IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205059 |

Network Intrusion Detection System Using IoT

Manisha Ghode[1], Prof Lowlesh Yadav[2], Prof Neehal Jiwane[3]

Student, Dept. of CSE, Shri Sai College of Engineering and Technology, Chandrapur, India[1]

Assistant Professor, Dept. of CSE, Shri Sai College of Engineering and Technology, Chandrapur, India[2-3]

ABSTRACT: Each network's security design must include an intrusion detection system. Monitoring and analysing network traffic is its main purpose in order to spot and halt hazardous activities. Machine learning algorithms have shown considerable promise in the realm of intrusion detection systems due to their ability to learn from large and complex data sets (IDS). In intrusion detection systems, the Multilayer Perceptron (MLP) and Long Short-Term Memory (LSTM) classifiers are two of the more popular machine learning techniques (IDS). This highlights the need to use flexible solutions such as Intrusion Detection Systems (IDS) which is the subject of our research. Our main objective is to determine the flaws and limitations of the existing solutions. To achieve this goal, we more than 60 articles on Intrusion Detection Systems in the Internet of Things. We utilised label encoding to perform some basic processing on the dataset before using feature selection to identify the most important features. Using the preprocessed dataset for training and testing, the MLP and LSTM classifiers performance was assessed twice, and the results were compared in terms of accuracy and loss.

KEYWORDS: IDS, IoT, Intrusion Detection System, Internet of Things, IoT Security;

I. INTRODUCTION

Mobile Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. IDSes can be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network. Intrusion detection systems work by either looking for signatures of known attacks or deviations from normal activity. These deviations or anomalies are pushed up the stack and examined at the protocol and application layer. They can effectively detect events such as Christmas tree scans and Domain Name System (DNS) poisonings.

An IDS may be implemented as a software application running on customer hardware or as a network security appliance. Cloud-based intrusion detection systems are also available to protect data and systems in cloud deployments.

The goal of a network intrusion detection system is to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. An intrusion detection and prevention system (IDPS) is a solution that monitors a network for threats and then takes action to stop any threats that are detected

II. RELATED WORK

IDSes come in different flavors and detect suspicious activities using different methods, including the following:A network intrusion detection system (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.

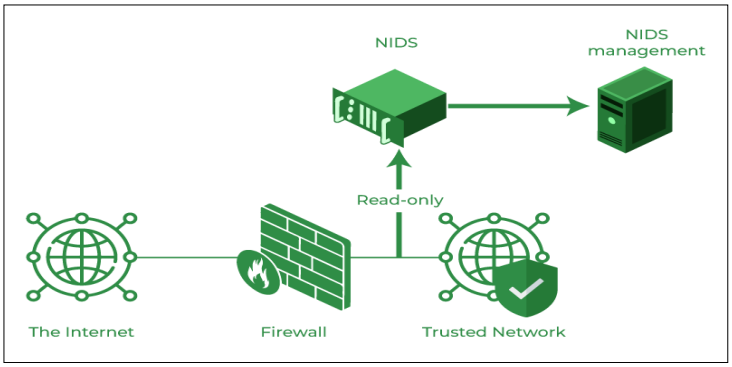

Fig 1: NIDS architectural model

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205059 |

A. Types of Intrusion Detection

1) **Host intrusion detection system** (HIDS) runs on all computers or devices in the network with direct access to both the internet and the enterprise's internal network. A HIDS has an advantage over an NIDS in that it may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that an NIDS has failed to detect. A HIDS may also be able to identify malicious traffic that originates from the host itself, such as when the host has been infected with malware and is attempting to spread to other systems.

