Dijlah Journal of Engineering Sciences (DJES) Vol. 2, No. 2, June 2025, pp. 161-170
ISSN: **Printed: 3078-9656, E: 3078-9664**, paper ID: 45

Accurate and High Security of IoT System using Machine Learning Algorithms

Bushra Naeem Abdul Razzaq Al-mafrachi
Department of Computer Sciences, College of Education for women, Kufa University

Article Info

Article history:

Received April, 15, 2025
Revised May, 2, 2025
Accepted June, 4, 2025

Keywords:

Security
Machine Learning
Internet of Things

ABSTRACT

The network computing device that work and communicated without human interference is referred to term of "Internet of Things" (IoT). Currently, this technology is the utmost excite area of computing with its application in numerous areas like city, home, infrastructures, hospital, and transportations. The security issue surrounds IoTs device increased as they develop. In order to addressed this issue, this paper present a new idea for enhance the security of IoTs system by use machines learning (MLs) classifier. The suggested methods analyze latest technology, security, intelligent solution, and vulnerability in MLs IoTs-base intelligent system as an vital technologies to develop IoTs security. This paper illustrate the benefit and limitation of apply the MLs in an IoTs environments and provide a security models depend on MLs that manage originally the increasing numbers of security issue associated to the IoT domains. In addition, this approach suggests an ML-base security models that independently handle the rising numbers of security issue related to the IoT area. This investigation introduced a significant contributions by developed a cyber-attacks recognition solutions for IoTs device by use machine learning algorithms. Many ML algorithms has been used to classify the greatest accurate classifier for their AI-base reactions agent implementations stage, which could recognize attacks activity and pattern in network connecting to the IoTs. The suggested approach realized 99.98% accuracies, 99.97% detections, and 99.93 F1 scores, compare to the current methods. Also, this paper highlight the outperforming previous ML-based model in term of implementation speeds and accuracies and proves that the proposed method outperform preceding ML-based model in performance accuracy and time.

Corresponding Author:

Bushra N. Al-Mafrachi
Department of Computer Sciences, University of Kufa
Email: bushran.almafrachi@uokufa.edu.iq

1. INTRODUCTION

The internet of things (IoT) is one of the most developing paradigms in the networking realm. It can be defined as the "interconnections of things" have controlled computational power and capability. It can be used to send and receive data through the internet without needing human-to-computers or human-to-human interactions [1].

The industry utilizes the knowledge planned for exploiting their commercial purposes with clever and business intelligences approach. Though, the expertise loophole is ignored which lead the industry to face cyber-attack. Internet of things system presents numbers of security challenge because of their exclusive characteristic like the larger numbers of equipment complicated the variety of communications protocol and data format, and the needs for real-time communications [2].

The utmost important security challenge in IoTs system is the security of devices, data, communication, privacy, firmware, and supply chain as show in Figure 1. The IoTs has becomes a vital aspects of our live, and due

to its increasing uses, there has been a expanding numbers of cyber-attack on IoTs device. Security professional and academic is particularly concern about the present condition of IoTs cyber-attack [3].

Internet of thing devices threat decrease under numerous spaces, include networks assault, software attack, and physical attack. Attacker can overcome the networks with traffics and carry it to a halts by use many Techniques [4].

Internet of things devices safety and privacies is important problem, and poor authentication and authorizations could resultant in privacy issue at the devices levels [5].

These devices weakness and threat is rising every day, thus it's serious to produce robust defense to save them harmless. Encryptions, confirmation, and accessing guide are insufficient of the countermeasure [6].

It's dangerous to keeping up with the utmost current securities methods and technology advancement to avoid assault on IoTs device.

