

Cyber-fraud detection methodology by using machine learning algorithms

Ahmed Abu-Khadrah¹, Sahar Al-Washmi², Ali Mohd Ali¹, Muath Jarrah³

¹Department of Electrical Engineering, College of Engineering Technology, Al-Balqa Applied University, Amman, Jordan

²College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia

³School of Computing, Skyline University College, Sharjah, United Arab Emirates

Article Info

Article history:

Received Oct 16, 2024

Revised Mar 26, 2025

Accepted May 23, 2025

Keywords:

Cyber fraud

Cybercrime

Logistic regression

Naïve Bayes

Random forest

ABSTRACT

Cybercrime covers a wide array of illegal online activities such as hacking and identity theft, while cyber fraud specifically involves deceptive practices like phishing and fraudulent financial transactions. The rise in technology and digital communication has exacerbated cyber fraud. Although prevention technologies are advancing, fraudsters continually adapt, making effective detection methods essential for identifying and addressing fraud when prevention fails. The proposed model aims to reduce online fraud through new detection algorithms. It utilizes statistical and machine learning techniques, including logistic regression, random forest, and naïve Bayes, to identify non-transactional fraud behaviors. By analyzing a meticulously collected and fine-tuned dataset, the study enhances detection capabilities beyond traditional transaction-focused approaches. The algorithms monitor user interactions and device characteristics to create profiles of normal behaviors and detect deviations indicative of fraud. The evaluation of proposed model showed 100% accuracy. A unified model incorporating all decision-making processes was used, leading to a voting phase and accuracy assessment. This approach consolidates multiple algorithms into a single framework, proving highly effective for comprehensive fraud detection. The research demonstrates the value of integrating machine learning techniques with real-world data to advance fraud detection and emphasizes the importance of continual adaptation to address evolving cyber threats.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Ahmed Abu-Khadrah

Department of Electrical Engineering, College of Engineering Technology, Al-Balqa Applied University
Amman, Jordan

Email: a.abukhadrah@bau.edu.jo

1. INTRODUCTION

Cyber-fraud research began in the 1990s. Early studies explored cyber-crime investigations and offered guides that addressed key concepts such as data privacy and computer security [1]. The rapid evolution of computer networks, with technologies like the cloud and the internet of things (IoT), has increased cyber security threats. It is essential for nations to adopt proactive defense measures, advanced technology, and guidance to protect their information and communication systems. The Kingdom, in particular, must ensure the confidentiality, integrity, and availability of its critical assets and infrastructure, aligning with its Vision 2030 by enhancing information sharing and establishing clear legal frameworks for data security and privacy [2]. In today's world, technology permeates every aspect of our lives, from banking and shopping to communication. However, this convenience comes with increased risks of fraud and identity theft. Learning to avoid becoming a victim of such crimes is crucial. While criminological discussions over

the past 25 years have focused on the reduction of property crime, fraud has often been excluded from this analysis despite being a significant issue [3]. The rise of virtual currencies like Bitcoin, Ethereum, Ripple, and Litecoin has attracted malicious actors who use ransomware to obtain virtual currency. This ransomware infiltrates victims' systems, encrypting their files through sophisticated methods. This paper aims to analyze banking customer data from the financial sector to detect and prevent the rise in online fraud crimes [4]. With the expansion of electronic payments, credit card transactions have surged, leading to increased account theft and bank losses. As a result, improved fraud detection methods have become essential. Recent advancements in information technology and machine learning have driven researchers to apply these techniques to the financial sector to combat cyber fraud, which involves illegal activities conducted via the internet, electronic communication, or digital means [5]. Machine learning (ML) significantly enhances information management through smart algorithms, data-driven decision-making, and improved data analysis. The application of ML will improve historical based outcome predictions by lowering error rates. Over the last decade there has been a great deal of investigation in this area due to the effectiveness of ML techniques in dealing with online fraud problems [6]–[10]. ML is favored for its rapid computation capabilities, allowing quick data analysis and pattern recognition. Compared to ML techniques, rule-based fraud prevention systems that use logic-based approach are not as efficient. Since fraudulent transactions are rare, the balance class when labeled becomes a crucial consideration. The Ali *et al.* model [11] attempts to mitigate fraud out of data by employing supervised learning algorithm to detect fraudulent behavior based on past instances of fraud and unsupervised learning to discover new types of fraud. Classifiers including logistic regression, which flags transaction as either 'fraud' or 'non-fraud', are implemented using Python [11]–[15].

