EAI Endorsed Transactions
on Creative Technologies
Research Article EAI.EU

# IOTA Based Anomaly Detection Machine learning in Mobile Sensing

Muhammad Shoaib Akhtar*, Tao Feng

School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China

## Abstract

In this proposed method, iMCS can detect and prevent fake sensing activities of mobile users using machine learning techniques. Our iMCS solution uses behavioral analysis based on participants' reliability scores to detect variation in behavior of users and introduces a new role in a distributed system of MCS architecture to validate the collected data. To evaluate the incentive based on the participant's sensory data and data quality, to properly distribute profit among the participants, we employ the Shapley Value approach. The evaluation results demonstrate that our method is effective in both quality estimations and incentive sharing.

**Keywords:** machine learning, deep learning, deep neural network, anomaly detection

Received on 20 August 2021, accepted on 05 January 2022, published on 11 January 2022



doi: 10.4108/eai.11-1-2022.172814

*Corresponding author. Email: 13.cs.194@gmail.com

## 1. Introduction

IOTA is a ground-breaking computing model that has rapidly evolved in practically every technology field during the previous decade, including smart anomaly detection and smart security systems, smart banking systems, crypto currencies, sensor use, smart cities, and satellites (Wang et al. 2020). It is made up of a range of IOTA mobile devices (Things) with sensors, actuators, storage, processing, and networking capabilities for data collection and sharing over the internet (K. Singh et al. 2020). The data collected and processed by a IOTA network is sensitive, and it must be safeguarded against possible attacks (Hao et al. 2019). Firewalls, authentication systems, various types of encryption, antivirus, and other security measures are presently being used to safeguard sensitive data from vulnerable mobile device security threats, such as the distributed denial-of-service (DDoS) attack, which is the first line of defence (Alrashdi et al. 2019). IOTA has the potential to create networking [SDN], future network structure, Deep learning (DL), artificial intelligence (AI), and machine learning are examples of data networking (NDN) and cloud network computing (VoIP fibre optics, global microwave access interoperability (WiMAX), deep learning (DL), AI, and machine learning). Numerous new anomalies (both unique and mutations of an old anomaly) are produced on a regular basis as a result of the inclusion of a large amount of data (Shafiq et al. 2021). As a result, a second-line defensive intrusion detection system (IDS) can offer additional security protection for an IOTA network (Shafiq et al. 2020). The methods of deployment and detection can be used to classify IDSs. Depending on the detection technique, an IDS can be either host-based or network-based, as well as signature-based, specifier-based, or hybrid detection. The goal of this research is to use the Network-based IDS (NIDS) detection technique to provide IOTA security at the entrance points. The current IDS have a basic flaw: when zero-day abnormalities are identified, the False Alarm Rate (FAR) increases (Bhuvaneswari and S. 2020). Machine Learning (ML) and Deep Learning (DL) techniques have recently been investigated as ways to improve detection accuracy and minimise the FAR for NIDS. In research, both ML and DL techniques have been proven to be effective in extracting meaningful patterns from network data in order to classify flows as anomalous or benign. Thanks to its deep architecture, which requires no human contact, DL has demonstrated speed in learning valuable characteristics from raw data, and has emphasised the importance of integrating IOTA networks into NIDS (Kuang et al. 2020). Deep Neural Networks (DNNs) are a form of deep learning approach being researched by

academics in domains such as linguistic processing, computer vision, and network security (Santos et al. 2020). Because of their in-depth design, DNNs have done remarkably well in certain industries, providing various abstractions for the usage of complex learning elements to effectively predict. Because of the vast amount of data produced by IOTA mobile devices, these qualities of DNN have made it ideal for an IDS designed for an IOTA network. In this research, we look at the possibility of employing DNN to present a cost-effective IOTA NIDS solution. The study's major contributions are divided into four categories. (1) To investigate the current state-of-the-art in DL-based Crowd Fake Sensing through Mobile Devices. (2) Using the DNN, provide an effective technique for detecting IOTA anomalies. (3) Using the IoT-Botnet 2020 dataset and analysing its effectiveness, we intended to evaluate the efficiency of our model with other deep learning models based on different DL techniques. (4) The goal of this study was to see how numerical and categorical factors affected the performance of DL-based NIDS models. (5) For coordinating the Machine learning architecture for fake sensing, the Shapley value for a fair partition of group is used.

## 2. Related Work

Throughout the last decade, researchers have been investigating artificial intelligence technologies such as machine learning and deep learning in order to provide effective NIDS solutions (Gupta et al. 2020; Stoyanova et al. 2020). Because of advances in graphical processing unit (GPU) technology, which answered the speedy calculation need for DL algorithms, DL methods have been favoured over ML algorithms over the last three years, according to current NIDS trends. This has inspired scientists to apply the DL algorithms in an IOTA network to develop effective security solutions that process large numbers of raw data (Al Zamil et al. 2017; Zielonka et al. 2021). [8] Because of its deep structure, the DL can learn the complex pattern and aid in the classification of benign and pathological traffic. Researchers in the field of NIDS commonly use machine learning techniques. Ali et al., for example, suggested IDS based on the Particle Swarm algorithm that uses a fast-learning network. Despite being efficient enough to predict most attacks, the performance of the minority class label detection model was not encouraging. Shen et al. developed an ensemble approach methodology that included applying the BAT optimization algorithm during the ensemble cutting step. Yao et al. explain a multi-level semi-supervised machine learning model that incorporates clustering as well as the Random Forest approach (Chaterji et al. 2021; Unal 2020), in another noteworthy piece. Their methodology has been successful in detecting multi-level assault classes. [9] ML and DL methodologies are also being used by researchers to produce successful NIDS solutions using a variety of hybrid strategies. All of these methods are investigated utilising DL algorithms for feature and complexity reduction, followed by a machine learning predictor (Mohamad Noor and Hassan 2019; Taneja et al. 2020).