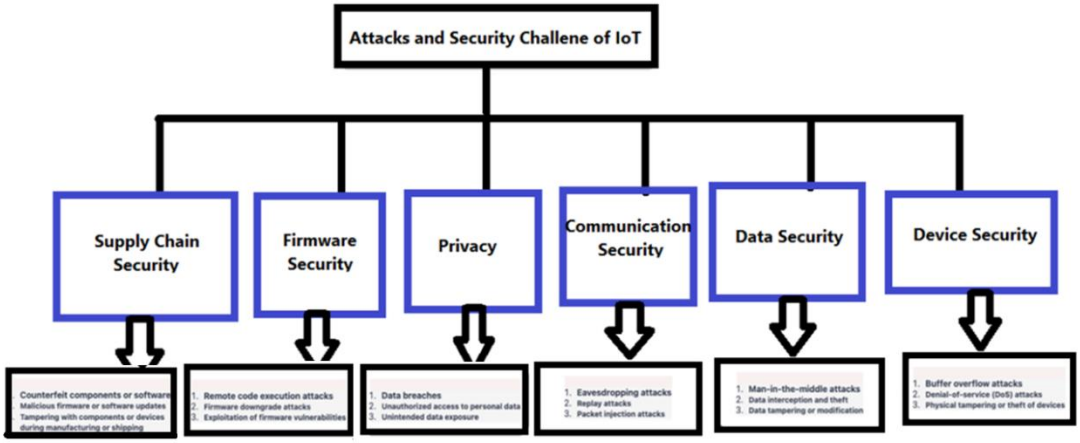

Figure 1: Attacks and security challenge in IoT

Cyber-attack on the IoTs is become communal, and their incidence is increasing. Rendering to [7], the total numbers of daily attack on IoTs device per commercial increase by 20% in the first month of 2023 compare to 2022. The resultant of this increase concern, MLs algorithm has raised as vital instrument in proactive identify and mitigate the cyber threat in IoTs ecosystem. Through capitalize on pre-exist dataset and conduct statistic analyzing, ML technique has confirmed their capability to detects threat earlier, identifying networks vulnerability, and reduction operation expense [8-12].

Complete benchmarks for the utmost operative ML algorithm to identify IoTs cyber threat hitherto to be recognized, producing a important emptiness in the arena of IoTs cyber securities researches [13-15].The researches in [16-19] conducts a literatures analyzing on MLs and DLs techniques for IoTs security. In [20], they used MLs and data analytic for IoTs security are enclosed by use random forest, decisions tree, and neural network to provide the accuracy rates of the RF techniques was 99.6%. Machine learning algorithm is proposed for automation the detections of cyber-attack for rapid predictions and analyze of attacks type [21].

The DL method is introduced by [22] for forestalling cyber security assault on the IoTs. This proposal use DLs and MLs approaches to prudently extracts significant data from a BoT datasets. He shows that the developed accuracy performances and reliability of cyber threats predictions in IoTs scenario. In [23], the DLs and MLs methods for evaluating cyber security in IoTs, numerous MLs technique are explore for irregular activity and cyber threat detections by use the KDD-99 datasets.

Machine learning approach has been used by [24] to produce the greatest security model for noticing IoTs intrusion with the emphasis on the model that reached high detections F1-scores, the value of the model was tested over multiclass and binary classifications. Their finding demonstrates that ML-base model, in specific deeps learning model were fruitful in identify botnets attack on IoTs device. In addition, this finding exposed how MLs technique enhanced the IoTs security and resolve issue carried on the propagation of device and threat.

For IoTs system, [25-29] proposes a model for the next-generation cyber-attacks predictions that use the CHAID decisions trees and multi-classes SVMs to predicts cyber-attack with a 99.72% accuracy rates. In order to identify cyber-attack in IoTs network, [30] introduce DL-base detections methods. They use LSTMs to recognize networks intrusion and focus on the detections of DDoS attack. They also achieve abundant accuracy rate in complex assaults detections and predictions.

Despite all the fore mention fact about the IoT, cyber security vulnerability is public in the IoTs. Developing this security vulnerability hacker can establish a botnet and execute command either remotely or locally. They can also gain unauthorized accessing and modifying sensitive data, disrupt normal operation of the IoTs, or damage the IoTs altogether. The vulnerability can exist in both hardware and software component of the IoT. Hardware vulnerability are difficult to detect and much harder to fix due to various embedded micro program in them.