The study data analysis by Todorović *et al.* [16] concluded that perceived cyber fraud does not significantly influence e-commerce usage behavior. However, perceived ease of use positively affects e-commerce adoption, highlighting the importance of user-friendly systems. Risk perception also influences e-commerce behavior, indicating that awareness of transaction risks increases the desire to use e-commerce systems. Todorović *et al.* model, using the technology acceptance model (TAM), provides insights for designing effective online transaction systems, emphasizing fraud perception, risk levels, and transaction ease to enhance e-commerce in Indonesia.

Koibichuk *et al.* [17] explores the risk typology for peer-to-peer lending in a digitally transformed financial landscape. Key features include access infrastructure, transaction infrastructure, fulfillment infrastructure, human condition indicators, device and broadband uptake, digital inclusion, digital payment uptake, institutional efficiency, trust indicators, and the digital ecosystem. Understanding these factors is essential for local banks to navigate digitalization and regulatory environments. The innovation and change factor assesses the state of key innovation ecosystem inputs and outputs, crucial for advancing digital products and services [18]. Corporate governance is a critical element in preventing and detecting fraud. Effective internal control systems, accountability, and transparency are vital. Research shows that governance policies, board characteristics, and ownership concentration reduce accounting fraud and enhance financial information reliability [19]–[21]. Auditors play a significant role in detecting fraud, and their duties should be expanded to include understanding white-collar crime patterns and improving audit standards. The study in [22] emphasizes the importance of understanding self-protective and crime prevention behaviors to develop effective cyber fraud prevention programs. The research advocates for a victim-centric policing approach and cyber fraud crime prevention education to achieve positive outcomes.

The problem of credit card fraud in online environments has received considerable attention, but other significant issues like intellectual property theft, pagejacking, fake money orders, and wire-transfer fraud need more focus. The best fraud detection results are achieved by supervised learning techniques like support vector machines, artificial neural networks, and decision trees. Future research should aim to improve algorithms to cover other types of online fraud with high accuracy and low costs, focusing on hybridizing the most effective machine learning techniques [23], [24]. Qualitative research involving structured questionnaires completed by bank staff can promote cyber fraud reduction, enhance management control systems, and improve customer and shareholder satisfaction [25]. Reviews of various machine learning algorithms for detecting credit card fraud show that supervised learning techniques, such as Random Forest, effectively classify transactions as fraudulent or authorized based on accuracy, precision, and specificity metrics [26]. The internet's ability to reach vast audiences makes it easy for fraudsters to spread credible-looking messages, making it hard to differentiate between fact and fiction. Despite numerous studies on fraud patterns, a systematic solution to understand and detect abnormal customer behaviors remains elusive. Most previous work has focused on fraud detection rather than prevention. Improved approaches based on ensemble classifiers are necessary to swiftly and reliably detect and prevent digital fraud. Combining historical data sets enhances prevention accuracy and aids decision-makers in distinguishing between fraud, suspicious, and genuine activities.

In this paper, a new algorithm is proposed to detect non-transactional fraud behaviors, enhancing fraud prevention strategies. Using real data from the financial sector, the study validates the results and evaluates the effectiveness of logistic regression, random forest, and naïve Bayes based on detection accuracy. The research highlights the importance of incremental improvements and persistence in cybersecurity advancements.

2. METHOD

Fraud protection is a high-load system designed to detect, prevent, and combat fraud across all digital channels (web and mobile applications) in real time. This solution defends against online fraud and social engineering attacks, representing the next generation of engineers and cybersecurity professionals who introduce bold and innovative ideas to identify cyberattacks before they begin. These solutions are based on exhaustive threat-hunting operations and monitoring the tactics, tools, and infrastructure used by attackers.

