Webology (ISSN: 1735-188X)
Volume 16, Number 1, 2019

Building Explainable AI Systems With Federated Learning On The Cloud

Vijaya Venkata Sri Rama Bhaskar[1] , Pradeep Etikani[2] , Krishnateja Shiva[3] , Ashok Choppadandi[4] , Arth Dave[5]

[1-5]Independent Researcher, USA.

Abstract

The extensive usage of data processing-based systems and services—many of which rely on Artificial Intelligence (AI) and, more precisely, Machine Learning (ML) algorithms—defines the present day. Detecting fraudulent transactions continues to be a major challenge for financial institutions worldwide. The banking sector must have sophisticated fraud detection systems in place to protect their assets and maintain consumer confidence, but there are a few obstacles that must be overcome in order for such systems to be developed effectively and efficiently. Sensor networks, which constitute the basis of the Internet of Things, are employed in applications related to safety, healthcare, and the military. Threats to the safety of the Internet of Things-based Wireless Sensor Networks (IoT-WSNs) can come from a variety of sources. This research presents safe attack localisation and detection in IoT-WSNs to improve security and the provision of services. Before beacons nodes broadcasted data to the base location, the approach generated block chain trust values using a hierarchical architecture based on block network-based cascade encrypting and trust assessment. Furthermore, deep learning systems lack the explain ability of the projected outcomes, which is often needed in medical health. This makes them similar to "black boxes." This restricts how deep learning may be used in actual healthcare systems. Malicious nodes are classified using federated learning. Federated learning combines methods such hybrid random forests, gradients boost, collective wisdom, K mean clustering, and guidance vector machine learning with a feature evaluation process to classify risky nodes. Compared with the current approaches, average recognition and categorization accuracy of the proposed system is 100% for binary and 98.95% for multiple classes. This demonstrates the effectiveness of the suggested approach for large-scale IoT-WSNs in terms of both performance and security. The suggested approach leverages heterogeneous wireless sensor networks to provide secured services.

Keywords: - IoT-WSNs, Artificial Intelligence (AI), Fraudulent Transactions, Federated Learning, Machine Learning (ML), Deep Learning Models, Malicious Nodes, Classification Accuracy, Blockchain-Based, Fraud Detection Systems, Detection Systems.

I. INTRODUCTION

Technological products and applications are increasingly being built on the de facto standard foundations of Artificial Intelligence (AI) and Machine Learning (ML) techniques [1]. These

days, they are often used in both the public and commercial sectors in a wide range of everyday procedures. In fact, they are so widespread that organisations have been forced to consider whether or not to implement certain policies that also take ethical considerations into account [1, 2]. The G7 partners emphasised the significance of the “vision of centred around people AI which drives advancement and development in the online economics” in a Declaration they released in 2017 [2]. A group of impartial experts was commissioned by the European Commission to create the "Ethic Instructions for Reliable AI" a year later, in 2018. A proposal for a "control of the European parliament and of the council laying down uniform guidelines on artificial intelligence" was then submitted in 2021 [2]. The authors outline certain conditions that an AI system must satisfy in order to be deemed "trustworthy": All parties involved, from service providers to end users, often see "privacy and data governance" and "transparency" as essential first steps in building confidence [2, 3]. Organisations that own data often see privacy as of the highest importance and are hesitant to share it with other parties [3]. This may be the result of disparate internal procedures used by several firms or even by divisions within the same company; also, data is valued highly by businesses and is sometimes used to gain a "unfair advantage" over rivals. Lastly, sensitive information found in user data must be handled cautiously to prevent privacy concerns [3]. Because standard machine learning techniques depend on the availability of the whole dataset, which is kept on a single, centralised server, they are not necessarily practical in these situations when private raw data is dispersed across many different geographic regions [3, 4]. However, not every data owner may have enough data to adequately train an AI model when data are inherently and organically [5], dispersed in separate silos. These factors make it necessary to develop new paradigms and provide substitute techniques. A few months ago, Federated Learning (FL) was offered in the literature as a potential solution to the data security problem. The basic concept behind FL is to use local data to build local AI models, which are then aggregated to create a global aggregating models [4, 5].

What makes so-called trustworthy AI so trustworthy is its explanation; for instance, as stated in "[...] artificial intelligence systems and their decisions should be clarified in a manner adapted to the stakeholders concerned." Additionally, GDPR recital 71 states that: "[...] In any case, this processing should be supported by suitable safety precautions, which ought to offer specific details regarding the data displayed and the right to collect human oversight, [5], to express one's point of view, to acquire an explanation of the decision that was reached after such evaluation, and to difficulties the selection." This has led to increased interest in Explicable Artificial intelligence (XAI) from companies and academics. FED-XAI, an acronym for federation instruction of XAI models, [5], is a project that attempts to progress the creation of trustworthy artificial intelligence. Fed-XAI's goal is to provide the following technical and methodological solutions: on the one hand, to use the FL technique to protect privacy while ML/AI models are jointly trained. Conversely, [6], in order to guarantee a sufficient level of explain ability of the systems constructed using AI themselves. In fact, from the first studies in the FL literature, the majority of solutions have centred on Federated Averaging (Fed Avg), [6, 7], which was first proposed as a protocol for carrying out Stochastic Gradient Descent (SGD) in a federated fashion. Specifically, [7], the authors demonstrated how

Deep Neural Network (DNN) architectures may be jointly trained to address tasks like language modelling and picture classification [8].

