IRJAEH

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

Anti-Counterfeit Product Tracking System

Sivaranjani M[1], Dineshkumar S[2], Hariraman P[3], Guna S[4]
[1]Assistant Professor, Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, India.
[2,3,4]Department of Computer Science and Engineering, Paavai Engineering College, Namakkal, India.
Email ID: *ranjanimecse@gmail.com[1], dineshkumars1804@gmail.com[2], hariraman1011@gmail.com[3], gunashanmugam96@gmail.com[4]*

Abstract
The rapid growth of e-commerce platforms has led to a rise in counterfeit products and fake websites. This has caused financial losses and decreased consumer trust. Manually spotting such fraud is difficult because of the high number of online transactions and the increasingly clever tactics used by counterfeiters. This work introduces an Anti-Counterfeit Product Tracking System that combines Artificial Intelligence and Blockchain technology to offer a dependable way to detect fraud and verify products. The system carries out dual verification by examining both website features and product-related details like pricing patterns. It evaluates suspicious signs, such as insecure protocols, unusual domain structures, and unrealistic product prices, using smart rules to produce a risk score between 0 and 100. Based on this score, the system labels inputs as Authentic, Suspicious, or Counterfeit, which helps in making clear decisions. To maintain security and transparency, all verification results are recorded using blockchain technology, which creates a secure and decentralized record. This method improves detection accuracy, allows for real-time verification, and lessens reliance on centralized systems, thereby boosting trust and security in online transactions.
Keywords: *Anti-Counterfeit Detection, Fraudulent Website Detection, Artificial Intelligence, Blockchain Technology, Risk Score Analysis, Product Authentication, E-Commerce Security, Machine Learning.*

1. Introduction
The rapid growth of e-commerce platforms has changed how people buy goods. It offers convenience, accessibility, and a wide range of products from around the world. As more consumers turn to online shopping, they can compare prices, explore various brands, and make purchases from their homes. However, this quick shift to digital has also led to a rise in counterfeit products and fake websites. This creates serious issues for both consumers and businesses. Counterfeit goods lead to financial losses for customers and also hurt product quality, safety, and brand reputation. One major issue in online marketplaces is the challenge of verifying product authenticity and seller credibility. Many fake websites imitate real platforms, making it difficult for users to tell the difference between real and bogus sources. Counterfeit products are often sold at suspiciously low prices, which lures consumers but results in subpar or fake items. These problems lower consumer trust in online transactions and harm the overall growth of e-commerce. Manufacturers and brands also face significant losses due to intellectual property theft and the spread of fake products in the market. Traditional ways of authenticating products, like barcodes, QR codes, RFID tags, and holograms, have been used to tackle counterfeiting. While these methods offer basic tracking and identification, they have several drawbacks. Barcodes and QR codes can be easily copied, and holograms can be faked with advanced printing. RFID systems are effective but can be costly to implement and need specialized hardware. Additionally, many current verification systems depend on centralized databases, which are at risk of hacking, data manipulation, and failures. Another key issue is that these methods mainly verify products and do not evaluate the trustworthiness of the websites selling them. Recent progress in Artificial Intelligence (AI) and blockchain

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

technology provides new ways to address these problems. AI helps analyze data by examining website URLs, domain features, pricing patterns, and product information to spot suspicious behavior. Machine learning can uncover hidden patterns and anomalies that suggest fraud, improving detection accuracy and efficiency. Conversely, blockchain technology offers a decentralized and tamper-proof way to store verification records. By ensuring transparency, consistency, and data integrity, blockchain reduces risks linked to centralized systems and builds trust among users. A combined approach that merges AI analysis and blockchain storage can greatly enhance counterfeit detection and prevention. Such systems can conduct dual verification by assessing both website authenticity and product-related factors, producing a risk score that classifies outcomes as authentic, suspicious, or counterfeit. This method not only boosts detection accuracy but also gives users reliable, real-time verification results. By overcoming the limitations of traditional methods and using modern technologies, we can create a more secure, scalable, and trustworthy online transaction environment. An integrated approach that combines AI-based analysis with blockchain-based storage can significantly improve counterfeit detection and prevention. Such systems can perform dual verification by evaluating both website authenticity and product-related factors, generating a risk score that helps classify outcomes into meaningful categories such as authentic, suspicious, or counterfeit. This approach not only increases detection accuracy but also provides users with reliable and real-time verification results. By addressing the limitations of traditional methods and leveraging modern technologies, a more secure, scalable, and trustworthy environment for online transactions can be established.

