Anomaly Detection Algorithm with Blockchain to Detect Potential Security Attacks in the IIoT Model of Industry 5.0

Piyush Pant[1], S. B. Goyal[2(✉)], Anand Singh Rajawat[1], Amol Potgantwar[3], Pradeep Bedi[4], and Chawki Djeddi[5]

[1] School of Computer Sciences and Engineering, Sandip University, Nashik, India
[2] Faculty of Information Technology, City University, 46100 Petaling Jaya, Malaysia
drsbgoyal@gmail.com
[3] Sandip Institute of Technology and Research Center, Nashik, India
[4] Galgotias University, Greater Noida, India
[5] Laboratoire de Vison et d'intelligence Artificielle, Université Larbi Tebessi, Tébessa, Algérie

Abstract. The research presents a model for detecting potential security attacks in the Industry 5.0's Internet of Things (IIoT) model using an Anomaly Detection Algorithm, with Blockchain technology to further enhance security. One-class Support Vector Machines (SVM) is used as the Anomaly Detection Algorithm, to identify any unusual behavior in the IIoT system. The proposed model ensures the integrity of data by implementing the decentralized features of Blockchain technology. This paper aims to address the current security challenges faced by Industry 5.0 and enhance the reliability of the IIoT model. Since Industry 5.0 is not here yet, hypothetical data is used to train the model which is generated after seeding using Numpy. The Blockchain technology enhanced the overall security of the Industrial Internet of Things (IIoT) model whereas, to secure it even further by detecting anomalous activities, the machine learning algorithm is proposed. Anomaly detection algorithm with Gaussian distribution is proposed through One-class SVM. The threshold for an activity to be classified as unusual or anomalous is discussed in the paper along with the difference between classification algorithm and anomaly detection algorithm. The research implemented One-class SVM algorithm to train the model by randomly seeding data using Numpy with an average accuracy of 92.8% after 5 different runs with different datasets. The algorithm also focused on other applications of the model like detection of faulty driver, device, or equipment.

Keywords: Artificial Intelligence · Machine learning · Blockchain · IIoT · Industry 5 · Anomaly Detection Algorithm · Gaussian distribution

1 Introduction

The existing technologies and models are being upgraded to new levels because of the improvement in some of the technologies like Artificial Intelligence, Blockchain, IoT, etc. Most of the domains are grateful to these technologies as their flow is dependent on

A. Ortis et al. (Eds.): ICAETA 2023, CCIS 1983, pp. 175–188, 2024.
https://doi.org/10.1007/978-3-031-50920-9_14

them. The world is stepping into a new world where the interaction between humans and machine will increase drastically. Even a lot of places like restaurants, stadiums, clubs, etc. are using varieties of machines to ease their work and labour. In the research, the trending, powerful and futuristic technologies are studied along with implementation of the integration. The aim of the research is to provide the security and is useful for the next industry and also for any major model that deals with sensitive data and requires an advanced security model.

Internet of Things (IoT) is everywhere these days, however, it is not the best version of its true capability. As the device communication increase, the network needs to be stronger and after that comes the model power of the device, which is, is it able to communicate well and perform the task well for which it is made. Improving the IoT would surely solve these issues. IoT are classified in various category mostly based on their applications like IoNT, IIoT, etc. In this study, we will focus on the Industrial Internet of Things (IIoT). As its name says, it is an extension of the IoT which is primarily developed for the industrial application. Since we are on the verge from going to Industry 5.0 from Industry 4.0, we could only reach after some major improvements in the IoT. The device-to-device communication can be made faster by using networks like 5G or 6G [1], but its security cannot be guaranteed. Moreover, as the IoT will replace all traditional tools and will spread in every home all over the world, one weak frame or loophole will let the hacker get access to all the devices and its data, which would be a disaster. Therefore it is the need of the model to be secure. In the further sections, the paper discusses how the security can be implemented in the model along with making it intelligent to detect any kind of bugs, objects, etc. that might harm the system [3].

Blockchain technology is considered as an ideal system for security and it does stand up to its reputation. It is a decentralized system, which means that the authority or power is not central (controlled by one who could modify for selfish reasons), but distributed. All the changes are tracked in the system which makes it one of the most organized too. One of the most important feature it has is its ability to encrypt the data and store it in that form, it cannot be changed back to normal without the correct algorithm and methods. Encryption is a major part of the blockchain but this is not the only ability it has, one of the most impressive and the one from where it got its name is the “chains” of blocks. Each block stores the address of the previous hash and so on, this makes a chain of block and so comes the name Blockchain. The research proposes the blockchain for the IIoT model to improve its security at its best [10]. The research proposes blockchain with 256-bit AES encryption method. This would contribute to a better understanding of AI and Blockchain integration in the real world.