1.1 Federated Learning: Foundational Ideas

There are several surveys accessible on FL. We cover some of the key fundamental principles in this section. In FL, an ML model is cooperatively trained by a number of parties (or clients). In standard FL, a central server manages the learning process, [8, 9], and the primary goal of FL algorithms is to jointly optimise a globally differentiable objective function, for example, by using suitable Stochastic Gradient Descent (SGD) versions like Fed Avg and Federation SGD (Fed SGD). Fed Avg repeats the following stages in a round-based process:

(i) A selected number of the data owner receives the global model from the server;
(ii) Using its local data, [8], each data owner modifies the model using one or more SGD steps before sending it back to the service;
(iii) To create a new global model, the server averages the locally updated models and weights them based on the quantity of samples.

In several practical situations, Fed Avg has been utilised to perform federated learning of models like DNN and SVM. The enhancement of Google Keyboard's query suggestion is a well-known case study. The primary way that Fed SGD and Fed AVG vary from one another is that clients send gradients—instead of model parameters—to a centralised server, [8], which aggregates them and modifies the model parameters. FL schemes are generally divided into three categories: horizontal, vertical, and hybrid teaching schemes, depending on how the data are divided up among the many local devices [8, 9].

1.2 Federated Learning

AI models may perform better (i.e., achieve high precision based on decreased bias) when they make use of data from many sources. But wirelessly gathering and storing auxiliary data for analysing on a central server has grown more and more unfeasible for two primary explanations: first, it usually introduces significant overhead in terms of computing and communication costs because of the transfer and storage of huge training data sets; second, [8, 9], it breaches data owners' confidentiality and safety necessities by increasing the area available for potential over-the-air assaults that could lead to biased decision making. Stated differently, people who possess data often have reservations about sharing it with outside parties, [9], hence AI/ML systems of today need to put user privacy first. Users may choose to authorise to the sharing of data that is significant to their privacy in particular countries (e.g., in accordance with the General Security and Privacy Regulation—GDPR in the European Union) [9]. But demand to preserve data owners' privacy is driven by the necessity to collect data in order to train accurate machine learning designs, which are frequently database-hungry throughout their learning stage. To circumvent these limitations, [9, 10], FL was originally proposed as a privacy-protecting paradigm for collaboratively building AI models. In a FL system, players continually train a shared model by communicating just local improvements to the model and an aggregation shared models update, compared to data in its entirety [10].

1.3 FED-XAI: Integrating Explainable AI and Federated Education

The following issues are ignored by current AI-based solutions for wireless network planning, design, and operation:

(i) The need to protect data privacy everywhere, [11], especially while transferring and storing data wirelessly, and
(ii) The models' capacity for explanation [10, 11].

Furthermore, in order to meet the latency and reliability requirements of safety-critical automotive interaction, centralised and lighter intelligence must be seamlessly available. This allows data to be generated and decisions to be taken at any time and from any place [12].

FL approaches currently only handle the first condition. Less research has been done on explain ability because the majority of techniques use post-hoc techniques like Shapley values to measure feature relevance. For intrinsically comprehensible designs, [12, 13], there are relatively few ways to FL. However, a federated approach to developing interpretable-by-design models that guarantees accountability for each decision would be an important milestone towards reliable AI. Thus, we present the idea of FL of XAI (FED-XAI) models as an structure with two goals: first, to use FL for privacy protection during cooperative training of AI develops, which is particularly appropriate in heterogeneous B5G/6G situations; and second, to guarantee a sufficient degree of mutual explanation among the models (which involves the combined model that was acquired as the consequence of FL).

1.4 Federated Learning Frameworks

We provide an index of generally used platforms in which FL methods have been implemented. The webpage reference for each structure, together with the appropriate creating organisation, is mentioned [13].

- **Tensor Flow Federation Framework (TFF):** is an open-source system for Deep Learning (DL) using distributed data [13]. It offers a limited number of aggregation algorithms and presently supports only a simulation versions on only one node (as such, it is unable to be deployed in an actual federated environment with several nodes).
- **Federated AI Technologies Enablers Framework (FATE):** This is an open-source project [13, 14]. We Bank's AI Department began it to create a safe foundation for a federation artificial intelligence system.
- **Open Federated Training (Open FL):** is a platform for open-source software for Federated Learning created by Intel Labs in conjunction with the University of Pennsylvania [14]. It runs a federated training process using a centralised approach: a server component (Aggregator) accepts the parameters for the model from users (Collaborators) and aggregate them to construct the global model.
- **IBM Federated Learning (IBM FL):** is a production-oriented FL architecture designed to be simple to use and deploy quickly in a real-world distributed setting. It's a modular Python library [14, 15].

This study offers a centralised IDS (intrusion detection system) for pooled mining in the block chains enabled Internet of Things networks, which is built on fog computing. It includes secure architecture and modelling, identifying attacks, and classification. Machine learning

approaches for hybrid federalism are used to train the suggested IDS. A brief overview of the suggested distributed methodology is presented in Figure 1 [15]. The essential parts of the recognition system are the sensing nodes, which are in charge of tracking and detecting any moving objects coming within range. All IoT sensors are divided into a number of groups, each with the same detection capabilities, based on the outcomes obtained in lab and classroom settings. This cluster sends information to nearby nodes that generate fog. Fog nodes need to include a system with an intrusion detection system as part of their security architecture since they act as IoT device gateways or access points. IDS analyses incoming traffic and, based on its analysis, takes the right response [15, 16].

