Nexus : Journal of Innovative Studies of Engineering Science ( JISES )
Volume: 02 Issue: 04 | 2023 ISSN: 2751-7578
http://innosci.org/

# Security Framework Implementation of Internet of Things Network to Detect Attacks

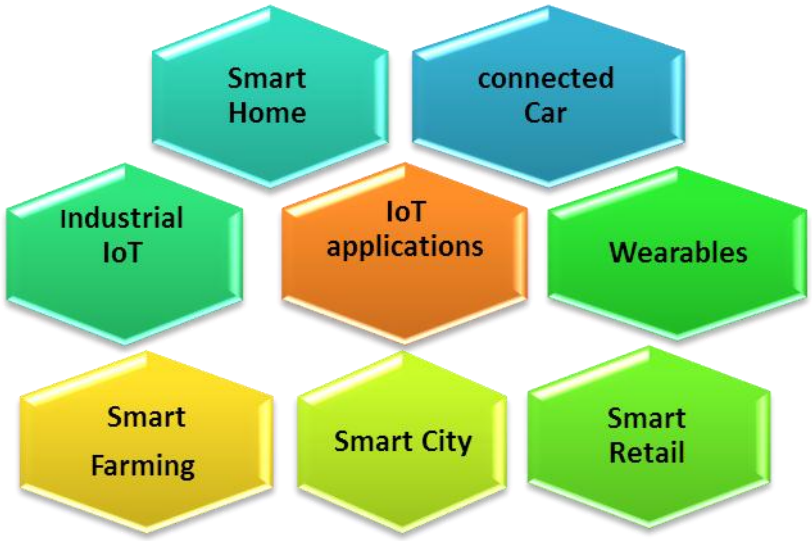
**Rasha Muhseen Hadi**
*Computer Unit, College of Agriculture, Al Muthanna University,IRAQ. *Corresponding*

**Abstract:** Nowadays, Internet-of-Thing IoT associated to human's day to day life. It represents a network which includes devices that are resource-constrained. IoT-Networks could face multiple types of attacks, therefor, security of IoT system is a necessary issue. To build a security framework, Machine-Learning could be a powerful tool for training models to detect attacks. The classifier would be trained by Random-Forest (RF) algorithm. Results present that the proposed framework achieve good performance on (ContiKi) nodes in the studied (IoT) network. The accuracy was 98%. By comparing with other algorithms such as CNN, hybrid CNN+LSTM, SVM, LSTM, Random-forest has the best performance.

**Key words:** Attack, security, security, detection.

## Introduction:

Security of Internet-of-things (IoT) has been more concentrated recently by industry and academic communities. There are multiple applications of (IoT) for houses, vehicles, cities, industry and trade(Shamsadini,2022). The basic feature of (IoT) implementations is that the gathered data based on intelligent devices with blended sensors are collected and employed over the network. Applications based on (IoT) are increasing daily. Which expanding the employing area and simplify the human's life. There is a massive amount of personal data gathered by convenient applications based on IoT which capping smart (cities, environments, metering, farming, livestock, health), emergency, security, should be shared and analyzed(Krishna,2021). IoT applications are designed basically to be applied in multiple sectors which are crucial, particularly, for economy as well as the National-Security therefore the issues which are related to security need basic attention to reduce the attack's surface and prevent the issues of security(Tiwary,2018). Presently , data-security and protection of privacy must be adopted to provide powerful data-security. Securing the data based on static strategy has been inadmissible, because it is not capable to treat the evolvable (IoT) data-Security. (Kumar,2018). The security backing is not constantly preserved. knowledge of the user in the issues related to security of IoT is weak: incidents of security could be hard for detection or resolving for using(Chen,2018). The attack's surface in the field of IoT had increased considerably as well as the potential threats for these entities protection in the scale(Lin,,2016). For instance, the attacks could lead to ominous consequences for the industry which is self-driving. Additionally, the autonomous-Vehicles could be experiencing the attacks related to sensors such as magnetic, speed,…) sensors. Attackers could gather the data to convey malware, as well as trigger malignant action(Rajendran, 2019)




**fig(1): The basic applications of IoT**

Moreover, compact systems and Smartphones contribute to an ecosystem that is digital for the world communication which make lives simplifier by being it is flexible, and sensitive, and responding to the human requirements. However, security could not be confirmed , this because the vulnerabilities which are associated to IoT. When the signal of users is intercepted or disrupted, then the privacy of the users could be endangered, and thereby, their data could be leaked(Chen,2017).

