Section A-Research paper

IoT Medical Forensic Network Level Intrusion Detection Systems

G. Rekha[1] Dr. T. Sudha[2]

1.Research scholar, Department of CSE, SOET, Sri PadmavatiMahilaVisvavidyalayam, Tirupati, AP, India.
E-mail: rekha.spmvv@gmail.com

2. Professor, Department of Computer Science, Sri PadmavatiMahilaVisvavidyalayam, Tirupati, AP, India.
E-mail: thatimakula_sudha@yahoo.com

Abstract

The Internet of Things (IoT) is fast growing to have a bigger influence on everything from ordinary living to massive industrial systems. However, this has drawn the attention of hackers, who have turned IoT into a focus for harmful activity, potentially allowing access to an assault on terminal nodes. In order to avoid assaults on IoT environments, a variety of IoT intrusion detection systems (IDS) have indeed been described in the literature, with the main categories being detecting technology, evaluation approach, and rollout strategy. This article includes a comprehensive assessment of current IoT IDS, in addition to an outline of the methodologies, deployment approach, testing technique, and datasets often employed in IDS development.IDS. They also look at just how current IoT IDS identify invasive attacks and safeguard IoT connections. It also classifies IoT threats and highlights upcoming research difficulties to resist these attacks to make IoT better and more reliable. These goals assist IoT security experts by bringing together, comparing, and summarizing disparate scientific research. As a result, we offer a one-of-a-kind IoT IDS taxonomy that throws fresh light on IoT IDS approaches, their benefits and drawbacks, IoT threats that make use of IoT communications networks, as well as matching increased IDS and detecting abilities to identify IoT hazards.

Keywords: Network level Forensics, IoT intrusion detection systems

Introduction

The Internet of Things is a network of networked devices which enable continuous data sharing among physical items. IoT devices are predicted to outnumber mobile devices in popularity as well as having exposure to private data, such as personally identifiable information. As an outcome, the surface area under assault will grow, as well as the likelihood of an assault. Because security will be a critical component of the majority of to protect communication enabled by these IoT technologies [1] [2], IoT apps and intrusion detection systems must be developed. AI advancements such as ML and DL approaches have been applied to enhance IoTIDS in recent years. The present requirement is to conduct an up-to-date, comprehensive taxonomy and critical analysis of this latest work. Artificial intelligence (AI) advancements such as ML and DL approaches have been applied to enhance IoT IDS in recent years. The current requirement is to do a complete classification and deep review of this most recent work. Numerous relevant research validated the development of IoT IDS by using various ML & DL algorithms on varied datasets [3] [4]. However, it remains unclear which dataset, ML, or DL approaches are most successful for developing an effective IoT IDS. Second, although being a major aspect in the success of 'online' IDSs, the time spent constructing & evaluating IoT IDS also isn't addressed in the assessment of different IDSs methodologies [5] [6].

Axelssonet.al presented an assessment of IDS and taxonomy, and categorized IDS based on detection techniques. The well-regarded survey conducted by Debar et al. assessed detection approaches based on the behavior and knowledge profiles of the assaults. Liao et al proposed a taxonomy of IoT intrusion systems that gave a classification of five subclasses with an in-depth look at their characteristics: Statistics, Patterns, Rules, States, and Heuristics. Alvarenga et al proposed a highly recognized survey examining IoT safety vulnerabilities broadly speaking [7] [8]. Targeting IoT devices, such as Denial of Service attacks, and attacks on RPL, are not included in their research [9] [10]. An IoT attacker might disrupt critical infrastructures like electrical systems, transportation, the internet, air traffic control, trains, and power plants. They examined threat detection in IoT and offered an excellent taxonomy for categorizing IoT IDSs based on detection technique, Strategy for IDS implementation, security threats & validation [11] [12]. Alvarenga et al., also stated in 2017 that IDS for IoT is still in its early stages and the existing IDSs are insufficient for a wide range of IoT threats [13]. This research investigated and debated whether the most recent IoT IDSs are enough for dealing with various IoT assaults. Existing review studies concentrate on intrusion detection algorithms, dataset issues, types of computer attacks, and IDS evasion [14] [15]. No publications fully evaluated IoT IDS, dataset issues, implementation strategies, IoT Intrusion tactics, and various types of attacks. Liao et al. presented, the evolution of IoT IDS has been such that multiple distinct systems have been offered in the meantime, necessitating the necessity for an up-to-date. Li Yang et.al, proposed a novel technique of ensembles, namely [16] [17]
oks into IDS for IoT on a large technological scale.

