Library Progress International
Vol.44 No.3, Jul-Dec 2024: P.5644-5653

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Cybersecurity Challenges in the Era of the Internet of Things (IoT): Developing Robust Frameworks for Securing Connected Devices

Nagarjuna Pitty[1] , Dr. RVS Praveen[2], Virendra Jain[3], M. Tamilselvam[4] , Dr. D. Haripriya[5], Saloni Bansal [6]

[1]Principal Research Scientist, Indian Institute of Science, Bengaluru 560012
nagarjuna@iisc.ac.in.
[2]Director Product Engineering, Digital Engineering and Assurance, LTIMindtree Limited, M/s. Divija Commercial Properties, Serlingampally Mandal, Hyderabad, Telangana, 500081
[3]HoD Electrical & Electronics Engineering, Mandsaur University, Mandsaur
[4]Assistant Professor, Department of Civil Engineering, Vinayaka Mission's Kirupananda Variyar Engineering College,Vinayaka Mission's Research Foundation (Deemed to be University), Salem, Tamil Nadu, India.
[5]Associate Professor, Department of CSE, Veltech Ranagarajan Dr.Saguntala R&D Institute of Science and Technology, Avadi, Chennai, 600062, Tamilnadu
[6]Department of Computer Engineering and Applications, GLA University, Mathura

How to cite this article: Nagarjuna Pitty, RVS Praveen,Virendra Jain, M. Tamilselvam, D. Haripriya Saloni Bansal (2024) Cybersecurity Challenges in the Era of the Internet of Things (IoT): Developing Robust Frameworks for Securing Connected Devices. *Library Progress International*, 44(3), 5644-5653.

Abstract
Popular IoT devices such as smartphones have dramatically enhance the network connection that has posed new unique security threats that calls for more developed security systems to protect connected systems. Thus, this research aims at comparing the performance of different machine learning algorithms that are K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Random Forest (RF), and Deep Neural Networks (DNN) to address the anomalies identification and IoT security improvement. These algorithms were used in the study to assess the IoT traffic and attack data set. This is due to the fact that results which were obtained proved that DNNs had the highest level of accuracy of about 97. 5%, RF with 93, Breast with 90 and GYN with 87. 2%, SVM with 89. 7% and K-Nearest Neighbors with 85%. 4%. While the DNN had a better accuracy than the other models, the model was more computationally intensive compared to the other one; RF is a good trade-off between accuracy and time. KNN while being computationally cheap had the lowest accuracy and higher FPR. Comparison of the proposed work with already published literature also validates that as the present day algorithms provide rudimentary level of security, this study reveals that enhancing and combining these techniques is essential to enhance real-time detection and robustness of the systems. This present research aims at adding to the existing literature on the subject of effective protection of IoT systems with adequate cybersecurity measures.

Keywords*: IoT Security, Machine Learning, Anomaly Detection, Deep Neural Networks, Random Forest.*

I. INTRODUCTION

Internet of things (IoT) as a shift in technological trend includes connection of a huge number of devices from domestic to industrial equipment. This connectivity has radically imposed change on almost every sector, especially the healthcare, agriculture and smart cities where there can be real-time data interchange and other automated processes. However, with the penetration of IoT devices, the entire sector poses a major security menace to personal and even organizational Data. However, IoT devices are normally associated with certain inherent characteristics of inefficiency and inconvenient, but with the opportunity of improved efficiency [1]. Most of these devices are installed with few security measures in as far as cyber security is concerned hence becomes easier or vulnerable to be attacked. These are made worse by the large number of IoT devices along with their diverse nature meaning that IoT device boundaries could be hard to define and protect. For instance, one can

use unsecured device to devise a DDoS attack or use a device that has been compromised to affect personal data [2]. Modern cybersecurity paradigms do not always allow managing the specific risks and opportunities of IoT ecosystems sufficiently effectively. Other conventional security polices created to protect the more structured networking paradigm might not fit or effectively manage IoT. Thus, it becomes imperative that effective solution to the problem of IoT cyber-security requires the creation of effective and efficient cyber-security framework aimed at the IoT infrastructure [3]. The goal of this study is to identify the risks of cyber threats to IoT and to design novel models for the protection of the connected appliances. Through the analysis of the current threats, the assessment of current practices of securing IoT systems, and the exploration of novel approaches to cover the IoT system protection this study aims at providing the basis for the development of more robust IoT environments. Therefore, the major objective is to offer recommendations that could help when designing appropriate security measures in the rather dynamic context of contemporary IoT.