**Related works:**

(Bagaa,2020) had presented a security-framework based on machine-learning which automatically deals with the expanding aspects of security that is associated to IoT. The proposed framework takes a benefit both Network-function virtualization as well as software-defined-networking enablers to reduce various threats,

in addition to combining monitoring factor and reaction based on artificial-intelligent, which use models based on machine-learning as well as the ability to intrusion based on anomaly in IoTdetection. (Pacheco,2016) had presented another security-framework for smart-homes and buildings. this framework uses continued monitoring to catch the operational information of sensor for detection unusual behavior in domain of IoT. This data is employed to determine the sensor and contrast its performance to "normal" performance. The detected attack is classified by this framework according to the abnormality type and takes pertinent recovery procedures such as re-authentication of sensor, changing the structure of network, and ignoring the data of the sensor. Results had presented that the mitigation procedures are limited and sometimes causes disruptions of service. (Kshira,2015) had defined the frameworks of security based on software-defined-networking(SDN). The additional functionalities provided via (SDN) allow to integrate novel tools of security such as accurate manipulations routing and filtering the traffic and the employing of safe network's channels for critical data transferring. (Ali,2022) had presented an overview to recognize the matters and constructs in the present literature based on inclusion, merit, checking and identification, 568 papers had been reviewed from good journals. (Sani,2019) had proposed a framework of Cyber-Security has the ability to provide suitable security as well as privacy and

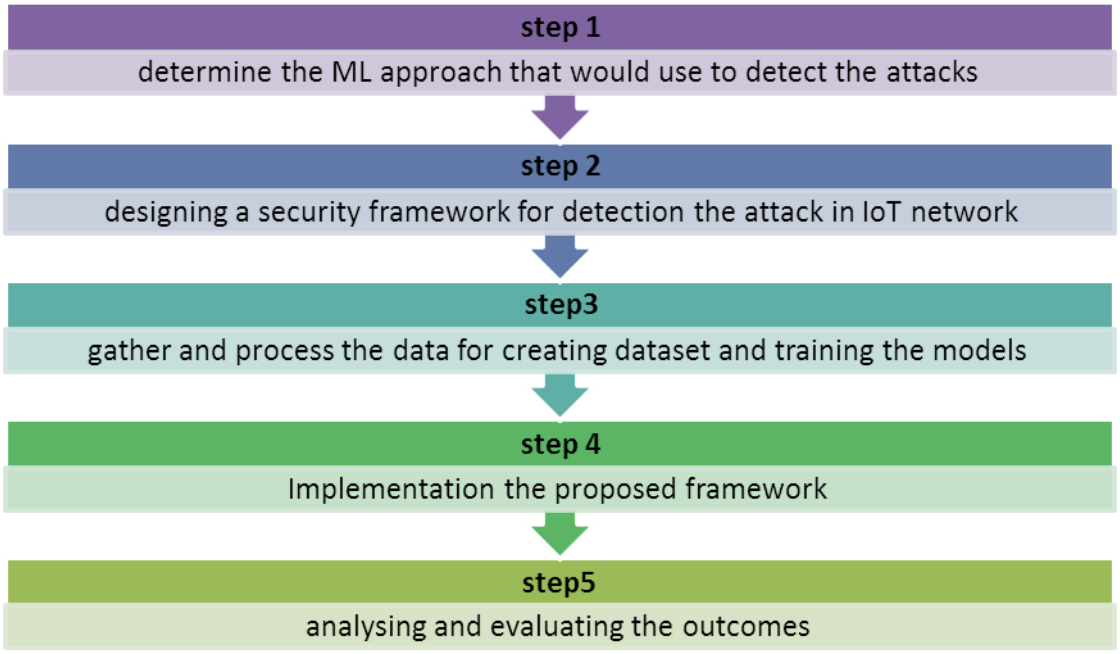
backing powerful management of energy. This framework employs an security technique based on identity in addition to protocol for safe communication to confirm the privacy and security. The study of (Liu,2017) had proposed a novel framework depending on the future architecture of the Internet (MobilityFirst), which concentrate on backing (IoT)security, this framework combines the local system of (IoT) into the world Internet without leave the usability, security and interoperability. This framework is implemented based on Middleware-layer which links heterogeneous device un the local systems with the world network. Other works (Lee,2014), (Cirani,2015)& (Blazquez,2015) had concentrated on founding license ( IoT )framework, as well as provide the access-ability controlling in IoT, despite that, this framework is a partial solution because it has not the ability to address multiple issues which are facing the systems of( IoT ) such as mobility, identification, interoperability, addressing and scalability. (Badshah,2019) had employed the main techniques of, Cloud-Computing, Edge-Computing and (IoT) to create a framework based on intelligent Emergency-Alarm, it consists of (3)Layers, the first is sensors and intelligent devices that are linked to the emergency-room for control, and this control-room represents next layer, and the last layer depending on techniques of Cloud-computing for transmission and processing the information and data to various command and centers of control. (Sethi,2018) established a new framework for analysis the smart malware depending on behavioral resemblances for static and dynamic analysis of the models that are malware, the proposed models to identify and categorize the malware files based on( Weka ) machine-learning had been examined and offered acceptable outcomes. (Paricherla,2022) described the selection of feature and patterns based on machine-learning to enhance the security in the (IoT), due to the abundant of network-data, it should be decreased in the size prior processing, reducing the dimension is a process of building a subgroup data of an original one which mitigate the excessive content from the basic data set. The work of (Alam,2020) aimed to establish a mobility framework employing Clout-computing to offer secure communication via (IoT ) among intelligent devices. (Ren,2016) discussed the issues associated to IoT network resulted by the attack of Selective-forwarding. (Tariq,2019) had employed Intrusion detection model based on artificial neural network for identification the attacks in the (IoT)network. (Rodríguez,2022) had designed a framework based on deep-Learning to detect attacks, depending on CNN algorithm, the proposed framework had applied to IoT-Network for various families of Zero-Day attacks, the results had proved the effective performance of this algorithm. (Smys,2020) had proposed hybrid framework to detect various types of attacks based on CNN, it is convenient for different application of IoT. The framework that had been presented by (Popoola,2020) had also depended on (Deep-BLSTM) integrated with (LAE) method for Dos, DDoS attacks.

