IDS in IoT using Machine Learning and Blockchain

Nada Abdu Alsharif
Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia
nadaabdu120@email.com (corresponding author)

Shailendra Mishra
Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia
s.mishra@mu.edu.sa

Mohammed Alshehri
Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Saudi Arabia
ma.alshehri@mu.edu.sa

Received: 27 April 2023 | Revised: 17 May 2023 and 22 May 2023 | Accepted: 30 May 2023

 DOI: https://doi.org/10.48084/etasr.5992

ABSTRACT

The rise of IoT devices has brought forth an urgent need for enhanced security and privacy measures, as IoT devices are vulnerable to cyber-attacks that compromise the security and privacy of users. Traditional security measures do not provide adequate protection for such devices. This study aimed to investigate the use of machine learning and blockchain to improve the security and privacy of IoT devices, creating an intrusion detection system powered by machine learning algorithms and using blockchain to encrypt interactions between IoT devices. The performance of the whole system and different machine learning algorithms was evaluated on an IoT network using simulated attack data, achieving a detection accuracy of 99.9% when using Random Forrest, demonstrating its effectiveness in detecting attacks on IoT networks. Furthermore, this study showed that blockchain technology could improve security and privacy by providing a tamper-proof decentralized communication system.

Keywords-IoT; blockchain; cyber security; neural networks; IDS; machine learning

I. INTRODUCTION

The IoT is a cutting-edge innovation with explosive growth, enormous influence, and great promise. IoT refers to a network of devices that share data to enable new applications. IoT devices exist in a variety of shapes and sizes, ranging from low-power equipment to smart objects. Using IoT, processes can be automated, saving time and money. Instruments, cameras, and other IoT devices frequently collect data that are then transmitted to a server for evaluation and tracking. The quality of the information stored on the server should be maintained in a way to prevent malicious attempts to modify the data, while other individuals and systems must always have access to the data [1]. The expansion of IoT networks has led to a growth in the number of IoT devices, with an estimated increase from 7.74 in 2019 to 25.44 billion in 2030. The fundamental issue with these gadgets is that security is generally not taken into consideration, as the login and password are often not modified during deployment. So, IoT devices have become the primary target of attackers, as they attempt to breach them to launch Distributed Denial-of-Service (DDoS) attacks or use them as botnets to steal data [2]. This is evident from the estimated 105 million attacks on IoT devices in the first half of 2019. Various authentication methods, architectural designs, and algorithms have been proposed that take into account the resource constraints of IoT devices [3-4].

IoT networks are frequently linked to cloud computing and data centers. As IoT devices typically generate a large amount of data, various algorithms are used to extract important information and automate processes. Machine Learning (ML) techniques are also used to create Intrusion Detection Systems (IDSs). Data from IoT devices are often transferred to servers where they are stored before being examined [5]. Typically, data should be kept in a way that protects their integrity and thwarts hostile attempts to alter them while being constantly accessible to other users and systems. Data can be stored securely using blockchain (BC) [3]. The possibility of combining ML methods and BC approaches to address cyber

risks in the IoT area is a new concept that warrants further investigation. Security and privacy are interconnected, and privacy is a collection of rules that vary depending on the application [5].

BC is made up of a series of linked blocks. The hash code of the preceding block is included in each new block when inserted. The header of the block includes the timestamp, the preceding block's hash, the block's hash code, and additional data. Transactions make up the body of the block, which contains most of the BC data [6]. BC has attracted a lot of interest in addressing security issues in numerous systems, including banking, voting, education, etc. [7]. Although the use of BC in IoT systems has numerous benefits, such as decentralization, security improvement, tractability, and immutability, its implementation presents some difficulties. In [8], some of these issues were described when using BC with IoT, such as storage, scalability, and vulnerabilities. Corrupted data saved in BC is one of the vulnerability problems, due to the immutability of BC. Thus, corrupted data must be detected before being transferred and stored in the BC. Such corrupted data typically originate from infected devices. However, since BC must contain a substantial amount of data and must be scalable, IoT uses a proof-of-authority consensus process. In contrast to the proof-of-work approach, this algorithm does not require additional computing to answer a mathematical problem [9].