Artificial intelligence, often referred to as AI is one of the most powerful technology on the planet if not the best. It is often seen as the future of humankind. However, the development of AI is not enough for it to be called truly intelligent. Artificial intelligence is a broad term and there are its sub field which are its main core, they are machine learning and deep Learning. Machine learning is implemented by the research to detect the anomaly. Now to dive into the machine learning domain, there are mainly two types – Supervised learning and Unsupervised learning [3]. Just alongside of Unsupervised learning, lies another subtypes like Recommender systems, Dimensionality reduction, etc. and this is the domain where the Anomaly detection algorithm belongs to [11].

Anomaly detection means to detect those objects, entities or things which are not usual or which are different than the rest of their own. For example, in a pride of 20 lions, there is a black lion (a very rare specimen), this is a small and easily detected example, 100000 batteries with full charge but 11 of them are faulty as they do not have any charge. These are examples of anomalies in the data, and the detection of these anomalies is called as Anomaly detection which could be based on Visuals or its features from the rest. One important thing to note here is that the anomalies are different than classification. The paper discusses it in later sections, how they are both different and why do we actually need the anomaly detection algorithm if we already had the classification algorithm. The upcoming sections also gives the detailed implementation of the algorithm along with the theoretical concepts of the anomaly detection algorithm.

The advent of Industry 5.0 has brought about a new wave of innovation in the field of industrial internet of things (IIoT). With increasing digitization of industrial processes, the need for securing these systems has become a top priority. Anomaly detection algorithms play a crucial role in identifying potential security threats in IIoT systems. This paper presents an innovative approach to anomaly detection by combining the robustness of blockchain technology with the power of one-class support vector machines (SVM). The proposed system uses blockchain to store and verify the authenticity of the data, while one-class SVM is used to detect anomalies in the data. The proposed system aims to improve the accuracy and security of anomaly detection in the IIoT model of Industry 5.0, thus preventing potential security attacks.

2 Related Work

Various research that were based on the same technologies as this paper were studied and below is the discussion of some of the references.

P. Pant et al. [1], research is based on Artificial intelligence and blockchain integration with IIoT in the 5G environment of industry 5.0. The research proposed the supervised learning algorithm like multivariate linear regression and Artificial Neural Network for the IIoT. This research presents future work as it proposes the unsupervised learning algorithm for the IIoT as a security purpose.

W. Liu et al. [11], an architecture based on a dual-threaded blockchain was suggested in this paper to identify large-scale abnormalities in intelligent networks. Then, an adaptive encoder is used to implement anomaly detection. The research used blockchain on intelligent network and then the anomaly detection. Our research implements the blockchain for real-time data security and then the anomaly detection is added as a secondary layer of security to detect any kind of potential security attacks.

Z. Il-Agure et al. [13], paper proposed a link mining tool for the blockchain that is based on anomaly detection. This is for the IoT devices which had the blockchain network. Our research implements the optimized anomaly detection algorithm for the IIoT that is using blockchain for real-time data security.

M. Signorini et al. [14], presented a framework called as BAD (Blockchain Anomaly Detection). This framework was focused to reduce the false positive rate of the output. The goal was to detect the anomalies in the blockchain based system with a reduction in the false positive result. Our research fills the research gap and proposes a model that is practical as it is implemented for the IIoT.

The concepts of machine learning especially anomaly detection algorithm which were put forward by Andrew NG were studied by the author and they are grateful for the mathematical concept taught by him in his courses.

3 Proposed Methodology

In this section, the implementation of the Anomaly detection algorithm along with its theoretical concept is discussed. After that the blockchain integration is studied as well.

3.1 Understanding the Security Problem in IIoT

IIoT is definitely the future and the medium for human-machine interaction. The security attacks would be much easier and dangerous as there could be increase in devices, networks and models, and so in the weak spots as well. First we need to understand how the interaction between humans and machine would take place, refer the Fig. 1.