Techniques for IoT intrusion detection systems

IoT An incursion is defined as any illegal action or behavior that has an impact just on the IoT platform. An intrusion is described as any assault that compromises the privacy, integrity, or availability of data [18]. An incursion, for instance, is an assault that prevents legitimate users from entering computer systems. Liao and colleagues proposed An IDS is a software application or hardware solution that detects suspicious attacks on computer systems and maintains the system safe [19] The basic purpose of an IDS is to identify unauthorized computer usage and harmful network activity, which a standard firewall cannot achieve. As a result, systems are heavily fortified against hostile operations that threaten their availability, integrity, or confidentiality [20].

Intrusion detection systems based on signatures (SIDS)

Signature intrusion detection systems (SIDS) utilize pattern-matching approaches to identify existing attacks; this is known as Knowledge-based Identification or Malicious Behavior. In SIDS, similar approaches are employed to detect a previous breach. In other words, an alarm message is generated when an invasion fingerprint matches one in the data repository. SIDS examines the host's logs for previously recognized malware request patterns or behaviors. In the literature, SIDS is also known as Knowledge-Based Detection or Misuse Detection. SIDS, on the other hand, is unable to identify zero-day attacks since the database lacks a matching identity until the fingerprint of the new assault is collected and saved. Intrusion detection systems are used by Snort and NetSTA,for example Conventional SIDS approaches have trouble detecting attacks that involve many packets since they monitor the network traffic and match them to a signature database. With the rising complexity of current viruses, it may be necessary to extract signature data from a large number of packets.

Intrusion detection systems based on anomalies (AIDS)

Because their capability to surpass the restrictions of SIDS and AIDS has caught the curiosity of many scientists. AIDS uses machine learning, statistical, or knowledge-based approaches to construct a system. in the sequence of a computer system's behavior. Any significant distinction between the predicted and observed conduct is considered an abnormality, this might be interpreted as an invasion. This method is predicated based on the notion that detrimental conduct differs beyond ordinary user activity. An invasion is described as unusual user behavior that deviates from regular behavior.

Threats to the IoT ecosystem

Because IoT technology includes various devices such as sensors, and processors, as well as other innovations, the goal of exchanging data and connecting to other networks has been accomplished. Because it includes multiple linked devices, information given could not be safe, raising security concerns. The safeguarding of data is referred to as IoT security, transferred across networks via IoT devices utilizing IoT technologies. Such devices are linked to others through the internet, causing weaknesses to occur by permitting an attacker to take control of the information. Unsafe information causes numerous problems and large losses for many companies or even consumers, resulting in the loss of data from various systems. IoT has attracted the interest of individuals and organizations from a variety of industries due to the numerous benefits it offers. Along with its phenomenal expansion, various security vulnerabilities have arisen, resulting in IoT hacks that prohibit consumers from using many of its forthcoming applications. As a result, this part report examines the idea of IoT security, the IoT Security Issue, the Implications, and the Internet of Things exploit as well as its variants. On a secure network, IoT devices can be controlled from almost anywhere. As a result, there is a high risk of hostile assaults in the Network infrastructure. As a result, to safeguard the IoT from hostile assaults, privacy, security, and confidentiality problems must always be handled effectively. For instance, targeting traffic signals and driverless cars not only causes disruption and pollution, but it may also cause injury and catastrophic crashes, resulting in injuries. With the aid of the internet, many gadgets including workplace equipment may be remotely connected. They can carry out their tasks by watching the devices remotely.IoT encompasses a wide range of connections at the network layer, including WSNs, WiMAX networks, WLAN, and so on. Such networks enable IoT sensors to share data. A gateway may make things easier. the network-based interaction of multiple sensors As a result, a gateway might be useful. There are several difficult factors to communication. throughout the network Whereas the program is running, the core network guarantees that data is successfully sent.

The network layer

Data transmission occurs at this layer, in which security vulnerabilities arise and this can result in assaults. IoT threats include many types of information attack vectors that can be directed at single components, networks, or data sets. Items within IoT networks might be attacked, and physical security breaches could occur. These are frequently purposeful assaults designed to disrupt the accessibility of an IoT application or to compromise the confidentiality of data. The following Figure 1 depicts the categorization of network threats in the Internet of Things context.