**Aim of search:**

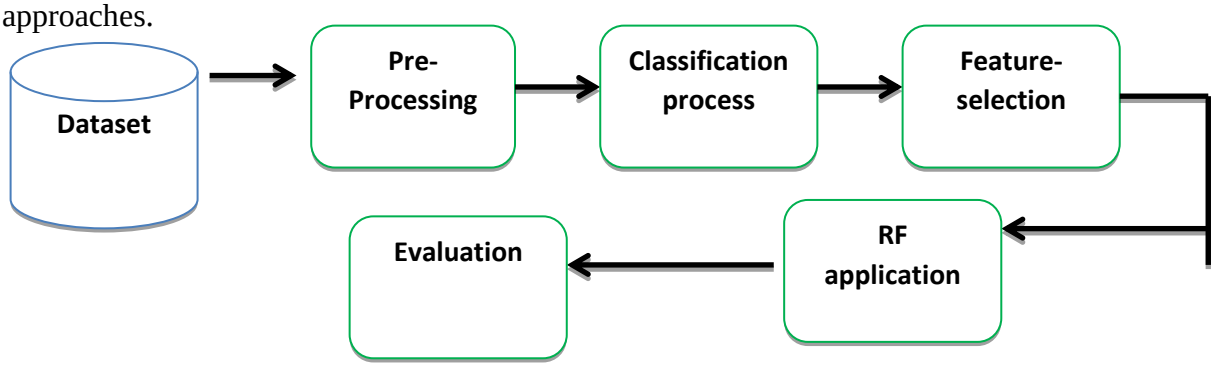
This search basically aims to implement a framework based on machine-learning to detect sinkhole attacks on an IoT-Network and evalyate the performance of this framework.