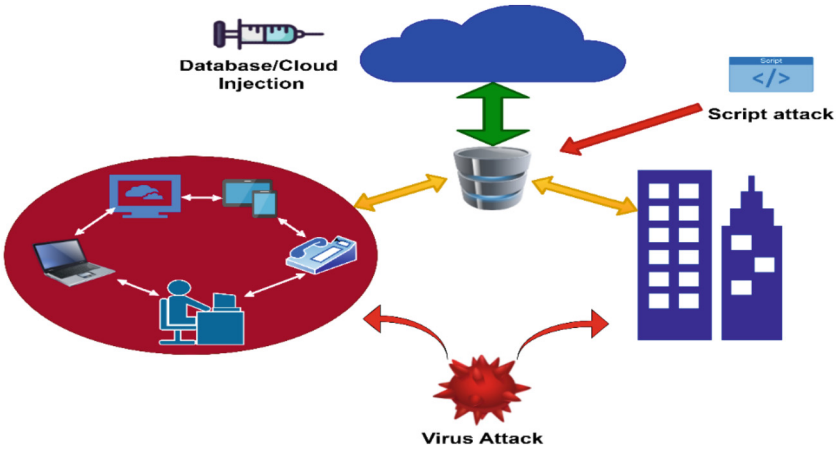

Fig. 1. Security attacks in IIoT

The attackers could inject scripts of malicious code that would alter the original program, they could inject any kind of virus to shut system or even Database injection to get access of the database. The network hijacking is also possible which would allow the hacker to get access to all the devices and communications [20]. All of these attacks could be handled and detected earlier and be dealt with. The data would be the main target of the attacker, so the blockchain would keep it secure and make sure that there are no contacts with the data blocks from unauthorized party. The machine learning, on

the other hand would hinder such attacks to happen as it would be different from the rest of the program.

3.2 Why Anomaly Detection Algorithm? Why Not Classification?

To detect any malicious and faulty activity beforehand, the anomaly detection algorithm will be used in the model. To some people, the anomaly detection algorithm might look similar to classification but they are not. Even some may suggest to use classification to classify the anomalies but this would not be optimal.

First thing to understand is that anomalies are quite rare that is, refer Eq. (1)

$$number\ of\ anomalies \ll number\ of\ normal\ objects \tag{1}$$

Second thing is that, the anomalies and normal objects are same and they belong to a same group, however they differ in some property or performance due to their faulty nature, which makes them anomalous. Although the implementation and concept may look similar but the meaning is totally different, hence there is an algorithm for anomaly detection.

For classification, the main idea is to classify various ungrouped objects into a group or a category, example could be, among 1000 animals, classify them as 'cat' or a 'dog'. Now both are different species and hence would belong to a different group. This is classification, however, let's say that in a pack of 1000 dogs, there are 2 different species animals we need to find, this is an anomaly and hence the difference in the concept.

Thirdly, for classification, we already know the number of classes or category and we know all the dataset would go in one of the category. But, for anomaly, we don't know if there is any anomaly, that is why it is unsupervised learning. It is also crucial to understand that the dataset is unlabelled for anomaly detection algorithm whereas the classification requires labelled dataset.

3.3 Requirements for the Model

Before the development of model start, our system needs to be ready to take the load and process the model. The below Table 1 describes the technologies and requirements for the algorithm to be implemented.

Table 1. Requirements for the model

Model Requirements	Solutions/Fulfilments
Programming language	Python (Recommended), R
System RAM	At least 4 GB RAM is recommended, 4+ would be great as larger amount of data could be trained faster
IDE	Anaconda Navigator, Jupyter notebook, VS code, Python IDE – This would be the choice of the developer
Libraries (For Python)	Numpy, Pandas, Matplotlib, Seaborn, Sklearn, etc.
Conceptual knowledge	Probability, Statistics, Linear Algebra, Programming in python, Data Structures, Gaussian Distribution, Threshold, etc.
Data	Data should be cleaned (If not clean, then must be pre-processed), In CSV or excel

3.4 Threshold for an Anomaly

As we have seen above that the anomalies are quite rare, hence the threshold for an example to be an anomaly would be low as well. If the threshold is larger or even half, then almost half of the example would be marked as an anomaly which would create tense condition in the model and it will not work properly. As a probability measure, the anomaly should range below 0.2 or above 0.8. One important thing to understand is that it also depends on the problem statement and the dataset, the value of the threshold may change. Threshold is the most important part of the model as on its basis the anomalies would be marked. If it is too large, even the legal activities would be marked as anomaly and if it is too low, some anomalous activities might escape and cause harm to the system [22].