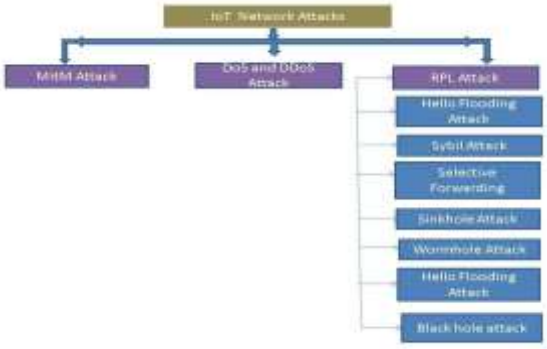

Fig 1.IoT Network Attacks classification

Man-in-the-middle (MITM) attack

Smart sensor interactions are at risk.vulnerable MITM attacks that might jeopardize the IoT communicant's confidentiality, integrity, and availability Neshenko et al. Encryption breaking, Eavesdropper, MAC faking, packet sniffing, and other wireless attacks are all conceivable. A MITM attack happens when the attacker does not have the authentication authorization user to disrupt communication between two persons who believe they are secretaries interacting with one another. It's similar to an eavesdropping assault in which the attacker may listen in on two

participants' conversations. MITM attacks include Email eavesdropping, WIFI eavesdropping, session hijacking, DNS spoofing, and IP spoofing are all examples of cybercrime. Conducting a reconnaissance operation and grabbing the network packet while it is in transit Furthermore, every device on the network between both the sending and receiving devices, as well as the final and original devices, is exposed to attackers.

DoS Assault

A denial of service attack prevents a system's services from being available on a regular basis. Legitimate system users are denied access to the resources. If a large number of hostile actors conduct this assault, This is known as DDoS. A DOS assault will cost the victim time and money instead of losing data as a result of service holders migrating from the original supplier. Regarding security issues DoS, attacks have the potential to deplete network resources, speed, and Computational time. Since IoT devices & infrastructure are always connected to the internet and switched on, the IoT network is vulnerable to attack. Malware payloads could be distributed at any time in the IoT network of a house or company. For example, 'Mirai' isa botnet that conductsa DDoS attack, rendering the bulk of the system accessible.

Distributed denial of service (DDoS)

In a DDoS assault, an intruder momentarily infects numerous IoT gadgets into a botnet before sending coordinated demands to a host or a network of servers for a certain service, overloading the server and forcing it to respond to legitimate requests from end users.

RPL (low-power and lossy routing protocol) attacks

Low-Power and Lossy Device Routing Protocol The transmitter broadcasts the DODAG Information Object during the DODAG generation process.Following receipt of the DIO, the recipient transmits its changed parent list, sibling list, rings, and transmits a DAO signal with route information.An attacker node does not update upon getting the DIO message; instead, they always broadcast a false rank. The second non-malicious component gets the message from the compromised node and changes its rank based on the bogus rank.The minimal and minimal intensive wireless networking resource nodes make innovative applications like intelligent electric grids and health solutions feasible.

Sybil attack

This attack is characterized as a group of nodes impersonating various peer identities in order to disrupt an IoT ecosystem. It is employed to send bogus data from a network. In the context of an e-health system, Sybil attacks, in which a sensor node claims numerous false identities, might be extremely harmful. An attacker might utilize phony identities to deliver fraudulent information using these tactics. As a result, either a real emergency situation is ignored. A rogue node within a network adopts numerous ids in this assault. A node that is malignant in a peer-to-peer system can disturb its routing scheme, routing protocol, and detecting procedure.

Attack with selective forwarding

The malicious nodes appear normal yet deliberately reject packets of information from a network or A group of nodes used in a selective forwarding invasion. A hostile link refuses to transmit data sent via it and disconnects the connection. A rogue or compromised node may deliver the message over the improper access link.

Sinkhole invasion

It is employed to disrupt data transfer between nearby nodes. It is mostly accomplished through the application of such a routing algorithm. An inside attack, A case in point is when a rogue node attempts to entice network traffic by promoting bogus routing changes. an assault on a sinkhole An attacker initiates an attack by inserting bogus nodes into a network. A sinkhole attack's principal purpose is to reroute traffic from such a region through a compromised node that seems extremely desirable to adjacent peers.

Wormhole invasion

In a wormhole attack, hostile nodes always provide an illusion to both the sender and recipient devices. A virtual tunnel is constructed that purports to be the most direct route between two places, in which nodes are infected, in order for the ground station to deliver data without losing it. The attacker node takes data and sends it to a remote site, where it is sent locally. The assault can be carried out in either a concealed or a mode of involvement.