2. Related Work

In recent years, a lot of research has been done on how to find fake products and make sure that products are safe. Different methods have been suggested, using both old and new technologies. In the beginning, most solutions used physical and visual verification methods like barcodes, QR codes, holograms, and serial numbers. These methods offered a fundamental degree of identification and traceability, enabling consumers to authenticate products via scanning or manual examination. But these kinds of methods are very easy to copy and change, so they aren't good for stopping complicated counterfeiting. Radio Frequency Identification (RFID)-based systems were put in place to make it easier to track and automate products. RFID tags make it possible to track products in real time throughout the supply chain and make authentication easier by cutting down on manual work. These systems are more accurate than barcode-based methods, but they are expensive to set up and need special infrastructure. RFID systems also often use centralized databases, which can be at risk of security holes like data breaches and unauthorized changes. As digital technologies have improved, blockchain-based solutions have become very popular for making sure that products are safe and easy to verify. Blockchain is a decentralized and tamper-proof ledger that can safely store information about products and transactions. A number of studies have looked into how blockchain can be used in supply chain management to make it easier to track things and stop data from being changed. Blockchain improves data integrity and transparency, but many current implementations have problems with scalability, transaction speed, and working with real-time verification systems. AI and machine learning have also been used to find fake products and activities that are not real. AI models can look at patterns in website URLs, product descriptions, pricing behavior, and user reviews to find suspicious behavior. Some methods use classification algorithms to tell the difference between real and fake websites, while others use deep learning models like Convolutional Neural Networks (CNNs) to check the authenticity of products based on images. These methods make things more accurate and automatic, but they usually only look at one thing at a time, like product verification or website analysis, instead of both. Recent research endeavors have sought to amalgamate various technologies to construct more resilient systems. Some people have suggested using both AI and blockchain together to take advantage of the best features of each. AI can be used for smart

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

detection, and blockchain can be used for safe data storage. A lot of current systems still don't have a single framework that can do dual verification of both products and websites while still being fast and able to grow. Overall, the current literature shows that there have been big strides made in techniques for detecting and authenticating counterfeit goods. However, there is still a need for a complete, efficient, and scalable system that combines smart analysis with safe data management.

3. Proposed Methodology

The methodology suggested herein describes a framework that utilizes AI and Blockchain technologies to detect counterfeit products and fraudulent websites. The detection process involves the simultaneous analysis of the features of the website and the features of the product. A multi-step pipeline is created to make sure that the verification process is efficient, reliable, and secured.

3.1.Data Collection

Data gathering refers to the process whereby relevant data is gathered that will be used to detect any cases of fraud. This entails information like URLs of the websites under study, pricing of the products, as well as general information about the products. Datasets with examples of genuine sites and fraudulent sites are gathered too. As Shown in Figure 1

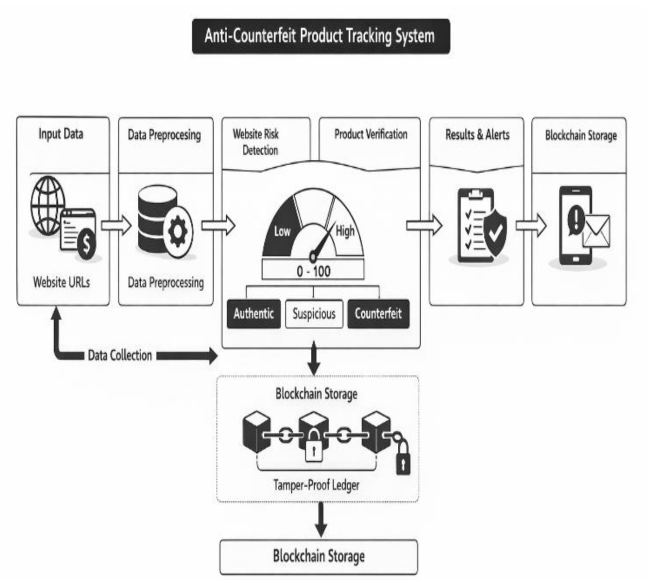

Figure 1 **Anti-Counterfeit Product Tracking System**

3.2.Data Preprocessing

Pre-processing of gathered data helps in ensuring the consistency and accuracy of data. Validation of the data, removing inconsistencies or incomplete data records, and ensuring normalization is part of the process of preprocessing data. The preprocessing stage also involves normalization of URL structures, validating numerical variables like pricing, among others. This will help minimize noise, improve data quality, and boost the performance of other stages of analysis.