Let the threshold for anomaly be 'ε'. p(x) is the probability of an example 'x' to be an anomaly. Therefore, the condition for an example to be anomalous is given in Eq. (2).

$$p(x) < \varepsilon \tag{2}$$

3.5 Implementation of the Algorithm

The Gaussian distribution (also referred to as the normal distribution) is required for the implementation of anomaly detection algorithm, so some of the terminologies are –

$$\aleph - Gaussian; \sim - distributed\ as; \mu - Mean; \sigma^2 - Variance \tag{3}$$

For 'x' to be a distributed Gaussian with mean 'μ' and variance 'σ^2'

$$x \sim \aleph(\mu, \sigma^2) \tag{4}$$

More the example is in denser region of Gaussian distribution, lesser chances for it to be an anomaly. The Gaussian density would be highest in the part where there are

large number of example congested together. It would slowly become less dense as it spreads.

The implementation of the algorithm would require to understand the concept and use of the following equations.

$$\text{Trainingset} - \{x^1, x^2, x^3, x^4, \ldots, x^{m-1}, x^m\} \tag{5}$$

The training set is represented as x^i, where i = 1,2,3…,m as shown in Eq. (5). Since this is unsupervised learning so the dataset is not labelled. Each example would be represented as part of a probability equation with mean and variance passed with the input as per Eq. (6). The 'n' represents the feature as 'j' = 1,2,3,…,n

$$p(x) = p\left(x_1, \mu, \sigma^2\right) \cdot p\left(x_2, \mu, \sigma^2\right) \cdot p\left(x_3, \mu, \sigma^2\right) \cdot \cdots \cdot p\left(x_n, \mu, \sigma^2\right) \tag{6}$$

The above Eq. (6) is the conceptual representation to understand the algorithm implementation, this would be simplified as-

$$p(x) = \prod_{j=0}^{n-1} p(x_j^i; \mu_j; \sigma_j^2) \tag{7}$$

This would be the final implementation after the fitting of parameters, which are μ_j and σ_j^2, where j = 0, 1, 2, 3, …, n−1. After the fitting, the model would be ready for testing and deployment. The Eq. (2) would be used to flag the anomaly that is produced after the Eq. (7).

3.6 Testing of the Model and Deployment

After the successful training of the model with the help of Gaussian distribution, now the testing will take place. First the cross validation set will be used and then the testing set.

The cross validation set - $\{x_{cv}^1, x_{cv}^2, x_{cv}^3, \ldots, x_{cv}^m\}$

The Testing set – $\{x_{test}^1, x_{test}^2, x_{test}^3, \ldots, x_{test}^m\}$

After the successful testing of the model, it would be ready for deployment in the industry 5.0 environment alongside of the IIoT and blockchain.

3.7 Blockchain for the IIoT

Blockchain technology is often considered the ideal technology for security which ensures the integrity of the data and transaction because of its decentralized system. The IIoT deals with a lot of data and communication, hence the data is in real-time which requires a system capable enough to handle it and provide security at the same time. The IIoT consists of network between devices and performs device-to-device or machine-to-machine communication with human interaction. The blockchain would help to store the data and perform secure communication between the devices.

The below Fig. 2 shows the structure of the blockchain and why is it named as it is. It describes the encrypted data and the chains that connects in block in order to ensure the data integrity.