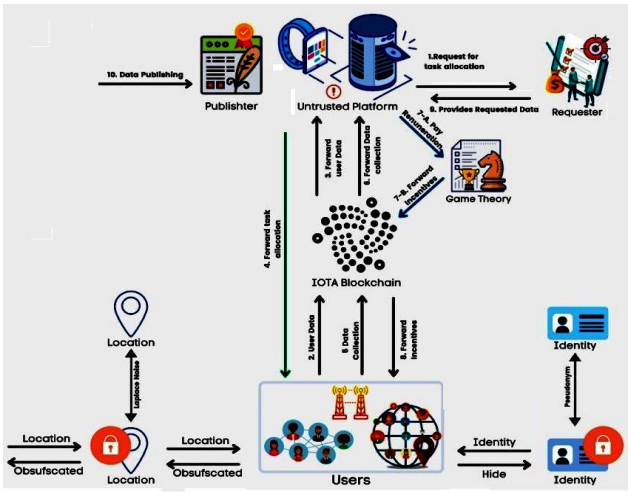



**Figure 1.** IOTA Block chain Methods

For example, Shone et al. use a advance method to integrating auto encoder (AE) and RF by using the AE encoder only. [10] Their non-symmetric solution detected the abnormalities successfully with the exception of some labels due to lower instances.

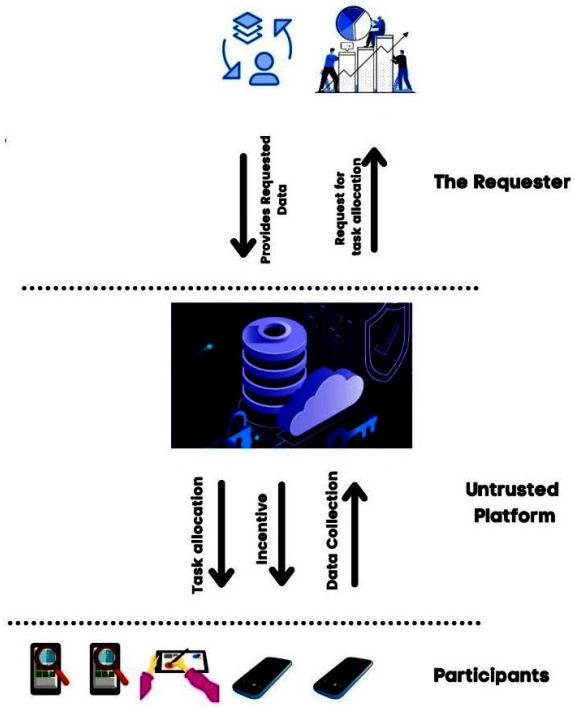



**Figure 2.** Example of Untrusted Platforms

(Gage et al. 2006) Another hybrid concept occurs when sparse AE is combined with vector support (SVM). Using

this methodology, minor anomaly labels have also proven difficult to locate. Marir et al. established another hybrid way to merge the deep-faith network (DBN) with SVM, this time using the ensemble approach. Researchers have also proposed effective NIDS models using stand-alone DL techniques including AE, recurrent neural network, DBN, convergence neural network (CNN), Morlet neural wavelet network, and so on. For example, (He et al. 2018). As a memory unit, [11] suggest an RNN-based NIDS that uses Gated Recurrent Units. Xiao et al. Also available is a CNN-based technique that uses main component analysis and AE for functional extraction tasks, followed by CNN for prediction (Chalapathy and Chawla 2019). Using their approaches, only the class label with the most occurrences was successful (Hu et al. 2008) merge the CNN with a bidirectional short-term memory to give another extremely complex NIDS technique (LSTM). (Zhao et al. 2010) Using a variety of optimization techniques such as particle swarm optimization, fish swarm optimization, and DBN genetic algorithms, they've developed a comprehensive solution. Many researchers are suggesting DNN-based NIDS solutions as well. Jia et al., for example, offer a DNN-based NIDS with four hidden layers that is efficient. The model performed admirably when it came to identifying the data sets KDD cup 99 and NSL-KDD. Their recommended methods do not detect user to root (U2R) assault cases quickly. [12] Wang's suggested adversary IDS, which is based on DNN, also investigates the role of each attribute in the generation of unfavourable cases. In the same way, for host and network intrusion detection, (Vinayakumar et al. 2019) based on the Apache Spark cluster computing platform, proposes a scalable DNN hybrid architecture. They put their proposed methodology to the test on a number of new and old datasets to show that it was superior. Based on a study of the pertinent literature (Endler 1998; Lee and Stolfo 2000; R. Singh, Kumar, and Singla 2015), It's worth noting that the majority of the systems on offer have trouble detecting minority class classifications. For DL approaches, a vast amount of training data is necessary. The DL algorithm does not learn enough intricate patterns in this example with very few samples in a particular class dataset, resulting in erroneous label predictions. Furthermore, DL-based IDS research is still in its infancy on the IOTA network, thus there is plenty of space for additional research in this area. [13]We describe a DNN-based NIDS solution for an IOTA network to achieve this goal. The importance of DL methods' performance qualities for an IOTA network is discovered in particular (Al-Haj Baddar et al. 2018; SpringerLink n.d.; Chebrolu, Abraham, and Thomas 2005).