The reason why hardware vulnerability cannot easily be fixed include lack of expertise, cost, incompatibility and interoperability. Defiantly, software vulnerability exist in the software components of the IoT, such as OSec, communication protocol, and other applications. According to TechRadar, an IT security firm, the number of threats against Internet of Thing (IoT) gadgets and smartphones increased quickly. McAfee also believes that malware attacks on IoT gadget will continue to occur, as more than 25 million smart speaker or voice assistants are already in use.

In this paper we definitely recompense attention to understand cyber-attacks detections in IoTs network. Beforehand, we realize the idea of the cyber-attacks and we use new Techniques to increase the accuracy to detect the threats over IoTs devices.

2. MATERIAL AND METHODS

By select the ML model for this paper, we deliberated the inherent deficiency of conventional approaches in case of identify and addressed developing cyber threat in IoTs network. The incapability of traditional methods to handles any change, different, and dynamics characteristic of attacks vector attended as the impulse for examine into additional resilient model that can recognize difficult pattern in IoTs traffics.

Likewise, the chosen of evaluations metric was influence by the deficiency recognized in earlier evaluation, aiming to resolve the issue and offers a holistic calculation of the models efficiency that extends beyond conventional metric. The datasets, MLs model, and valuation measure that we employ in this paper are protected in details.

Figure 2 shows the complete workflows of proposed techniques. Employed the CIC-IoT2023 datasets is required subsequent a prearranged process. Load the datasets is the main phase, following by the necessary phase of data preprocess, which involve control lost value, clean the data, and format modification. Afterward, to create training and evaluation model more easily, the datasets is divide into two subsets include testing and training. Machine learning technique is then evaluated on the test sets to define their performances after being chosen and train on the training sets.

A comprehensive evaluations of the model efficiency is conducts by use relevant measure, include F1 scores, accuracy, precisions, and recalls. The finale objective is to select the models that finest fit the requirement of the current development or to deliberate more optimizations for better accuracy. These systematic methods for occupied by use the CIC-IoT2023 datasets is guaranteed by this well-organize procedure, important to intelligent decision and dependable machine learning outcome.

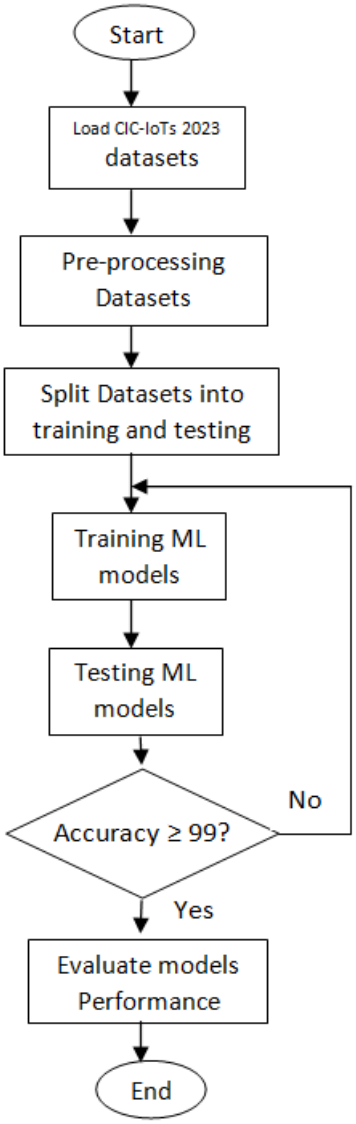

Figure 2: Proposed ML Architecture models

A. Dataset

The dataset from CIC-IoT2023 [31] is a widely accessible datasets that covers definite networks traffics from many IoTs device under normal and attacks situations, is the one that we working in this paper. A smart homes environments with 20 IoTs devices, include camera, thermostat, smart TV, smart watch, etc., was simulate to produce the datasets. There is about 80 million packet in the datasets, 64 million of which are classify as malicious and 16 million as normal. Every packets in the datasets, there is 115 topographies, include the protocols, payloads sizes, timestamps, and sources and endpoint IP address. The diverse cyber-attack distributes numerous cases in the datasets classify few communal attack into an others class whereas highlight the frequency of numerous attacks types. These others class is utilize when the number of occurrence for a detailed attacks are lesser than a programmed thresholds. These methods offer a brief instant of the utmost commonly attacks route without overcrowd the charts with label.