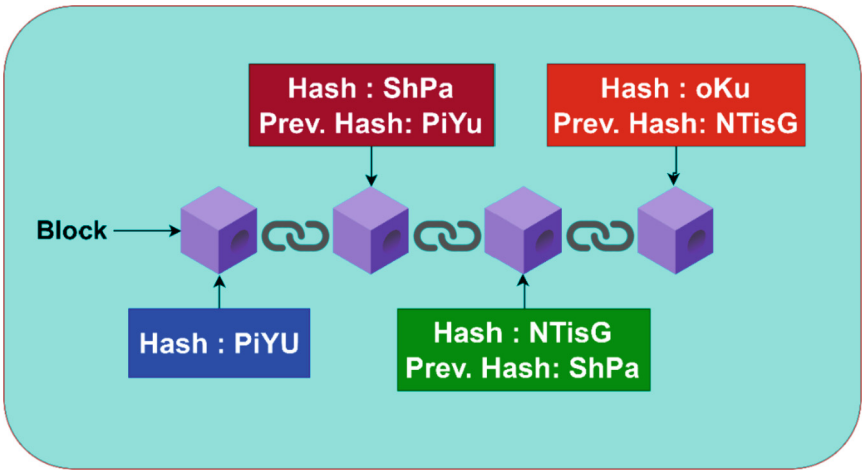

Fig. 2. Structure of Blockchain

As the data would be in real-time so the data storing would also require a strong and secure system. To understand the process of how the data or transaction would take place and added in the blockchain, refer the below Fig. 3 which shows the proposed blockchain for the IIoT and describes the process step by step, how the transaction would be added in the blockchain.

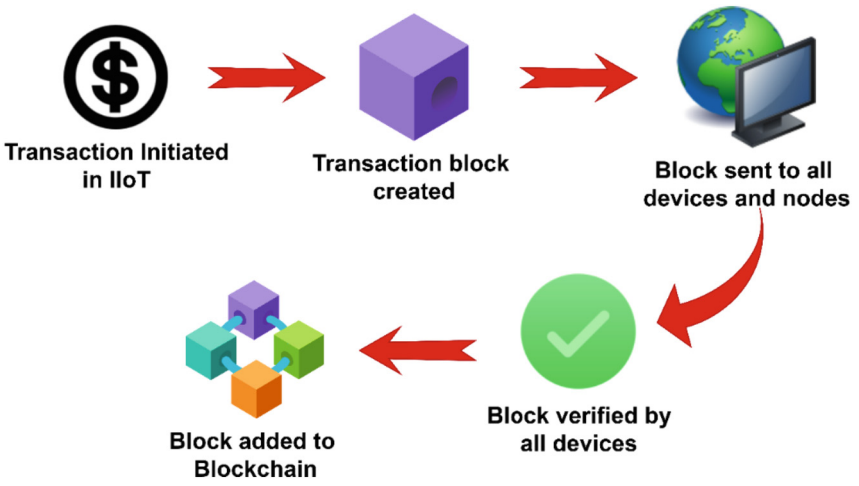

Fig. 3. Process of Block addition

4 Result and Discussion

It is important to understand that the data to train the model does not exist yet because the Industry 5.0 isn't here. Because of this, the research used "Hypothetical data" to train the anomaly detection model. The data is generated using the random seed method by the research. The Fig. 4 is the screenshot of the code that shows the method to randomly seed the data using the Numpy module.

```
import numpy as np
import matplotlib.pyplot as plt
from sklearn import svm

# Generate sample data
np.random.seed(42)
X = 0.3 * np.random.randn(100, 2)
X_train = X[:80]
X_test = X[80:]
```

Fig. 4. Code to randomly seed the data using Numpy

The research used the OC-SVM (One Class Support Vector Machine) for anomaly classification, which is one of the best anomaly detection algorithm. After seeding the

```
# Plot training data
plt.subplot(121)
plt.title("Training Data")
inlier_idx = y_pred_train > 0
outlier_idx = y_pred_train < 0
plt.scatter(X_train[inlier_idx, 0], X_train[inlier_idx, 1], c='green', marker='o', label='inliers')
plt.scatter(X_train[outlier_idx, 0], X_train[outlier_idx, 1], c='red', marker='x', label='outliers')
plt.legend(loc='best')

# Plot testing data
plt.subplot(122)
plt.title("Testing Data")
inlier_idx = y_pred_test > 0
outlier_idx = y_pred_test < 0
plt.scatter(X_test[inlier_idx, 0], X_test[inlier_idx, 1], c='green', marker='o', label='inliers')
plt.scatter(X_test[outlier_idx, 0], X_test[outlier_idx, 1], c='red', marker='x', label='outliers')
plt.legend(loc='best')
```

Fig. 5. Plotting of Inliers and Outliers for Training and Testing data

data and training the model, the below Fig. 5 shows the plotting of testing and training data which has labels inliers and outliers for non-anomalous and anomalous data respectively.

After training the model, the result is represented by Fig. 6. The Fig. 6 generates two scatter plots that show the training and testing data with the predicted outliers marked in red and the inliers marked in green.