A typical organization loses an estimated 5% of its yearly revenue to fraud. This course teaches how to fight fraud using data, applying supervised learning algorithms to detect fraudulent behavior based on past fraud and using unsupervised learning methods to discover new types of fraudulent activities. Given that fraudulent transactions are rare compared to normal ones, it is essential to learn how to properly classify imbalanced datasets. Python is the programming language used to implement classifiers.

This section will discuss algorithms for detection and prevention of fraud using machine learning, which includes logistic regression, a supervised learning method for making categorical decisions such as classifying transactions as either 'fraud' or 'non-fraud'. Also used is the random forest, which improves results by checking several different conditions using a combination of decision trees. Other algorithms that will be discussed include naïve Bayes, a supervised machine learning algorithm used for classification problems, most notably for text categorization. He is a member of a class of algorithms known as generative learning algorithms that model a given class or category by capturing the input distribution. The steps of the proposal algorithm are demonstrated in Figure 1.

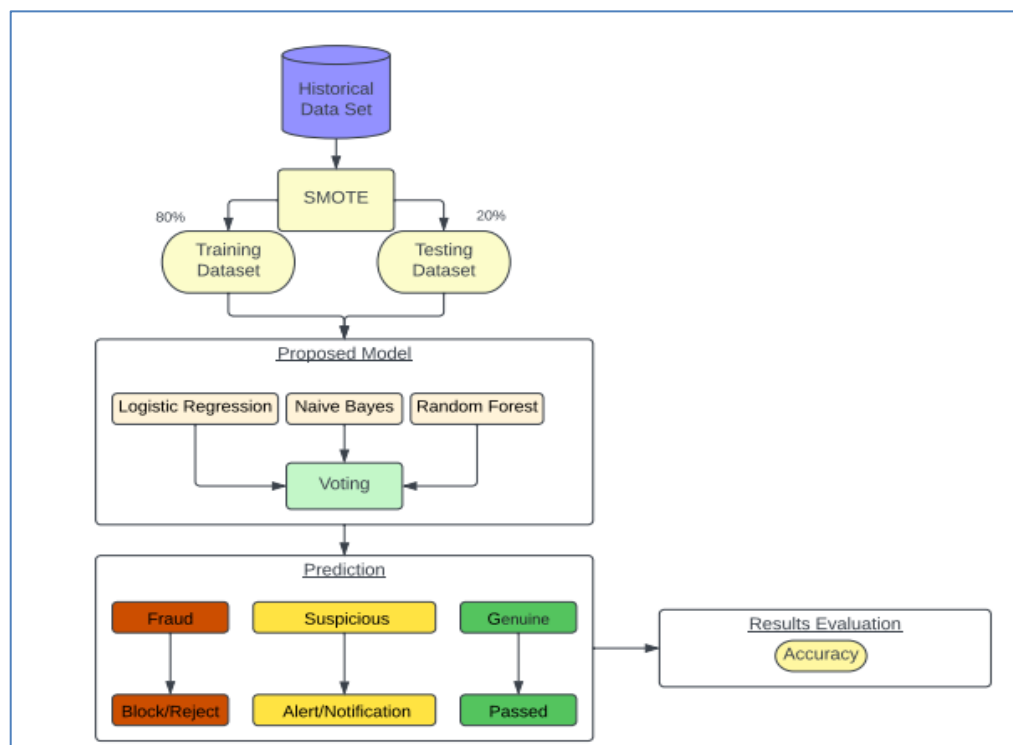


Figure 1. Overall methodology

To detect fraudulent behavior, supervised learning algorithms are applied based on past fraud, while unsupervised learning methods discover new fraud activities. Since fraudulent transactions are rare, it's crucial to properly classify imbalanced datasets. Python is used to implement the classifiers.

Logistic regression, a supervised learning technique, categorizes transactions as 'fraud,' 'suspicious,' or 'genuine.' Random forest improves results by combining decision trees, each checking different conditions. naïve Bayes further enhances fraud detection accuracy. The methodology trains random datasets, with each tree assigning probabilities to behaviors as 'fraud,' 'suspicious,' or 'genuine,' and the model predicts outcomes accordingly. Training data, a subset of original data, trains the model, while testing data checks its accuracy.

