Adopting Machine Learning Blockchain Intrusion Detection for Protecting Attacks on Internet of Things

[1]Saheed, Y.K. [2]Magaji, R.D., [3]Tosho, A. & [4]Longe, O.B.
[1]School of IT & Computing, American University of Nigeria, Yola, Nigeria
[1,2,3]Department of Computer Science, Al-Hikmah University, Ilorin, Nigeria
[2]Department of Computer Science, Shehu Idris College of Health Sciences and Technology, Makarfi, Kaduna State Nigeria
E-mails: [1]yakubu.saheed@aun.edu.ng; [2]dmrmakarfi@gmail.com; abdtosh@gmail.com; [3]olumide.longe@acity.edu.ng

ABSTRACT

Intrusion Detection Systems (IDSs) are widely used in various computer networks with the goal of spotting cyber threats and potential incidents. Collaborative intrusion detection networks (CIDSs) have been developed to augment the detection power of a single IDS by allowing IDS nodes to exchange data. The Internet of Things (IoT) can be thought of as a network or connectivity of sensors and actuators that share data in a unique way. Blockchain technology has been applied in a variety of fields to foster trust and data protection by enabling participants to trade transactions and communicate information while preserving a level of trust, integrity, and greater transparency. However, there are numerous security concerns associated with the implementation architectures and technologies that will form the Internet of Things' backbone. Hence, this paper proposes a machine learning technique leveraging on blockchain technology with IDS for detecting attacks on IoT. In this paper, we used Naïve Bayes (NB), K-Nearest Neighbor (KNN) and Support Vector Machine (SVM) models for performing the experiment on NSLKDD dataset. The experimental findings for KNN model achieved 99.6% detection rate with a false alarm rate of 0.4. The NB and SVM models also gave competitive results.

Keywords: Machine Learning, Blockchain, Intrusion Detection System, Internet of Things, K-Nearest, Online Safety, Neighbor, Collaborative IDS

Proceedings Reference Format
Saheed, Y.K. Magaji, R.D., Tosho, A. & Longe, O.B. (2021): Adopting Machine Learning Blockchain Intrusion Detection for Protecting Attacks on Internet of Things. Proceedings of the 27th iSTEAMS Multidisciplinary Innovations & Technology Transfer (MINTT) Conference. Academic City University College, Accra, Ghana. June, 2021. Pp 343-354 www.isteams.net/ghana2021.
DOI - https://doi.org/ 10.22624/AIMS/iSTEAMS-2021/V27P30

1. INTRODUCTION

The Internet of Things (IoT) can be defined as an integrated system centered on authorized protocols that communicate data among internet-connected devices[1]. Recent breakthroughs in the Internet of Things (IoT) have introduced the concept of smartness to machines, detectors, houses, streets, and even entire cities[2]. IoT is a rapidly emerging hallmark of modern computing and communication technology that has made significant contributions to a variety of sectors, ranging from agriculture to vehicle automation.

Nowadays, the Internet of Things is sometimes referred to as the Internet of Everything (IoE), as it encompasses all linked devices in daily life. By 2025, the number of connected devices is expected to reach 21.5 billion[2]. The internet of things can be thought of as a network or connectivity of sensors and actuators that share data in a unique way. The IoT is not bound by any particular protocol but is open to any state-of-the-art protocol available today in order to maximize range[3],[4]. Additionally, as all devices become smart, data and network management may be automated, and efficiency can be boosted through M2M interactions. Even customer inputs can be computerized with the use of sensors, and solutions will be conveyed directly to the objects where they are expected to occur[5], [6].

This paradigm shifts from connected computers to a network of 'things' transformed the digital world and ushered in a new era of development. The concept of digital identity and linkage to each entity has boosted the Internet's influence on new heights. The IoT has encroached into our daily lives through wireless connections and new digital identification systems such as RFID.

