concerned with IoT and primarily it was not created for security purposes, but only for improving the network traffic. Therefore, it is crucial to combine QoS with other

technologies for enhancing complete security. The architecture of IoT for QoS consists of three main layers: application layer, network layer, perception layer as shown in figure 4. All three layers communicate with each other via a router, gateways, sensors, and actuators creating a secured environment for sharing data on the cloud.

The main purpose of QoS solutions is to improve the security performance at all three layers namely the application layer, network layer, and protection layer. But QoS provides its best effect on improving the security at the network layer. Therefore, depending on the intention, there are several ways to optimize the quality of service. For improving the efficiency and reducing the amount of data transmitted to the cloud for processing, analysing, and storage, the concept of fog computing may also be used. But the main drawback of fog computing is that the network at virtual nodes can be attacked by intruders. The techniques such as machine learning (ML), cognitive radio networks (CRNs), and QoS can be used to improve performance.

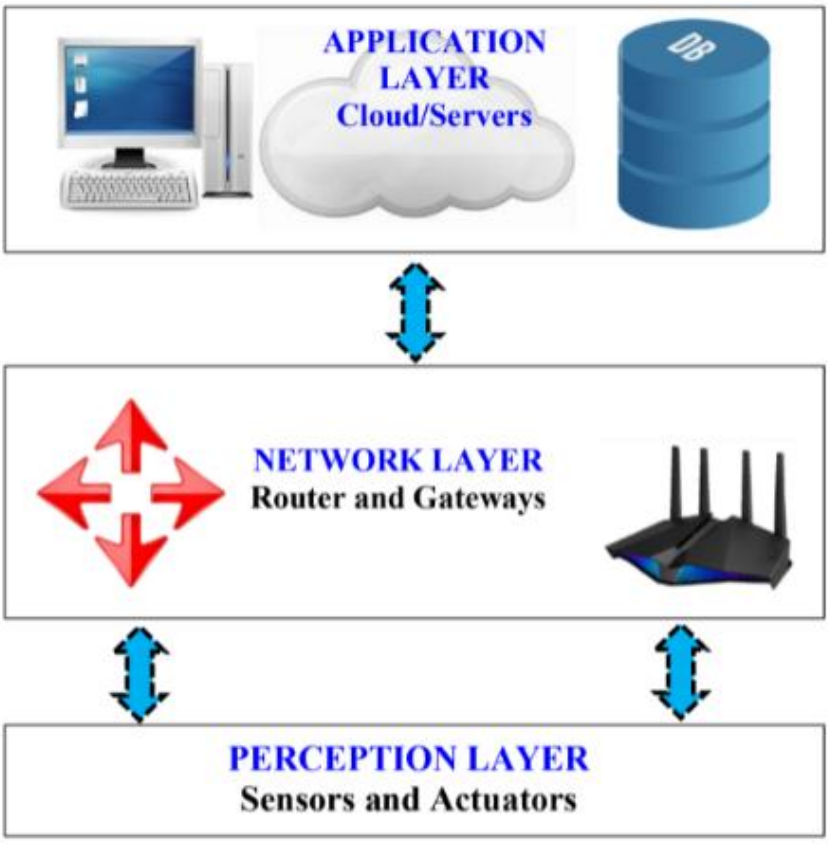


Figure 4: Layers in QoS optimization.

Figure 5 shows the steps applied for QoS optimization. The process is cyclic and continued until the performance of the network meets to desire threshold.