Using a real dataset from the financial sector, the system centralizes account lifecycle events for continuous monitoring and protection. This dataset trains the machine learning algorithm to make predictions while complying with data protection regulations. The fraud detection system design consists of three main steps:

- Defining training and test sets: the training set includes historical data for model training, while the test set assesses model accuracy.
- Training the prediction model: the training set is used to develop a model that predicts whether customer behavior is genuine or fraudulent. Python's sklearn library facilitates this task.
- Assessing model performance: the test set, consisting of new data, evaluates the model's performance. In a fraud detection context, test set transactions occur after those used for training.

This approach ensures reliable outcomes by utilizing real financial data while respecting data protection regulations. Figure 1 and Table 1 highlight the detailed steps and features used in proposed model.

Table 1. Measures used for machine learning

Features	Description
Identity	Unified Customer ID, that uniquely assigned to each customer
Channel	The channel used by Customer for each session Mobile/Desktop
Login Timestamp	DD-MM-YA - HH:MM:SS
Logout Timestamp	DD-MM-YA - HH:MM:SS
Device ID	Unique device number \Application ID
VPN	VPN usage detection
Login IP	Login from a blacklisted country or Activity from black-listed IP
Geolocation	User geolocation latitude & longitude such as country and city
Biometric Behaviors	Range of customers Biometric Behaviors, such as the speed of typing or the figure print pressure
Concurrent Session	To indicate in case the session is active in parallel from a different channel
Event Title	Exact event captured for different users within each login session
Event Id	Unique identifier for each event title which capture those event and transmitted to event score
Event Score	To indicate the status of each session Either Genuine, Suspicious or Fraud based on the event title
Risk Level	To indicate status of each session Either Low, Medium or High based on the event score

3. RESULTS AND DISCUSSION

In this section, the proposed algorithm, which includes logistic regression, random forest, and naïve Bayes classification, is implemented. The dataset is divided into training and testing sets after balancing the data using SMOTE. During testing, the data and desired behavior are applied to produce the machine's logic. This process is repeated to ensure the learned logic remains consistent, confirming that the system understands the logic and develops a model according to the desired behavior. Figures 2, 3, and 4 show the confusion matrices for logistic regression, random forest, and naïve Bayes, respectively.

Voting ensembles are ensemble techniques that train multiple machine learning models, then combine predictions from all the individual models for output. The voting classifier is an ensemble learning method that merges several base models to produce the final optimum solution. Figure 5 shows the results after applying the voting method.

Based on the collected and fine-tuned dataset, three different machine learning models were used and evaluated using the accuracy metric. The accuracy mechanism was chosen due to the high accuracy of data output for all three machine learning models. Given that the dataset is a multi-classification problem, accuracy and confusion matrix were appropriate evaluation tools. Instead of creating separate dedicated models, a single model was created that includes all the decisioning and predicts output to the voting phase, followed by the accuracy evaluation approach. The accuracy correlation has values between -1 and 1, with 0 implying no correlation, indicating no linear relationship between the two variables. A value closer to 1 implies a strong positive correlation, while a value closer to -1 implies a strong negative correlation.

The dataset that used in proposed model consists of current banking data, extracted specifically for this purpose, and includes only the most suitable features. This approach reduces the complexity of the model while maintaining accuracy. Below are the details of the model results using each decision model. Accuracy, which is one metric for evaluating classification models, is the fraction of predictions the model got right.

The formula used is:

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (1)$$

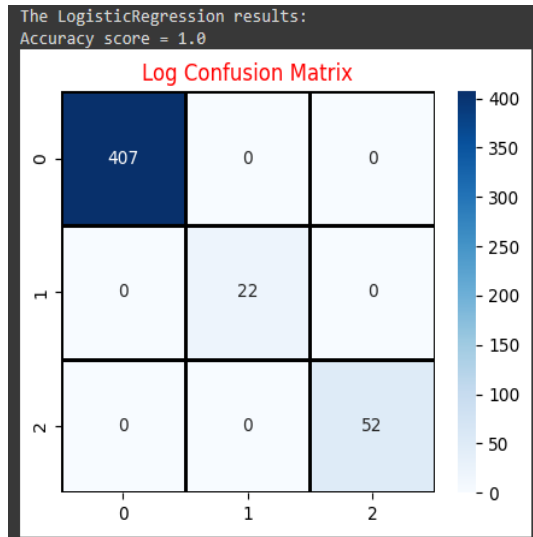


Figure 2. Logistic regression testing results

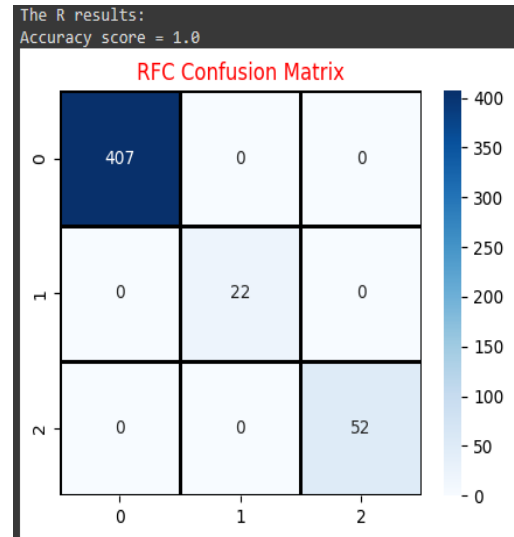


Figure 3. Random forest testing results

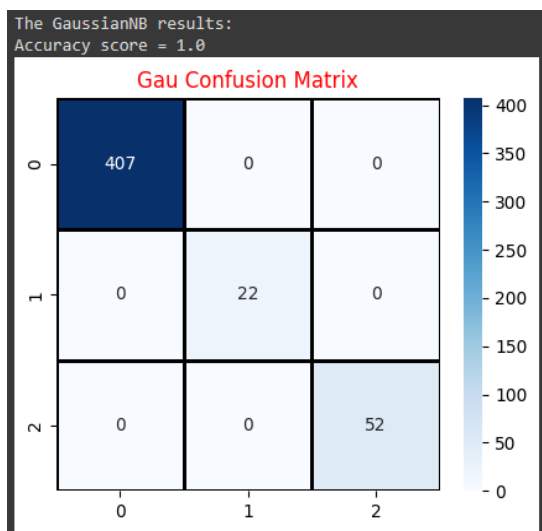


Figure 4. Naïve-Bayes testing results

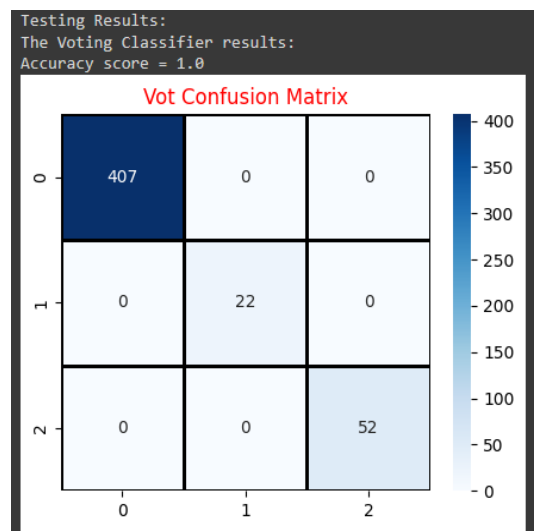


Figure 5. Voting classifier results for the tested data

Since all results reached 100% accuracy, indicating highly accurate alerts, the recommended approach is to integrate these results into the monitoring system to suspend sessions based on high-risk events captured. From the findings, one banking user was associated with 18 suspicious mobile application alerts, and VPN usage should be declined, with all sessions terminated accordingly.

As shown in Figure 6, low-risk events constitute only 6% compared to 84% of high-risk events. This significant number of high-risk events is due to the absence of current prevention mechanisms to eliminate such activities by banking customers. Therefore, the proposed solution should include clear guidelines to prevent digital fraud by implementing the necessary controls.

When applying this fraud prevention approach and integrating it with a robust solution, it is essential for transactional banks and the financial sector to design strategies that uphold systemic integrity. This approach aims to mitigate risks, reduce wasted time and effort, and prevent substantial financial losses.