It is crucial to identify the challenges and threats that these systems face and the potential consequences if they are not addressed. The distributed and resource-constrained nature of IoT systems presents significant challenges in detecting and preventing attacks. Attackers are becoming more sophisticated, making it easy to bypass traditional security measures, and the generation of massive amounts of data from IoT devices raises privacy and security risks. The consequences of failing to address these challenges could be severe, including unauthorized access to sensitive data, disruption of critical services, financial losses, and damage to the reputation of organizations that deploy IoT systems [10]. To address these challenges, innovative solutions, such as the combination of ML and BC techniques, can significantly improve the effectiveness and efficiency of IDSs in IoT. Such solutions could help mitigate the potential consequences of security breaches by providing more robust and effective security measures [11].

The network architecture is constructed for a reputation transfer mechanism, adopted for the reputation value performance analysis system. Usually, the network architecture uses low-power IEEE 802.11 Wi-Fi for data communication [12]. Effective internet communication is structured with a monitoring system, cloud computing, a server, and a database management system. The network server is connected through a firewall and accepts details, while operations are processed through virtual servers and data centers [13]. Traditional security measures face challenges in detecting and preventing attacks due to the distributed and resource-constrained nature of IoT systems. To address these challenges, innovative solutions are needed, such as the combination of ML and BC technology [14]. A proof-of-authority process can be used to ensure scalability and efficient data handling, as this algorithm eliminates the need for additional computing to answer a mathematical problem compared to the proof-of-work approach. Several studies explored the potential benefits and drawbacks of using ML and BC in IDSs for IoT and aimed to assess their effectiveness in improving security and privacy. The objectives included comparing the performance of ML and blockchain-based IDS with traditional approaches, suggesting viable solutions to security and privacy vulnerabilities, evaluating the impact of adversarial attacks on ML algorithms, and assessing the effectiveness of combining ML and BC with other security methods [15].

This study aims to contribute to the development of a more secure and reliable IoT ecosystem while addressing potential security and privacy concerns that may arise. This study aims to assess the effectiveness of using ML and BC for IDS in IoT devices. The main purpose was to examine the benefits and drawbacks of using ML and BC in IDS for IoT, as well as potential anonymity and safety risks. The primary objectives are to:

- Compare the performance of ML and BC in IDS for IoT devices with traditional IDS approaches.
- Identify and suggest viable solutions to the security and privacy vulnerabilities raised by the use of ML and BC in IDS for IoT.
- Examine the possible impact of adversarial attacks on ML algorithms and find techniques to defend against such attacks.
- Assess the impact of combining ML and BC with other security methods, such as encryption and access control, in the development of holistic security solutions for IoT systems.
- Contribute to the development of a more secure and reliable IoT ecosystem by exploring the potential of using ML and BC in IDS, while also addressing potential security and privacy concerns that may arise.

II. LITERATURE REVIEW

Several studies explored the challenges and vulnerabilities in IoT systems, such as the lack of security measures and the susceptibility of devices to attacks. In [16], a widespread IDS was proposed that used fog computing to detect DDoS attacks against edge nodes in BC-based IoT networks. The system's efficacy was assessed using an actual IoT-based dataset that included current assaults in BC-based IoT networks. Random Forest (RF) and XGBoost trained on dispersed fog nodes were used to measure performance. XGBoost beat RF in binary attacks, whereas RF exceeded XGBoost in terms of multi-attack detection. Furthermore, compared to XGBoost, RF needed less time for instruction or testing on dispersed fog nodes. In [17], pattern recognition, AI, and BC were examined to address IoT security challenges, highlighting the security concerns that can be handled using them and the research obstacles that must be addressed. In [18], a random subspace learning KNN was used to protect against forged commands aiming at manipulating an industrial control process, and a BC-

based Integrity Checking System (BICS) was used to prevent misrouting attacks that alter the OpenFlow rules of SDN-enabled industrial IoT systems. In [19], an IDS based on neural network clustering was proposed to help administrators identify and reduce the risk of attacks in the early stages, reducing power consumption. The RP protocol has a clear objective and enables real-time applications to conserve energy while ensuring security. Increasing the number of online applications that require protection against different risks, the demand for security will only increase. An ML system was proposed to address the nonlinear identity problem, detect faults, and reconstruct the system. To detect and classify malicious attacks on network integrity and node power consumption in a wireless sensor network, a self-organizing map could be trained to monitor the network using a learning technique and identify any nodes that behave abnormally. In [20], the possible uses and limitations of distributed ledger technology were explored in domains that interact with social impacts, including social justice and concerns.