3.3.Website Risk Assessment

Website risk assessment concentrates on analyzing various features of the website using its URL. Among the elements that may be assessed when checking for website risks include the existence of unusual extensions, use of the HTTP protocol instead of the HTTPS protocol, among others. Other features that may be examined include keywords, URL patterns, among others.

3.4.Product Verification

Product verification involves assessing product-oriented attributes that would help identify possible cases of product counterfeiting. Pricing is an important factor at this stage. If the price of the product is much lower than average market rates, there could be a case of product counterfeiting.

3.5.Calculation of Risk Score

A risk score is computed based on a combination of analysis outcomes from website evaluation and product identification. Each attribute receives a weighted score depending on its significance for detecting fraud. The total score lies within the range between zero and hundred, where the higher score suggests a higher likelihood of counterfeiting.

3.6.Blockchain Incorporation

The incorporation of blockchain technology helps guarantee reliable storage of the obtained verification outcomes. In particular, all transactions related to a specific product or website, including its classification as well as the calculated risk score, will be registered in a distributed ledger. This solution helps eliminate any doubts regarding data security and transparency. As Shown in Table 1.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

Table 1 Risk Parameters Used for Fraud Detection

Parameter	Condition Checked	Weight Assigned
Domain Pattern	Suspicious keywords (.xyz, cheap)	30
Website Security	HTTP instead of HTTPS	25
Product Price	Unusually low pricing	35
Content Trust Score	Missing or fake product details	10

4. System Architecture

The architecture of the proposed system is created in such a way that it will help the system work efficiently by providing the detection of fake products and websites. Different layers perform different functions in the process of data processing, helping the system to have an effective and high-performing structure. Also, the proposed system allows data to flow from user input to the output smoothly and in a secure manner, thanks to the usage of blockchain technology.

4.1.Overall System Architecture

The overall system architecture includes different layers that include input layer, processing layer, analysis layer, storage layer, and output layer. All components of the architecture are connected through well-defined interfaces and are able to exchange data effectively. Data goes from one layer to another in a sequential order, and each of the layers serves its function in a proper way.

4.2.User Input Layer

The user input layer is a starting point of our system, which helps collect necessary information. The user input layer provides such important inputs as website URL and product price. The user interface is intuitive enough to facilitate input operation. Besides, data validation takes place in this layer.

4.3.Processing Layer

The processing layer is focused on making the input data ready for analysis. Data validation, data cleaning, and data normalization are performed within this stage. Invalid entries are eliminated, and structure formatting is preserved in order to provide consistent data processing. This stage provides the input data that can be analyzed effectively due to improved accuracy and optimization.

4.4.AI Analysis Layer

The AI analysis layer conducts the main operation in terms of fraud detection. Website analysis, including identification of its domain, safety level, and use of any suspicious words is done by this layer. Alongside website analysis, analysis of attributes of products is conducted. Specifically, prices and offers are assessed based on provided information, and risk score is calculated. The layer improves detection accuracy by means of intelligent patterns identification.

4.5.Database & Blockchain Layer

This layer deals with data storage and security aspects of the process. Verification results such as risk assessment scores and final classification along with the input data are all stored in an organized way in a database. Besides, blockchain technology can be applied for storing the most significant verification results.

4.6.Output and Alert Layer

This is where the output layer will show the findings in a simple and understandable manner. The system displays the risk value in addition to its classified category like Authentic, Suspicious, or Counterfeit. Where necessary, the alert system gets activated to raise the alarm whenever there is a higher risk level detected. As Shown in Figure 2.