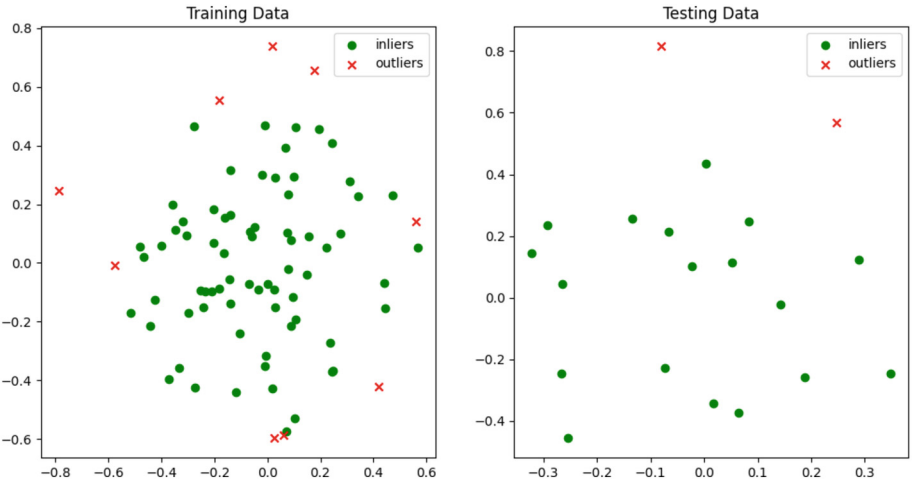

Fig. 6. Inliers and Outliers representation

The above model can now be successfully deployed in the real world after training the model using real world data. The proposed model has an average accuracy of 92.8% after 5 different runs with different datasets to ensure stability of the model. The blockchain is proposed to be added with the 256-bit AES encryption method that would be imported with the encryption modules like Bcrypt which the Industry 5.0 would have inbuilt since it is based on Blockchain.

To have better analysis of the research, the paper have some research questions as RQs. They are based on the research and gives focus on theory of the paper.

RQ1. Can we implement the classification algorithms like Logistic regression for anomaly detection?

Answer: As discussed in the section where difference between classification and anomaly detection is described, the answer would be No. It is because, the dataset would not be labelled like the supervised algorithms need. Along with that, the anomaly detection is not classification of anomaly but to detect the unusual out of the usual. Therefore logistic regression, which is a classification algorithm of supervised learning cannot be used for anomaly detection, even if it is modified to do so, it won't give just as good result as the actual algorithm.

RQ2. Why the threshold matters for the algorithm and why is it so low?

Answer: The threshold is really important as it is the condition to mark the example as an anomaly or not. Anomalies are rare and it would not be advised to mark a large

number of example as anomaly as the model may become slow and produce many false positives [14].

RQ3. Pictorial representation of the model.

Answer: The below Fig. 7 shows the architecture of the final model with blockchain and machine learning in IIoT of industry 5.0. The figure shows how the marked anomalies are not allowed to enter the model and the attack is prevented by the proposed model.

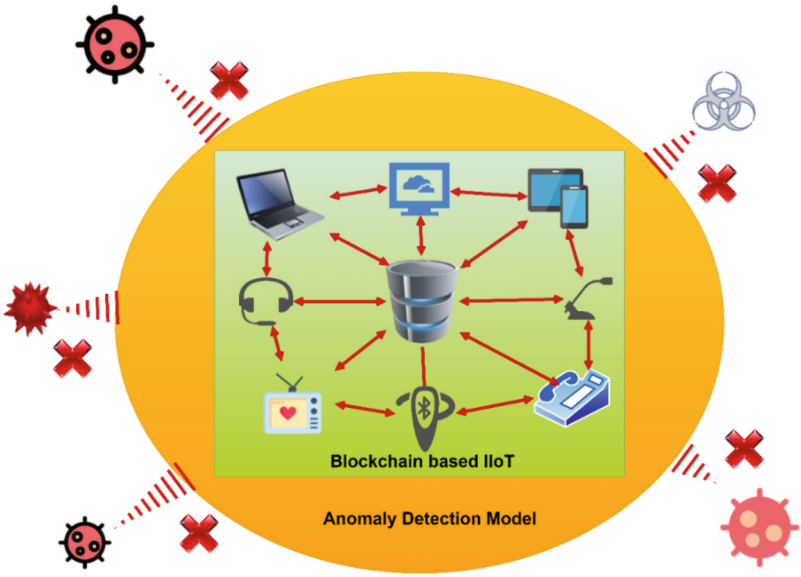

Fig. 7. Proposed model diagram

RQ5. How is the data divided for the overall development of the model and why?