There is a research gap that lies in the security issues related to IDS in the IoT when using ML and BC. While ML and BC offer potential benefits in enhancing the security and privacy of IoT devices, there are security concerns that need to be addressed to ensure the effectiveness of IDS. One specific security challenge is the potential for adversarial attacks on ML algorithms. Adversaries can manipulate the input data to cause misclassification or other errors in the ML model. This can lead to IDS failing to detect intrusions or flag benign behavior as malicious. Techniques such as adversarial training and input sanitization can be employed to mitigate these attacks and improve the robustness of the ML model. Previous studies have shown that ML algorithms can effectively detect anomalous behavior in IoT devices, making them suitable for IDS applications.

A major challenge is that ML algorithms require large amounts of data to train effectively. This can be a problem in the context of IoT, as devices may have limited processing and storage capabilities. Furthermore, ML algorithms may be vulnerable to attacks that can be used to fool the algorithm into making incorrect predictions [21]. Another challenge is to develop a system that can efficiently and securely store the ML algorithms to the of data required for slarge amount work effectively. Additionally, more research is needed on how to effectively integrate ML algorithms with BC in the context of IoT [22]. Future research should focus on developing efficient and secure data storage systems and explore ways to integrate ML in IoT BC algorithms with [23].

III. RESEARCH METHODOLOGY

A. *System Design*

The proposed system was designed to improve the security of IoT devices using ML and BC to detect and prevent intrusions and preserve the integrity of the data generated by these devices. The system consists of four main components: IoT devices, an IDS, BC nodes, and the BC network. IoT devices are responsible for collecting data from the environment and sending it to the IDS. The IDS is the first line of defense against intrusions, and its primary function is to identify any compromised devices and remove any corrupt data. The IDS was powered by ML algorithms to detect unusual patterns in the data generated by IoT devices. This allows the IDS to distinguish normal and abnormal data and identify devices that are compromised or behave suspiciously.

When the IDS has filtered the regular data, they are forwarded to the BC nodes. These nodes encrypt the data and send them to the BC network. The BC network is public, accepts signed data from the BC nodes, and creates a block containing the data. The BC network ensures that data are authentic and irrevocable and provides a decentralized architecture for IoT devices, improving data preservation security. BC networks are in charge of validating the data and ensuring that only legitimate data is uploaded to the BC network. This is achieved by using cryptography, such as cryptographic algorithms and SHA256. The BC servers are also in the position of safeguarding the BC network by verifying new blocks and keeping the network safe. The suggested solution for intrusion prevention in IoT intends to improve IoT device security by identifying and blocking intrusions and protecting the integrity of data generated by these devices.

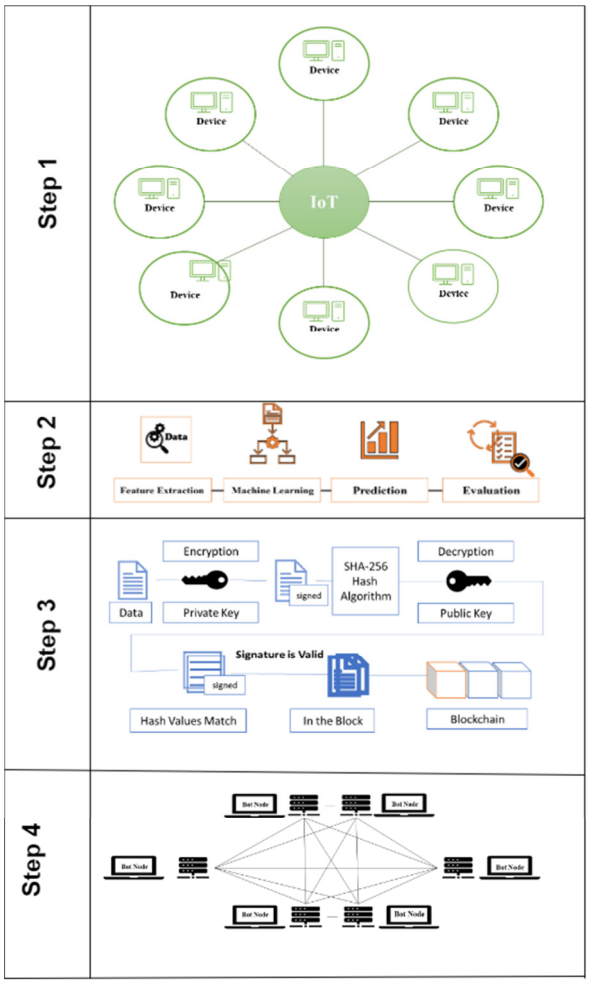

Fig. 1. System design.