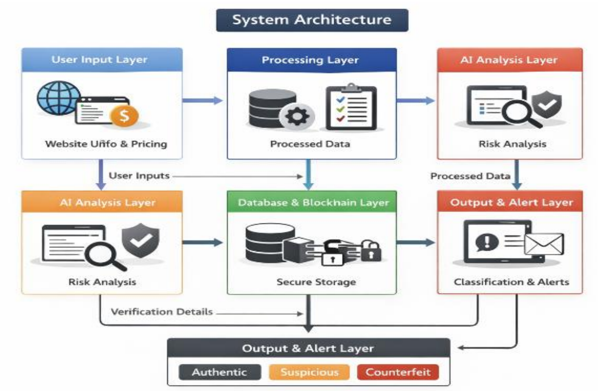

Figure 1 System Architecture of Anti-Counterfeit Product Tracking System

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

5. Experimental Setup

This experiment aims at testing the effectiveness, efficiency, and performance of the Anti-Counterfeit Product Tracking System. This section describes the implementation environment, test dataset, evaluation criteria, and process of conducting experiments. Such an approach allows us to assess how well the system works in real-world situations.

5.1. Implementation Environment

Python language has been used in order to develop the Anti-Counterfeit Product Tracking System because of its powerful capabilities to analyze data and apply machine learning techniques. Application development involves usage of various frameworks, for example, Flask for backend solutions and standard web development tools for UI design. Testing is performed on a computer with a recent CPU and enough RAM.

5.2. Dataset Description

The dataset is composed of website and product data. Websites data consist of both genuine and suspicious websites and contain features such as website structure, security, and keyword usage. Product data consist of pricing information and characteristics that help detect counterfeit behavior. Labeled data into classes such as authentic, suspicious, and counterfeit is used for classification purposes.

5.3. Evaluation Metrics

Performance evaluation is carried out using traditional metrics that gauge accuracy and dependability. Accuracy, precision, and recall are used to determine the effectiveness of the classifier. In addition, the accuracy of risk scoring and the reliability of classification are evaluated. Response time is used to determine the speed at which the system produces its results.

5.4. Training and Testing Procedure

The system uses an organized framework to learn and test the performance of the system. First, the data set undergoes preprocessing and split into training and testing sets. Training consists of learning from labeled data such as suspicious websites and irregular prices. Testing consists of the assessment of classification performance.

5.5. System Testing

System testing is done both with sample inputs as well as live user data. Test scenarios with good websites, doubtful websites and counterfeit products are conducted. Results from such testing are analyzed for correctness, speed of response and reliability. In addition, stress testing is carried out to check if the system handles multiple request simultaneously with ease.

6. Algorithms Used

Multiple algorithms are used for detecting any fake websites and counterfeit products. These algorithms analyze the input, calculate risk levels and classify their output. Multiple algorithms increase the reliability, efficiency and scalability of the system.

6.1. Website Risk Analysis Algorithm

Website Risk analysis algorithm checks the credibility of the given URL by analyzing its security parameters. Parameters like domain, suspicious keywords and HTTPS are checked to determine the trust factor. Each of these parameters are assigned weight factors according to their significance.
Working:

- Domain structure check
- Check if there is HTTPS protocol
- Check for presence of suspicious keywords
- Assign weight to each parameter
- Calculate intermediate risk factor

6.2. Price-Based Fraud Detection Algorithm

The detection of counterfeit goods relies on detecting the anomaly in the price. Goods that are priced significantly below the market price are deemed suspicious. Functioning:

- Compare input price against the expected market price range
- Find unusual or unrealistic prices
- Evaluate the risk factor based on deviations
- Utilize multiple parameters for the final assessment

This technique can assist in detecting counterfeit goods that lure buyers with their low pricing.

6.3. Risk Score Computation Algorithm

The computation of risk score is done by adding up the results of various modules of analysis using weight-based summation.

Formula:

Risk Score = (W_1 × Website Risk) + (W_2 × Price

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

Risk)

Where:

- W_1, W_2 – weights assigned to the individual parameters
- Website Risk, Price Risk – intermediate risk scores

The result is scaled between 0 and 100. The higher the score, the more likely the fraud.

6.4.Classification Algorithm

The classification algorithm will categorize the risk score into appropriate classes.

Criteria for Classification:

- 0 – 30 = Genuine
- 31 – 70 = Dubious
- 71 – 100 = Fake

This process makes it easier to make decisions as it provides categorical outputs depending on the risk scores.