**Methodology:**

The basic steps in this work are:



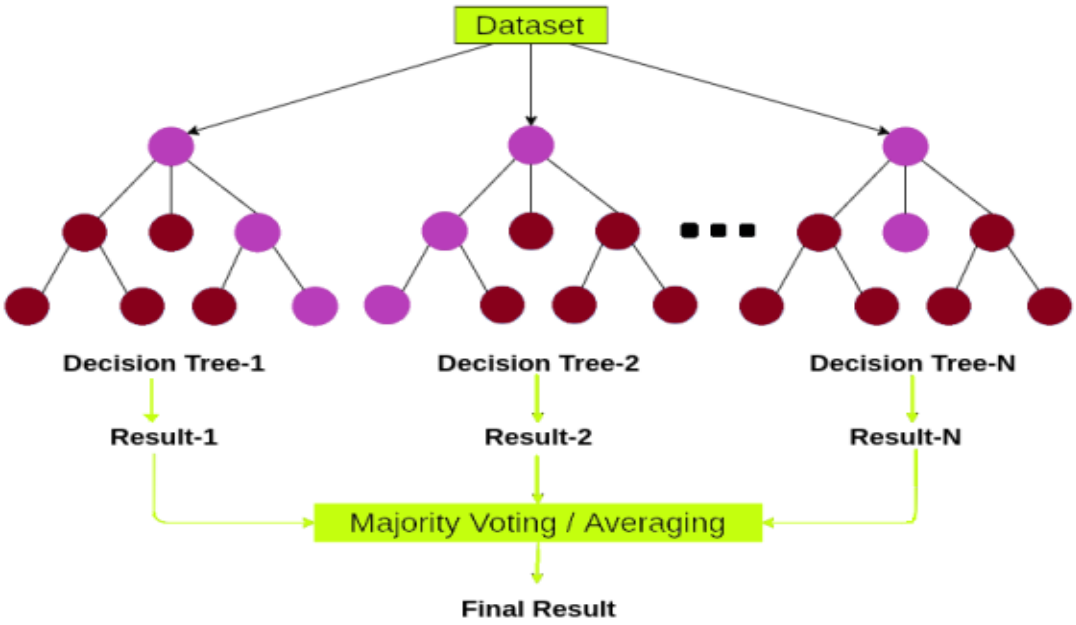

In this search, machine-Learning would be designed and implemented for the (IoT) network to detect the (sinkhole) attacks, thereby a frame work to achieve the intrusion-detection systems (IDS). Firstly, the (IoT)-network dataset would be created, then the classifier to detect the intrusion would be trained via, and Random-Forests (RF) which is backed by (Scikit-Learn) in Python. The accuracy of detection achieves 91.99% under various setups. It provides acceptable outcomes. RF is one of the ensemble approaches for classification which had been created by Breiman (Breiman,2001). It is characterized by its fast and good accuracy comparing to other approaches.




**Fig(2):The framework designing for attacks detection**

RF is built based on specific number of Tree-Predictors which is determined prior the training.

The tree classifies a specific set of samples by a group of feature. From fig(3) from the tree's top to its bottom, nodes is formed a series. The predictor splitting the samples that are the input into parts at every node depending on the feature




**fig(3): the architecture of Random-Forest**

Based on this classifier, the outputs represent the class-prediction, the class which has the most Votes would be the prediction outcome of the classifier based on random-forest algorithm. the main point during creating the trees that the weak correlation among these trees. thereby, one of trees error is not associated to other trees. these algorithm support both type of variable discrete and continuous. These algorithm could find a solution for over-fitting issue of the Decision-Trees.

**Dataset:**

In this work, dataset is taken based on recent detection of the intrusion activities for the studied (IoT) Network, in this study (RPL)network, and it includes 7230 samples employed for training the ML approach. Every sample includes 16 feature and one label.

The samples have been extracted from different simulations with multiple client-nodes. The nodes number (25), and every scenarios involves number of simulations with various topologies of network. The framework is designed for IoT-Network and implemented on the (Contiki)nodes. Features are fed to the classifier, a binary prospection for indicating if the network is facing an attack or not. Normalization of data is necessary for ML datasets, the data of every feature is normalized within {-1,1} as the following equation:

$$y = \frac{x - x_{min}}{x_{max} - x_{min}} (y_{max} - y_{min}) + y_{min}$$

$x$, the original value of data, $x_{max}$ & $x_{min}$ are the original group values of the data. $y_{min}$ & $y_{max}$ the new data after normalization process values (1 &-1), $y$ is the normalized output of $x$.