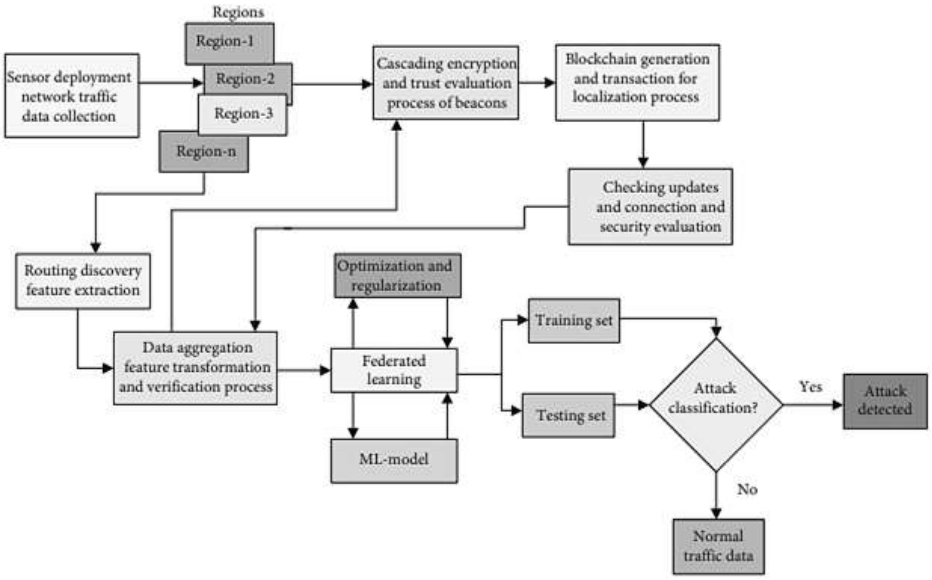

Fig. 1 Using federated learning to perform block chain-based secured localisation detects assaults in IoT-based wireless sensing networks. [16].

1.5 IoT-based Networking Design

The network model is made up of ten zones with various types of nodes containing wireless sensors operating under various processing processes. As seen in Figure 2, each area has been divided into groupings. The nodes' computer capacity and data processor abilities determine whether they are categorised as nodes for sensors, [16, 17], sink nodes, or heads of clusters. Every node's sensors are thought to be dispersed randomly and are oblivious to their precise position and orientation. Simultaneously, [17, 18], the sink and a beacon node locations know where they're located and powers, and they help other nodes that sense find the sensor nodes and identify the malicious nodes by calculating the distance between every one of them and where it is at the moment, since each node has a unique identifier [18, 19].

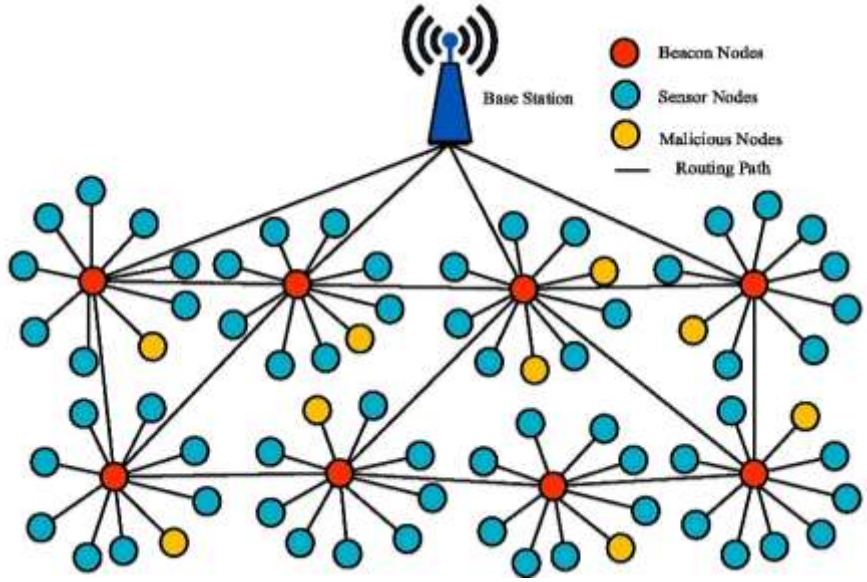

Fig. 2 A proposed hierarchy IoT-based wireless sensors network paradigm for safe location of hostile components. [20].

1.6 Objectives of the study

- A proposed hierarchy IoT-based wireless sensors network paradigm for safe location of threatening components.
- Evaluate federated learning model' performance and scalability, including training effectiveness, accuracy, and resources utilisation on cloud infrastructure.

II. LITERATURE REVIEW

(Konečný, J., 2016) [21] The goal of federated learning, in in an AI setting, is to train an outstanding centralised model with training data distributed across numerous clients with erratic and slow connection to the network. In this case, we study learning strategies where each client uses its local input to compute a modification to the existing modelling and transmits it to a central server where the client-side adjustments are combined to calculate a new global model. Since mobile phones are the typical clients in this situation, communication efficacy is crucial.