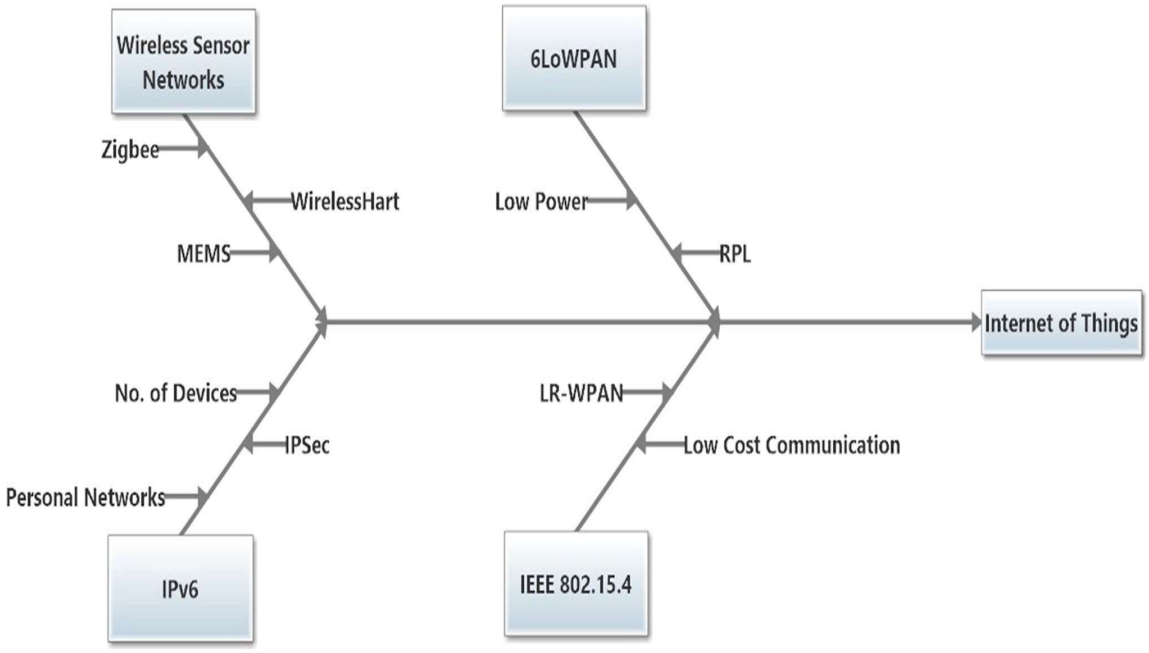

Figure 1. Internet of Things Background[1]

Wireless Sensor Networks (WSN) advancements and low-power, resource-constrained devices have expanded the types of devices that can be connected to the Internet. However, IPv6 [7] and IEEE 802.15.4 have been instrumental in expanding the address space and incorporating additional components and networks into the realm of IoT. As illustrated in Figure 1, these newer technologies have played a critical role in the evolution of the Internet into the Internet of Things.The security issues inherent in a fully-fledged IoT system have drawn the attention of numerous academics, owing to the growing demand for secure IoT devices. There are numerous security concerns associated with the implementation architectures and technologies that will form the Internet of Things' backbone.

The research problems in the IoT security arena are numerous and fascinating. The technologies that underpin IoT are still in their infancy from a security standpoint. The IP-based WSN and WSN[8], which will serve as the primary data collection points in the majority of IoT structures, are perpetually susceptible and pose a serious security risk. Attacks on these fundamental parts can result in major data breach and privacy issues. If the attacker compromises the nodes, he or she can change the data that is sent to the upper tiers. It can have a significant impact on the organizational center's processing and activities, as well as disrupt the overall system. Malicious intrusions, such as DDoS and ransomware, phishing attack and IoT networks' availability. These assaults are becoming more sophisticated and complicated, ensuing in disruptive repercussions that jeopardize data integrity, availability and confidentiality [9]. The capacity to identify and react to that kind of attacks is critical for mitigating any damage to IoT architecture and minimizing any damage inflicted. IDS are frequently used to screen and detect complex assaults on IoT network environments and their sensors[10].

The IoT and cloud systems continue to confront complex attack scenarios, which are becoming more prevalent with the advent of blockchain[11]. For instance, around June 2018, numerous blockchain cryptocurrencies, including Gold Bitcoin and MonaCoin, were subjected to fifty-one percent attacks, resulting in the loss of around eighteen million worth of tokens[12]. The hackers gained control above more than half of the total global hash rate of mining by exploiting each cryptocurrency network. This susceptibility allowed attackers to dual-spend transactions, jeopardizing the network's integrity.