## 3. Methodology

### 3.1 IOTA Framework

The IoTA Framework is on the caller's side. [14] It includes the sensor platform, the sensor data interface and the SIP client, as shown in Fig.1. The calling side can also be fitted with other instruments (e.g. computers, tablets, televisions, microphones, and speakers), sensors for fake and anomaly detection.

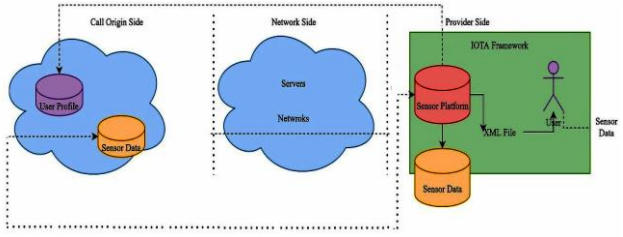



**Figure 3.** IOTA Architecture

As a user-server model, the sensor data interface has been established to facilitate communication between the sensor platform and the user. In XML format, the interface accepts the critical data. Sensor Model Language has been chosen as the standard, unified data representation model. This file will also be utilised as a parameter in a Deep Learning Model.

### 3.2 Deep Learning Model

DNN is part of the supervised learning algorithm family to train the model with several layers. The DNN employed in this study is based on the notion of an artificial neural feed-forward network with numerous hidden layers to enhance abstraction capabilities.

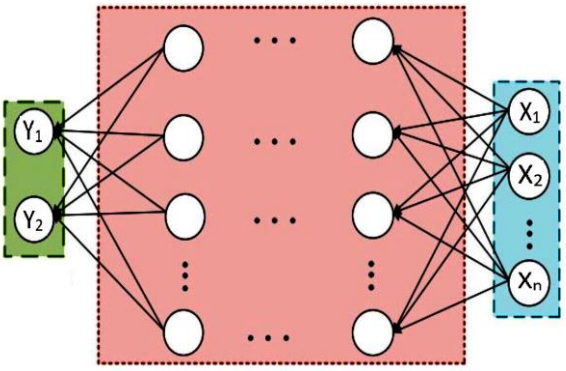



**Figure 4.** Deep Neural Network Model

The input layer of the DNN structure employed in this study has a set of 64, 32, 16, or 8 neurons. After that, we used four dense layers with 210, 29, 28, and 27 neurons, followed by a sigmoid classification layer with two outputs to demonstrate the anomalous and benign traffic categorization. [15] For the experiment, only five neurons with numerical and category information are used in the input layer, After that, there are two thick layers with 28 and 27 neurons, as well as an output layer with a sigmoid

activation function, which determines if mobile activity is benign or pathological.

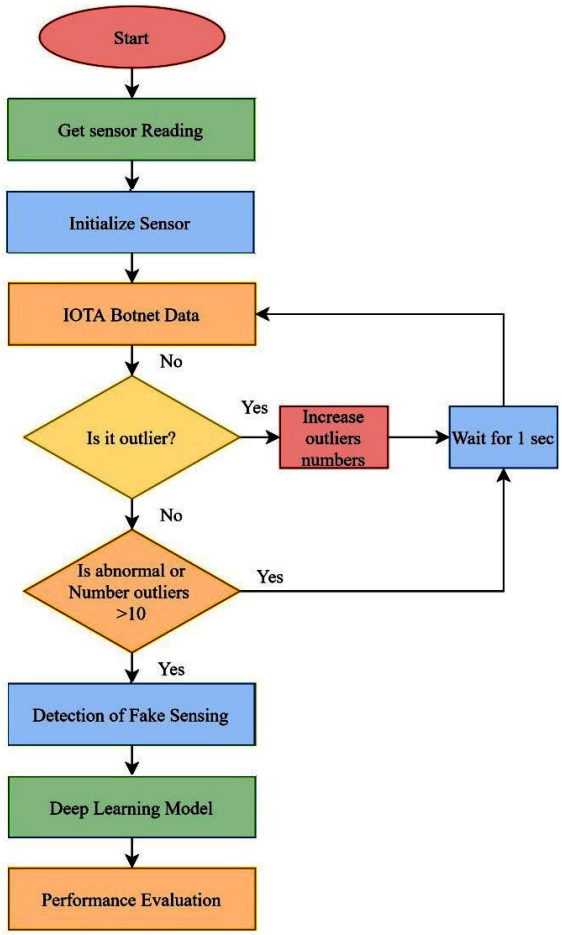



**Figure 5.** Deep Learning based IOTA Architecture

The study investigated a two-stage IDS system to safeguard the IOTA network based on Deep Learning against potential attacks as illustrated in Figure 3. The several phases of the considered model are (1) the phase of data collection, preparation and (2) the stage of detection of deep neural networks. The many procedures taken to implement and assess DL models include.