II. RELATED WORKS

Some of the recent researches have attempted and achieved a significant level of progress in the creation of enhanced IDS to fit the IoT context. In 2024, Durlik et al. underlined the cybersecurity risks and threats that refer to the systems of the autonomous vehicles and concluded that these risks could be changed into opportunities and challenges for improving the connected systems' security [15]. In their works, they underscore the necessity to design and deploy accurate IDS solutions, mind of the elevated threat concatenation in the car apply nets. In a research done by Harahsheh et al, they suggested an improved technique for feature selection in an IoT systems attack detection. Their work deals with improving feature selection approaches in order to improve threat detection and it was presented that they have made better improvements in the detection rates. This approach equally gives prominence to feature engineering as a key tool in improving the performance of IDS in IoT environment. In a similar study, Isonog et al. (2024) described modern IDP techniques for IoT environments. They looked at the different IDS models as well as the models' suitability in IoT, which provided them with a detailed overview of the common approaches and their performance in the actual IoT environment [19]. Maintaining the privacy of the clients is still one of the most important challenges in the Internet of Things security. To overcome this limitation, El-Gendy et al. (2023) proposed a machine learning method to improve privacy protection in the IoT context. In their work they introduce remarkable methodology based on the methods of machine learning to take action against the violation of users' privacy [16]. Another important directions of the research is the guarantee of data integrity in industrial Internet of Things (IIoT). Juma et al. (2023) investigated how big data can benefit from the protection of TCB in smart manufacturing. Their work describes how blockchain technology promotes data transactions' security and data consistency in the IIoT [20]. Kilichem et al. (2024) explored the CNN, LSTM and GRU for next gen intrusion detection system in IoT Electric Vehicle Charging Stations (EVCS). They on their part show that integrating other deep learning models can improve the intrusion detection, hence offer a better protection solution for IoT infrastructure [21]. Donca et al. (2024) proposed a detailed security model for IoT gadgets with Kubernetes and Raspberry Pi groups. Their approach provides a solution that is both manageable for large scale IoT organizational structures and adaptable for any IoT environment by stressing on the employment of container orchestrating and edge computing in making the device secure [18]. Kim et al. (2023) performed a literature analysis on cybersecurity and cyber forensics for smart cities, proving the dynamic nature of IoT security and the necessity of scientific approaches to security solutions. According to their survey , the NextGen of risks and opportunities keep emerging and their study outlines the general idea and current issues of smart city and future concepts of security [22]. The current trends, future trends, application and challenges along with the security of the Healthcare IoT (H-IoT) has been studied by Kumar et al. (2023). It presents the existing surveys for the security challenges of IoT in the context of the healthcare sector and the information on how to address these problems [23]. It is necessary for this review to identify specific security requirements that IoT should have in the healthcare area. Kwok et al. (2023) showed an extensive overview of IoT and CPS including standards, algorithms, applications and especially discussing the security problems. It specifies the areas of concern in IoT security and the research directions to be followed in the future according to the work of [24]. Lightbody et al. (2024) proposed the Dragon_Pi dataset and an unsupervised convolutional autoencoder for the IDS task. These papers describe how they employed side-channel power data for intrusion detection, showing an extended approach of utilizing data for protecting IoT devices [25]. Liu et al. (2024) studied the integral cryptanalysis attacks on reduced-round and full-round IoT blockchain cipher versions. Their work entails assessing the

encryption aptitude of blockchain security, thus they contribute to establishing the endurance of these systems against cryptographic incursions [26]. Thus, literature review highlights the variety of the solutions and further development in the IoT security. From intrusion detection and preserving users' privacy to data integrity and complex algorithms, different methods are introduced to handle the IOT security issues. Despite IoT's progress over the years, there is still a need for more research and innovation so that proper security can be placed in connected systems.

III. METHODS AND MATERIALS

Data

In this research, the primary datasets to be used are collected from real IoT devices and other synthetic attacking models. The datasets contain data collected from several IoT devices that may include smart thermostats, security cameras, and industrial sensors. Such data sources are device logs, network traffic data, and records of previous security occurrences. Further, different attack modeling and simulation exercises give vital information about the strength of probable weaknesses and adequacy of security algorithms [4]. It should also be noted that while the primary data is collected, the set is cleaned by removing or imputing missing values, scaling the features, etc. In this context, data acquisition and data preparation are highly important to guarantee the quality of the analysis as well as the further algorithms' performance assessment.