Blockchain technology has been applied in a variety of fields to foster trust and data protection by enabling members to trade businesses and communicate data while preserving a level of integrity, trust and greater slide. Besides, blockchain technology has uses outside of digital currency and financial service[13], including the energy sector, online voting[14], supply chain and manufacturing[15], [16], the Internet of Things (IoT) [17],[18], big data[19], pharmaceutical and healthcare[20], cyber security, and government service area[21], [22]. IDS with blockchain can be used in conjunction on IoT networks to detect cyberattacks and protect sensitive data. The Internet of Things is the future, and it must be developed with a safe design. Since IoT is still in its infancy and security solutions are not well developed, security concerns must be considered for IoT devices from the start. Hence, this paper proposes a blockchain based IDS for detecting attacks on IoT. This paper is structured as follow. We present related work in Section 2. The methodology was discussed in section 3. The results and discussion were highlighted in section 4. Conclusion and future work were presented in section 5.

2. RELATED WORKS

Numerous researches have examined the usage of blockchain technology to increase confidence among collaborative IDSs in IoT networks. The study [23] suggested a securely sharing framework to collects data in IoT applications. They proposed coupling Ethereum's blockchain technology with deep reinforcement learning. The learning model made use of three primary elements: surroundings, behavior, and incentives. This enhanced the fairness ratio for IoT software applications by more than 35%. In summary, when applied in cloud systems, the integration of blockchain and CIDS technologies significantly improves security levels. The authors [24] have classified 18 blockchain application cases, four of which are for IoT. Alaba et al. [25] classify security concerns into application, architecture, communication, and data categories. This proposed IoT security taxonomy is distinct from the traditional layered design. Following that, the dangers to IoT are examined in terms of hardware, network, and application components.

Granjal et al.[26] address and examine security concerns associated with the protocols designed for the Internet of Things. The authors [27] suggested an unsupervised hybrid IDS framework in 2017 for spotting selective-forwarding and sinkhole attacks on IoT. It utilizes MapReduce engineering to perform an unsupervised optimum-path timberland (OPF) calculation. The study [28] advocated utilizing a cutting-edge interruption detection methodology for the IoT context in conjunction with a demonstration of automation. This technique classifies IoT assaults into three categories: false, jamming, and reply-attacks. It is an augmentation of the aforementioned frameworks. The configuration of this IDS might be central, as the data gathered by position hubs is provided to the discovery unit, which assists in the construction of the event databases. To identify interruptions, the IDS employs an analyzer occasion built on a specification-based technique.

This IDS can competently recognize false-attacks, jam-attacks, and reply-attacks in IoT systems through relating the pre-occupied activity streams. Ref.[29] also in 2017, suggested a way for increasing message amongst numerous independent agents participating in an unmanned Aerial vehicles by combining blockchain and multi-agent systems (UAV). They developed an architectural approach for integrating communication using Ethereum's blockchain into peer-to-peer (p2p) networks. As a result, we have a procedure that may be well-matched with independent agents. The proposed procedure safeguards the message process's security and aids in forestalling the heftiness of variable operating conditions. This has prompted additional research into the intersection of blockchain and multi-agent systems.

3. MATERIALS AND METHODOLOGY

3.1. Blockchain

The primary motive behind blockchain technology is decentralization[30]. Due to the transparent and distributed nature of the blockchain's ledger, the failure of a single node would not affect the whole system. The Blockchain technology shifted the contract network's architecture from a star to a P2P arrangement. Using security based on code, encryption and algorithm protection, this modified framework enables two parties to communicate directly with one another. Because the parties to the contract system are required to trust the algorithm used to build mutual confidence, no prior knowledge of the parties' trustworthiness is necessary[31]. Additionally, the architecture eliminates the need for third-party security endorsements, since the algorithm itself is solely accountable for all types of verification.

Ethereum[32] and Hyperledger[33] fabric are popular widely used platforms for developing blockchain applications. Their fundamental technologies are same. The primary distinction between Ethereum and Hyperledger is in their architecture and intended audience. Ethereum supports the Ethereum virtual machine (EVM). Smart contracts and public blockchains are geared toward consumer-facing applications. The architecture of the model is shown in figure1.