## 3.3 Shapely Value

We describe the user data's Shapley value as a sum of two user data's Shapley values, which gives every coalition its rational value:

The user data in which the worth of a coalition is decided by its restricted rational value—the total coalition consumption given the optimal load optimization method. Every coalition's value is its logic, according to the user data (i.e., the difference between its rational and bounded rational values). [18] Importantly, while the restricted rational coalition values can be calculated, the rational values and rationality differences do not apply due to the limited processing resources. [16] As a result, we can only calculate the Shapley value of the user data with limited logic using appropriate coalition values. The limited rational Shapley value is what we refer to it as [19]. We believe that this pay-off method is fair since it generates a pay-off distribution using the technique described below (which is not feasible in view of the restricted resources available):

**Step 1:** Divide the Grand Coalition's rational value among the agents "equitably," according to Shapley's axioms. Intuitively, each agent's role may be considered as a reward for making a reasonable contribution.

**Step 2:** Divide the rational difference between agents of the Grand Coalition – again, unknown – according to Shapley's axioms. Every share can be thought of as a monetary punishment for not determining the logical value in a reasonable length of time. For example, if an agent's existence [12] in a coalition generates rational discrepancies on a regular basis (for example, due to the agent's severe constraints, which increases the time required to calculate the rational value), that agent will be penalised. If coalition values suggest a cost, the penalty could be negative.

**Step 3:** Assign a fair reward less a fair punishment to each agent.

In view of this mechanism of division, we offer two greedy algorithms to optimize individually and collectively the cooling plan for apartments. These methods will let to find a pretty excellent (but not always optimum) answer in time, and the useful parts of these algorithms, as we will see later, considerably assist us in optimizing the coalition load. More precisely, the first algorithm detects times in a particular day, When the air conditioner is turned on, the gap between householder preferences and the expected temperature during the comfort period is the smallest. The second strategy relieves stress on a group of apartments by reassigning a significant number of occupants to apartments with more flexible preferences (subject to a specified temperature threshold and individual temperature preferences). The more adjustable an apartment is, the easier it will be to accommodate its preferences. [17] This programme takes use of the fact. These two algorithms can be used to detect sub-optimal load coordination (which results in a potentially lesser discount saving than the optimal option) whilst fulfilling the household temperature preferences. Then, our limited rationality proposal proves that the fair distribution of the discount may be obtained using the Shapley value.

## 3.4 Dataset Description

We used the publicly accessible dataset IoT-Botnet 2020 to evaluate the performance of the DL techniques explored in this study. This dataset is provided in CSV format and is used from BoT-IOTA Pcap files by producing extra network and flow-based attributes. The original dataset contains samples of many sorts of attacks, such as denial of service, distributed denial of service, acknowledgement and attacks on theft of information. We picked the benign samples from the original dataset, while the random samples from [23] every anomaly class were evaluated for fair model assessment. For the anomaly class.

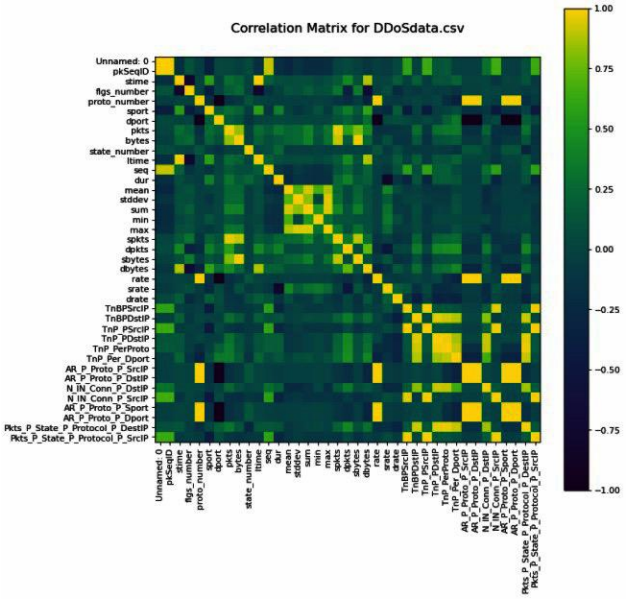
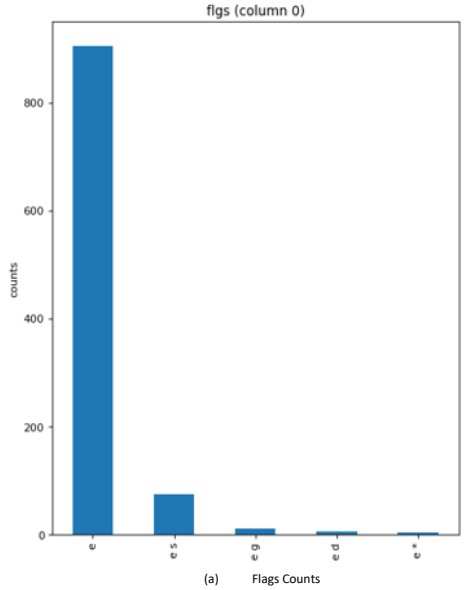