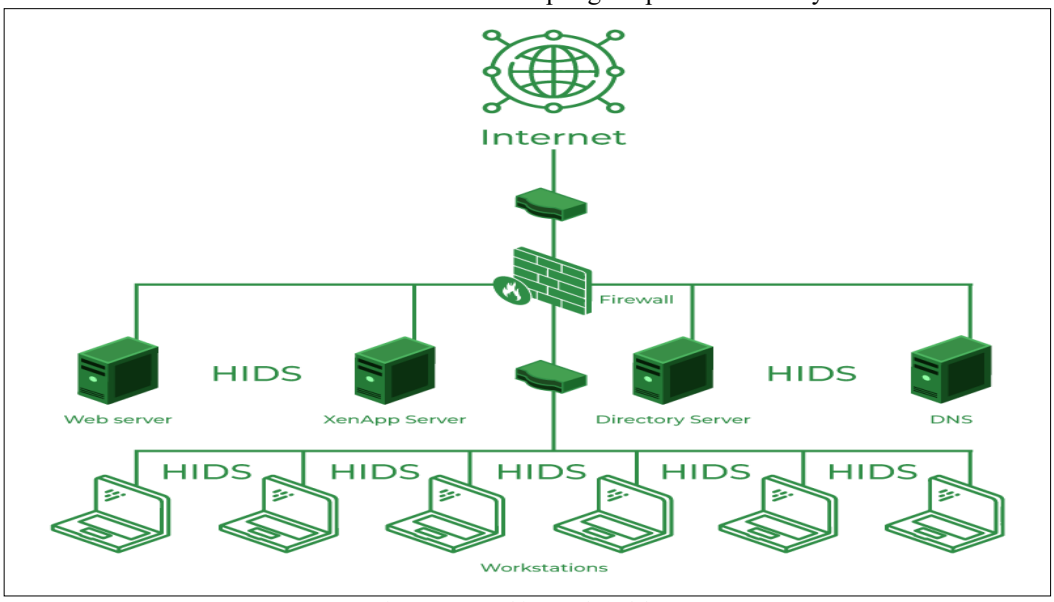

Fig 2: HIDS architectural model

2) **Signature-based intrusion detection system** (SIDS) monitors all the packets traversing the network and compares 0them against a database of attack signatures or attributes of known malicious threats, much like antivirus software.

3) **Anomaly-based intrusion detection system** (AIDS) monitors network traffic and compares it against an established baseline to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type often uses machine learning to establish a baseline and accompanying security policy. It then alerts IT teams to suspicious activity and policy violations. By detecting threats using a broad model instead of specific signatures and attributes, the anomaly-based detection method improves upon the limitations of signature-based methods, especially in the detection of novel threats.

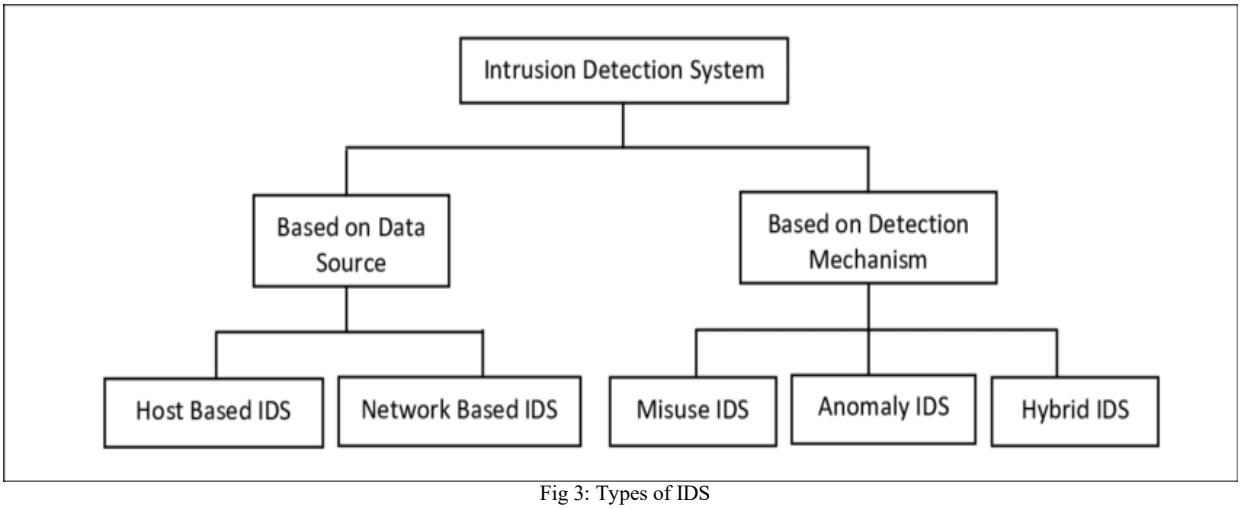

Fig 3: Types of IDS

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205059 |

Historically, intrusion detection systems were categorized as passive or active. A passive IDS that detected malicious activity would generate alert or log entries but would not take action. An active IDS, sometimes called an intrusion detection and prevention system (IDPS), would generate alerts and log entries but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

Snort -- one of the most widely used intrusion detection systems -- is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems (OSes), with a version available for Windows as well.