Conversely, focusing cybersecurity efforts solely on protecting account-based information without monitoring user activities leaves firms vulnerable to various forms of attack. This model has been designed to identify non-transactional fraud, which can help enhance the ongoing conversation in the field. To make a substantive change, it is often necessary to improve systems gradually and to be persistent, as effective approaches depend on gradual movement towards the ambitious goals set.

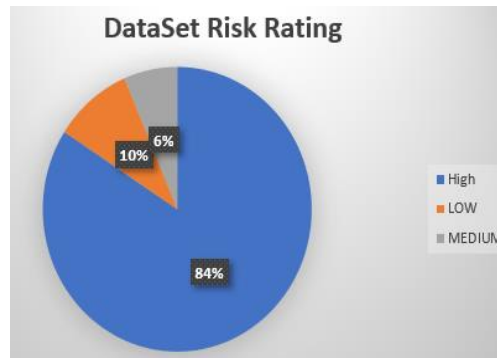


Figure 6. Ration of the high risk events within the Dataset used

4. CONCLUSION

Cybercrime and cyber fraud are two challenges that need to be separately addressed. Cybercrime includes all illegal acts committed using a computer or the internet, while cyber fraud refers to misleading activities that are performed digitally. In particular, as technology develops and more transactions are conducted electronically, cyber fraud has emerged as one of the most important issues, resulting in enormous financial losses and damage to the reputation of many sectors. This model exemplifies the need for well-planned fraud detection methods because traditional approaches are usually not sufficient due to the cleverness of the fraudsters. This model facilitates detecting non-transactional fraud risks utilizing algorithms of Logistic Regression, Random Forest, and Naïve Bayes. Using a complete set of data in one model, which reached 100 percent accuracy in all assessed algorithms, evidences the possibility of employing machine learning with actual data for effective fraud detection. Model 1 and the annexed set of rules prove that one consolidated model with the user's behavioral and device information can solve the difficulty of non-transactional fraud. This technique does not only enhance detection, but also strengthens the need for cooperation between people, business entities, and governments to protect the digital world. With the growing cyber fraud, improving detection techniques will be fundamental in reducing the effects and protecting against possible threats.

ACKNOWLEDGEMENTS

Thanks to the Al-Balqa Applied University and Saudi Electronic University for sponsoring this work.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Ahmed Abu-Khadrah	✓	✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	
Sahar Al-Washmi	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓
Ali Mohd Ali	✓		✓	✓			✓	✓		✓	✓			✓
Muath Jarrah			✓	✓	✓		✓		✓	✓				✓

C : Conceptualization
M : Methodology
So : Software
Va : Validation
Fo : Formal analysis

I : Investigation
R : Resources
D : Data Curation
O : Writing - Original Draft
E : Writing - Review & Editing

Vi : Visualization
Su : Supervision
P : Project administration
Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Derived data supporting the findings of this study are available from the corresponding author AA on request.