Hello flooding attack

The Hello flooding attack is among the frequent network layer attacks that force IoT gadgets that send data Hello packets were sent to neighbors to promote themselves. In order to connect the network As a Hello packet, the node broadcasts the original message. By sending a Hello packet, the malicious user can advertise oneself as a neighbor node to a large number of nodes. When a node gets a Hello packet, it assumes it is within the radio transmission node's range that transmitted the message.

Blackhole attack

The malevolent actor in a Black Hole assault gadget inaccurately displays the quickest path to the destination & then stealthily removes all packets in its route. creating a networking blackhole.

Results and Discussion

The following results shows the IoT Network Intrusion Detection Using the UNSW-NB15 Dataset and several machine learning and deep learning methods.

Data sets used :

UNSW_NB15.csv - Source Dataset.

UNSW_NB15_features.csv - The class designation is associated with 49 attributes.

bin_data.csv-Binary Classification Dataset.

multi_data.csv - Multi-class Classification Dataset.

Data Preparation

The dataset contained 45 characteristics with 175341 rows.Dataset comprised 45 characteristics and 81173 entries after missing hypotheses wereremoved.The data structure of characteristics is transformed to use the identifier information supplied by the characteristics dataset.

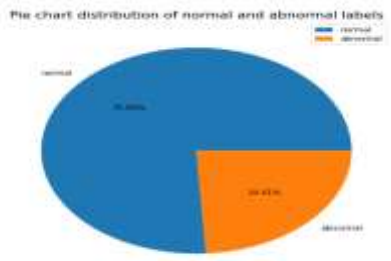

Figure :2.Pie chart distribution of Normal and Abnormal labels

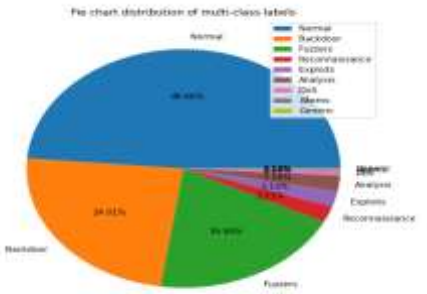

Figure :3.Pie chart distribution of Multi class labels.

The above fig 2 and 3 shows the binary and multi class label classification of attack artifacts in the data sets.And we have run through the various ML algorithms to check the accuracy of attack prediction and categorization at

Network level in IoT environment .The following table shows the comparison of various ML algorithms test results while running through the data sets.

Name of the ML /DL Algorithm	Binary Classification				
	Accuracy	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error	R2 Score
Decision Tree Classifier	98.09545118570 99	0.019094548881429 9114	0.019094548814290134	0.13883402650575473	89.55757103838088
K-Nearest-Neighbor	98.36612873421 62	0.016938712657838004	0.016938712657838004	0.13014880966738807	90.74435871039374
Linear Regression	97.80720665220443	0.021927933477055742	0.021927933477055742	0.14880083426647 67	88.28923968871647
Linear Support Vector Machine	97.85832337542347	0.021496766245765322	0.021496766245765322	0.14661775556106888	0.14661775556106888
Logistic Regression	97.88104712041884	0.021988528795881152	0.021989528795881152	0.14828866711868819	88.17947258428785
Multi Layer Perceptron	98.36772405297197	0.016322759470288826	0.016322759470288026	0.12776055522060474	91.16646288100463
Random Forest Classifier	98.64400298737296	0.013559070126278403	0.013559070126270403	0.11640883424278 46	92.59506512345335

Table:2. Parameter comparison of ML/DL algorithms using Binary label classification

Name of the ML /DL Algorithm	Multi Class Classification				
	Accuracy	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error	R2 Score
Decision Tree Classifier	97.39948867279895	0.068002628120889355	0.28532294480946123	0.45312464589650 86	86.17743096336013
K-Nearest-Neighbor	97.36777206754 27	0.065087056304559521	0.1941133666 2286466	0.44058871521897 624	86.92848100772136
Linear Regression	85.12976346911958	0.068249014450646491	0.12146846254927726	0.34852325969621 78	91.82055676180129
Linear Support Vector Machine	97.5936268685311	0.059912943495480786	0.1794103153 7450722	0.42356854861345 317	87.53449282203455
Logistic Regression	97.58952036793693	0.060077201851248356	0.1805681182 6544022	0.42492366169165 647	87.87674567880146
Multi Layer Perceptron	97.54434954807884	0.060652102496714	0.1758890275 95269	0.42259795029705 1	87.97913435505 16
Random Forest Classifier	97.31849540078844	0.066113666228646652	0.1985052562 417871	0.44553828687903 52	86.6379909424011

Table:1. Parameter comparison of ML/DL algorithms using Multi label classification.