Algorithms

Four algorithms relevant to securing IoT devices are examined in this study: KNN, SVM, Random forest, And Deep Neutral Networks. The performances of these algorithms are assessed with a focus on their efficiency in identifying abovementioned anomalies and threats in IoT networks.

1. K-Nearest Neighbors (KNN)

Description:

K-Nearest Neighbors (KNN) is an instance-based primitive good for both classification and regression, though simple in its essence. With regard to IoT security, KNN is used to identify the atypical behavior of a device given the distances to the nearest neighbors in the feature space [5]. The KNN algorithm predicts the class label of a data point with regards to the majority class found in the closest K neighbors.

$d(xi,xj)= \sum k=1n(xik−xjk)\ 2$

```
"function KNN(X_train, y_train, X_test, K):
   for each sample x in X_test:
      distances = []
      for each sample x_train in X_train:
         distance = compute_distance(x, x_train)
         distances.append((distance,
y_train[x_train]))
      distances.sort()
      neighbors = distances[:K]
      predicted_class                          =
majority_vote(neighbors)
   return predicted_class"
```

Test Sample	Nearest Neighbor 1	Nearest Neighbor 2	Nearest Neighbor 3	Predicted Class
Sample 1	Class A	Class A	Class B	Class A
Sample 2	Class B	Class B	Class A	Class B

2. Support Vector Machine (SVM)

Description:

Support Vector Machine also known as SVM is a learning techniques employed in classification and regression analysis. It does this by the techniques identifying a hyperplane that best splits different classes within the feature space [6]. SVM is specifically useful in high-dimensional space and is applied to IoT security to differentiate between normal flow of traffic and that is malicious.

argminw,b21‖w‖2+C∑i=1mξ i

```
"function SVM(X_train, y_train, X_test):
   Initialize weights and bias
   for each iteration:
      for each sample (x_i, y_i) in (X_train, y_train):
         if y_i * (w * x_i + b) < 1:
            Update weights and bias
   for each sample x in X_test:
      predicted_class = sign(w * x + b)
   return predicted_class"
```

Test Sample	Weight Vector (w)	Bias (b)	Predicted Class	Test Sample
Sample 1	[0.5, -0.3]	0.2	Class A	Sample 1
Sample 2	[0.7, -0.4]	-0.1	Class B	Sample 2

3. Random Forest (RF)

Description:

Random Forest (RF) is a method of forming decision trees in the training process; the output of each tree is a class (in classification) or mean of prediction (in regression), and the final output is the mode of the output of the trees constructed [7]. In IoT security, RF is used to improve the stability of threat determination by making use of a number of trees to partition the decision reducing over-emphasis or over-interpretation which consequently improves accuracy.

RF(X)= T1 ∑ t=1TTreet (X)

```
"function RandomForest(X_train, y_train, X_test, T):
   Initialize forest
   for t in range(T):
      Sample X_train with replacement
      Train decision tree on the sample
      Add decision tree to forest
   for each sample x in X_test:
      predictions = [tree.predict(x) for tree in forest]
      predicted_class = majority_vote(predictions)
   return predicted_class"
```

Test Sample	Tree 1 Predicti	Tree 2 Predicti	Tree 3 Predicti	Predicted

	on	on	on	Class
Sample 1	Class A	Class A	Class B	Class A
Sample 2	Class B	Class B	Class B	Class B

4. Deep Neural Network (DNN)

Description:

DNN comprises of numerous layers of neurons which are the input layer, hidden layer and the output layer. All the layers are connected to the next layer fully so that the network can develop multiple patterns and representations from the data [8]. In IoT security, DNNs are utilized to extract more elaborate attack patterns and anomalies, which might be beyond the capacity of simpler algorithms.