REFERENCES

- [1] A. Bequai, "Balancing legal concerns over crime and security in cyberspace," *Computers & Security*, vol. 17, no. 4, pp. 293–298, 1998, doi: 10.1016/s0167-4048(98)80008-4.
- [2] J. Shires, "Career connections: transnational expert networks and multilateral cybercrime negotiations," *Contemporary Security Policy*, vol. 45, no. 1, pp. 45–71, 2023, doi: 10.1080/13523260.2023.2274775.
- [3] M. S. Yousefpoor, E. Yousefpoor, H. Barati, A. Barati, A. Movaghar, and M. Hosseinzadeh, "Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review," *Journal of Network and Computer Applications*, vol. 190, p. 103118, 2021, doi: 10.1016/j.jnca.2021.103118.
- [4] N. Quadar, A. Chehri, B. Debaque, I. Ahmed, and G. Jeon, "Intrusion detection systems in automotive Ethernet networks: Challenges, opportunities and future research trends," *IEEE Internet of Things Magazine*, vol. 7, no. 2, pp. 62–68, 2024, doi: 10.1109/iotm.001.2300109.
- [5] M. Nasr, M. Farrag, and M. Nasr, "E-payment systems risks, opportunities, and challenges for improved results in e-business," *International Journal of Intelligent Computing and Information Sciences*, vol. 20, no. 1, pp. 1–20, 2020, doi: 10.21608/ijicis.2020.31514.1018.
- [6] J. C. P. Cheng, W. Chen, K. Chen, and Q. Wang, "Data-driven predictive maintenance planning framework for MEP components based on BIM and IoT using machine learning algorithms," *Automation in Construction*, vol. 112, p. 103087, 2020, doi: 10.1016/j.autcon.2020.103087.
- [7] K. A. Kareem and W. H. Ali, "Implementation of washing machine system via utilization of fuzzy logic algorithms," in *2021 4th International Symposium on Agents, Multi-Agent Systems and Robotics (ISAMSR)*, 2021, pp. 45–50. doi: 10.1109/isamsr53229.2021.9567796.
- [8] Y. Zhou, Y. Liu, D. Wang, X. Liu, and Y. Wang, "A review on global solar radiation prediction with machine learning models in a comprehensive perspective," *Energy Conversion and Management*, vol. 235, p. 113960, 2021, doi: 10.1016/j.enconman.2021.113960.
- [9] K. Arumugam, M. Naved, P. P. Shinde, O. Leiva-Chauca, A. Huaman-Osorio, and T. Gonzales-Yanac, "Multiple disease prediction using Machine learning algorithms," *Materials Today: Proceedings*, vol. 80, pp. 3682–3685, 2023, doi: 10.1016/j.matpr.2021.07.361.
- [10] L. Yang and A. Shami, "On hyperparameter optimization of machine learning algorithms: Theory and practice," *Neurocomputing*, vol. 415, pp. 295–316, 2020, doi: 10.1016/j.neucom.2020.07.061.
- [11] M. M. Ali, B. K. Paul, K. Ahmed, F. M. Bui, J. M. W. Quinn, and M. A. Moni, "Heart disease prediction using supervised machine learning algorithms: Performance analysis and comparison," *Computers in Biology and Medicine*, vol. 136, p. 104672, 2021, doi: 10.1016/j.combiomed.2021.104672.
- [12] M. Alshurideh, B. Al Kurdi, S. A. Salloum, I. Arpacı, and M. Al-Emran, "Predicting the actual use of m-learning systems: a comparative approach using PLS-SEM and machine learning algorithms," *Interactive Learning Environments*, vol. 31, no. 3, pp. 1214–1228, 2020, doi: 10.1080/10494820.2020.1826982.
- [13] J. Senanayake, H. Kalutarage, and M. O. Al-Kadri, "Android mobile malware detection using machine learning: A systematic review," *Electronics*, vol. 10, no. 13, p. 1606, 2021, doi: 10.3390/electronics10131606.
- [14] U. A. Bhatti, H. Tang, G. Wu, S. Marjan, and A. Hussain, "Deep learning with graph convolutional networks: An overview and latest applications in computational intelligence," *International Journal of Intelligent Systems*, vol. 2023, pp. 1–25, 2023, doi: 10.1155/2023/8342104.
- [15] R. Murugan and T. Goel, "E-DiCoNet: Extreme learning machine based classifier for diagnosis of COVID-19 using deep convolutional network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 9, pp. 8887–8898, 2021, doi: 10.1007/s12652-020-02688-3.
- [16] Z. Todorović, D. Tomaš, and B. Todorović, "Anti-fraud strategy," *ECONOMICS*, vol. 8, no. 2, pp. 69–78, 2020, doi: 10.2478/eoik-2020-0010.
- [17] V. Koibichuk, N. Ostrovska, F. Kashiyeva, and A. Kwilinski, "Innovation technology and cyber frauds risks of neobanks: gravity model analysis," *Marketing and Management of Innovations*, no. 1, pp. 253–265, 2021, doi: 10.21272/mmi.2021.1-19.
- [18] S. L. Burton, "Cybersecurity leaders: Knowledge driving human capital development," *Scientific Bulletin*, vol. 26, no. 2, pp. 109–120, 2021, doi: 10.2478/bsaft-2021-0013.
- [19] M. Rashid, A. Al-Mamun, H. Roudaki, and Q. R. Yasser, "An overview of corporate fraud and its prevention approach," *Australasian Business, Accounting and Finance Journal*, vol. 16, no. 1, pp. 101–118, 2022, doi: 10.14453/aabfj.v16i1.7.
- [20] J. M. Drew and L. Farrell, "Online victimization risk and self-protective strategies: developing police-led cyber fraud prevention programs," *Police Practice and Research*, vol. 19, no. 6, pp. 537–549, 2018, doi: 10.1080/15614263.2018.1507890.
- [21] M. Josiah and A. Samson, "Evaluation of roles of auditors in the fraud detection and investigation in Nigerian industries," *American Journal of Social and Management Sciences*, vol. 3, no. 2, pp. 49–59, 2012, doi: 10.5251/ajsms.2012.3.2.49.59.