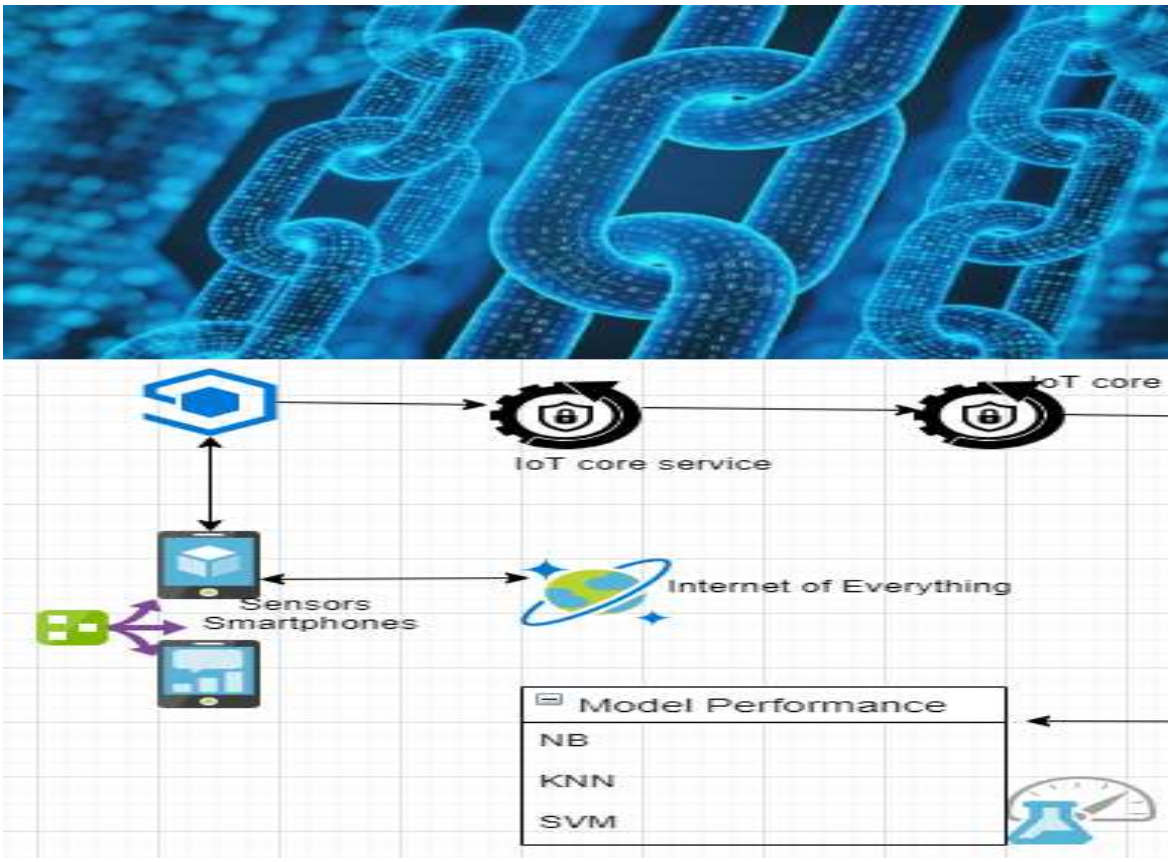

Figure 1. Architecture of the propose model

3.2 Principal Component Analysis

PCA is a widely used technique for extracting features[34], [35] and also essential technique in data compression[36]. Principal Component Analysis has been demonstrated to be extremely successful at reducing dimension in intrusion detection. When data is noise-free, noise reduces classification accuracy, while PCA improves classification accuracy. By incorporating PCA into the design of an intrusion detection system, you can reduce the system's complexity while increasing classification accuracy[37].

3.3 Naïve Bayes

Naive Bayes is a methodology for supervised machine learning that is used to solve classification problems[38], [39]. NB is a very powerful classification technique[40]. It is fundamentally based on the Bayes classification rule. It is predicated on the notion that each feature is self-contained; that is, the presence of one feature in a class has no bearing on the presence of any other feature in that class. It is a simple model to construct and performs better on huge datasets[39], [41].

3.4. K-Nearest Neighbor

The k-nearest neighbor algorithm (KNN) is a non-parametric methodology for pattern recognition that can be used for classification or regression. It compares the unlabeled samples to the training samples[42]. The training samples are vectors in a multidimensional feature space; each sample has a class name associated with it. k is a user-defined constant variable in the classification phase, and an unknown vector (a query or test point) is identified by assigning the label that occurs most frequently among the k training samples closest to the query point. Euclidean distance is a frequently used distance metric[43],[44].

3.5 Support Vector Machine

The support vector machine (SVM) is a widely used machine learning technique for solving classification and regression problems. The basic SVM uses a collection of input data to forecast which of two possible classes will form the binary linear classifier's output for each given input[45],[46]. SVM outperformed neural networks and other standard machine learning methods in terms of overfitting and generalization abilities[47]. SVM provides apparent advantages for high-dimensional and small sample network intrusion detection. However, numerous studies demonstrate that the performance of the SVM-based network intrusion detection model is directly proportional to its parameters (penalty factor C and kernel function parameter g, etc.). If the parameter selection is incorrect, the network intrusion detection accuracy will be reduced[48], [49].