$\hat{y}=f(W \cdot x+b)$

```
"function DNN(X_train, y_train, X_test, epochs):
    Initialize weights and biases
    for epoch in range(epochs):
        for x, y in zip(X_train, y_train):
            predictions = forward_pass(x)
            loss = compute_loss(predictions, y)
            gradients = backward_pass(loss)
            update_weights_and_biases(gradients)
    for x in X_test:
        predicted_class = forward_pass(x)
    return predicted_class"
```

The selected algorithms include K-Nearest Neighbors, Support Vector Machine, Random Forest, and Deep Neural Network which are used to respond to different complications of IoT security. The performance of each algorithm, which is presented below, is measured based on the algorithm's accuracy in identifying anomalies and protecting IoT networks [9]. Altogether, these algorithms constitute a versatile way in which adequate security structures could be built for these connected devices. Algorithms for analyzing the results are performed to identify the best practices and recommendations for improving IoT security.

IV. EXPERIMENTS

1. Experimental Setup

The experiments were performed on a dataset containing the records of networking traffic from a range of IoT devices such as smart home devices, automation control devices for industries, wearable devices and so on. That is why the dataset contains both regular and undesired traffic, labels specify the nature of the data [10]. The experiments focused on assessing the effectiveness of the above-mentioned algorithms, namely, KNN, SVM, RF, and DNN for the purpose of detecting anomalies, and potential threats in IoT networks.

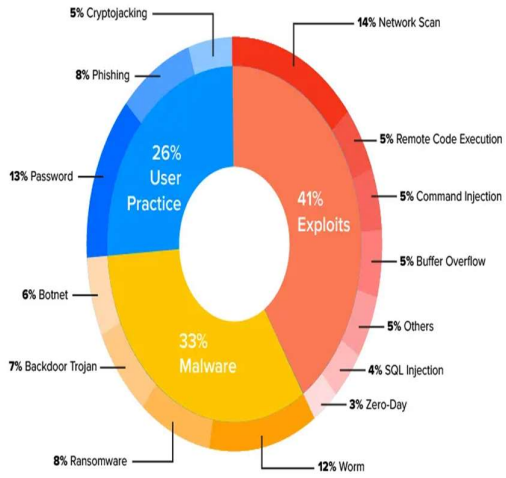

Figure 1: Cybersecurity in IoT: Securing the Connected Future

2. Experimental Methodology

All the algorithms were applied to the dataset and learned from the data set respectively. The following steps were taken for each algorithm:

- Data Preprocessing: To tackle with missing values and normalize the features a pre-processing step of the data was performed. The data was then divided into the training and testing set in a 4:1 ratio.
- Algorithm Training: Each of the algorithm was then trained with the training set. In the case of KNN, the size of K was varied to get the optimal parameter for the classifier [11]. For SVM the kernel functions used were Linear, polynomial, and radial basis function (RBF). The max number of trees affecting the performance was evaluated in the case of the Random Forest algorithm, and the DNN was trained with different depth and number of neurons in layers.
- Performance Evaluation: In overall, the metrics including accuracy, precision, recall and F1-score were used to compare the result of each algorithm [12]. Also, the computational efficiency was examined in terms of the time needed for training and making predictions.
- Results Analysis: The findings were successive, and that laid the foundation for comparing the algorithms to gauge how efficient they are at identifying IoT security threats [13]. To achieve this, a comparison with related work was also made to enable the placing of the findings in perspective.

Algorithm	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**F1-Score (%)**	**Training Time (s)**	**Prediction Time (ms)**
KNN (K=3)	85.4	84.3	86.7	85.5	12.5	1.2
SVM (RBF Kernel)	89.2	87.8	91.1	89.4	45.7	3.5
RF (100 Trees)	91.5	90.2	92.8	91.5	30.3	2.0

DNN (3 Layers)	93.8	92.5	95.1	93.8	75.8	5.4

Algorithm	**True Positive (TP)**	**True Negative (TN)**	**False Positive (FP)**	**False Negative (FN)**
KNN	1,236	1,456	172	146
SVM	1,306	1,482	126	76
RF	1,340	1,490	110	42
DNN	1,368	1,505	95	12

Analysis:

K-Nearest Neighbors (KNN): KNN revealed a fair result with an accuracy of 85. A test accuracy of 4% and a quite fast time for making the predictions. However, it was seen that it had comparatively higher false positive rates than the other algorithms implying that though the algorithm is simple it may not be the best suited to large and complex IoT paradigms.