(Hu, B., 2018) [22] Sparse sensory data as a result of limited monitoring locations and missing recordings becomes the primary problem of fine-grained environment sense. In this research, we provide Federated Region-Learning (FRL), a new inference framework for urban environment sensors. The proposed approach builds on the fundamental notion of federated learning while additionally taking regional factors into account when distributing training samples in order to increase inference accuracy. Furthermore, we use an edge computing architecture to implement the FRL and improve the computational speed. We also use FRL for PM2.5 monitoring in Beijing.

(Holzinger, A., 2018) [23] The study of digital pathology is a rapidly emerging field in basic research as well as one of the most promising areas of diagnostics healthcare. There is more to digital pathology than just scanning histopathology slides and turning them into digital images.

Through the integration of diverse data sources such as images, records for patients, and *omics data, along with the latest developments in AI and machine learning, an individual specialist can now retrieve and measure new information that is presently unobtainable and not utilised in healthcare environments. The ultimate goal is to develop a level of employable intellect to comprehend the data within the framework of the programming task, making machine decisions observable, comprehensible, and understandable.

(Selviandro, N., 2013) [24] Increased research in technology-related subjects has a favourable influence on the field of education. The adoption of e-learning is one of information technology's contributions to the field of education. Several colleges and universities in Indonesia have introduced e-learning programmes. E-learning offers several advantages, including flexibility, variety, and assessment. Whether commercial or open source, modern e-learning solutions need significant expenditures in infrastructure technologies.

III. PROPOSED SYSTEMS

The suggested method for detecting and localising malicious nodes comprises of multiple steps for recognising and [25], eliminating threats in IoT-based wireless networked sensors that use hybrid and federation learning-based block chain technologies [25, 26].

$$|N| = |B| + |U|. \ldots\ldots..1$$

$$T_R = (T_{max} - 1) + \text{random}\ (0,1) \times [(T_{min} - 1) - (T_{max} - 1)] + 1. \ldots.2$$

$$D = \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2}. \ldots\ldots.3$$

$$D_{tri} \begin{cases} \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2} \\ \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2} \\ \sqrt{(u_i - u_j)^2 + (v_i - v_j)^2} \end{cases} \ldots\ldots\ldots.4$$

3.1 Data Pre-processing and Feature Identification

Data about traffic from a set of benchmarks or a neighbourhood network can be gathered using the data collection a component. Before the data is used, it is gathered and filtered by the preliminary processing modules (Fig. 3) [26]. For significantly more efficient data transfer, this information is also supplied to the trust-based safer route module and clusters [26, 27].

$$Z_{norm} = \frac{Z - \min(z)}{\max(z) - \min(z)} \ldots\ldots\ldots..5$$

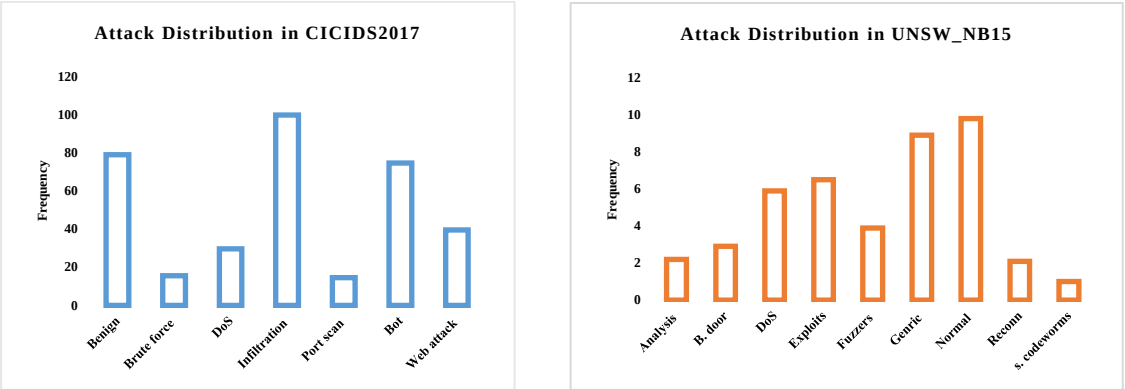

Fig. 3 Attacks in the CICIDS2017 and UNSW_NB15 comparable datasets were shown as a frequency distribution. [27].

$$\emptyset(X) = \sum_{k=1}^{k} f_k(X) \quad f_e eF, \ldots\ldots\ldots 6$$

$$\mathfrak{H}(\emptyset) = \sum l(f_{t-1} + f_t) + \Omega(f_t), \ldots\ldots\ldots 7$$

$$w = \sum_{i=1}^{n} a_i y_i x_i \min\left\{\frac{||w||^2}{2} + C\sum_{i=1}^{n} \varepsilon_i\right\}, \ldots\ldots 8$$

IV. SIMULATION RESULT

Simulations data from many simulated situations is used to validate the suggested design. Table 1. The recommended method effectively locates and identifies rogue nodes in Internet of Things-based sensor networks that are wireless, according to the simulated data.

Table 1 Simulations setup for the proposed networking model. [26].