Conclusion

We detailed a comprehensive review of IoT intrusion detection system approaches in this research, including deployment approach, validation method, dataset, and technology, as well as their benefits and drawbacks. Several intrusion detection systems using ML and DL have been compared and suggested to IoT attacks.

References

1.A. Abbasi, J. Wetzels, W. Bokslag, E. Zambon, S. Etalle, "On emulation-based network intrusion detection systems," in Research in attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden,

September 17–19, 2014. Proceedings, A. Stavrou, H. Bos, G. Portokalidis, Cham: Springer International Publishing, 2014, pp. 384–404

2.Aburomman AA, IbneReaz MB (2016) A novel SVM-kNN-PSO ensemble method for intrusion detection system. Appl Soft Comput 38:360–372

3.Aburomman AA, Reaz MBI (2017) A survey of intrusion detection systems based on ensemble and hybrid classifiers. Comput Security 65:135–152

4.Agrawal S, Agrawal J (2015) Survey on anomaly detection using data mining techniques. Procedia Computer Science 60:708–713

5.Alazab A, Hobbs M, Abawajy J, Alazab M (2012) Using feature selection for intrusion detection systems. In: 2012 International Symposium on Communications and Information Technologies (ISCIT), pp 296–301

6.Alazab A, Hobbs M, Abawajy J, Khraisat A, Alazab M (2014) Using response action with intelligent intrusion detection and prevention system against web application malware. InfManagComputSecur 22(5):431–449

7.Alcaraz C (2018) Cloud-assisted dynamic resilience for cyber-physical control systems. IEEE WirelCommun 25(1):76–82.

8.Annachhatre C, Austin TH, Stamp M (2015) Hidden Markov models for malware classification. J ComputVirolHack Technique 11(2):59–73.

9.Axelsson S (2000) "Intrusion detection systems: A survey and taxonomy,"Technical report.

10.Bajaj K, Arora A (2013) Dimension reduction in intrusion detection features using a discriminative machine learning approach. IJCSI Int J ComputSci Issues 10(4): 324–328.

11.Benkhelifa E, Welsh T, Hamouda W (2018) A critical review of practices and challenges in intrusion detection systems for IoT: toward universal and resilient systems. IEEE Commun Survey Tutor 20(4):3496–3509.

12.Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection:methods, systems and tools. IEEE Commun Survey Tutorial 16(1):303–336.

13.Breiman L (1996) Bagging predictors. Machine Learn 24(2):123–140

14.Buczak AL, Guven E (2016) A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Commun Surveys Tutorial 18(2):1153–1176

15.Butun I, Morgera SD, Sankar R (2014) A survey of intrusion detection systems in wireless sensor networks. IEEE Commun Survey Tutorial (1):266–282

16.Can O, Sahingoz OK (2015) A survey of intrusion detection systems in wireless sensor networks. In: 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO), pp 1–6 IEEE

17.Cervantes C, Poplade D, NogueiraM, Santos A (2015) Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In: 2015 IFIP/IEEE International Symposium on Integrated Network Management(IM), pp 606–611 IEEE

18.Chaabouni N, Mosbah M, Zimmer A, Sauvignac C, Faruki P (2019) Network Intrusion Detection for IoT Security Based on Learning Techniques, in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671–2701,third quarter 2019. https://doi.org/10.1109/COMST.2019.2896380

19. H. Gupta, A.Srinivasulu, et al.,"Category Boosting Machine Learning Algorithm for Breast Cancer Prediction", Revue Roumaine Des Sciences Techniques, SérieÉlectrotechnique et Énergétique, vol. 66, issue. 3, pp. 201–206, 2021.

20. Chao L, Wen S, Fong C (2015) CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. Knowledge-BasedSyst 78:13–21

21.A.S.Bharati, R.N.Pise, P.Reddy, A.Bhargav, A.Srinivasulu, M.S.Khan,N.Bizon, "Sentiment Analysis of COVID-19 Tweets Using Deep Learning and Lexicon-Based Approaches", Sustainability,15, 2573, 2023. https://doi.org/10.3390/su15032573

22.Chebrolu S, Abraham A, Thomas JP (2005) Feature deduction and ensemble design of intrusion detection systems. Comput Security 24(4):295–307.