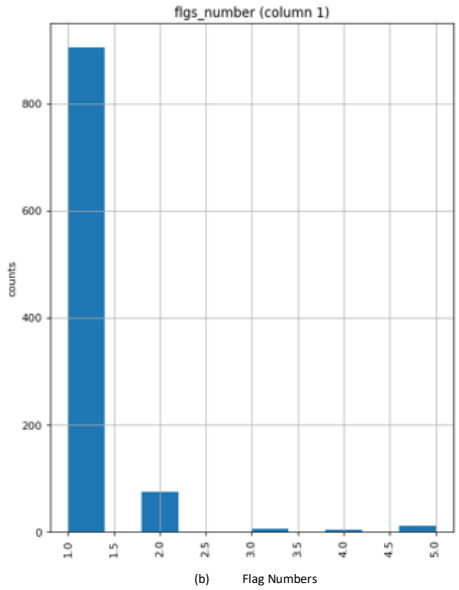

**Figure 6.** Feature Correlated Matrix

The initial data set included attacks such as denial of service, distributed denial of service, recognition, and robbery. The benign samples were taken from the original data set, whereas random samples from each anomaly class were evaluated to ensure a fair model evaluation. In information theory, [21] the MI is a key concept that provides information about other variables in exchange for a reduction in the uncertainty of a single random variable The MI can be calculated as follows:

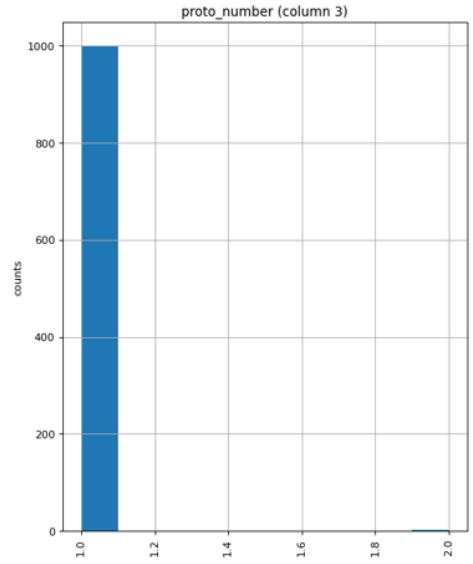
$$I\,(U;V) = \sum_{ueU}^{n} p(u,v) \sum_{veV}^{n} \mathrm{p(u,v)} \log_2 \frac{p(u,v)}{p(u),p(v)} \quad \ldots (1)$$