4. RESULTS AND DISCUSSION

4.1 Experimental Dataset

Due to many problems in KDD cup 1999, such as irregular spreading of samples, duplication and redundant records, and so on, Tavallaee et al. presented NSL-KDD dataset[50].The NSL-KDD dataset describes each sample using forty one conditional features followed by a class label. The features are classified as (i) Basic attributes (ii) Characteristics Contents (iii) Time-based features traffic (iv) Host traffic attributes. Any comportment on a network that deviates from "Normal" is regarded as an attack class label. The NSL-KDD dataset contains information on twenty-four different types of assaults, which can be classified as U2R, R2L, Probe, and DoS.

4.2 Evaluation Measures

Along with detection rate and false alarm rate, the number of features was used to evaluate the performance of the proposed blockchain-based BoTIDS in this work, since it has a significant impact on the complexity of the learning model. As a result, the PCA was utilized to extract features. As explained below, the detection rate and false alarm rate were evaluated using True Positive, False Positive, True Negative and False Negative.

This metrics are the most suited metrics for evaluating IDS performance[51].

- True Positive is measure of malicious behaviors correctly identified as an attack.
- True Negative is measure of benign behaviors correctly identified as benign.
- False Positive is measures of benign behaviors misclassified as an attack.
- False Negative is measures of malicious behaviors misclassified as benign.

4.3 The 10-Fold Cross Validation

In the discipline of machine learning, the 10-fold cross validation is used to measure the accuracy with which a learning system can predict data that was not trained on. The training dataset is partitioned randomly into ten groups; the first nine groups are utilized to train the classifier, while the tenth group serves as the testing dataset. The procedure is continued until all groups have been covered, and performance is calculated as the sum of all ten folds.

4.5. Performance Evaluation of NB, KNN and SVM

From Table 1, among the three classifiers used in this research work, KNN predicts better than other classification algorithms with 99.1% detection accuracy, 99.6% detection rate, 0.4 false alarm rate, 99.4% precision and 99.5% F-measure. Also, the SVM performed better than the NB as a result of its generalization capacity with 95.3% detection accuracy, 94.7% detection rate, 1.3 false alarm rate, 97.6% precision and 96.2% F-measure. The NB achieved 81.2% detection accuracy, 87.5% detection rate, 1.5false alarm rate, 97.1% precision and 92.0% F-measure.

Table 1. Performance of the three-classification models

Algorithms/Metrics	Detection Accuracy	Detection rate	False Alarm rate	Precision	F-measure
NB	81.2	87.5	1.5	97.1	92.0
KNN	99.1	99.6	0.4	99.4	99.5
SVM	95.3	94.7	1.3	97.6	96.2

The Figure 2 depicts how each of this model performed in terms of the performance metrics. The low detection rate and high false alarm rate are issues in BoTIDS. In this research, our model gave a superior detection accuracy of 99.6% and low false alarm rate of 0.4%.

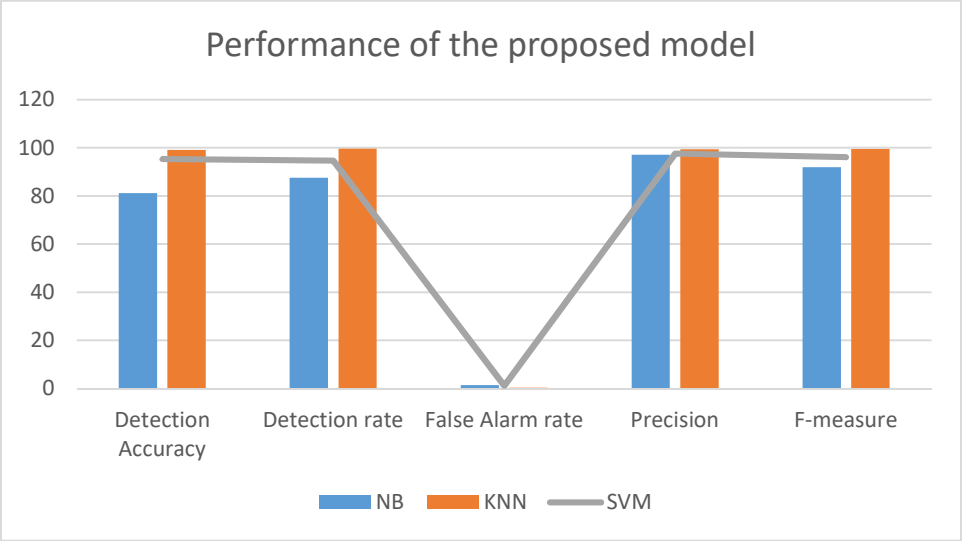

Figure 2. Performance of the proposed model based on NB, KNN and SVM classifiers.