B. Proposed IDS using ML and BC (IDS-MLBC)

An IDS can employ a variety of ways to identify assaults in IoT networks. For example, the signature-based strategy identifies attacks based on certain characteristics or patterns in network traffic. Signature-based intrusion detection systems are excellent at identifying attacks with attack patterns, but they may fail to detect new or undiscovered malware assaults because their structures or signatures are not yet recognized. Anomaly-based techniques were developed to alleviate this restriction using ML algorithms to provide a reliable activity model. Any traffic that does not match this model is deemed suspicious and labeled as a possible attack. As they do not rely on existing signatures, anomaly-based IDS can identify fresh or undiscovered malware threats. Furthermore, as ML-based algorithms may be taught on a variety of applications and hardware configurations, they offer higher generalization features. The initial component of the platform are the IoT devices that collect data and transfer them to the IDS for analysis. The IDS is responsible for identifying infected devices and removing damaged data. Various ML methods were chosen for this procedure, based on their prominence and time efficiency. The proposed framework offers several advantages over traditional security measures. First, the use of ML algorithms allows the detection of compromised devices with high accuracy and efficiency, minimizing false positives and negatives. Second, the use of BC improves the security of data storage in a decentralized manner, making it more resistant to attacks. Finally, the use of feature selection techniques allows for the identification of the most important features to detect compromised devices, improving the efficiency of the IDS.

C. IDS Algorithm

The IDS algorithm consists of the following steps:

- Step 1: Collect data from IoT devices.
- Step 2: Check if the device is compromised using an ML-based IDS.

  If the device is compromised:

  Filter corrupted data.

  else:

  Sign data using public key cryptography.
- Step 3: Add signed data to BC nodes.
- Step 4: Train a machine learning model using relevant features to detect compromised devices.
- Step 5: Use the trained model to predict if a device is compromised based on collected data.
- Step 6: If the reputation value (Rv) equals 0 to n:

  Create a New Transaction (NT) with an attached reputation value: NT(Rv).
- Step 7: If Rv equals Rv-1, terminate.
- Step 8: Validate the block for NT(Rv).
- Step 9: Verify all values of the transaction.
- Step 10: If NT(Rv) is greater than 1:

  Insert a new transaction NT(Rv).
- Step 11: End.

IV. EXPERIMENTAL SETUP

A. Setup for Investigation

This model was implemented in Jupyter Notebook format, along with the code used to obtain the results. The model was implemented in Python [21]. The following steps were used to implement the ML-based IDS in IoT:

- Collect and preprocess the dataset: This step involved collecting data from IoT devices and pre-processing it to remove any noise or outliers. The pre-processed data were then split into training and testing sets.
- Design the neural network architecture: This step involved selecting the appropriate neural network architecture, such as a feedforward or a convolutional neural network. The number of layers and nodes in each layer were also determined in this step.
- Train the neural network: This step involved using the training set to train the neural network. The weights and biases of the network were adjusted during this process to minimize the error between the predicted and actual output.
- Evaluate the neural network: This step involved evaluating the performance of the trained neural network on the testing set. Metrics such as accuracy, precision, recall, and F1-score can be used to evaluate the performance.

B. Machine Learning for IDS

1) Dataset

NSL-KDD is a network intrusion detection dataset, which is an improvement over the original KDD Cup '99 dataset. The NSL-KDD dataset has been modified to remove redundant records and balance the number of records in each category. It is a widely used dataset in studies related to network IDSs [24]. The NSL-KDD dataset contains various features related to network traffic, such as the number of bytes and packets transmitted, the protocol used, and the source and destination IP addresses. It also contains various attack categories, including Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R).

2) Model Evaluation and Validations

The accuracy, precision, recall, and F1-score metrics were used. Accuracy measures correctly classified instances, while precision and recall measure true positives and false negatives, respectively. The F1-score is the harmonic mean of precision and recall and provides a more balanced measure of performance.

3) Machine Learning

The validation procedure involves training the model on a training set, evaluating its performance on a separate testing set using appropriate evaluation metrics, and potentially

employing additional validation techniques to ensure the reliability and effectiveness of the developed models. Linear Regression (LR) is a simple and commonly used method for predictive modeling and works by finding a linear relationship between the independent and dependent variables and then using it to make predictions.