Answer: The dataset is divided using the 60%-20%-20% rule which means that the training set would be the 60%, cross validation set would be 20% and the testing set would be 20%. This would ensure that the model is efficient and the parameters are fitted correctly.

5 Conclusion

The world is stepping in an era where the Human-Machine and Machine-To-Machine interaction will rise significantly. The drastic rise in these interaction leads to the need for a secure model so that the data could be safe from the hands of attackers. The research integrated the Blockchain technology in the IIoT model, which is an extension of the IoT, to improve its overall security and gave it anti-corruption powers. However, to add an extra layer of security, Machine learning is also proposed and integrated by the research. The anomaly detection algorithm form the domain of machine learning is used by the paper. The anomaly detection algorithm detects any kind of activity that is unusual and marks it as an anomaly. This activity could be any kind of attack from the side of

hacker, injection of some virus, unusual data, unwanted scripts, sudden changes in the IIoT, etc. Such activities are usually done by the hackers to get into the model and steal from it. Our secondary layer of security, which is the machine learning algorithm would protect from such attacks whereas the primary layer, the blockchain would prevent any kind of unwanted interaction with the data or the model. This would give the ultimate security to the model for Industry 5.0, hence the research proposes these algorithm and methodologies for the practical approach towards the development of IIoT model for the Industry 5.0. By integrating One-class SVM as an Anomaly Detection Algorithm with blockchain technology in the IIoT model of Industry 5.0, it is possible to improve the overall security of the system and prevent potential security attacks. The use of an Anomaly Detection Algorithm helps to detect any suspicious activity and prevent it from causing damage to the system. By combining this with the decentralized and secure nature of blockchain, the security of the IIoT model can be further strengthened. This integration can play a crucial role in ensuring the safe and secure functioning of Industry 5.0's IIoT model and safeguarding it from potential security attacks. The research encourages other researchers to study and implement some future work of this research like what to do after an anomaly is found, how to deal with it and safeguard the model. Even the Deep Learning can be integrated in the model in place of machine learning to make the system even more advance.

References

1. Pant, P., et al.: Blockchain for AI-enabled industrial IoT with 5G network. In: 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–4 (2022). https://doi.org/10.1109/ECAI54874.2022.9847428
2. Lee, C., Kim, J., Kang, S.-J.: Semi-supervised anomaly detection with reinforcement learning. In: 2022 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC), pp. 933–936 (2022). https://doi.org/10.1109/ITC-CSCC55581.2022.9895028
3. Almalawi, A., Tari, Z., Fahad, A., Yi, X.: A Global anomaly threshold to unsupervised detection. In: SCADA Security: Machine Learning Concepts for Intrusion Detection and Prevention, pp. 119–149. Wiley (2021). https://doi.org/10.1002/9781119606383.ch6
4. Babaei, M., Imani, M.: Anomaly detection improvement using sparse representation and morphological profile. In: 2020 6th Iranian Conference on Signal Processing and Intelligent Systems (ICSPIS), pp. 1–5 (2020). https://doi.org/10.1109/ICSPIS51611.2020.9349597
5. Ziemann, A., Simonoko, H., Flynn, E.: Temporal anomaly detection in multispectral imagery. In: IGARSS 2020 - 2020 IEEE International Geoscience and Remote Sensing Symposium, pp. 3975–3978 (2020). https://doi.org/10.1109/IGARSS39084.2020.9324627
6. Potgantwar, A., Aggarwal, S., Pant, P., Rajawat, A.S., Chauhan, C., Waghmare, V.N.: Secure aspect of digital twin for industry 4.0 application improvement using machine learning (2022). https://doi.org/10.2139/ssrn.4187977.SSRN: https://ssrn.com/abstract=4187977
7. Song, J., Nang, J., Jang, J.: Design of anomaly detection and visualization tool for IoT blockchain. In: 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pp. 1464–1465 (2018). https://doi.org/10.1109/CSCI46756.2018.00292
8. Voronov, T., Raz, D., Rottenstreich, O.: Scalable blockchain anomaly detection with sketches. In: 2021 IEEE International Conference on Blockchain (Blockchain), pp. 1–10 (2021). https://doi.org/10.1109/Blockchain53845.2021.00013