Parameter	Value	Parameter	Value
Software	Mat lab	Total sink nodes	10
Number of sensors	1600	Number of cluster	56
Protocol type	Crusting	Attacks	500, 2960
Total beacon nodes	30000×2400 m2	Mobility	Routing
Total unknown nodes	120	Transmission radius	Random
Total edge servers	10	Data size	240

When the PoA agreement method is used, predesignated stations are in charge of accepting transaction and appending additional blocks to the current block chain [26, 27]. The variation in IoT-WSN gas consumption by area and power level in region 1 IoT-WSNs during network providing is depicted in Figure 4(a). For instance, [28], Figure 4 (b), contrasts PoW and PoA with the average petrol usage for IoT-WSNs across all 10 destinations.

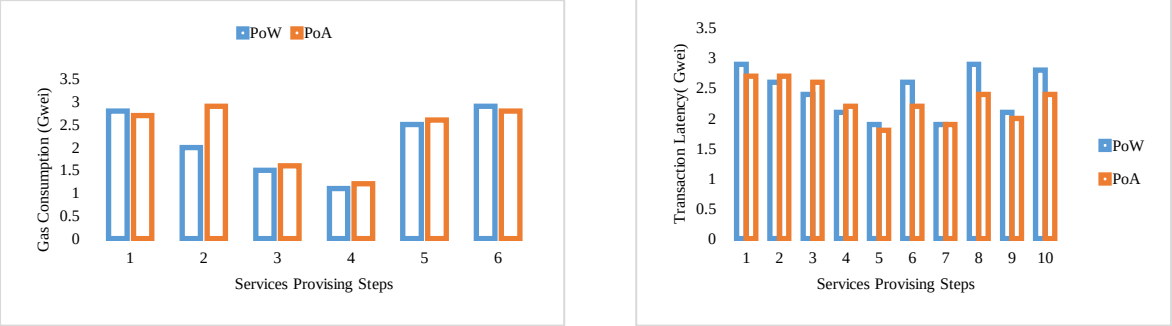

Figure 4 Gas usage and transaction delay of various locations in IoT-based wireless sensor networks. [28].

4.1 The localization process Accuracy

Localization Error (LE), Average Localization Error (ALE), localization accuracy of unknown nodes of sensors, [28], and the matrix of confusion derived on the CICIDS2017 benchmarks dataset for attack categorization are used to test the profitability of the proposed system. The distance between the anticipated location and the actual place is measured by a localization inaccuracy [28, 29].

$$\mathrm{LE}\sqrt{(u_i' - u_i')^2 + (v_i - v_j)^2}, \ldots\ldots..7$$

$$\mathrm{ALE} = \sum_{n=1}^{n} \frac{\sqrt{(u_i' - u_i')^2 + (v_i - v_j)^2,}}{nR} \ldots\ldots..9$$

$$\mathrm{ALA}\left(1 - \left(\sum_{n=1}^{n} \frac{\sqrt{(u_i' - u_i')^2 + (v_i - v_j)^2,}}{nR}\right)\right) \times 100\%, \ldots\ldots.10$$

The performance of the suggested technique is measured using performance measures such as detection rate, false alarm, accuracy, and recall [29]. Equation provide a mathematical picture of this:

$$\mathrm{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN}, \ldots\ldots\ldots.11$$

$$\mathrm{Detection\ rate} = \frac{TP}{TP+FN}, \ldots\ldots..12$$

$$F1 - \mathrm{score} = \frac{2\times TP}{2\times TP+FP+FN}, \ldots\ldots\ldots13$$

$$\mathrm{Precision} = \frac{TP}{TP+FN}, \ldots\ldots\ldots14$$

4.2 Performance Assessment and Validation

The suggested method is evaluated and validated by simulating and classifying hybrids and federated machine learning algorithms. Our simulation findings show that the proposed system's federated-based artificial intelligence algorithms can detect, [29, 30], localise, and categorise hostile nodes in a virtual network. The suggested model was simulated to estimate

its gas utilisation, delay and response time, gathering of data, remained networking energy, and lost packet count.

In a genuine class, the best student is the one who can complete the task in the least amount of time and with the most honest value. Malicious nodes, however, have a low integrity score and a large end-to-end delay. The recall, [30], preciseness, F1 score, and preciseness of RF and SVM in Internet of Things-based wireless sensor networks are shown in Figures 5a and 5b [31].

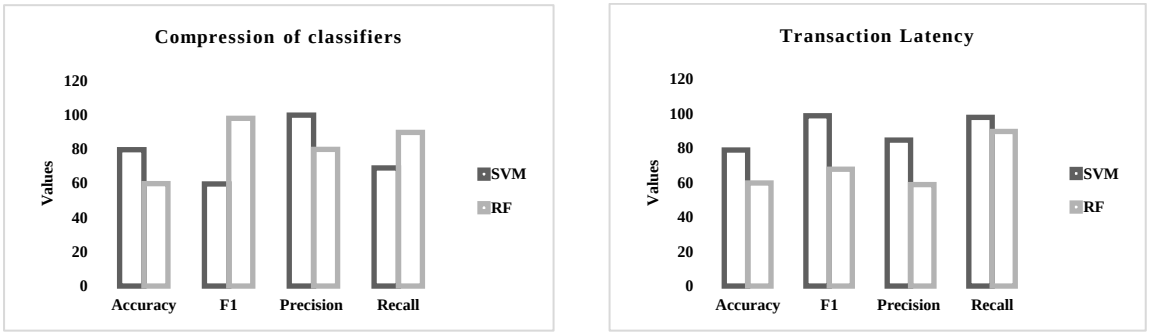

Fig. 5 Classifier performance compressing and transactional latency utilising block chain approach for identifying and localising rogue nodes in IoT-based WSNs. [31].