TABLE I. THE NSL KDD DATASET

Dataset	Number of Records					
	Total	Normal	DoS	Probe	U2R	R2L
KDDTrain+20%	25192	13449 (53%)	9234 (37%)	2289 (9.16%)	11 (0.04%)	209 (0.8%)
KDDTrain+	125973	67343 (53%)	45927 (37%)	11656 (9.11%)	52 (0.04%)	995 (0.85%)
KDDTest+	22544	9711 (43%)	7458 (33%)	2421 (11%)	200 (0.9%)	2654 (12.1%)

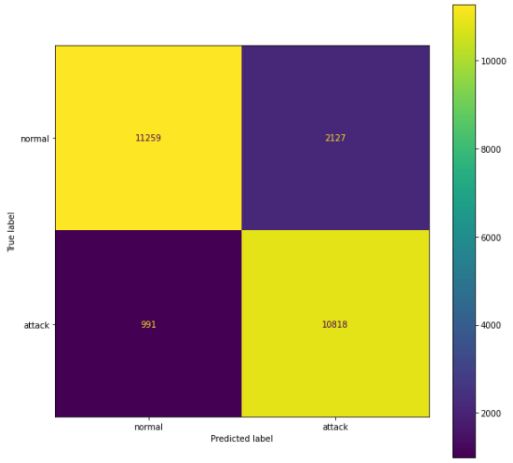

Fig. 2. LR result.

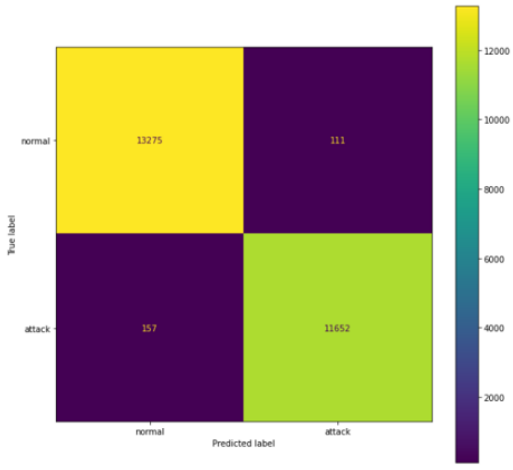

Fig. 3. KNN result.

The K-Nearest Neighbors (KNN) is a non-parametric ML algorithm that can be used for classification and works by finding the K closest data points to a given input and using the majority vote or averaging their output values to make a prediction. The Decision Tree (DT) is a popular ML algorithm for both classification and regression that uses a flowchart-like structure to represent different decisions and their possible consequences. Random Forest (RF) is an ensemble learning algorithm that uses multiple decision trees to improve the accuracy and robustness of predictions. It works by training multiple decision trees on random subsets of the data and then combining their outputs to make a final prediction. Support Vector Machines (SVM) is a powerful ML algorithm for classification and regression problems that works by finding the optimal hyperplane that separates the different classes of data points in a high-dimensional space.

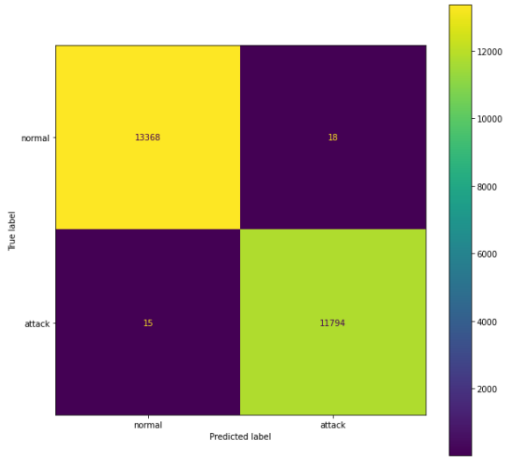

Fig. 4. DT result.

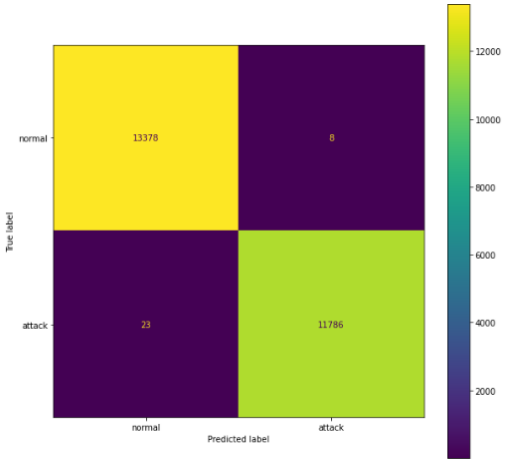

Fig. 5. RF result.