- [22] E.-A. Minastireanu and G. Mesnita, "An analysis of the most used machine learning algorithms for online fraud detection," *Informatica Economica*, vol. 23, no. 1/2019, pp. 5–16, 2019, doi: 10.12948/issn14531305/23.1.2019.01.
- [23] R. Octora *et al.*, "The urgency of the Indonesian non-penal policy in regulating misuse of bank accounts as a means of online frauds," *Croatian International Relations Review*, vol. 28, no. 90, pp. 135–153, 2022.
- [24] S. A. Ansar, "A critical analysis of fraud cases on the Internet," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 12, pp. 2164–2186, 2021.
- [25] O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "The use of the balanced scorecard as a strategic management tool to mitigate cyberfraud in the South African banking industry," *Heliyon*, vol. 8, no. 12, p. e12054, 2022, doi: 10.1016/j.heliyon.2022.e12054.
- [26] N. Boutaher, A. Elomri, N. Abghour, K. Moussaid, and M. Rida, "A review of credit card fraud detection using machine learning techniques," in *2020 5th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech)*, 2020. doi: 10.1109/cloudtech49835.2020.9365916.

BIOGRAPHIES OF AUTHORS






Ahmed Abu-Khadrah    was born in United Arab Emirates in 1981. He received a Bachelor of Engineering in Computer Engineering from Alblqa Applied University in 2003. He received the master's degree in electronic engineering (Computer Engineering) from Universiti Teknikal Malaysia Melaka (UTeM) in 2013. He received a PhD in computer engineering and communications from Universiti Teknikal Malaysia Melaka (UTeM) in 2017. He is currently Faculty member at the Department of Electrical Engineering, College of Engineering Technology, Al-Balqa Applied University, Amman. His research interests in wireless network protocols, networking, communications, wireless mathematical model, also multimedia service over the networks. He can be contacted at email: a.abukhadrah@bau.edu.jo.






Sahar Al-Washmi    received the master's degree from the College of Information Computing, majoring in Cyber Security from Saudi Electronic University. Her research interests in cyber security, machine learning, and malicious URL detection. she can be contacted at email: Sahar.Alwashmi@gmail.com.



Ali Mohd Ali    was born in 1982 in Jordan. Mutah University awarded him a Bachelor of Engineering in computer engineering in 2005. In 2013, he received a master's degree in computer and communication engineering from Universiti Kebangsaan Malaysia (UKM). In 2021, he received a Ph.D. in Computer and Communications Engineering from the University of Huddersfield in the United Kingdom. He is currently faculty member at Department of Electrical Engineering, College of Engineering Technology, Al-Balqa Applied University, Amman. His primary research interests are in the analysis of communication system reliability using complex modelling techniques, as well as approaches to WLAN optimization. He can be contacted at email: ali.mohamad@bau.edu.jo.



Muath Jarrah    received his master and Ph.D. degrees in computer science from the Technical University of Malaysia, Melaka, in 2014 and 2018, respectively. He specializes in artificial intelligence and software engineering. His research interests include industrial computing, artificial intelligence, data science, machine learning, and modeling and optimization algorithms. Muath has been working at different universities at different countries. He can be contacted at email: aljarrahmuath@gmail.com.