The same benchmarking dataset is used using hybrid optimised machine learning to assess the efficiency of suggested routing attacker localisation and detection in wireless sensor networks. Figure 6 (a) (b) compares the performance of several machine learning algorithms. The suggested system's performance is further enhanced by using Cluster Labelling (CL) K-means categorization algorithms [31, 32].

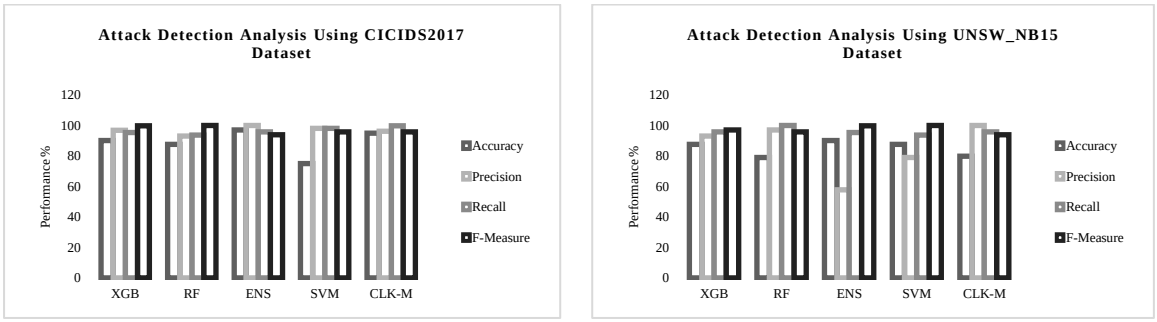

Figure 6 CICIDS2017 and UNSW_NB15 benchmark data sets are used to compare the performance of various models of machine learning using a number of performance indications. [32].

The findings reveal that the recommended technique outperforms the previously described block chain-based trust assessment approach for storing the identities of Sensor Nodes (SN) and Aggregators Nodes (AN). The approach used private and public block chains to identify nodes that were malicious with a detection rate of 75%, [33], taking malicious nodes from 20 to 80, while the recommended method achieves an accuracy rate for detection of 95%, reducing the number malicious nodes to 5-30. A system for trust assessment and security that used block chain and federated learning methods achieved average rate of detection with an accuracy of

96% and 98%, respectively [33]. Utilising a secure block chain with trust management and assessment, we achieved an average localization detection accuracy of 96.5% and an averaged localization error of 6.97 [32, 33]. Using a set of benchmark data to assess the system's detection efficiency, the DNN, CNN, and RNN learning algorithms produced average detecting accuracy rates of 98.63%, 99.71%, and 99.05 percent for FELIDS, respectively.

V. CONCLUSION

With the rising prevalence of big data-based applications in everyday life, legislative institutions have begun to debate and develop legislation to improve the efficacy of new techniques, particularly those based on AI/ML, while protecting the population's basic rights. In this setting, data privacy and the capacity to comprehend model results are two critical features to guarantee. Among various ways to addressing confidentiality of data, Federated Learning is regarded as a successful technique since it is built on the concept of developing AI/ML models without exchanging raw data with multiple data owners while incorporating information collected from all of them. In a word, this is accomplished by training the models on localised data and subsequently updating the model globally without transferring data but modelled attributes.

The suggested approach uses a block chain-based protection method to identify and localise rogue nodes in based on hierarchy dispersed IoT-WSNs. Using XG Boost and CL K-means machine learning federation classifier for multiple classes and binary identification approaches, the block chain strategy effectively detects and locates rogue the nodes in IoT-based sensor networks that are wireless. Other aims of this approach were the provision of services without the danger of attack and increased network performance, as well as feature assessment and cascade methods of encryption. Utilising multiple classes or binary labelling conduct with the CICIDS2017 benchmark data set, simulation and classification findings demonstrate that the proposed methodology meets requirements for malicious nodes identification and localization, with average determining accuracy scores of 98.69% and 100% for XG Boost and CLK-means, respectively. A novel method for identifying and localising risks in IoT-WSNs is the hybrid a federated educational system machine technological devices.

Future work

Our goal is to investigate and develop state-of-the-art block chain-based secure IoT-WSNs in the near future, utilising hybrid federalism and hybrid ML techniques for large-scale, secure, and intelligent IoT-WSN deployments. We will look at advanced hybrid control over access approaches based on block chains in order to find and recognise malicious nodes in IoT-WSNs.

VI. REFERENCES

[1] M. Marjani, F. Nasaruddin, A. Gani, A. Karim, I. A. T. Hashem, A. Siddiqa, I. Yaqoob, Big IoT data analytics: architecture, opportunities, and open research challenges, ieee access 5 (2017) 5247–5261.

[2] D. Mourtzis, E. Vlachou, N. Milas, Industrial big data as a result of IoT adoption in manufacturing, Procedia CIRP 55 (2016) 290–295.

[3] M. Mohammadi, A. Al-Fuqaha, S. Sorour, M. Guizani, Deep learning for IoT big data and streaming analytics: A survey, IEEE Communications Surveys & Tutorials 20 (4) (2018) 2923–2960.