The model consisted of five densely connected layers with different numbers of neurons, nonlinear activation functions, and dropout regularization to prevent overfitting. The first layer had 64 neurons, followed by two more hidden layers with 128 and 512 neurons, respectively. All these layers have the Rectified Linear Unit (ReLU) as the activation function. The output layer had a single neuron, which used the sigmoid activation function to produce a binary classification result. In addition, the model used L1L2, L2, and activity regularization techniques to reduce overfitting, which are commonly used for this reason. L1L2 regularization applies both L1 and L2 regularizations to the model, whereas L2 regularization adds

the square of the weights to the loss function, and activity regularization adds a penalty to the activation values to encourage the network to produce more sparse representations. Overall, this model is a powerful tool for binary classification problems, as it can learn complex patterns from the data and produce accurate predictions on unseen data.

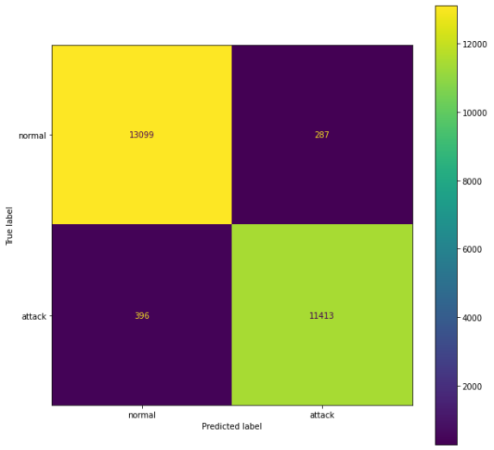

Fig. 6. SVM result.

V. RESULTS

To evaluate the performance of the proposed ML and BC-based IDS, several models were trained and tested on an IoT traffic dataset. Table II presents the results of the comparison.

TABLE II. MACHINE LEARNING MODEL COMPARISONS.

Model	Accuracy	Recall	precision
LR	87.6%	91.80%	83.81%
KNN	99.05%	98.73%	99.22%
Naïve Bayes	91.80%	89.47%	92.62%
SVM	97.48%	96.70%	97.85%
DT	99.90%	99.98%	99.84%
RF	99.99%	99.99%	99.99%
NN	97.53%	97%	97%

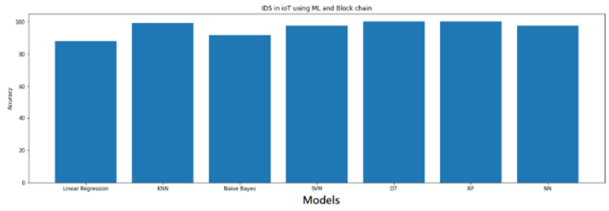

Fig. 7. The accuracy of the models.

The LR model had an accuracy of 87.60%, KNN had 99.05%, NB had 91.80%, SVM had 97.48%, DT had 99.90%, RF had 99.99%, and NN had 97.53%. For LR, the precision was 83.81% and recall was 91.80%. Similarly, KNN had a precision of 99.22% and recall of 98.73%, NB had a precision of 92.62% and recall of 89.47%, SVM had a precision of 97.85% and recall of 96.70%, DT had a precision of 99.84% and recall of 99.98%, RF had a precision of 99.99% and recall of 99.99%, and NN had a precision of 97% and recall of 97%. Figure 7 illustrates the accuracy of the models.

VI. DISCUSSION

The results of using RF for intrusion detection in IoT systems are impressive, with a 99.9% accuracy score. This highlights the potential of this ML algorithm to improve the security of IoT systems by detecting and preventing intrusions. The challenge for an ML-based IDS is the potential for data poisoning attacks, where attackers inject malicious data into the training dataset to manipulate the behavior of the ML model. Data poisoning attacks can also compromise the integrity and reliability of the system by inducing false positives or negatives. To mitigate these threats, a range of countermeasures can be employed, including data sanitization and validation, model robustness testing, and model interpretability and transparency. In addition, the integration of blockchain technology can enhance the security and privacy of ML-based IDS by providing a decentralized and tamper-proof data management framework. The RF model achieved higher accuracy than the NN models from previous studies, as the RF is an ensemble of DTs which are relatively simple models that are easy to train and interpret. By combining many DTs, the RF model can capture complex patterns in the data without overfitting, which can lead to high accuracy.