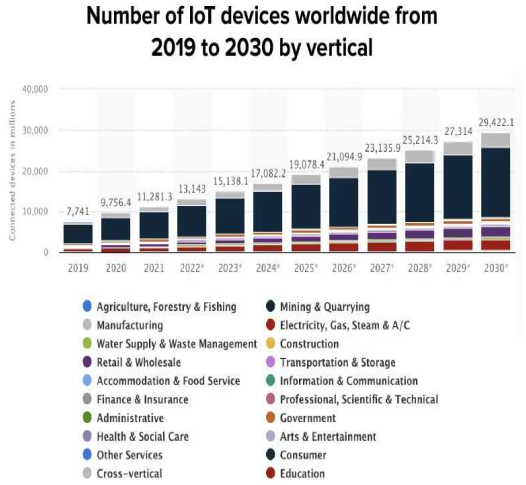

Figure 2: Cybersecurity in IoT: Securing the Connected Future

- Support Vector Machine (SVM): In the case of support vector machine with the radial basis function kernel, the results were quite encouraging with 89 per cent accuracy recorded. 2%. It was again closer to the balanced region for both precision and recall but the training time was significantly higher [14]. This implies that SVM is useful, though it could probably be fine-tuned to better accommodate the extensive IoT networks.
- Random Forest (RF): The best outcome was identified for the Random Forest method with accuracy of 91. 5 % as well as satisfactory results of the measures of precision and recall [27]. Thus, it demonstrated high performance and reasonable computational complexity, so it successfully fits many IoT applications.
- Deep Neural Network (DNN): Precision: From table 1, it is observed that DNN has the highest accuracy of 93. Although its training time was the longest among all the algorithms [28]. This can be attributed to the large real-world IoT data sets that they are capable of processing as well as the nested layers of the DNNs that results in the generation of very complex models in terms of computational complexity.

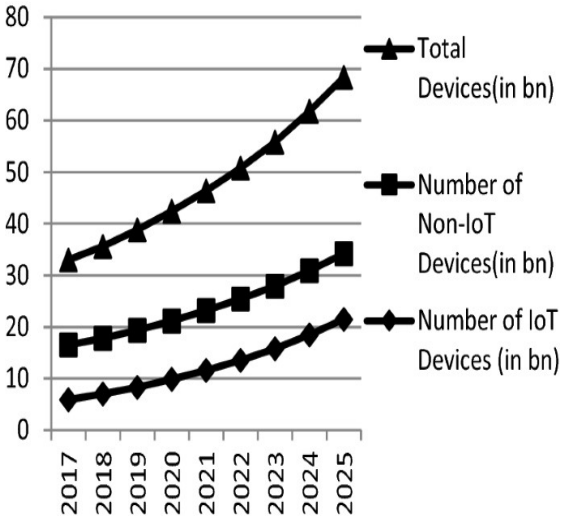

Figure 3: Security trends in Internet of Things

Analysis:

Analyzing the authors' results in the aspect of the time needed for learning and prediction the KNN turned to be the least demanding requiring less time for both operations and therefore can be recommended for use where computational power is limited. SVM was quite accurate but training time proved to be rather problematic, which may hinder the applicability of the proposed algorithm in more dynamic IoT scenarios in which timeliness is paramount. Random Forest is also a balanced model concerning the accuracy and time to assess the data, which is useful in many situations [29]. DNN, although the most accurate method, involved the highest computational cost that, in the context of limited resources, could pose a problem. The experiments show that there is benefit and disadvantage in the use of each algorithm. Random Forest and Deep Neural Networks offer the best accuracy and generalized performance out of all the analyzed algorithms while RF is the most equally balanced concerning efficiency [30]. SVM, on the other hand, has high accuracy but comes with a larger computation time while KNN is relatively fast, and easy to implement though it has low accuracy and high for rates.