6.5.Blockchain Storage Algorithm

This algorithm uses blockchain technology for secure and immutable storage of the verification results.

Working Principle:

- Generation of transaction with inputs and outputs
- Creation of unique hash for each record
- Storage of information on the blockchain database
- Immutable and transparent

This will guarantee that the verification information is not alterable or modifiable.

6.6.Algorithm Integration

All algorithms are incorporated into an automated workflow where each component will work in tandem to process inputs. The outputs generated from the website and product analysis algorithms will be used to calculate the risk score.

7. Results and Discussion

Anti-Counterfeit Product Tracking System's performance is assessed using criteria that include detection accuracy, risk score evaluation, system efficiency, and comparison with other approaches. The testing of the system includes scenarios involving legitimate websites, suspicious sites, and counterfeit products.

7.1.Detection Accuracy

The detection accuracy achieved by the proposed system is very high in terms of the ability to recognize both suspicious websites and counterfeit products. Thanks to the combined use of web detection and product verification, fewer mistakes occur. Valid entries are recognized as legitimate, while suspicious and counterfeit products/website cases are recognized as well.

7.2.Risk Score Evaluation

The risk score system is an effective way of quantifying authentication. Scores between 0 and 100 are determined by parameters with assigned weights. Lower scores indicate sources that are safe and reliable, whereas high scores imply possible fraud. Thresholds are set to classify results (Authentic, Suspicious, Counterfeit). The risk score evaluation tool accurately distinguishes legitimate patterns from suspicious ones.

7.3.System Efficiency

The risk assessment system works efficiently, delivering rapid response with minimal computing cost. The system's architecture enables seamless communication between modules, thus allowing almost instant evaluation. Even when dealing with several input sources simultaneously, the system retains its efficiency without experiencing significant lags. This property makes it deployable in practical applications.

7.4.Comparison to Alternative Approaches

This project has many advantages over traditional methods, such as barcodes, QR code systems, and centralized databases. First of all, those are prone to duplication and have a weak security component. Second, AI integration allows detecting fraud intelligently, and, finally, blockchain technology makes database access both secure and unalterable. Thus, the proposed dual verification approach gives many advantages compared to alternative approaches.

8. Performance Evaluation

In this section, the performance of the proposed system will be analyzed. Performance can be estimated in the context of efficiency, reliability, accuracy, speed, and others. This project involves developing an Anti-Counterfeit Product Tracking System that can operate effectively under different

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 05 May 2026
Page No: 3368-3376
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0434

conditions. It is capable of performing multiple tasks simultaneously without compromising the system's reliability and output results.

8.1.Processing Speed

Speed is one of the key performance characteristics of any real-time system designed to detect fraudulent activity. Users' input is processed instantly, and results are provided promptly. Data processing technologies used in this project are quite optimized, which makes it fast and reliable. Simultaneous processing of multiple requests is possible without slowing down the operation speed.

8.2.Accuracy

Accuracy stands for the degree of correct classification of inputs into authentic, suspicious, and fake categories. By using the combination of website analysis and verification of products, the system reaches high levels of accuracy without generating excessive amounts of both false positives and false negatives. The multi-parameter approach helps ensure the validity of classification outcomes.

8.3.Efficiency

Efficiency is defined as the most effective use of computational resources in connection with the system's performance. Efficiently structured input data and pre-processing procedures help minimize unnecessary computations. As all modules perform different functions, there are no redundant computations within the framework of this system, which makes the system highly efficient.

8.4.Scalability

Scalability means the ability of a system to operate under heavy loads. The modular structure allows easily scaling the system by adding some modules or increasing the number of datasets analyzed by the system. Decentralized blockchain storage used in the process makes the system scalable as it does not depend on any other system.

Conclusion

In summary, the anti-counterfeit product tracking system is a highly effective tool for dealing with the ever-increasing number of counterfeit products and fraudulent websites. With the integration of artificial intelligence technologies with blockchain, it guarantees precision in identifying frauds and the secure management of the data. In addition, the use of dual verification based on analysis of the website characteristics and information about the product increases the effectiveness and minimizes the risks of false identification. The system shows high performance in terms of accuracy, speed of calculations, and overall effectiveness. In particular, the risk score method allows users to evaluate the authenticity of the website and the products quantitatively and makes a well-grounded decision in real time. Moreover, due to the use of blockchain, the system can ensure high transparency and security of all the processes involved in data management. The modular architecture and scalability make it possible for the system to operate in real-time mode and process multiple requests simultaneously without considerable performance decrease.