**Validation:**

The required data to generate the Training-Set is obtained based on simulations via the simulator (Cooja) and extracting process of data the outputs of simulation is done in Python via (coojatrace-module).evaluation process was basically a Binary-classification. The output of the framework is that ( Network facing attack) or (Network not facing attack). In this case, it could be easily determined whether the output of framework is true through comparison between label

that is predicted and the real one of a sample that is input. Depending the data that is extracted from the outcomes of simulation the performance has been evaluated under multiple parameters.

**Results& discussion:**

The experiments are carried via Cooja-simulation. The results of the proposed system for detecting the ( sinkhole)attacks is a Binary-value: (1) represents that the IoT-Network is facing an attack or (0) which represents that IoT-Network is not facing an attack,

thereby the prediction process would be either true or false. Thereby, four types of relation among attacks predictions and real Labels as shown by table (1) as following:

| Outcomes | Attacks prediction | Real-Labels |
|---|---|---|
| True-Positive (tp) | Network facing attack | Network facing attack |
| false-Positive (fp) | Network facing attack | Network not facing attack |
| True-negative (tn) | Network not facing attack | Network not facing attack |
| False-negative (tn) | Network not facing attack | Network facing attack |

Table(1): relation types among attacks predictions and real Labels

$$TP\ rate = \frac{tp}{tp + fn}$$

$$tn\ rate = \frac{tn}{tn + fp}$$

based on these relations the accuracy as well as precision are obtained as following:

1-Accuracy:

$$Accuracy\ = \frac{tp+tn}{tp+tn+fp+fn}$$

2- Precision:

$$Precision = \frac{tp}{tp + fp}$$

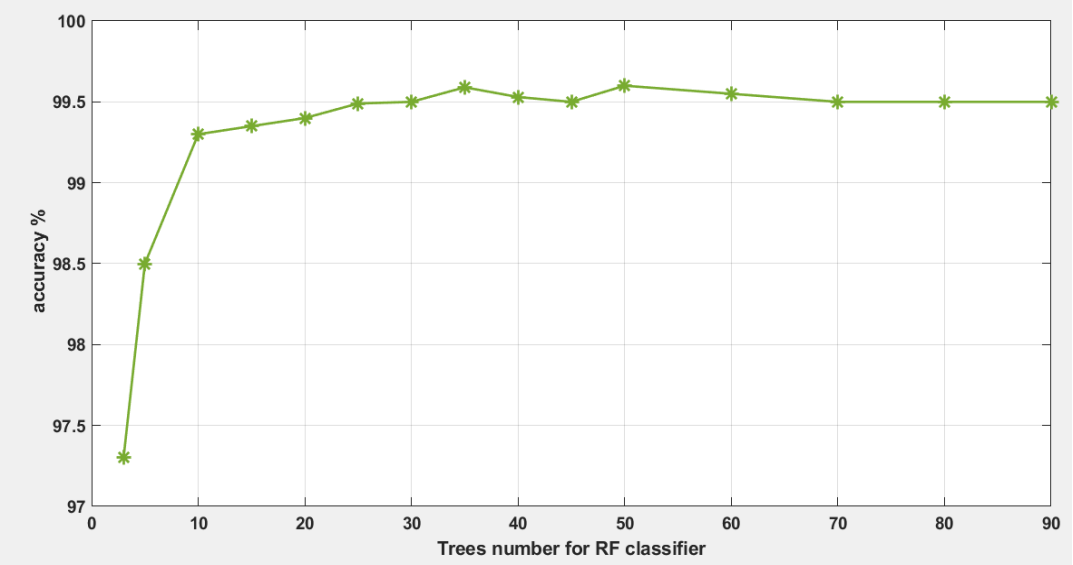


Fig (4) explained the relation between the accuracy and the trees number for RF classifier fig(4): the accuracy of RF % against the trees number It could be seen that the accuracy values are over than 90% with increasing the trees number.