These datasets differ from others IoTs dataset use in networks intrusions detections study in that it possessing the feature include instead of simulate or emulate device, it use actual IoTs device as attacker and victim, in difference to a smaller numbers of device from a single vendors or protocols, it encompass a broad change of IoTs device from numerous manufacturer and protocol, instead of a single kind of attacks that target a specific layers or services, it consist of numerous DDoS attacks kind that targets many layer of the networks stacks, and instead of a smaller

quantity of dataset with lower variety and difficulty, it offer a massive quantity of dataset with abundant variety. These datasets could compromise additional compound and realistic environments to test how well machine learning algorithm works for classifying IoTs cyber-attack.

B. Machine Learning Algorithm

By use the CIC-IoT2023 datasets, we select and compare 4-ML algorithm INCLUDE LR, KNN, RF, and DT. These algorithms were pickup base on operative in previous study on networks intrusions detections. By Python we advanced these techniques. Excluding in KNN, in case of changing the numbers of neighbor to 5, we use the defaults setting for every algorithm parameter. Beforehand supply the datasets to the machine learning model, we perform definite preprocess operation on it. This action comprised, remove feature like packets ID, check sum, and other unused or super flours component, convert category characteristic like protocols types and services types into numeric value. Also by use min-max scale, numeric feature is normalize into a ranged of zero and one. By use the random under-sample methods; one can equalize the class's distributions by dropping the numbers of hateful packet to the similar levels as the numbers of legitimate packet. And finally, divide the datasets, keep the classes proportions constants into a train sets of (70%) and a test sets of (30%) by use stratify sampling approaches.

C. Evaluation Matrices

Based on CIC-IoT2023 datasets, we measured the evaluations of the machine learning algorithm by use numerous metric that is normally engaged in the classifications task. The utmost commonly evaluations metric is accuracy, precisions, recalls, and F1- Scores which temporarily defined underneath with the equations to compute:

- The accuracy is proportion of properly categorize packet to all packet as:
  $Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$ ……(1)
- The precision is proportions of harmful packet accuracies identify relate to malicious packet expects.
  $Precision = \frac{TP}{TP+FP}$ ……(2)
- The Recalls is proportions harmful packet when accuracy identify to all packet
  Recalls= $\frac{TP}{TP+FN}$ ……..(3)
- F1-scores is the harmonics mean of precisions and recalls
  $F1 - Scores = \frac{Precision+recall}{2}$ ……..…….(4)

3. RESULTS AND DISCUSSION

To recognize IoTs cyber-attack, 4-machine learning model was improved by use LRs, KNNs, RF, and DTs algorithm. The performances valuation of the model with precisions-recalls curve is showed in Figures 3, 4, and 5. Precision-recalls curves are a graphical that displays the trade-off among precisions and recalls at diverse probabilities threshold. Precisions are the section of accurate positives prediction, while recalls are the amount of positives incident that were properly predicts.

The curves of perfects models would attain the top right corners, representative 100% recalls and 100% precisions. The model performance across wholly threshold is evaluated by the areas under the curves. RF and DT have the high area under curve follow by KNNs and LRs, as could be show. Because of their capability to discriminate among the utmost hostiles and legitimates packet, DTs and RFs are then the utmost accuracy and dependable model for detects the IoTs intrusion.

Whereas, KNNs also work better but its precisions are less than that of DTs and RFs. The algorithms with the low area under curve, LRs, are unsuitable for these tasks because of its higher rates of false positive and false negative. The confusions matrices for every machine learning based model are displayed also.