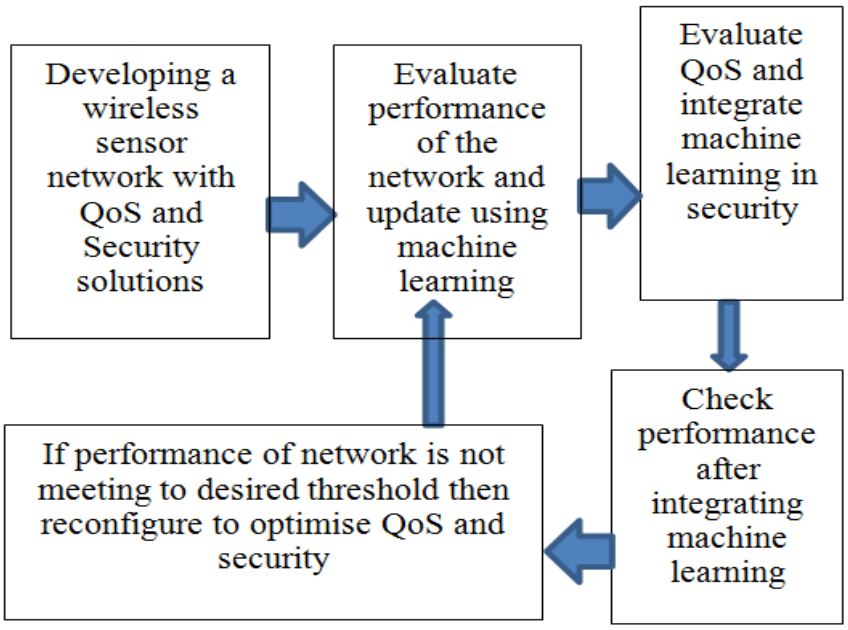


Figure 5: Process for QoS Optimization.

6. Banking security using biometrics

In digital banking and e-commerce, it is a demand to develop and implement a reliable security mechanism (Hutchinson and Warren, 2003). This necessity needs to be designed using effective methods that can work efficiently for user verification and authentication at a remote platform. Biometric technology especially using fingerprint, face recognition, iris recognition,or vein recognition has become trending as a secure way for user authentication. Biometric technology has numerous benefits on both sides i.e., the financial company and the customer (Mills et al., 2010). However, it is yet to be adopted in many developing and underdeveloped countries. Many studies are conducted on biometric technology, and several contributors have examined the impact of biometric technology as a highly reliable solution for many purposes as the biological data is unique for every user, (Mills et al., 2010; Debbarma and Das, 2011; Harris and Yen, 2002). In the nutshell, the majority of banks are using fingerprint and face recognition as biometric security and the use of vein recognition is very limited.

Biometric authentication technology has emerged as a potential solution to authenticate banking users in a user-friendly manner using a graphical user interface. The use of biometric authentication is rapidly growing over the years and now it has enabled smartphones, kiosks, and computers connected with sensors to use fingerprint (Kumar and Sharma, 2009), (Gupta and Kumar, 2010; Kiyani et al., 2020), face recognition (Soundari et al., 2021), vein recognition

(Kumar et al., 2019; Kumar et al., 2020; Kumar et al., 2021; Garcia-Martin and Sanchez-Reillo, 2020), iris recognition (Tyagi et al., 2019), etc. The authentication of a bank customer may be verified by different means like login and password, ATM card with PIN, OTP, and biological identity like a fingerprint, face recognition, iris recognition, vein recognition, etc. All these are nonrepudiation ways of authentication that cannot be denied by the user if done. After entering the log in detail by keypad or sensor, the identity is checked for authentication, and accordingly, the log file is created and the information of login attempt is saved. The login session is time-bound for security reasons. Once the transaction is complete no matter it was successful or unsuccessful the details are updated in the log file so that in case of any discrepancy the log file is referred to resolve the issue. Many ATMs of ICICI, State Bank of India have upgraded for card-less ATM withdrawal. The ATMs use customers' fingerprints for authentication along with OTP. But fingerprint for authentication is not the hygienic method in the Covid-19 pandemic. Kumar et al. (2021) presented a patent model for the touchless (hygienic) method for ATM cash withdrawal using dorsal hand vein recognition.

Figure 6 shows the process of authentication by different means and the use of a firewall to protect the system from intruders. Once the authorized user gets access to the system, the authentication report in the form of a log file is created and stored on the server. A time-bound session is created and once the session is inactive the automatic log-out process from the session is executed.