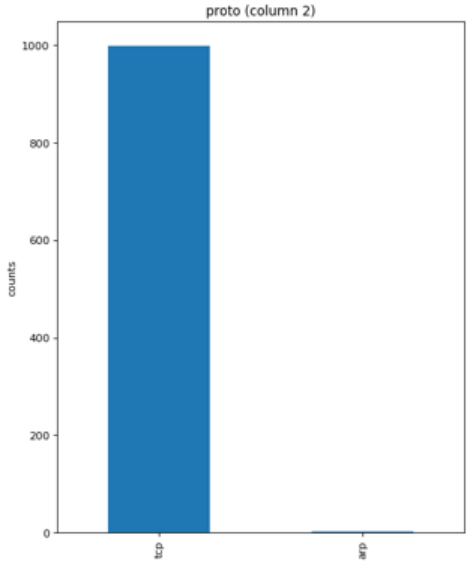

(a) Flags Counts



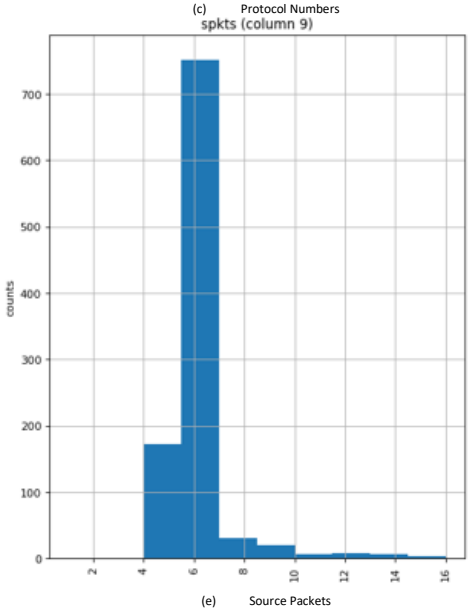

(b) Flag Numbers



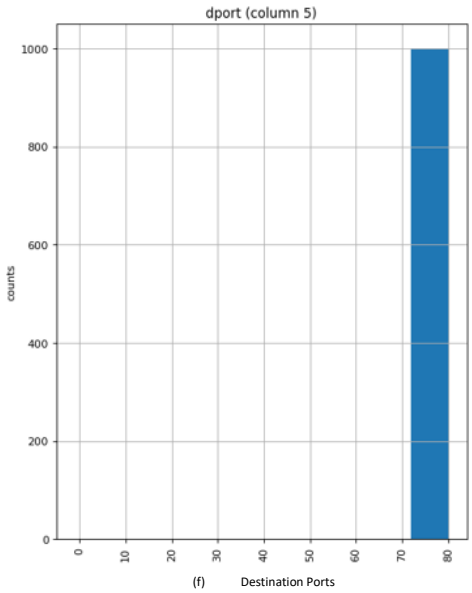

(c) Protocol Numbers



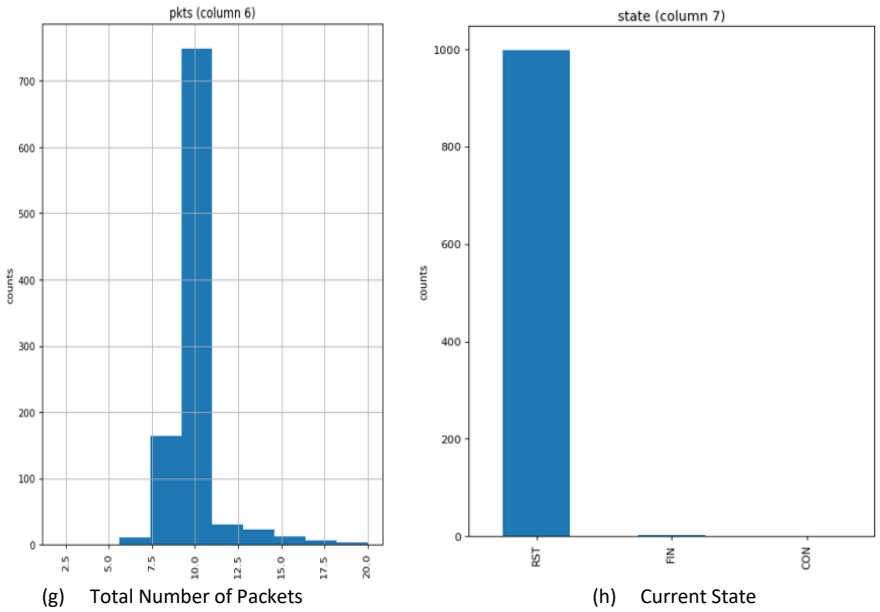

(d) Protocols (TCP or IRP)




(e) Source Packets




(f) Destination Ports




(g) Total Number of Packets (h) Current State

**Figure 7.** Outliers Detection

## 4. Results

To build the various DL based IDS techniques, we employed a batch size of 27, [21] a learning rate of 0.01, an Adam Optimizer, and a binary cross entropy Loss function ReLU and sigmoid activation functions were used in this work for DL methods.

| Techniques | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| DNN | 99.5 | 99 | 98 | 97.7 |
| LSTM | 97.34 | 97 | 96.78 | 97.6 |
| RNN | 85.55 | 87.6 | 87.6 | 85.5 |
| GRU | 86.6 | 87.5 | 84.4 | 86.5 |
| CNN | 85.7 | 86 | 85 | 86.44 |

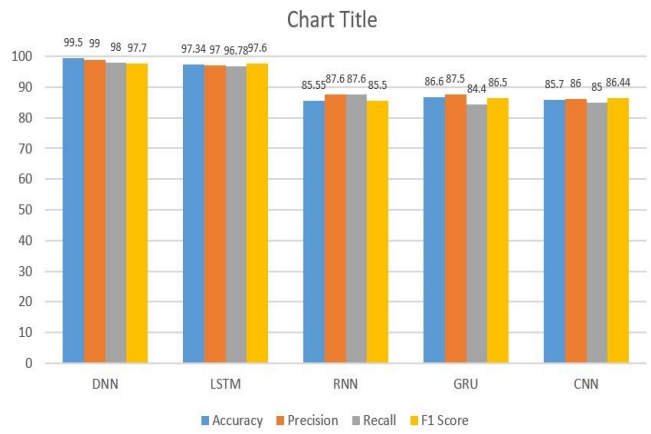



Table 1. Performance Rates of Models

| Techniques | False Positive Rate | True Positive Rate | False Negative Rate | True Negative Rate |
|---|---|---|---|---|
| DNN | 4.4 | 15 | 4.5 | 1.4 |
| LSTM | 4 | 1 | 3 | 1 |
| RNN | 5 | 2 | 4 | 4 |
| GRU | 4 | 2 | 8 | 4 |
| CNN | 8 | 2 | 2 | 6 |

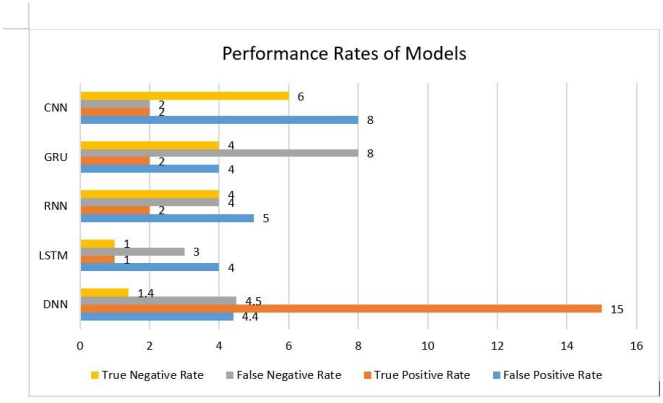



Table below Analysis of individual labels (Benign and Anomaly) with regard to accuracy, reminder and F1 score percentages. We have seen that all techniques showed a

very high percentage of anomaly flow detection, with the top DNN score of 99.5%. On the other hand, it has been noted that the rates for detecting benign traffic have marginally fallen by 3.87–10.99 percent and DNN performs even better than other 96.085 percent methods. [22] We have also noticed that the LSTM model was inadequate at detecting benign flows with a deterioration of nearly 11%. We estimate that the imbalanced character of the data set with anomaly records is nearly 3.2 times higher than the benign data, which have helped to degrade the detection rate for the benign label. Increased data for benign labels can also enhance their detection rate.