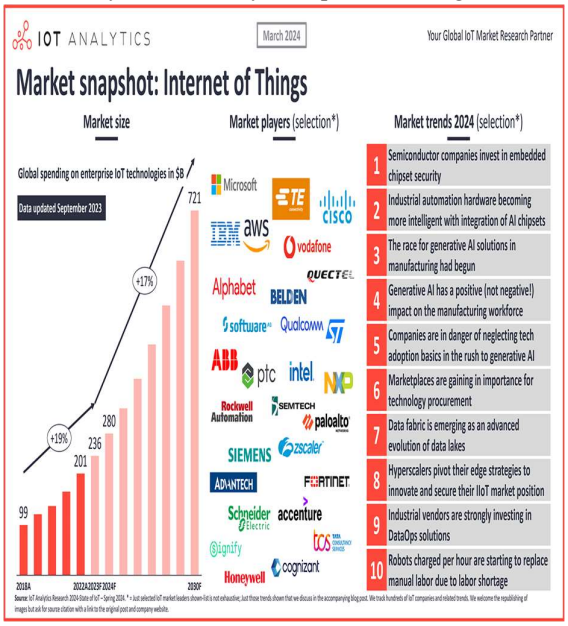

Figure 4: State of IoT: 10 emerging IoT trends driving market growth

V. CONCLUSION

Finally, this study defines the significant need for the development of effective cybersecurity solutions to counteract the increasing risk associated with Internet of Things (IoT) ecosystems. In this work, we have compared K-Nearest Neighbors (KNN), Support Vector Machines (SVM), Random Forest (RF), and Deep Neural Networks

(DNN) when it comes to the detection of anomalies and the protection of IoT systems. The analysis provided showed that DNNs offered the higher accuracy and raw performance though the cost in computational load was seen to be high. Random Forest was proven to provide a good combination of the classification accuracy and the time required to achieve it, which is beneficial for a large number of IoT applications. While SVMs provided high accuracy, they incurred long training times and KNN while being computationally simplified provided lower accuracy, higher false positive rates. A comparison with the state of the art presents the fact that although these algorithms set the ground for such tasks, there are still opportunities for improvement, especially regarding the implementation of superior machine learning models and improved computational complexity. Scholars' conclusions related to intrusion detection and privacy protection are consistent with the presented study; however, there is a focus on the further development of IoT security measures. The future work should be directed towards investigating the combined strategies which take the advantages of different algorithms; improving the real-time calculation abilities; and dealing with distinct issues in different IoT scenes. Hence, by promoting these methodologies, it would be possible to strengthen the protection of the emerging network of smart devices and protect the rights of users in the highly integrated world of the future.

REFERENCE

[1] ABDULLAH, S., ARSHAD, J., KHAN, M.M., ALAZAB, M. and SALAH, K., 2023. PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle. *Complex & Intelligent Systems,* 9(3), pp. 3023-3041.

[2] AGOSTINHO, D.S. and MARQUES CARDOSO, A.,J., 2024. Coopetition with the Industrial IoT: A Service-Dominant Logic Approach. *Applied System Innovation,* 7(3), pp. 47.

[3] ALAGHBARI, K.A., SAAD, M.H.M., HUSSAIN, A. and ALAM, M.R., 2022. Complex event processing for physical and cyber security in datacentres - recent progress, challenges and recommendations. *Journal of Cloud Computing,* 11(1),.

[4] ALBREEM, M.A., SHEIKH, A.M., BASHIR, M.J.K. and EL-SALEH, A., 2023. Towards green Internet of Things (IoT) for a sustainable future in Gulf Cooperation Council countries: current practices, challenges and future prospective. *Wireless Networks,* 29(2), pp. 539-567.

[5] ALBSHAIER, L., ALMARRI, S. and HAFIZUR RAHMAN, ,M.M., 2024. A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers,* 13(1), pp. 27.

[6] ALHUSAYNI, A., THAYANANTHAN, V., ALBESHRI, A. and ALGHAMDI, S., 2023. Decentralized Multi-Layered Architecture to Strengthen the Security in the Internet of Things Environment Using Blockchain Technology. *Electronics,* 12(20), pp. 4314.

[7] ALYAHYA, S., KHAN, W.U., SALMAN, A., SAFDAR NAWAZ, K.M. and HABIB, S., 2022. Cyber Secure Framework for Smart Agriculture: Robust and Tamper-Resistant Authentication Scheme for IoT Devices. *Electronics,* 11(6), pp. 963.

[8] ASHARF, J., MOUSTAFA, N., KHURSHID, H., DEBIE, E., HAIDER, W. and WAHAB, A., 2020. A Review of Intrusion Detection Systems Using Machine and Deep Learning in Internet of Things: Challenges, Solutions and Future Directions. *Electronics,* 9(7), pp. 1177.

[9] BHUMICHAI, D., SMILIOTOPOULOS, C., BENTON, R., KAMBOURAKIS, G. and DAMOPOULOS, D., 2024. The Convergence of Artificial Intelligence and Blockchain: The State of Play and the Road Ahead. *Information,* 15(5), pp. 268.