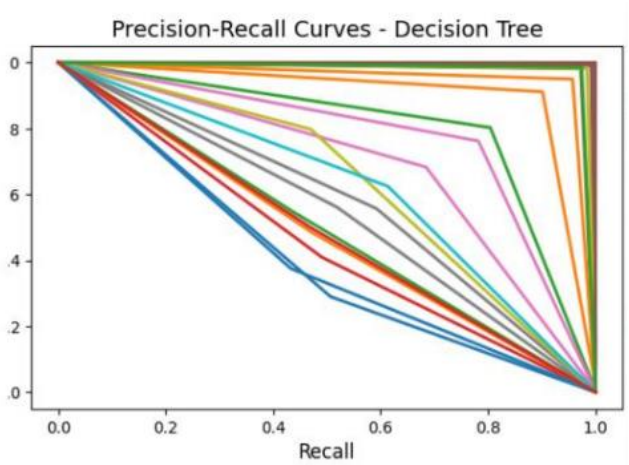

Figure 3: Precision recalls curves under decision trees

The confusions matric could be uses to compute the diversity of matrix like recalls, precisions, accuracies, and F1-scores. In divergence of false positive (FPs) and false negative (FNs), which is at their low level, the percentages of trues positive (TPs) and trues negative (TNs) is higher in DTs and RFs.

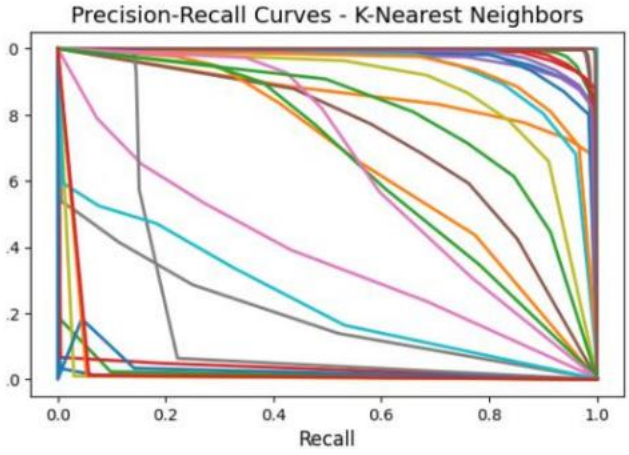

Figure 4: precision recalls curves under KNN

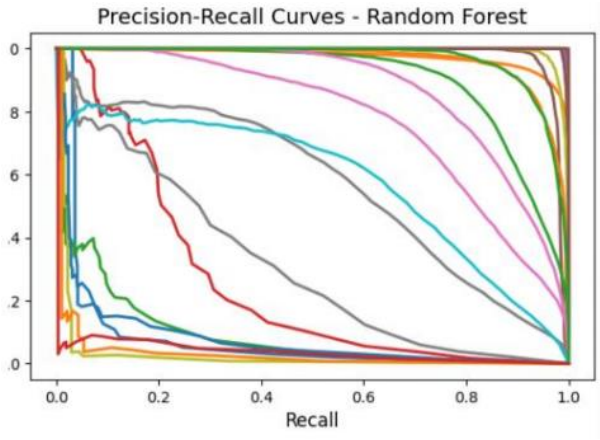

Figure 5: precision recalls curve under random forest

This indicated that they have lowest mistaken rates and could properly identifying the common of packet as malicious or legitimated. KNNs have high TPs and TNs, nevertheless it have further FPs and FNs than DTs and RFs. This indicates that it has larger errors rates and that certain packet might be incorrectly classifying as harmful or legitimated. The proportions of TPs and TNs are lower whereas the proportions of FPs and FNs are larger in LRs. This indicated that it have higher errors rates and could hardly distinguishing among malicious and legitimated message.

The outcome highpoint how critical it is to picks the finest machine learning algorithms for IoTs threats detections. Certain technique like features selections, dimensional decrease, parameters tune, and ensembles method could uses to advance the evaluations of machine learning algorithm. This technique could exploit the algorithm potentials and raised their efficiency in spotting IoTs assault.