| Number of RF trees | Accuracy % | | Precision | Accuracy of prediction |
|---|---|---|---|---|
| | $tp$ | $tn$ | | |
| 3 | 89 | 83 | 84 | 85 |
| 5 | 89 | 90 | 90 | 89 |
| 6 | 93 | 87 | 87 | 89 |
| 9 | 93 | 92 | 92 | 94 |
| 10 | 93 | 100 | 100 | 97 |
| 15 | 96 | 100 | 100 | 98 |
| 20 | 93 | 100 | 100 | 97 |
| 25 | 90 | 100 | 100 | 95 |

**Table(2): Accuracy of prediction process and Precision for various values of trees number**

It could be observed that, with increasing the trees number for RF classifier, then $tn$ rate is raised from (83%) to (100%) , and the high rate is achieved for tree number(10 ).

Additionally, $tp$ is also increasing, until trees number is equal to (15 )trees, the accuracy is (96%) then the rate returns to 93%. The highest accuracy of prediction was 98% for ten trees. for Precision the highest value was 100% for 10,15,20,25 trees in RF classifier.

| Ref | Method | Accuracy | Precision |
|---|---|---|---|
| [28] | CNN+LSTM | 97.16% | 95.99% |
| [29] | CNN | 97.46% | 97.43% |
| [30] | SVM | 67.31% | 88.18% |
| [31] | LSTM | 97.22% | 96.25% |
| This work | RF | 98% | 100% |

**Table(3): comparison between multi algorithms for detecting attacks of IoT-Network**

The table(3) had summarized the values of accuracy as well as Precision for other frameworks and the proposed framework in this study. It could be seen that, in this work, random-forest has achieved the best accuracy for prediction the attacks.

**Conclusion:**

This search describes basically implementing a security framework for detect the attacks in an IoT-Network. This process had implemented based on ContiKi-NG. Results had presented that the proposed framework based on Random-forest had implemented acceptable performance in (Cooja) Simulation. The performance is better when the trees number of the RF algorithm is increasing with 98% accuracy. The proposed framework has proved that Machine-Learning is a powerful tool to detect the attacks when it is integrated with good model for training.

**References:**

1. Shamsadini, M., Ghaffari, A.,(2022). Taxonomy of Threats and attacks in IoT. Computer & Robotics.
2. Krishna,R.R., Priyadarshini,A., Jha, A.V., Appasani, B., Srinivasulu, A.; Bizon, N.,(2021) State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. Sustainability, 13, 9463. https://doi.org/10.3390/su13169463.

3. Tiwary, A.; Mahato, M.; Chidar, A.; Chandrol, M.K.; Shrivastava, M.; Tripathi, M.(2018). Internet of Things (IoT): Research, architectures and applications.. Future Revolut. Comput. Sci. Commun. Eng., 4, 23–27.
4. Kumar, N.M., Mallick, P.K.,(2018) The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. Procedia Comput. Sci, 132, 117–119
5. Chen, K., Zhang, S., Li, Z., Zhang, Y., Deng, Q.,( 2018) Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. J. Hardw. Syst. Secur, 2, 97–110.
6. Lin, H.; Bergmann, N.W.,(2016) IoT Privacy and Security Challenges for Smart Home Environments. Information, 7, 44.
7. Rajendran, G., Nivash, R.S.R., Parthy, P.P., Balamurugan, S.,(2019) Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures. In Proceedings of the International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October; pp. 1–6.
8. Chen, L., Thombre, S., Järvinen, K., Lohan, E.S., Alén-Savikko, A., Leppäkoski, H., Bhuiyan, M.Z.H., Bu-Pasha, S., Ferrara, G.N., Honkala, S., Robustness,(2017). security and privacy in location-based services for future IoT: A survey. IEEE Access, 5, 8956–8977.
9. Bagaa, M., Taleb, T., Bernabe, J. B., Skarmeta, A.,(2020). A machine learning security framework for iot systems. IEEE Access, 8, 114066-114077..
10. Pacheco, J., Hariri, S., (2016). Iot security framework for smart cyber infrastructures," in 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W). IEEE, pp. 242–247.
11. Kshira, S., Sahoo, S. B., Panda, A., (2015). A secured sdn framework for lot," in International Conference on Man and Machine Interfacing (MAMI). IEEE, pp. 1–4.
12. Ali, A., Mateen, A., Hanan, A., & Amin, F. (2022). Advanced Security Framework for Internet of Things (IoT). Technologies, 10(3), 60.
13. Sani, A. S., Yuan, D., Jin, J., Gao, L., Yu, S., & Dong, Z. Y. (2019). Cyber security framework for Internet of Things-based Energy Internet. Future Generation Computer Systems, 93, 849-859.
14. Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe, W. (2017). A security framework for the internet of things in the future internet architecture. Future Internet, 9(3), 27.
15. Lee, C.T., Yang, C.H., Chang, C.M., Kao, C.Y., Tseng, H.M., Hsu, H., Chou, P.H. (2014). A Smart Energy System with Distributed Access Control. In Proceedings of the IEEE International Conference on Internet of Things, Cambridge, MA, USA, 6–8 October.
16. Cirani, S. Picone, M. Gonizzi, P., Veltri, L.; Ferrari, G. IoT-OAS: (2015). An OAuth-Based Authorization Service Architecture for Secure Services in IoT Scenarios. IEEE Sens. J., 15, 1224–1234
17. Blazquez, A., Tsiatsis, V., Vandikas, K.,(2015) Performance Evaluation of OpenID Connect for an IoT Information Marketplace. In Proceedings of the 81st IEEE Vehicular Technology Conference (VTC Spring), Glasgow, UK, 11–14 May; pp. 1
18. Badshah, A., Ghani, A., Qureshi, M. A., & Shamshirband, S. (2019). Smart security framework for educational institutions using internet of things (IoT). Comput. Mater. Contin, 61(1), 81-101.