TABLE III. RESULTS COMPARISON WITH OTHER STUDIES

Study	Method	Accuracy
[17]	K-Means + RF and Deep Learning	85%
[18]	DNN binary	96%
[19]	DSSTE method	82%
This study	RF	99.99%

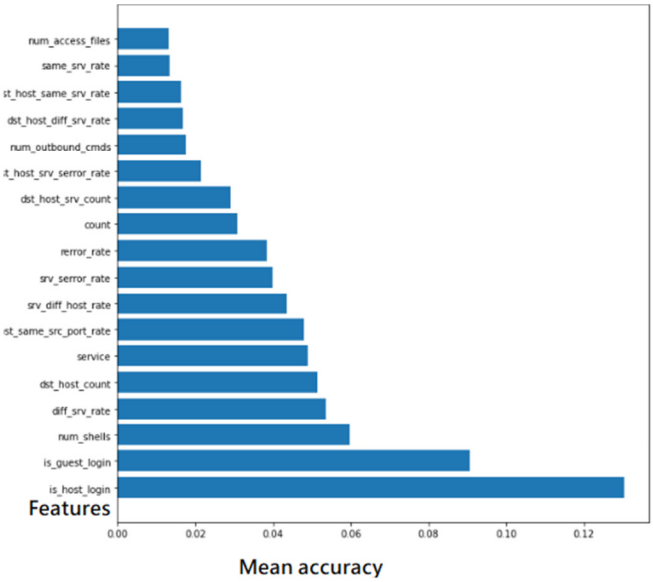

Fig. 8. RF features.

The use of ML and blockchain technology in IoT security can provide effective solutions to detect and prevent intrusions. However, the security and privacy threats associated with these technologies need to be carefully considered and addressed through a comprehensive and holistic approach that takes advantage of the strengths of different countermeasures and technologies. The adoption of hybrid approaches that combine

ML algorithms with blockchain-based data management and access control mechanisms can provide a robust and effective solution to IoT security challenges. Future plans involve exploring different ML algorithms, evaluating using diverse datasets, enhancing robustness against adversarial attacks, addressing scalability and resource constraints, and further integrating BC technology. These steps will contribute to advancing the progress of the research and addressing the limitations to improve the effectiveness and practicality of ML-based intrusion detection in IoT systems.

VII. CONCLUSION AND FUTURE WORK

The rise of IoT devices has led to concerns about their security. One potential solution to these issues is the integration of ML and BC. This study compared various approaches and recommended the use of the Random Forest algorithm for intrusion detection in IoT systems. The security of IoT systems can be improved by combining ML algorithms with BC-based data management and access control mechanisms,. The proposed algorithm achieved an accuracy of 99.99%, highlighting the potential of ML to improve IoT security. This study suggested several potential directions for future research. One possibility is to explore new techniques and approaches to enhance the development of ML algorithms for intrusion detection in IoT systems. Furthermore, it is important to evaluate the performance of different ML algorithms and BC-based solutions under real-world conditions to test their effectiveness. In the future, further studies could investigate the development of ML algorithms for intrusion detection and prevention in IoT systems. Although the Random Forest algorithm achieved high accuracy, new techniques and approaches can be explored to improve the performance and efficiency of IDS.

REFERENCES

[1] M. Anwer, S. M. Khan, M. U. Farooq, and Waseemullah, "Attack Detection in IoT using Machine Learning," *Engineering, Technology & Applied Science Research*, vol. 11, no. 3, pp. 7273–7278, Jun. 2021, https://doi.org/10.48084/etasr.4202.

[2] T. Alqurashi, "Arabic Sentiment Analysis for Twitter Data: A Systematic Literature Review," *Engineering, Technology & Applied Science Research*, vol. 13, no. 2, pp. 10292–10300, Apr. 2023, https://doi.org/10.48084/etasr.5662.

[3] P. Singh, Z. Elmi, V. Krishna Meriga, J. Pasha, and M. A. Dulebenets, "Internet of Things for sustainable railway transportation: Past, present, and future," *Cleaner Logistics and Supply Chain*, vol. 4, Jul. 2022, Art. no. 100065, https://doi.org/10.1016/j.clscn.2022.100065.