Table 1 show the performances evaluation of every model on the CIC-IoT2023 datasets for detects cyber-attack. The evaluations metric involve accuracies, precisions, recalls, and F1 scores to compare these methods depend on RFs, KNNs, DTs, and LRs algorithm.

One could made some important conclusion and observation on the machine learning algorithm performances in classifying IoTs cyber-attack base on the evaluations metric that the algorithm of DTs and RFs excel, reaching the maximum accuracy rating of 0.99 and 0.99 individually. In addition, they earn the maximum precisions, recalls, and F1-scores, viewing that they are dependable in properly categorized valid and malicious packet. Within the accuracy of 0.93, KNNs performs comfortingly, efficiently and capably.

Though, it might not be as correct as DTs and RFs, KNNs show ability with non-linear dataset. KNNs could, still be computation exclusive and is sensitively to noisy situation and outlier. With scores of 0.82, LR consumed lower accuracy of all the method. This might be explain by the linear statement make by LRs, which lead to a higher percentages of false positive.

Furthermore, it has lower precisions and F1-scores value because of its sensitive to noisy situation and outlier. The greatest effective and capable algorithm for identify the IoTs cyber-attack were DT and RF. This result offers significant data for selecting the best machine learning algorithm and protection tactic to keep the IoTs from online threat.

TABLE 1: EVALUATIONS METRIC OF THE PROPOSED MACHINE LEARNING MODEL

Algorithms	F1-score%	Recall%	Precision%	Accuracy%
LR	79.88	81.88	83.98	83.9
DT	98.9	99.9	99.8	99.9
KNN	92.76	93.89	93.99	94.9
RF	99.98	99.89	99.88	99.8

The details evaluations of the ML algorithm efficiency in modifying cyber threat to the IoT were conducts in this analysis of CIC-IoT2023 datasets. For observing the exact assessment metric related with every model, it was detected that DTs and RFs exhibits unresolved performances.

RFs demonstrated outstanding F1 Scores of 99.18%, recall1 of 99.21%, and precisions of 99.9%, in additions to accuracies rates of 99.14%. Similarly, DTs demonstrated exception performances with an accuracy of 99.20%, an F1 Score of 99.21%, a recalls of 99.19%, and a precisions of 99.19%. The strength of all model in distinguishing benign from malicious packet in IoTs network is highlight by this metric. The KNNs algorithms demonstrate a notable accuracy of 93.19%. This is supports by F1 Scores, recalls, and precisions value of 93.59%, 93.79%, and 93.77%, correspondingly.

The LRs perform lesser efficiently; achieve an accuracy of 82.80% resultant in moderately low value for F1 Score, recalls, and precision, which were 80.34%, 82.75%, and 84.73% respectively. This detailed inspection is

reliable with our study goal, as it clarify the complicated function of every models and provide indication for the advantage of DTs and RFs in establishment of IoTs cyber-security.

4. CONCLUSION

This paper presents the analysis of four machine learning algorithm to detect the IoTs cyber-attack by use the datasets from CIC-IoT2023. These algorithms include LR, KNN, DT, and RF. The datasets used in this work offers inclusive and accurate benchmarks comprising numerous kinds of DDoS attack on diverse IoTs device. The dataset training, models training, and performances evaluations by use applicable metric suchas accuracy, precisions, recalls, and F1-scores. The result indicates that DTs and RFs are the maximum effective and effective algorithm for classifying IoTs cyber-attack, with accuracy rate of 0.99.

The two algorithms is the greatest in term of precisions, recalls, and F1-scores standards, representing that they could dependably discriminate among malicious and normal packet. With an accuracy of 0.93, KNNs does estimably as well, whereas LRs has the lower accuracy at 0.82. This paper offers a considerable analysis of the inherent restraints that occur in present methods to IoTs cyber-security.