[4] L. Van Zoonen, Privacy concerns in smart cities, Government Information Quarterly 33 (3) (2016) 472–480.

[5] J. Konečny, H. B. McMahan, D. Ramage, P. Richtárik, ` Federated optimization: Distributed machine learning for on-device intelligence, arXiv preprint arXiv: 1610.02527 (2016).

[6] U. R. Acharya, H. Fujita, O. S. Lih, Y. Hagiwara, J. H. Tan, M. Adam, Automated detection of arrhythmias using different intervals of tachycardia ECG segments with convolutional neural network, Information Sciences 405 (2017) 81–90.

[7] G. B. Moody, R. G. Mark, The impact of the MIT-BIH Arrhythmia Database, IEEE Engineering in Medicine and Biology Magazine 20 (3) (2001) 45–50.

[8] P. Angelov, D. P. Filev, N. Kasabov, Evolving intelligent systems: methodology and applications, Vol. 12, John Wiley & Sons, 2010.

[9] B. McMahan, E. Moore, D. Ramage, S. Hampson, B. A. y. Arcas, Communication-Efficient Learning of Deep Networks from Decentralized Data, in: A. Singh, J. Zhu (Eds.), Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, volume 54 of Proceedings of Machine Learning Research, PMLR, 2017, pp. 1273–1282.

[10] J. Konečný, H. B. McMahan, D. Ramage, P. Richtárik, Federated optimization: Distributed machine learning for on-device intelligence, 2016.

[11] S. M. Lundberg, S.-I. Lee, A unified approach to interpreting model predictions, in: I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, R. Garnett (Eds.), Advances in Neural Information Processing Systems, volume 30, Curran Associates, Inc., 2017.

[12] A. Abdallah, M. A. Maarof, and A. Zainal, ‘‘Fraud detection system: A survey,’’ J. Netw. Comput. Appl., vol. 68, pp. 90–113, Jun. 2016.

[13] Pascual, K. Marchini, and S. Miller. (2017). 2017 Identity Fraud: Securing the Connected Life. Javelin.

[14] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, ‘‘Data mining for credit card fraud: A comparative study,’’ Decis. Support Syst., vol. 50, no. 3, pp. 602–613, Feb. 2011.

[15] M. Zareapoor and P. Shamsolmoali, ‘‘Application of credit card fraud detection: Based on bagging ensemble classifier,’’ Proc. Comput. Sci., vol. 48, pp. 679–685, 2015.

[16] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, ‘‘Credit card fraud detection using AdaBoost and majority voting,’’ IEEE Access, vol. 6, pp. 14277–14284, 2018.

[17] McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. Y. Arcas, ‘‘Communication-efficient learning of deep networks from decentralized data,’’ in Proc. Artif. Intell. Statist. 2017, pp. 1273–1282.

[18] S. M. Lundberg and S.-I. Lee, ‘‘A unified approach to interpreting model predictions,’’ in Proc. Adv. Neural Inf. Process. Syst., vol. 30, 2017, pp. 4768–4777.

[19] X. Wan, W. Wang, J. Liu, and T. Tong, ‘‘Estimating the sample mean and standard deviation from the sample size, median, range and/or interquartile range,’’ BMC Med. Res. Methodology, vol. 14, no. 1, pp. 1–13, Dec. 2014.

[20] M. Hegland, ‘‘Data mining techniques,’’ Acta Numerica, vol. 10, pp. 313–355, May 2001

[21] Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T., & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv:1610.05492.

[22] Hu, B., Gao, Y., Liu, L., & Ma, H. (2018, December). Federated region-learning: An edge computing based framework for urban environment sensing. In 2018 ieee global communications conference (globecom) (pp. 1-7). IEEE.

[23] Holzinger, A., Malle, B., Kieseberg, P., Roth, P. M., Müller, H., Reihs, R., & Zatloukal, K. (2017). Towards the augmented pathologist: Challenges of explainable-ai in digital pathology. arXiv preprint arXiv:1712.06657.

[24] Selviandro, N., & Hasibuan, Z. A. (2013). Cloud-based e-learning: A proposed model and benefits by using e-learning based on cloud computing for educational institution. In Information and Communication Technology: International Conference, ICT-EurAsia 2013, Yogyakarta, Indonesia, March 25-29, 2013. Proceedings 1 (pp. 192-201). Springer Berlin Heidelberg.

[25] Jia Guo, Ray Chen, and Jeffrey JP Tsai. A survey of trust computation models for service management in internet of things systems. Computer Communications, 97:1–14, 2017.

[26] Yuxin Meng, Wenjuan Li, et al. Evaluation of detecting malicious nodes using Bayesian model in wireless intrusion detection. In International Conference on Network and System Security, pages 40–53. Springer, 2013.

[27] Zeeshan Ali Khan and Peter Herrmann. A trust based distributed intrusion detection mechanism for Internet of Things. In 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA), pages 1169–1176. IEEE, 2017.

[28] Umashankar Ghugar and Jayaram Pradhan. NL-IDS: Trust based intrusion detection system for network layer in wireless sensor networks. In 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), pages 512–516. IEEE, 2018.

[29] Fenye Bao, Ray Chen, MoonJeong Chang, and Jin-Hee Cho. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. IEEE transactions on network and service management, 9(2):169–183, 2012.