Table 2. Accuracy according to the Class

| Techniques | Accuracy (Benign) | Accuracy (Anomaly) |
|---|---|---|
| DNN | 98 | 97 |
| LSTM | 97 | 97.8 |
| RNN | 97 | 98 |
| GRU | 95 | 96 |
| CNN | 99.5 | 99.63 |

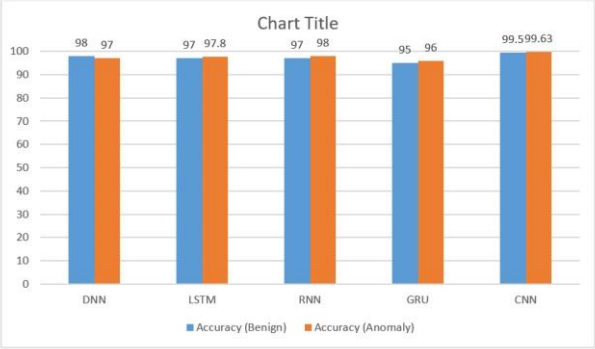



**Figure 9.** Benign and Anomaly Accuracy

We considered the real-world scenario where a mobile crowd sensing of fake users in a demand response programme so that a specified threshold does not surpass their aggregate. In return, the network receives a discount for their quality. A coalition of network users must therefore optimize the use of mobile network by its users.

Table 3. Shapely Value of Users

| Coalition (C) | Quality | Cost | Users | Cost |
|---|---|---|---|---|
| {} | Not Satisfied | $0 | {1},{2},{3} | $17.55 |
| {1} | Not Satisfied | $5.85 | {2}, {3} | $11.70 |
| {2} | Not Satisfied | $5.85 | {1}, {3} | $11.70 |
| {3} | Not Satisfied | $5.85 | {1}, {2} | $11.70 |
| {1, 2} | Satisfied | $6.24 | {3} | $5.85 |
| {1, 3} | Satisfied | $6.00 | {2} | $5.85 |
| {2, 3} | Satisfied | $6.24 | {1} | $5.85 |
| {1, 2, 3} | Satisfied | $9.36 | {} | $0 |

## 5. Conclusions

With this proposed method, iMCS can detect and prevent mobile users' false sensing behaviors with machine learning techniques. The iMCS solution uses behavioral analysis based on the reliability scores of participants to identify user behavior variation, and offers a new function for validation of acquired data in a distributed MCS architectural system. We apply the Shapley Value technique to equitably share the reward between participants to evaluate the incentive based on the participant's sensory input and data quality. The results of the evaluation show that our strategy is effective in both quality and incentive sharing estimates. The study of each label (Benign and This research offers an effective anomaly detection system based on a deep neural network for the architecture of the IOTA network, that effectively learns valuable complex patterns from IOTA network flows in order to classify traffic as good and anomalous. The new IoT-Botnet 2020 dataset tests the proposed methodology. The experimental findings revealed a superior model to the previous DL-methods by displaying a 99.01% detection accuracy with a false alarm rate of 3.9%, which improved the model's accuracy by 0.57–2.6% while simultaneously lowering the FAR by 0.23–7.98%. Results reveal furthermore that the best number features in the 16-32 range calculated by the MI are a feasible option to reduce the complexity of the model with a performance effect that is almost minimal. Moreover, incorporating the categorical features further increases detection precision by using only the top five characteristics) as regards percentage accuracy, recall and F1. We have seen that all techniques showed a very high percentage of anomaly flow detection, with the top DNN score of 99.95%. On the other hand, it has been noted that the rates for detecting benign traffic have marginally fallen by 3.87–10.99 percent and DNN performs even better than other 96.085 percent methods. We have also noticed that the LSTM model was inadequate at detecting benign flows with a deterioration of nearly 11%. We estimate that the imbalanced character of the data set with anomaly records is nearly 3.2 times higher than the benign data, which have helped to degrade the detection rate for the benign label. Increased data for benign labels can also enhance their detection rate.

## References


[1] R. Wang et al., “Deep Learning for Anomaly Detection,” Proc. ACM SIGKDD Int. Conf. Knowl. Discov. Data Min., vol. 1, no. 1, pp. 3569–3570, 2020, doi: 10.1145/3394486.3406481.

[2] K. Singh, S. Rajora, D. K. Vishwakarma, G. Tripathi, S. Kumar, and G. S. Walia, “Crowd anomaly detection using Aggregation of Ensembles of fine-tuned ConvNets,” Neurocomputing, vol. 371, pp. 188–198, 2020, doi: 10.1016/j.neucom.2019.08.059.

[3] Y. Hao, Z. J. Xu, Y. Liu, J. Wang, and J. L. Fan, “Effective Crowd Anomaly Detection Through Spatio-temporal Texture Analysis,” Int. J. Autom. Comput., vol. 16, no. 1, pp. 27–39, 2019, doi: 10.1007/s11633-018-1141-z.