Future Work and Enhancements

Deep Learning Techniques for Product Verification

In the future, there can be an incorporation of deep learning approaches such as CNNs for analyzing images of goods in order to increase their efficiency in detecting counterfeits by focusing on logos, packaging, design patterns, etc.

Real-Time Image Verification

A new feature to be considered is the ability of uploading images in real time and performing verification tasks to ensure quick response rates and efficient authentication processes.

QR Code and Barcode Detection

Another development area could be the use of QR codes and barcodes in verifying the authenticity of products. The QR codes would link the product to its record in the blockchain system and help detect counterfeit products quickly.

Machine Learning Algorithms

The use of machine learning algorithms can also be considered to detect fraud efficiently. Adaptive algorithms that can learn from newly observed patterns can improve the ability of the system in detecting counterfeit products.

Deployment on the Clouds

Utilizing the cloud-based systems may help the organization become more scalable, storage-efficient, and accessible. Integration with the cloud may enable the system to cope with a lot of information and at the same time accommodate multiple users without performance issues.

Real-Time Notification and Alert Mechanisms

One of the improvements that can be done is the addition of the real-time notifications and alert features. Emails and alerts to user accounts or administrators can automatically be triggered upon detecting any high-risk or suspicious activities.

Integration with E-Commerce Sites

The application may be directly connected with the various online selling sites in order to provide product and merchant verification. This may help increase consumer confidence and prevent fake product listings.

Use of Big Data Analytics

Using big data analysis tools may assist in examining large amounts of information in order to establish patterns or trends regarding the counterfeit products.

Acknowledgements

Acknowledgment is hereby conveyed to the project guide for invaluable advice and support received during the preparation of this study. Thanks are also due to the faculty members and institution for offering necessary resources and facilities. Acknowledgment is also made to the friends and colleagues who have cooperated in the preparation of this study.

References

[1]. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. *Future Generation Computer Systems*, 107, 841–853.

[2]. Kshetri, N. (2018). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 42(4), 303–314.

[3]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4), 352–375.

[4]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep Learning*. MIT Press.

[5]. Chollet, F. (2018). *Deep Learning with Python*. Manning Publications.

[6]. Singh, S., & Singh, N. (2016). Blockchain: Future of financial and cyber security. *International Conference on Contemporary Computing and Informatics*, 463–467.

[7]. Gipp, B., Meuschke, N., & Gernandt, A. (2015). Decentralized trusted timestamping using the crypto currency Bitcoin. *Proceedings of the 15th ACM/IEEE-CS Joint Conference on Digital Libraries*, 85–94.

[8]. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection. *Decision Support Systems*, 50(3), 559–569.

[9]. Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. *Expert Systems with Applications*, 36(10), 11994–12000.

[10]. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81.

[11]. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. IEEE Access, 4, 2292–2303.

[12]. Dorri, A., Kanhere, S. S., & Jurdak, R. (2017). Towards an optimized blockchain for IoT. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, 173–178.

[13]. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700.

[14]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy, 305–316.

[15]. Sahoo, S. S., Sahoo, K. S., & Mohanty, S. P. (2020). Secure data sharing in blockchain-based systems. IEEE Internet of Things Journal, 7(5), 3979–3989.

[16]. Kumar, S., & Singh, M. (2019). Fraud detection in online transactions using machine learning algorithms. International Journal of Computer Applications, 178(7), 1–5.
[17]. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. IEEE Security and Privacy Workshops, 180–184.
[18]. Chen, T., Li, X., Luo, X., & Zhang, X. (2018). Underlying blockchain technology for secure data sharing. Journal of Network and Computer Applications, 103, 1–9.
[19]. Alzahrani, B. A., & Daim, T. U. (2019). Evaluation of blockchain implementation in supply chain management. Technological Forecasting and Social Change, 146, 383–397.
[20]. Abadi, M., Agarwal, A., Barham, P., Brevdo, E., Chen, Z., Citro, C., & Dean, J. (2016). TensorFlow: Large-scale machine learning on heterogeneous systems. arXiv preprint arXiv:1603.04467.