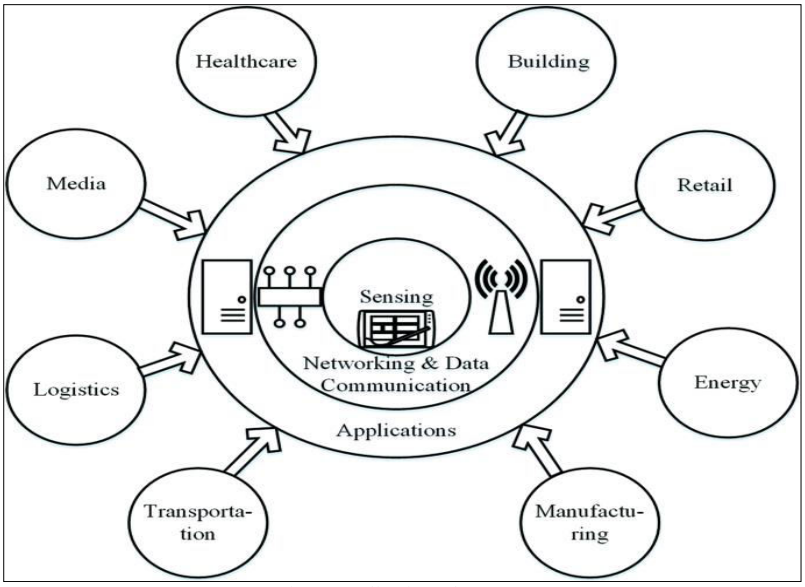

Fig 4: Application of IDS

B. Capabilities of Intrusion Detection Systems

- Intrusion detection systems monitor network traffic in order to detect when an attack is being carried out by unauthorized entities. IDSes do this by providing some -- or all -- of the following functions to security professionals:
- monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyberattacks;
- providing administrators a way to tune, organize and understand relevant OS audit trails and other logs that are otherwise difficult to track or parse;
- providing a user-friendly interface so nonexpert staff members can assist with managing system security;
- including an extensive attack signature database against which information from the system can be matched;
- recognizing and reporting when the IDS detects that data files have been altered;
- generating an alarm and notifying that security has been breached; and
- reacting to intruders by blocking them or blocking the server.

C. Intrusion Detection System Evasion Techniques

- Fragmentation: Dividing the packet into smaller packet called fragment and the process is known as fragmentation. This makes it impossible to identify an intrusion because there can't be a malware signature.
- Packet Encoding: Encoding packets using methods like Base64 or hexadecimal can hide malicious content from signature-based IDS.
- Traffic Obfuscation: By making message more complicated to interpret, obfuscation can be utilised to hide an attack and avoid detection.
- Encryption: Several security features, such as data integrity, confidentiality, and data privacy, are provided by encryption. Unfortunately, security features are used by malware developers to hide attacks and avoid detection.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205059 |