5. CONCLUSION AND FUTURE WORK

This research proposes an intrusion detection solution for IoT threats based on NB, KNN, and SVM algorithms utilizing blockchain technology. We have explained the operation of each model component and the system as a whole. Due to the systems' adaptability, this innovative blockchain-IDS may be used in a variety of IoT scenarios. All third-party hacking attempts will be logged on the blockchain, ensuring the system's security against threats such as Distributed Denial of Service (DDoS) attacks, Probe, User to Root (U2R), and Remote to Local (R2L). The future work direction will be to adopt deep learning model with block chain technology for detecting attacks on IoT.

REFERENCES

[1] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, 2018, doi: 10.1007/s11235-017-0345-9.

[2] C. Liang *et al.*, "Intrusion detection system for the internet of things based on blockchain and multi-agent systems," *Electron.*, vol. 9, no. 7, pp. 1–27, 2020, doi: 10.3390/electronics9071120.

[3] L. Kong, M. K. Khan, F. Wu, G. Chen, and P. Zeng, "Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 62–68, 2017, doi: 10.1109/MCOM.2017.1600422CM.

[4] V. Odelu, A. K. Das, M. Khurram Khan, K. K. R. Choo, and M. Jo, "Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size keys and ciphertexts," *IEEE Access*, vol. 5, no. 1, pp. 3273–3283, 2017, doi: 10.1109/ACCESS.2017.2669940.

[5] M. Syafiq, B. Ab, M. Anuaruddin, B. Ahmadon, and S. Yamaguchi, "On Privacy Verification in the IoT Service Based on PN 2," pp. 1–4, 2016.

[6] A. Tewari and B. B. Gupta, "A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices," *Int. J. Adv. Intell. Paradig.*, vol. 9, no. 2/3, p. 111, 2017, doi: 10.1504/ijaip.2017.10003568.

[7] A. F. Molisch *et al.*, "IEEE 802.15.4a Channel Model - Final Report," *Ieee P802*, vol. 15, no. 04, pp. 1–40, 2004.

[8] A. Rani and S. Kumar, "A survey of security in wireless sensor networks," *3rd IEEE Int. Conf.* , 2017, doi: 10.1109/CIACT.2017.7977334.

[9] A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013, doi: 10.1016/j.jnca.2012.08.007.

[10] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *J. Netw. Comput. Appl.*, vol. 60, pp. 19–31, 2016, doi: 10.1016/j.jnca.2015.11.016.

[11] O. S. Alkadi, N. Moustafa, B. Turnbull, and K. K. R. Choo, "An Ontological Graph Identification Method for Improving Localization of IP Prefix Hijacking in Network Systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, no. c, pp. 1164–1174, 2020, doi: 10.1109/TIFS.2019.2936975.

[12] O. Alkadi, N. Moustafa, B. Turnbull, and K.-K. R. Choo, "A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks," *IEEE Internet Things J.*, vol. 4662, no. c, pp. 1–1, 2020, doi: 10.1109/jiot.2020.2996590.

[13] G. W. Peters and E. Panayi, *Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money*. 2016.

[14] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," *Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree*, pp. 1561–1567, 2018, doi: 10.1109/Cybermatics_2018.2018.00262.

[15] . S. A. A., "Blockchain Ready Manufacturing Supply Chain Using Distributed Ledger," *Int. J. Res. Eng. Technol.*, vol. 05, no. 09, pp. 1–10, 2016, doi: 10.15623/ijret.2016.0509001.

[16] C. K. Oh, M. Neurath, J. J. Cho, T. Semere, and D. D. Metcalfe, "Two different negative regulatory elements control the transcription of T-cell activation gene 3 in activated mast cells," *Biochem. J.*, vol. 323, no. 2, pp. 511–519, 1997, doi: 10.1042/bj3230511.

[17] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018, doi: 10.1016/j.future.2017.11.022.