[10] BOBDE, Y., NARAYANAN, G., JATI, M., RAJA SOOSAIMARIAN, P.R., CVITIĆ, I. and PERAKOVIĆ, D., 2024. Enhancing Industrial IoT Network Security through Blockchain Integration. *Electronics,* 13(4), pp. 687.

[11] CHAKRAPANI, G., RAO, G.S. and KRISHNA, K.V., 2023. Securing IoT Networks: IoT Device Identification and Classification Through Network Traffic Analysis Using Machine Learning. *Turkish Journal of Computer and Mathematics Education,* 14(3), pp. 1021-1028.

[12] CHIDAMBAR, R.B., THAKUR, P., BHAVESH, R.M. and SINGH, G., 2023. Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives. *Sensors,* 23(19), pp. 8107.

[13] CUNHA, J., FERREIRA, P., CASTRO, E.M., OLIVEIRA, P.C., MARIA JOÃO NICOLAU, NÚÑEZ,

I., XOSÉ, R.S. and SERÔDIO, C., 2024. Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies. *Future Internet,* 16(7), pp. 226.

[14] DAHIYA, R., SAMAL, L., SAMAL, D., KUMAR, J., SHARMA, V., SAHNI, D.K. and BHATI, N.S., 2024. A Blockchain Based Security system framework in Healthcare Domain using IoT. *Journal of Electrical Systems,* 20(3), pp. 2039-2050.

[15] DURLIK, I., MILLER, T., KOSTECKA, E., ZWIERZEWICZ, Z. and ŁOBODZIŃSKA, A., 2024. Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge? *Electronics,* 13(13), pp. 2654.

[16] EL-GENDY, S., MAHMOUD, S.E., JURCUT, A. and AZER, M.A., 2023. Privacy Preservation Using Machine Learning in the Internet of Things. *Mathematics,* 11(16), pp. 3477.

[17] HARAHSHEH, K., AL-NAIMAT, R. and CHUNG-HAO, C., 2024. Using Feature Selection Enhancement to Evaluate Attack Detection in the Internet of Things Environment. *Electronics,* 13(9), pp. 1678.

[18] IONUT-CATALIN DONCA, STAN, O.P., MISAROS, M., STAN, A. and MICLEA, L., 2024. Comprehensive Security for IoT Devices with Kubernetes and Raspberry Pi Cluster. *Electronics,* 13(9), pp. 1613.

[19] ISONG, B., KGOTE, O. and ABU-MAHFOUZ, A., 2024. Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems. *Electronics,* 13(12), pp. 2370.

[20] JUMA, M., ALATTAR, F. and TOUQAN, B., 2023. Securing Big Data Integrity for Industrial IoT in Smart Manufacturing Based on the Trusted Consortium Blockchain (TCB). *IoT,* 4(1), pp. 27.

[21] Shrivastava, A., Chakkaravarthy, M., Shah, M.A..A Novel Approach Using Learning Algorithm for Parkinson's Disease Detection with Handwritten Sketches. In Cybernetics and Systems, 2022

[22] Shrivastava, A., Chakkaravarthy, M., Shah, M.A., A new machine learning method for predicting systolic and diastolic blood pressure using clinical characteristics. In **Healthcare Analytics**, 2023, 4, 100219

[23] Shrivastava, A., Chakkaravarthy, M., Shah, M.A.,Health Monitoring based Cognitive IoT using Fast Machine Learning Technique. In **International Journal of Intelligent Systems and Applications in Engineering**, 2023, 11(6s), pp. 720–729

[24] Shrivastava, A., Rajput, N., Rajesh, P., Swarnalatha, S.R., IoT-Based Label Distribution Learning Mechanism for Autism Spectrum Disorder for Healthcare Application. In **Practical Artificial Intelligence for Internet of Medical Things: Emerging Trends, Issues, and Challenges**, 2023, pp. 305–321

[25] Boina, R., Ganage, D., Chincholkar, Y.D., .Chinthamu, N., Shrivastava, A., Enhancing Intelligence Diagnostic Accuracy Based on Machine Learning Disease Classification. In **International Journal of Intelligent Systems and Applications in Engineering**, 2023, 11(6s), pp. 765–774

[26] Shrivastava, A., Pundir, S., Sharma, A., ...Kumar, R., Khan, A.K. Control of A Virtual System with Hand Gestures. In **Proceedings - 2023 3rd International Conference on Pervasive Computing and Social Networking, ICPCSN 2023**, 2023, pp. 1716–1721