During complete inspection of the efficiency of ML model in sensing cyber threat in the framework of the IoTs and utilize the CIC-IoT2023 datasets, this investigation shed highlight the limitation of traditional approaches in handling the ever-change and complicated natures of such threat. The probable of DTs, and RFs algorithm to correct these shortcomings is highlight by their greater performances. These results in extra reliable and effective technique of sensing and uncomfortable malicious activity in interconnect IoTs environment. The result of this study has considerable ramification for the practical implementations of ML in invigorating the security of the IoTs.

The algorithm capability of DTs, and RFs demonstrated excellent level of accuracy, precisions, and recalls, considering them possible contender for quick implementations in IoTs defenses system. The capability of this system to distinguish among benign and malicious traffics offers a robust basis for increasing strategy to detecting and mitigates threat in real times. This offers actual advantage for industries stakeholder who are interest in defensive IoTs ecosystem. Furthermore, the paper established a basis for numerous expansions and approaching trajectory in the realm of IoTs cyber-security.

Investigation the learning technique, integrating unsupervised learning approach, and incorporating DL model is all possibly productive paths for developing the scalabilities and flexibility of cyber threats detections mechanism in IoTs network. Besides, to addressed the every change cyber threats landscape, improving the security of IoTs infrastructure can be accomplish over the combination of ML algorithm that are unceasingly improve and varied dataset are utilize.

REFERENCES

[1] Kumar, R. et al. Blockchain-based authentication and explainable AI for securing consumer IoT applications. IEEE Trans. Consumer Electron. 70 (1), 2024, pp. 1145-1154

[2] Javeed, D., Gao, T., Kumar, P. & Jolfaei, A. An explainable and resilient intrusion detection system for industry 5.0. IEEE Trans. Consumer Electron. 70(1), 2024, pp. 1342–1350.

[3] Kumar, R. et al. Digital twins-enabled zero touch network: A smart contract and explainable AI integrated cybersecurity framework. Future Gener. Comput. Syst. 156, 2024, pp.191-205

[4] Sharma, A., Singh, P. K. & Kumar, Y. An integrated fre detection system using IoT and image processing technique for smart cities. Sustainable Cities and Society. 61, 2020, 102332

[5] Sinan, K. SDG-11: Sustainable Cities and Communities. Emerging Technologies, Sustainable Development Goals Series 1st edn. (Springer, 2020). B

[6] harati, S., Mondal, M. R. H., Podder, P. & Prasath, V. B. Federated learning: Applications, challenges and future directions. Int. J. Hybrid Intell. Syst. 18(1–2), 2022, pp. 19–35

[7] Omolara, A. E. et al. Te Internet of Tings security: A survey encompassing unexplored areas and new insights. Comput. Secur. 112, 2022, 102494

[8] Bharati, S., Podder, P., Mondal, M. R. H. & Paul, P. K. Applications and challenges of cloud integrated IoMT. In Cognitive Internet of Medical Tings for Smart Healthcare 1st edn (eds Hassanien, A. E. et al.) 67–85 (Springer, 2021).

[9] Özalp, A. N. et al. Layer-based examination of cyber-attacks in IoT. In 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (IEEE, 2022).

[10] Altunay, H. C. & Albayrak, Z. A hybrid CNN+ LSTM—Based intrusion detection system for industrial IoT networks. Eng. Sci. Technol. Int. J. 38, 2023, 101322

[11] Abbas, Y., Ali, D., Gautam, S., Hadis, K. & Reza, M. P. Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Tings. J. Syst. Archit. 148, 2024, 103088

[12] Abbas, Y., Ali, D. & Gautam, S. AP2FL: Auditable privacy-preserving federated learning framework for electronics in healthcare. IEEE Trans. Consumer Electron. 99, 1 2023.