19. Sethi, K., Chaudhary, S. K. , Tripathy, B. K., Bera, P.,( 2018). "A novel malware analysis framework for malware detection and classification using machine learning approach," ACM International Conference on Distributed Computing and Networking,.
20. Paricherla, M., Babu, S., Phasinam, K., Pallathadka, H., Zamani, A. S., Narayan, V., ... & Mohammed, H. S. (2022). Towards Development of Machine Learning Framework for Enhancing Security in Internet of Things. Security and Communication Networks. .
21. Alam, T. (2020). Internet of things: a secure cloud-based MANET mobility model. Tanweer Alam." Internet of Things: A Secure Cloud-Based MANET Mobility Model.", International Journal of Network Security, 22(3).
22. Ren, J, Yaoxue Z., Kuan, Z., Xuemin S., (2016). Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks. IEEE Transactions on Wireless Communications. 15(5): 3718-3731.
23. Tariq, N., Muhammad A., Zakaria M., Zubair Farooqi, M. , Baker ,T.,(2019). A Mobile Codedriven Trust Mechanism for detecting internal attacks in sensor node-powered IoT. Journal of Parallel and Distributed Computing.134:198-206.
24. L. Breiman, (2001), Machine learning 45, 5
25. Rodríguez, E., Valls, P., Otero, B., Costa, J. J., Verdú, J., Pajuelo, M. A., & Canal, R. (2022). Transfer-Learning-Based Intrusion Detection Framework in IoT Networks. Sensors, 22(15), 5621.
26. Smys, S., Basar, A., & Wang, H. (2020). Hybrid intrusion detection system for internet of things (IoT). Journal of ISMAC, 2(04), 190-199.
27. Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2020). Hybrid deep learning for botnet attack detection in the internet-of-things networks. IEEE Internet of Things Journal, 8(6), 4944-4956.
28. Roopak, M.,Yun Tian, Chambers, J., (2019). Deep learning models for cyber security in IoT networks, in: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0452–0457.
29. Ullah, F. Naeem, H. Jabbar, S. Khalid, Latif, F., M.A. (2019). Al-turjman, L. Mostarda, Cyber security threats detection in internet of things using deep learning approach, IEEE Access 7
30. Khatun, M.A. Chowdhury, N., Uddin, v( 2019). Malicious nodes detection based on artificial neural network in IoT environments, in: 2019 22nd International Conference on Computer and Information Technology (ICCIT), pp. 1–6, doi:
31. Hwang, R.-H, Peng, M.-C., Nguyen, V.-L., (2019).An LSTM-based deep learning approach for classifying malicious traffic at the packet level, Appl. Sci. 9 (16)