9. Rajawat, A.S., Goyal, S.B., Pant, P., Bedi, P.: AI-enabled internet of nano things methodology for healthcare information management. In: Kautish, S., Dhiman, G. (ed.) AI-Enabled Multiple-Criteria Decision-Making Approaches for Healthcare Management, pp. 222–239. IGI Global (2022). https://doi.org/10.4018/978-1-6684-4405-4.ch012
10. Liu, X., Jiang, F., Zhang, R.: A new social user anomaly behavior detection system based on blockchain and smart contract. In: 2020 IEEE International Conference on Networking, Sensing and Control (ICNSC), pp. 1–5 (2020). https://doi.org/10.1109/ICNSC48988.2020.9238118
11. Liu, W., Shen, Y., Yang, H., Bao, B., Yao, Q., Wang, L.: Anomaly detection based on dual-threaded blockchain in large-scale intelligent networks. In: 2022 International Wireless Communications and Mobile Computing (IWCMC), pp. 28–31 (2022). https://doi.org/10.1109/IWCMC55113.2022.9824976
12. Kim, J., et al.: Anomaly detection based on traffic monitoring for secure blockchain networking. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1–9 (2021). https://doi.org/10.1109/ICBC51069.2021.9461119
13. Il-Agure, Z., Attallah, B., Chang, Y.-K.: The semantics of anomalies in IoT integrated BlockChain network. In: 2019 Sixth HCT Information Technology Trends (ITT), pp. 144–146 (2019). https://doi.org/10.1109/ITT48889.2019.9075114
14. Signorini, M., Pontecorvi, M., Kanoun, W., Di Pietro, R.: ADvISE: anomaly detection tool for blockchaIn SystEms. In: 2018 IEEE World Congress on Services (SERVICES), pp. 65–66 (2018). https://doi.org/10.1109/SERVICES.2018.00046
15. Morishima, S.: Scalable anomaly detection method for blockchain transactions using GPU. In: 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), pp. 160–165 (2019). https://doi.org/10.1109/PDCAT46702.2019.00039
16. Yu, D., Xie, Y., Long, H., Jin, M., Li, X.: Container anomaly detection system based on rule mining and matching. In: 2022 International Conference on Blockchain Technology and Information Security (ICBCTIS), pp. 102–105 (2022). https://doi.org/10.1109/ICBCTIS55569.2022.00034
17. Iyer, S., Thakur, S., Dixit, M., Katkam, R., Agrawal, A., Kazi, F.: Blockchain and anomaly detection based monitoring system for enforcing wastewater reuse. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–7 (2019). https://doi.org/10.1109/ICCCNT45670.2019.8944586
18. Kim, J., et al.: A machine learning approach to anomaly detection based on traffic monitoring for secure blockchain networking. IEEE Trans. Netw. Serv. Manage. **19**(3), 3619–3632 (2022). https://doi.org/10.1109/TNSM.2022.3173598
19. Signorini, M., Pontecorvi, M., Kanoun, W., Di Pietro, R.: BAD: a blockchain anomaly detection solution. IEEE Access **8**, 173481–173490 (2020). https://doi.org/10.1109/ACCESS.2020.3025622
20. Pant, P., et al.: Authentication and authorization in modern web apps for data security using Nodejs and role of dark web. Procedia Comput. Sci. **215**, 781–790 (2022). https://doi.org/10.1016/j.procs.2022.12.080
21. Ning, W., Xie, X., Huang, Y., Hu, F.: Data sharing scheme for 5G IoT based on blockchain. In: 2021 International Wireless Communications and Mobile Computing (IWCMC), pp. 327–329 (2021). https://doi.org/10.1109/IWCMC51323.2021.9498712
22. Pant, P., Taghipour, A.: Machine learning and blockchain for 5G-enabled IIoT. In: Taghipour, A. (ed.), Blockchain Applications in Cryptocurrency for Technological Evolution, pp. 196–212. IGI Global (2023). https://doi.org/10.4018/978-1-6684-6247-8.ch012

23. Pant, P., et al.: Using machine learning for Industry 5.0 efficiency prediction based on security and proposing models to enhance efficiency. In: 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, pp. 909–914 (2022). https://doi.org/10.1109/SMART55829.2022.10047387
24. Pant, P., et al.: AI based technologies for international space station and space data. In: 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, pp. 19–25 (2022). https://doi.org/10.1109/SMART55829.2022.10046956