[18] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, no. c, pp. 32979–33001, 2018, doi: 10.1109/ACCESS.2018.2842685.

[19] A. Karafiloski, E. & Mishev, "Blockchain Solutions for Big Data Challenges," *IEEE EUROCON 17th Int. Conf.*, no. July, pp. 763–768, 2017.

[20] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control," *J. Med. Syst.*, vol. 40, no. 10, 2016, doi: 10.1007/s10916-016-0574-6.

[21] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services-Use cases, security benefits and challenges," *2018 15th Learn. Technol. Conf. L T 2018*, pp. 112–119, 2018, doi: 10.1109/LT.2018.8368494.

[22] S. Ølnes, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," *Gov. Inf. Q.*, vol. 34, no. 3, pp. 355–364, 2017, doi: 10.1016/j.giq.2017.09.007.

[23] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial iot with deep reinforcement learning," *IEEE Trans. Ind. Informatics*, vol. 15, no. 6, pp. 3516–3526, 2019, doi: 10.1109/TII.2018.2890203.

[24] M. Conoscenti, D. Torino, A. Vetr, D. Torino, and J. C. De Martin, "Unknown - Unknown - US20140357466A1.pdf.pdf," *ACS 13th Int. Conf. Comput. Syst. Appl.*, 2016.

[25] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," *J. Netw. Comput. Appl.*, vol. 88, no. December 2016, pp. 10–28, 2017, doi: 10.1016/j.jnca.2017.04.002.

[26] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: A survey of existing mechanisms, protocols and open research issues," *J. Fac. Eng. Archit. Gazi Univ.*, vol. 33, no. 4, pp. 1247–1272, 2018.

[27] H. Bostani and M. Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach," *Comput. Commun.*, vol. 98, pp. 52–71, 2017, doi: 10.1016/j.comcom.2016.12.001.

[28] Y. Fu, Z. Yan, J. Cao, O. Koné, and X. Cao, "An Automata Based Intrusion Detection Method for Internet of Things," *Mob. Inf. Syst.*, vol. 2017, pp. 6–10, 2017, doi: 10.1155/2017/1750637.

[29] A. Kapitonov, S. Lonshakov, A. Krupenkin, and I. Berman, "Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs," *2017 Work. Res. Educ. Dev. Unmanned Aer. Syst. RED-UAS 2017*, pp. 84–89, 2017, doi: 10.1109/RED-UAS.2017.8101648.

[30] R. R. Vokerla *et al.*, "An Overview of Blockchain Applications and Attacks," *Proc. - Int. Conf. Vis. Towar. Emerg. Trends Commun. Networking, ViTECoN 2019*, pp. 1–6, 2019, doi: 10.1109/ViTECoN.2019.8899450.

[31] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," *Proc. - 2016 IEEE Symp. Secur. Privacy, SP 2016*, pp. 839–858, 2016, doi: 10.1109/SP.2016.55.

[32] T. Sun and W. Yu, "A formal verification framework for security issues of blockchain smart contracts," *Electron.*, vol. 9, no. 2, 2020, doi: 10.3390/electronics9020255.

[33] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of IoT devices using blockchain," *Sensors (Switzerland)*, vol. 19, no. 4, 2019, doi: 10.3390/s19040856.

[34] A. K. Oladejo, T. O. Oladele, and Y. K. Saheed, "Comparative Evaluation of Linear Support Vector Machine and K-Nearest Neighbour Algorithm Using Microarray Data on Leukemia Cancer Dataset," vol. 11, no. 2, pp. 1–10, 2018.

[35] Y. K. Saheed, T. O. Oladele, A. O. Akanni, and W. M. Ibrahim, "Student performance prediction based on data mining classification techniques," *Niger. J. Technol.*, vol. 37, no. 4, p. 1087, 2018, doi: 10.4314/njt.v37i4.31.

[36] H. F. Eid, A. Darwish, A. Ella Hassanien, and A. Abraham, "Principle components analysis and support vector machine based Intrusion Detection System," *Proc. 2010 10th Int. Conf. Intell. Syst. Des. Appl. ISDA'10*, pp. 363–367, 2010, doi: 10.1109/ISDA.2010.5687239.

[37] K. Keerthi Vasan and B. Surendiran, "Dimensionality reduction using Principal Component Analysis for network intrusion detection," *Perspect. Sci.*, vol. 8, pp. 510–512, 2016, doi: 10.1016/j.pisc.2016.05.010.