[30] Matthew J Probst and Sneha Kumar Kasera. Statistical trust establishment in wireless sensor networks. In 2007 International Conference on Parallel and Distributed Systems, pages 1–8. IEEE, 2007.

[31] Jorg Swetina, Guang Lu, Philip Jacobs, Francois Ennesser, and Jaeseung Song. Toward a standardized common M2M service layer platform: Introduction to oneM2M. IEEE Wireless Communications, 21(3):20–26, 2014.

[32] Hamed Haddad Pajouh, Reza Javidan, Raouf Khayami, Ali Dehghantanha, and Kim-Kwang Raymond Choo. A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Transactions on Emerging Topics in Computing, 7(2):314–323, 2016.

[33] Ekgapark Wonghirunsombat, Teewalee Asawaniwed, Vassapon Hanchana, Naruemon Wattanapongsakorn, Sanan Srakaew, and Chalermpol Charnsripinyo. A centralized management framework of networkbased intrusion detection and prevention system. In The 2013 10th International Joint Conference on Computer Science and Software Engineering (JCSSE), pages 183–188. IEEE, 2013.

[34] P. Vijayakumar, V. I. Chang, L. J. Deborah, B. Balusamy, and S. G. Padinjappurathu, "Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks," Future Gener. Comput. Syst., vol. 78, pp. 943–955, 2018.

[35] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). AI Applications in Smart Cities: Experiences from Deploying ML Algorithms for Urban Planning and Resource Optimization. Tuijin Jishu/Journal of Propulsion Technology, 40(4), 50-56.

[36] Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service . (2019). International Journal of Transcontinental Discoveries, ISSN: 3006-628X, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98

[37] Kaur, J., Choppadandi, A., Chenchala, P. K., Nakra, V., & Pandian, P. K. G. (2019). Case Studies on Improving User Interaction and Satisfaction using AI-Enabled Chatbots for Customer Service. International Journal

[38] ofTranscontinental Discoveries, 6(1), 29-34. https://internationaljournals.org/index.php/ijtd/article/view/98

[39] Choppadandi, A., Kaur, J., Chenchala, P. K., Kanungo, S., & Pandian, P. K. K. G. (2019). AI-Driven Customer Relationship Management in PK Salon Management System. International Journal of Open Publication and Exploration, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

[40] AI-Driven Customer Relationship Management in PK Salon Management System. (2019). International Journal of Open Publication and Exploration, ISSN: 3006-2853, 7(2), 28-35. https://ijope.com/index.php/home/article/view/128

[41] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[42] Shah, J., Prasad, N., Narukulla, N., Hajari, V. R., & Paripati, L. (2019). Big Data Analytics using Machine Learning Techniques on Cloud Platforms. International Journal of Business Management and Visuals, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[43] Mahesula, Swetha, Itay Raphael, Rekha Raghunathan, Karan Kalsaria, Venkat Kotagiri, Anjali B. Purkar, Manjushree Anjanappa, Darshit Shah, Vidya Pericherla, Yeshwant Lal Avinash Jadhav, Jonathan A.L. Gelfond, Thomas G. Forsthuber, and William E. Haskins.

"Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis." Electrophoresis 33, no. 24 (2012): 3820-3829. https://doi.org/10.1002/elps.201200515.

[44] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/76

[45] Mahesula, S., Raphael, I., Raghunathan, R., Kalsaria, K., Kotagiri, V., Purkar, A. B., & ... (2012). Immunoenrichment microwave and magnetic proteomics for quantifying CD 47 in the experimental autoimmune encephalomyelitis model of multiple sclerosis. Electrophoresis, 33(24), 3820-3829.

[46] Mahesula, S., Raphael, I., Raghunathan, R., Kalsaria, K., Kotagiri, V., Purkar, A. B., & ... (2012). Immunoenrichment Microwave & Magnetic (IM2) Proteomics for Quantifying CD47 in the EAE Model of Multiple Sclerosis. Electrophoresis, 33(24), 3820.

[47] Raphael, I., Mahesula, S., Kalsaria, K., Kotagiri, V., Purkar, A. B., Anjanappa, M., & ... (2012). Microwave and magnetic (M2) proteomics of the experimental autoimmune encephalomyelitis animal model of multiple sclerosis. Electrophoresis, 33(24), 3810-3819.

[48] Salzler, R. R., Shah, D., Doré, A., Bauerlein, R., Miloscio, L., Latres, E., & ... (2016). Myostatin deficiency but not anti-myostatin blockade induces marked proteomic changes in mouse skeletal muscle. Proteomics, 16(14), 2019-2027.

[49] Shah, D., Anjanappa, M., Kumara, B. S., & Indiresh, K. M. (2012). Effect of post-harvest treatments and packaging on shelf life of cherry tomato cv. Marilee Cherry Red. Mysore Journal of Agricultural Sciences.

[50] Shah, D., Salzler, R., Chen, L., Olsen, O., & Olson, W. (2019). High-Throughput Discovery of Tumor-Specific HLA-Presented Peptides with Post-Translational Modifications. MSACL 2019 US.

[51] Big Data Analytics using Machine Learning Techniques on Cloud Platforms. (2019). International Journal of Business Management and Visuals, ISSN: 3006-2705, 2(2), 54-58. https://ijbmv.com/index.php/home/article/view/