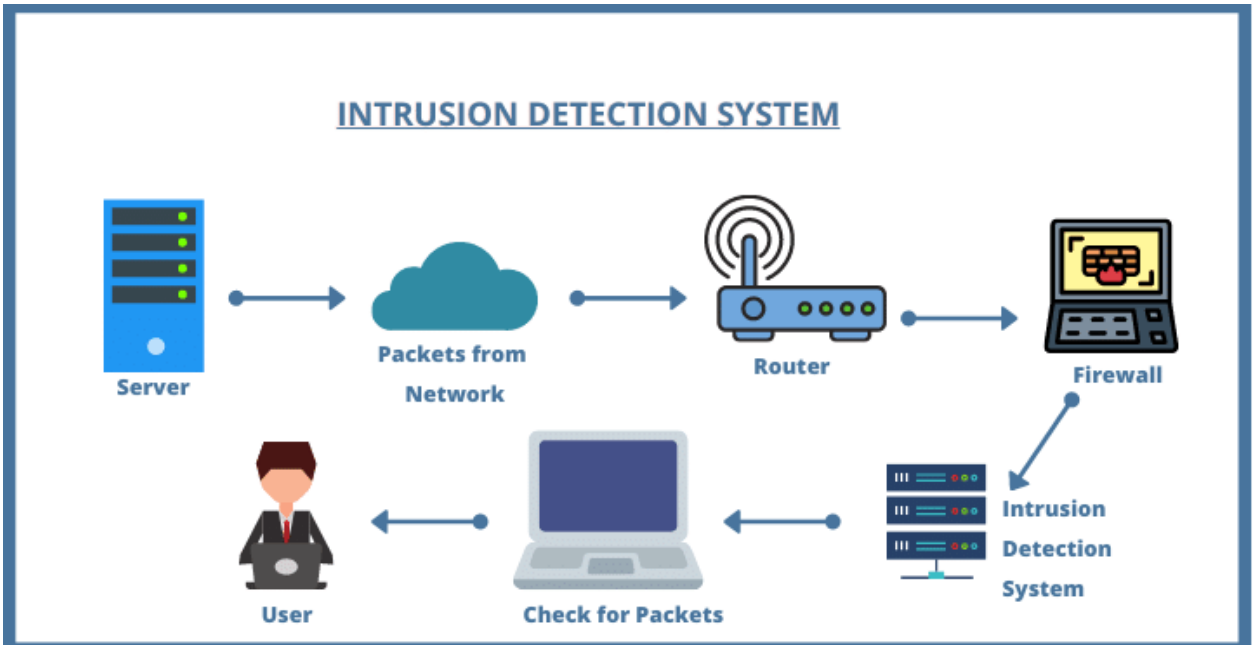

Fig 5: IDS architectural model

D. Working of IDS system

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

III. TECHNOLOGY USED

1.Detection-Based ID Methods

This technique is used to evaluate traffic on the basis of their attack type or their packet signature Detection-based IDS methods are functionally divided into three major categories (i.e., signature-based IDS, anomaly-based IDS and specification-based IDs)

Signature intrusion detection systems (SIDS) are based on signature matching techniques to find a known attack. These are also known as rule-based detection or misuse detection In SIDS, signature- or pattern-matching methods are used to find a previous intrusion. For example, if 3 login attempts are failed in first 5 min, then alarm is generated for brute force password attack So, if there is a match found, an alarm will be generated. SIDS generally has a high detection accuracy for known intrusions and low false alarm rate (FAR) because an alarm is only generated if any pattern is matched On the other hand, it also requires frequent updates of signatures to ensure a good detection SIDS has several issues while identifying zero-day attacks since no matching signature exists in the database until the new attack's signature is retrieved and saved SIDS is resource-consuming approach due to huge signature database maintenance and comparison of possible intrusion

2. Data-Based ID Methods

It also known as location-based IDS. Data-based IDS methods are divided into three main categories (i.e., host-based IDS, network-based IDS and hybrid-based IDS)

The first category is network-based intrusion detection system (NIDS). It monitors the network traffic that is extracted from a network. This type of IDS is independent in operating system that is a reason they can be deployed in all types of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205059 |

environments These types of IDS can detect some specific attacks due to their monitoring capability. These IDSs have their specific network segment, and they only monitor those attacks which are passing through that segment to identify malicious activity such as denial of services (DoS) and brute force

Second category is host-based intrusion detection system (HIDS). This type of intrusion detection system has vast set of segments for monitoring. They can monitor the behavior of several objects of a host device can detect non-network traffic insider attack. Tripwire and AIDE (Advanced Intrusion Detection Environment) are examples of HIDS , which is one of its incapability to detect network attack types.

IV. PROPOSED SYSTEM

One of our main goals is that the IDS should be lightweight and comply with the processing capabilities of the constrained nodes. Thus, according to [20], it is not possible to have an active intrusion detection agent in each node of an IoT due to the limited processing capacity and power consumption. Therefore, we have adopted a centralized IDS architecture to overhead the problem of limited capacity on the one hand and the peripheral heterogeneity issue on the other hand, where the IDS is implemented on the network layer of the IoT above the Gateway component.

Figure shows the activity diagram of our Lightweight Intrusion Detection System (LIDS) that consists in detecting an intrusion by observing the current behavior and comparing it to the normal behavior. If there is a deviation between the two behaviors, an alarm will be triggered. It is composed of three phases:

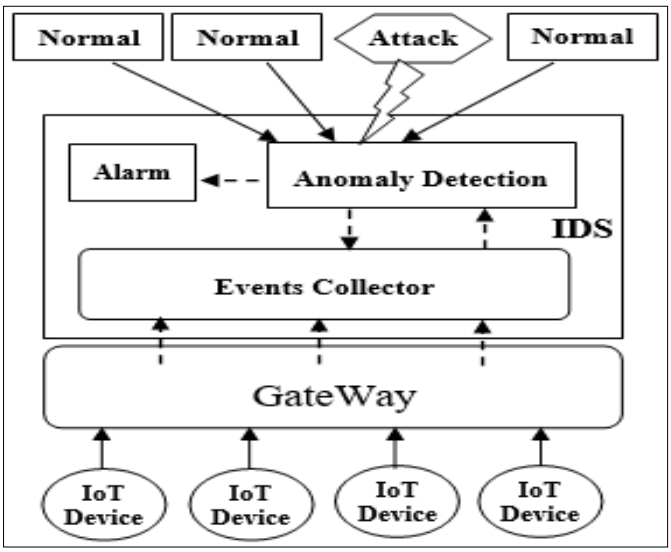

Fig No.1 LIDS architectural model

1. Events collection: In this phase, the component Events collector of LIDS collects and records all the events performed by the IoT devices in order to build the current behavior that will be represented as a feature vector as follows: Vi(t) = (c1, c2, …, c n).
2. Anomaly detection: The detection phase analyzes and detects intrusions. It is the main component of our LIDS, which will be detailed in the next section.
3. Alarm: After attack detection, the proposed system blocks the user and finishes his session, and then it sends an alert to the administrator to take the appropriate action.

V. SIMULATION RESULTS

The first process is the dataset acquisition. In this process, the dataset is collected and splitted into training and testing datasets. After, the process of pre-processing allows to clean the data while the feature selection process allows to reduce the data dimension. In this work, we have employed different classifiers model like: Logistic Regression, Random forest, Decision Tree, SVM, etc. The training set is used to train the models. Then, these models are evaluated against the testing set using different evaluation metrics. Finally, these processes will be repeated for three dataset.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205059 |

VI. CONCLUSION AND FUTURE WORK

The security of the Internet of Things is a major point for the confidential and sustainable use of this technology in various fields. Among the security techniques used to secure the Internet of Things are intrusion detection systems. In this paper, we presented a taxonomy of IDSs, the architecture of IoT, the threats against IoT, and a detailed state of the art on the use of IDSs for securing networks and IoT applications. This work is considered a starting point to understand the existing solutions and their limitations to present more effective solutions. Our future work will focus on the integration of Machine Learning techniques and distributed artificial intelligence into IDS solutions to secure IoT networks and applications.

REFERENCES

1. Abhishek, N.V., Lim, T.J., Sikdar, B. and Tandon, A., 2018, May. "An intrusion detection system for detecting compromised gateways in clustered iot networks". In 2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR) (pp.1-6).IEEE.
2. Adriano, D.B. and Budi, W.A.C., 2018, December. "Iotbased Integrated Home Security and Monitoring System". In Journal of Physics: Conference Series (Vol. 1140, No. 1, p. 012006).
3. Lowlesh Yadav and Asha Ambhaikar, "IOHT based Tele-Healthcare Support System for Feasibility and performance analysis," Journal of Electrical Systems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.
4. L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.
5. L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.
6. Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879, DOI: 10.13140/RG.2.2.15400.99846.
7. Lowlesh Yadav, Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).
8. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C. and Faruki, P., 2019. "Network Intrusion Detection for IoT Security based on Learning Techniques". IEEE Communications Surveys & Tutorials.
9. Deng, L., Li, D., Yao, X., Cox, D. and Wang, H., 2018. "Mobile network intrusion detection for IoT system based on transfer learning algorithm". Cluster Computing, pp.1-16
10. Gandhi, U.D., Kumar, P.M., Varatharajan, R., Manogaran, G., Sundarasekar, R. and Kadu, S., 2018. "HIoTPOT: surveillance on IoT devices against recent threats". Wireless personal communications, 103(2), pp.1179-1194.
11. Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.L., Iorkyase, E., Tachtatzis, C. and Atkinson, R., 2016, May. "Threat analysis of IoT networks using artificial neural network intrusion detection system". In 2016 International Symposium on Networks, Computers and Communications (ISNCC) (pp. 1-6). IEEE.
12. Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A. and Lloret, J., 2017. "Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in iot. Sensors", 17(9), p.1967
13. Pacheco, J. and Hariri, S., 2016, September. "IoT security framework for smart cyber infrastructures". In 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W) 121(9).
14. Roux, J., Alata, E., Auriol, G., Nicomette, V. and Kaâniche, M., 2017, September. "Toward an intrusion detection approach for IoT based on radio communications profiling". In 2017 13th European Dependable Computing Conference (EDCC) (pp. 147-150). IEEE.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details