[4] H. Liu and B. Lang, "Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey," *Applied Sciences*, vol. 9, no. 20, Jan. 2019, Art. no. 4396, https://doi.org/10.3390/app9204396.

[5] N. Behar and M. Shrivastava, "A Novel Model for Breast Cancer Detection and Classification," *Engineering, Technology & Applied Science Research*, vol. 12, no. 6, pp. 9496–9502, Dec. 2022, https://doi.org/10.48084/etasr.5115.

[6] R. Doshi, N. Apthorpe, and N. Feamster, "Machine Learning DDoS Detection for Consumer Internet of Things Devices," in *2018 IEEE Security and Privacy Workshops (SPW)*, Feb. 2018, pp. 29–35, https://doi.org/10.1109/SPW.2018.00013.

[7] A. Rahman *et al.*, "On the Integration of Blockchain and SDN: Overview, Applications, and Future Perspectives," *Journal of Network and Systems Management*, vol. 30, no. 4, Sep. 2022, Art. no. 73, https://doi.org/10.1007/s10922-022-09682-4.

[8] A. Rahman *et al.*, "Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions," *International Journal of Communication Systems*, 2023, Art. no. e5429, https://doi.org/10.1002/dac.5429.

[9] O. O. Mohammed, M. W. Mustafa, D. S. S. Mohammed, and A. O. Otuoze, "Available transfer capability calculation methods: A comprehensive review," *International Transactions on Electrical Energy Systems*, vol. 29, no. 6, 2019, Art. no. e2846, https://doi.org/10.1002/2050-7038.2846.

[10] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta, S. Garg, and M. M. Hassan, "A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network," *Journal of Parallel and Distributed Computing*, vol. 164, pp. 55–68, Jun. 2022, https://doi.org/10.1016/j.jpdc.2022.01.030.

[11] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2020, https://doi.org/10.1109/COMST.2019.2953364.

[12] S. M. Basha, D. Rajput, and V. Vandhan, "Impact of Gradient Ascent and Boosting Algorithm in Classification," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 1, pp. 41–49, Feb. 2018, https://doi.org/10.22266/ijies2018.0228.05.

[13] R. Darwin, "Implementation of Advanced IDS in Contiki for Highly Secured Wireless Sensor Network," *International Journal of Applied Engineering Research13*, vol. 13, no. 6, pp. 4214–4218, 2018.

[14] "The Internet of Things (IoT)," *Canadian Journal of Nursing Informatics*, vol. 13, no. 1, 2018.

[15] S. M. Basha and D. S. Rajput, "Chapter 9 - Survey on Evaluating the Performance of Machine Learning Algorithms: Past Contributions and Future Roadmap," in *Deep Learning and Parallel Computing Environment for Bioengineering Systems*, A. K. Sangaiah, Ed. Academic Press, 2019, pp. 153–164.

[16] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, "Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology," *Internet of Things*, vol. 11, Sep. 2020, Art. No. 100227, https://doi.org/10.1016/j.iot.2020.100227.

[17] A. Derhab *et al.*, "Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security," *Sensors*, vol. 19, no. 14, Jan. 2019, Art. no. 3119, https://doi.org/10.3390/s19143119.

[18] E. Kfoury, J. Saab, P. Younes, and R. Achkar, "A Self Organizing Map Intrusion Detection System for RPL Protocol Attacks," *International Journal of Interdisciplinary Telecommunications and Networking (IJITN)*, vol. 11, no. 1, pp. 30–43, Jan. 2019, https://doi.org/10.4018/IJITN.2019010103.

[19] N. Waheed, X. He, M. Ikram, M. Usman, S. S. Hashmi, and M. Usman, "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures," *ACM Computing Surveys*, vol. 53, no. 6, Sep. 2020, Art. no. 122, https://doi.org/10.1145/3417987.

[20] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020, https://doi.org/10.1109/COMST.2020.2986444.

[21] "Welcome to Python.org," *Python.org*, May 29, 2023. https://www.python.org/.

[22] *Python.org*, May 29, 2023. https://www.python.org/.

[23] M. Baz, "SEHIDS: Self Evolving Host-Based Intrusion Detection System for IoT Networks," *Sensors*, vol. 22, no. 17, Jan. 2022, Art. no. 6505, https://doi.org/10.3390/s22176505.

[24] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020, https://doi.org/10.1109/ACCESS.2020.2972627.