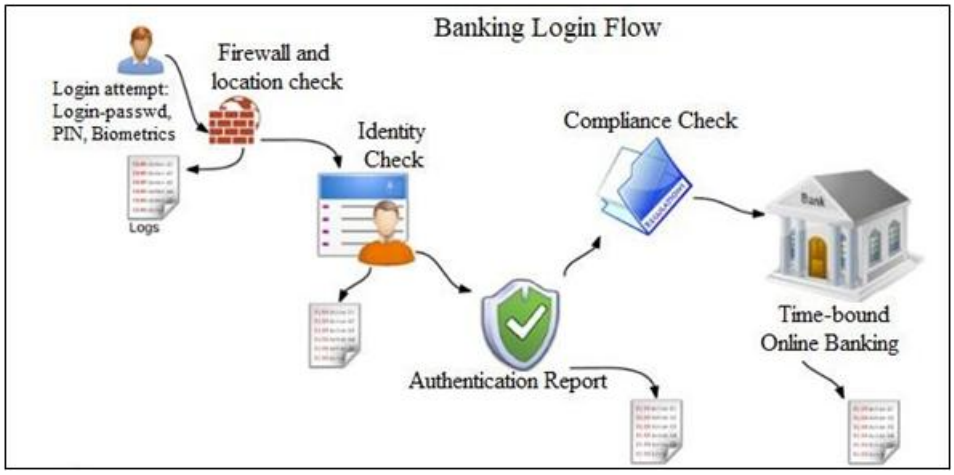


Figure 6: The authentication process for banking services.

7. CONCLUSION

In this paper, the issues related to security and quality of service are discussed and their promising solutions as well. A summary of various algorithms and techniques for banking

security is presented in the literature review section. A description of security issues is also presented along with possible and available solutions. After that, a framework for QoS optimization is discussed, and finally, the use of biometric security in banking is presented. With the security issues in online banking and other transactions, the risk of using cloud security may go at worst. Therefore, it is highly suggested to prefer the most secured cloud service provider like Amazon web services (AWS) with multi-factor authentication. Despite having many ways to penetrate a financial system, the intruders would not be able to trace vulnerabilities to target. Sufficient efforts are to be done and need to understand the modules contributing to an effective user experience insecure environment. The development of further communication processes between networks and applications as common components of a QoS framework is still needed to strengthen at a promising level.

REFERENCES

1. Kumar, R. Human Computer Interaction, Firewall Media, New Delhi, 2011.
2. Aloufi, O F, Djemame, K, Saeed F, Ghaban, F A Survey on Predicting Workloads and Optimizing QoS in the Cloud Computing, International Congress of Advanced Technology and Engineering (ICOTEN), 2021; 1-7.
3. Lata, M, Kumar, R An Approach to Optimize the Cost of Software Quality Assurance Analysis, International Journal of Computer Applications, 2010; 8(8): 1-4.
4. Kumar, R, Sharma, S. Paradigm Shift in Fingerprint Recognition on Pressure Variation and Impact of Information System in Crime Reduction, GJEIS, 2009; 1: 88-93.
5. Kumar, R, Singh, R C, Sahoo, A K SIFT based Dorsal Vein Recognition System for Cashless Treatment through Medical Insurance, International Journal of Innovative Technology and Exploring Engineering, 2019; 8(10S): 444-45.
6. Gupta, J K, Kumar, R An efficient ANN Based approach for Latent Fingerprint Matching, International Journal of Computer Application, 2010; 7(10): 18-21.
7. Kumar, R, Singh, R C, Kant, S Dorsal Hand Vein Recognition Using Very Deep Learning, Macromolecular Symposia, 2021; 397: 2000244 1-13.
8. Kumar, R, Singh, R C, Kant, S. Dorsal Hand Vein-Biometric Recognition using Convolution Neural Network, in Proceedings of Springer International Conference ICICC, 2020.
9. Kumar, R, Singh, R C, Khokher, R Dorsal Hand Vein based Touchless System for ATM Cash Withdrawal, India Patent App. No. 202111017902, 2021.
10. Nami, M E-Banking: Issues and Challenges, in Proceedings of ACIS International

Conference on Software Engineering, Artificial Intelligences, Networking and Parallel/Distributed Computing, 2009; 263-266.