[4] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, “AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning,” 2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019, pp. 305–310, 2019, doi: 10.1109/CCWC.2019.8666450.

[5] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, “CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques,” IEEE Internet Things J., vol. 8, no. 5, pp. 3242–3254, 2021, doi: 10.1109/JIOT.2020.3002255.

[6] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city,” Futur. Gener. Comput. Syst., vol. 107, pp. 433–442, 2020, doi: 10.1016/j.future.2020.02.017.

[7] B. A. Bhuvaneswari and S. S., “Anomaly detection framework for Internet of things traffic using vector convolutional deep learning approach in fog environment,” Futur. Gener. Comput. Syst., vol. 113, pp. 255–265, Dec. 2020, doi: 10.1016/j.future.2020.07.020.

[8] L. Kuang, P. Shi, C. Hua, B. Chen, and H. Zhu, “An enhanced extreme learning machine for dissolved oxygen prediction in wireless sensor networks,” IEEE Access, vol. 8, pp. 198730–198739, 2020, doi: 10.1109/ACCESS.2020.3033455.

[9] G. L. Santos, P. T. Endo, D. Sadok, and J. Kelner, “When 5G meets deep learning: A systematic review,” Algorithms, vol. 13, no. 9, pp. 1–34, 2020, doi: 10.3390/A13090208.

[10] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, “Security and Privacy in Smart Farming: Challenges and Opportunities,” IEEE Access, vol. 8, pp. 34564–34584, 2020, doi: 10.1109/ACCESS.2020.2975142.

[11] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues,” IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.

[12] A. Zielonka, M. Wozniak, S. Garg, G. Kaddoum, M. J. Piran, and G. Muhammad, “Smart Homes: How Much Will They Support Us? A Research on Recent Trends and Advances,” IEEE Access, vol. 9, pp. 26388–26419, 2021, doi: 10.1109/ACCESS.2021.3054575.

[13] M. G. Al Zamil, M. Rawashdeh, S. Samarah, M. S. Hossain, A. Alnusair, and S. M. M. Rahman, “An Annotation Technique for In-Home Smart Monitoring Environments,” IEEE Access, vol. 6, pp. 1471–1479, 2017, doi: 10.1109/ACCESS.2017.2779158.

[14] Z. Unal, “Smart Farming Becomes even Smarter with Deep Learning - A Bibliographical Analysis,” IEEE Access, vol. 8, pp. 105587–105609, 2020, doi: 10.1109/ACCESS.2020.3000175.

[15] S. Chaterji et al., “Lattice: A Vision for Machine Learning, Data Engineering, and Policy Considerations for Digital Agriculture at Scale,” IEEE Open J. Comput. Soc., vol. 2, no. April, pp. 227–240, 2021, doi: 10.1109/ojcs.2021.3085846.

[16] M. Taneja, N. Jalodia, P. Malone, J. Byabazaire, A. Davy, and C. Olariu, “Connected Cows: Utilizing Fog and Cloud Analytics toward Data-Driven Decisions for Smart Dairy Farming,” IEEE Internet Things Mag., vol. 2, no. 4, pp. 32–37, 2020, doi: 10.1109/iotm.0001.1900045.

[17] M. binti Mohamad Noor and W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” Comput. Networks, vol. 148, pp. 283–294, 2019, doi: 10.1016/j.comnet.2018.11.025.

[18] R. Chalapathy and S. Chawla, “Deep Learning for Anomaly Detection: A Survey,” pp. 1–50, 2019, [Online]. Available: http://arxiv.org/abs/1901.03407.

[19] D. Endler, “Intrusion detection. Applying machine learning to Solaris audit data,” Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC, pp. 268–279, 1998, doi: 10.1109/CSAC.1998.738647.

[20] R. Singh, H. Kumar, and R. K. Singla, “An intrusion detection system using network traffic profiling and online sequential extreme learning machine,” Expert Syst. Appl., vol. 42, no. 22, pp. 8609–8624, Dec. 2015, doi: 10.1016/j.eswa.2015.07.015.

[21] Muhammad Shoaib Akhtar, Tao Feng, "Deep Learning-Based Framework for the Detection of Cyberattack Using Feature Engineering", Security and Communication Networks, vol. 2021, Article ID 6129210, 12 pages, 2021. https://doi.org/10.1155/2021/6129210.

[22] "An effective combining classifier approach using tree algorithms for network intrusion detection | SpringerLink." https://link.springer.com/article/10.1007/s00521-016-2418-1 (accessed Sep. 02, 2020).

[23] S. Chebrolu, A. Abraham, and J. P. Thomas, "Feature deduction and ensemble design of intrusion detection systems," Comput. Secur., vol. 24, no. 4, pp. 295–307, 2005, doi: 10.1016/j.cose.2004.09.008.

[24] S. Al-Haj Baddar, A. Merlo, M. Migliardi, and F. Palmieri, "Saving energy in aggressive intrusion detection through dynamic latency sensitivity recognition," Comput. Secur., vol. 76, pp. 311–326, Jul. 2018, doi: 10.1016/j.cose.2017.12.003.