[13] Danyal, N., Abbas, Y., Ali, D. & Gautam, S. Federated quantum-based privacy-preserving threat detection model for consumer Internet of Tings. IEEE Trans. Consumer Electron. 10.1109/TCE.2024.3377550

[14] Sanaz, N., Behrouz, Z., Abbas, Y. & Ali, D. Steeleye: An application-layer attack detection and attribution model in industrial control systems using semi-deep learning. In 2021 18th International Conference on Privacy, Security and Trust (PST), IEEE Xplore (2021).

[15] Abbas, Y., Ali, D., Reza, M. P., Gautam, S. & Hadis, K. Secure intelligent fuzzy blockchain framework: Efective threat detection in IoT networks. Comput. Ind. 144, 103801 (2023).

[16] Gopi, K. J., Abbas, Y., Reza, M. P. & Seyedamin, P. Exploring privacy measurement in federated learning. J. Supercomput. 1, 43 2023.

[17] Otoum, Y. & Nayak, A. On securing IoT from deep learning perspective. In Proc. 2020 IEEE Symposium on Computers and Communications (ISCC) 1–7 2020.

[18] Butun, I., Sterberg, P. O. & Song, H. Security of the Internet of Tings: Vulnerabilities, attacks, and countermeasures. IEEE Commun. Surv. Tutor. 22(1), 2020, pp. 616–644

[19] Abiodun, O. I., Abiodun, E. O., Alawida, M., Alkhawaldeh, R. S. & Arshad, H. A review on the security of the Internet of Tings: Challenges and solutions. Wirel. Person. Commun. 119(3), 2021, pp. 2603–2637

[20] Hamad, Z. J. & Askar, S. Machine learning powered IoT for smart applications. Int. J. Sci. Bus. 5(3),2021, pp 92–100

[21] Bharati, S. & Mondal, M. R. H. Computational intelligence for managing pandemics. In 12 Applications and Challenges of AI-Driven IoHT for Combating Pandemics: A Review (eds Bharati, S. & Mondal, M. R. H.) 213–230 (De Gruyter, 2021).

[22] Podder, P., Mondal, M. R. H. & Kamruzzaman, J. Iris feature extraction using three-level Haar wavelet transform and modifed local binary pattern. In Applications of Computational Intelligence in Multi-Disciplinary Research 1st edn (eds Elngar, A. A. et al.) (Elsevier, 2022).

[23] Chandavarkar, B. R. Hardcoded credentials and insecure data transfer in IoT: National and international status. In Proc. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2020, pp1-7.

[24] Ferrara, P., Mandal, A. K., Cortesi, A. & Spoto, F. Static analysis for discovering IoT vulnerabilities. Int. J. Sofw. Tools Technol. Transf. 23(1), 2021, pp.71–88 .

[25] Yu, Y., Guo, L., Liu, S., Zheng, J. & Wang, H. Privacy protection scheme based on CP-ABE in crowdsourcing-IoT for Smart Ocean. IEEE Internet Tings J. 7(10), 2020, pp. 10061–10071

[26] Xiong, J. et al. A personalized privacy protection framework for mobile crowdsensing in IIoT. IEEE Trans. Ind. Inform. 16(6), 2020, pp. 4231–4241

[27] Visoottiviseth, V., Sakarin, P., Tongwilai, J. & Choobanjong T. Signature-based and behavior-based attack detection with machine learning for home IoT devices. In Proc. 2020 IEEE Region 10 Conference (TENCON 2020, 829–834

[28] Turk, Z., Soto, B. G. D., Mantha, B. R. K., Maciel, A. & Georgescu, A. A systemic framework for addressing cybersecurity in construction. Autom. Construct. 133(3), 2022, 103988

[29] Al Hayajneh, A., Bhuiyan, N. Z. A. & McAndrew, I. Improving internet of things (IoT) security with sofware defned networking (SDN). Computers 9(1), 8 2020.

[30] Hussain, F., Hassan, S. A., Hussain, R. & Hossain, E. Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. IEEE Commun. Surv. Tutor. 22(2), 2020, pp. 1251–1275

[31] CIC IoT dataset 2023 Available at: IoT Dataset 2023 | Datasets | Research | Canadian Institute for Cybersecurity | UNB