11. Musleh, M M, Ba, I D, Nofal, M A K, Ibrahim, J Improving Information Security in E-Banking by Using Biometric Fingerprint A Case of Major Bank in Malaysia, International Journal of Computer Science and Information Security, 2012; 10(3): 7-12.
12. Manthoulis, G, Doumpos, M, Zopounidis, C, Galariotis, E An Ordinal Classification Framework for Bank Failure Prediction: Methodology and Empirical Evidence for US Banks, European Journal of Operational Research, 2020; 282(2): 786-801.
13. Carmona, P, Climent, F, Momparler, A Predicting Failure in the U.S. Banking Sector: An Extreme Gradient Boosting Approach, International Review of Economics and Finance, 2019; 61: 304-323.
14. Jing, Z, Fang, Y Predicting US Bank Failures: A Comparison of Logit and Data Mining Models, Journal of Forecasting, 2018; 37: 235-256.
15. Keramati, A, Ghaneei, H, Mirmohammadi, S M Developing a Prediction Model for Customer Churn from Electronic Banking Services Using Data Mining, Financial Innovation, 2016; 2(1): 1-13.
16. Lv, F, Huang, J, Wang, W, Wei, Y, Sun, Y, Wang, B A Two-route CNN Model for Bank Account Classification with Heterogeneous Data, PLoS One, 2019; 14(8): 1-22.
17. Marinakos, G, Daskalaki, S Imbalanced customer classification for bank direct marketing, Journal of Marketing Analytics, 2017; 5(1): 14-30.
18. Smeureanu, I, Ruxanda, G, Badea, L M Customer Segmentation in Private Banking Sector Using Machine Learning Techniques, Journal of Business Economics and Management, 2013; 14(5): 923-939.
19. Ogwueleka, F N, Misra, S, Colomo-Palacios, R, Fernandez, I Neural Network and Classification Approach in Identifying Customer Behavior in the Banking Sector: A Case Study of an International Bank, Human Factors and Ergonomics in Manufacturing, 2015; 25(1): 28-42.
20. Ilham, A, Khikmah, L, Indra, A, Ulumuddin, A, Iswara, I Long-term Deposits Prediction: A Comparative Framework of Classification Model for Predict the Success of Bank Telemarketing, in Proceedings of Journal of Physics Conference Series, 2019; 1175(1): 1-6.
21. Farooqi, R, Iqbal, N Performance Evaluation for Competency of Bank Telemarketing Prediction using Data Mining Techniques, International Journal of Recent Technology and Engineering, 2019; 8(2): 5666-5674.

22. Lahmiri, S A two-step system for direct bank telemarketing outcome classification, Intelligent Systems in Accounting, Finance and Management, 2017; 24(1): 49-55.
23. Moro, S, Cortez, P, Rita, P A Data-Driven Approach to Predict the Success of Bank Telemarketing, Decision Support Systems, 2014; 62: 22-31.
24. Krishna, G J, Ravi, V, Reddy, B V, Zaheeruddin, M, Jaiswal, H, Sai Ravi Teja, P Sentiment Classification of Indian Banks' Customer Complaints, in Proceedings of IEEE Region 10 Annual International Conference, 2019; 429-434.
25. Rana, R, Kumar, R Performance Analysis of AODV in Presence of Malicious Node, Acta Electronica Malaysia (AEM), 2019; 3(1): 1-5.
26. Ayoub, R, Rodriquez, C A Best Practices Guide to Fingerprint Biometrics: Ensuring a Successful Biometrics Implementation, White paper, Retrieved from: http://www.frost.com/prod/servlet/cpo/240303611, 2011.
27. Hutchinson, D, Warren, M Security for Internet Banking: A Framework, Logistics Information Management, 2003; 16(1): 64 – 73.
28. Mills, J E, Meyers, M, Byun, S Embracing Broad Scale Applications of Biometric Technologies in Hospitality and Tourism: Is the Business Ready?, Journal of Hospitality and Tourism Technology, 2010; 1(3): 245-256.
29. Debbarma, S, Das, S Designing a Biometric Strategy (Fingerprint) Measure forEnhancing ATM Security in Indian E-Banking System, IJICT, 2011; 1(5): 197- 203.
30. Harris, A J, Yen, D C Biometric Authentication: Assuring Access to Information, Information Journal of Management and Computer Security, 2002; 10(1): 12-19.
31. Kiyani, A T, Lasebae, A, Ali, K, Ur-Rehman, M. Secure Online Banking with Biometrics, in Proceedings of International Conference on Advances in the Emerging Computing Technologies (AECT), 2020; 1-6.
32. Soundari, D V, Aravindh, R, Edwin, R K, Abishek, S Enhanced Security Featureof ATM's Through Facial Recognition, in Proceedings of 5th International Conferenceon Intelligent Computing and Control Systems (ICICCS), 2021; 1252-1256.
33. Garcia-Martin, R, Sanchez-Reillo, RVein Biometric Recognition on a Smartphone, IEEE Access, 2020; 8: 104801-104813.
34. Tyagi, A, Simon, I R, Khatri, S K Security Enhancement through IRIS and Biometric Recognition in ATM, in Proceedings of 4th International Conference on Information Systems and Computer Networks (ISCON), 2019; 51-54.