[38] S. M. Almansob and S. S. Lomte, "Addressing challenges for intrusion detection system using naive bayes and PCA algorithm," *2017 2nd Int. Conf. Converg. Technol. I2CT 2017*, vol. 2017-Janua, pp. 565–568, 2017, doi: 10.1109/I2CT.2017.8226193.

[39] Y. Saheed and A. Babatunde, "Genetic Algorithm Technique In Program Path Coverage For Improving Software Testing," vol. 7, no. 5, pp. 151–158, 2014.

[40] Y. K. Saheed and F. E. Hamza-Usman, "Feature Selection with IG-R for Improving Performance of Intrusion Detection System," *Int. J. Commun. Networks Inf. Secur.*, vol. 12, no. 3, pp. 338–344, 2020.

[41] I. A. Adeniji, "Comparative Analysis of Association Rule Mining Techniques for Monitoring Behavioural Patterns of Customers in a Grocery Store," vol. 8, no. 3, 2015.

[42] F. Chen, Z. Ye, C. Wang, L. Yan, and R. Wang, "A feature selection approach for network intrusion detection based on tree-seed algorithm and k-nearest neighbor," *Proc. 2018 IEEE 4th Int. Symp. Wirel. Syst. within Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. IDAACS-SWS 2018*, pp. 68–72, 2018, doi: 10.1109/IDAACS-SWS.2018.8525522.

[43] H. Benaddi, K. Ibrahimi, and A. Benslimane, "Improving the Intrusion Detection System for NSL-KDD Dataset based on PCA-Fuzzy Clustering-KNN," *Proc. - 2018 Int. Conf. Wirel. Networks Mob. Commun. WINCOM 2018*, pp. 1–6, 2019, doi: 10.1109/WINCOM.2018.8629718.

[44] S. Informatic, K. State, P. Sciences, and Y. O. Olatunde, "a Ap Pp Pl Li Ic Ca At Ti Io on N O of F D Di Im Me En Ns Si Io on Na Al Li It Ty Y R Re Ed Du Uc Ct Ti Io on N O on N C Cl La As Ss Si If Fi Ic Ca At Ti Io on N O of F C Co Ol Lo on N C Ca an Nc Ce Er R U Us Si in Ng G I Ic Ca a a an Nd D K K-N Nn N a Al," vol. X, 2018, [Online]. Available: http://anale-informatica.tibiscus.ro/download/lucrari/16-1-06-Olatunde.pdf.

[45] B. M. Aslahi-Shahri *et al.*, "A hybrid method consisting of GA and SVM for intrusion detection system," *Neural Comput. Appl.*, vol. 27, no. 6, pp. 1669–1676, 2016, doi: 10.1007/s00521-015-1964-2.

[46] Y. K. Saheed, A. O. Akanni, and M. O. Alimi, "INFLUENCE OF DISCRETIZATION IN CLASSIFICATION OF BREAST CANCER DISEASE."

[47] M. A. Oskoei and H. Hu, "Support vector machine-based classification scheme for myoelectric control applied to upper limb," *IEEE Trans. Biomed. Eng.*, vol. 55, no. 8, pp. 1956–1965, 2008, doi: 10.1109/TBME.2008.919734.

[48] Q. Yang, H. Fu, and T. Zhu, "An optimization method for parameters of SVM in network intrusion detection system," *Proc. - 12th Annu. Int. Conf. Distrib. Comput. Sens. Syst. DCOSS 2016*, pp. 136–142, 2016, doi: 10.1109/DCOSS.2016.48.

[49] K. Jimoh, S. Yakub, and M. Alimi, "Colon Cancer Classification and Patients ' Survival Detection Using Support Vector Machine Kernels Colon Cancer Classification and Patients ' Survival Detection Using Support Vector Machine Kernels," no. January 2019, pp. 159–164, 2018.

[50] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," *IEEE Symp. Comput. Intell. Secur. Def. Appl. CISDA 2009*, no. June 2014, 2009, doi: 10.1109/CISDA.2009.5356528.

[51] M. R. Gauthama Raman, N. Somu, K. Kirthivasan, R. Liscano, and V. S. Shankar Sriram, "An efficient intrusion detection system based on hypergraph - Genetic algorithm for parameter optimization and feature selection in support vector machine," *Knowledge-Based Syst.*, vol. 134, pp. 1–12, 2017, doi: 10.1016/j.knosys.2017.07.005.