



Advanced Intrusion Detection Framework For Industrial Iot Using Deep Learning

Mr.T.Vamsivardhan Reddy
Assistant Professor, Dept. of CSE,
N.B.K.R. Institute of Science and Technology.

ABSTRACT

There are many sensors and actuators that make up the IoT, all of which are linked together over wired or wireless networks. Recent years have seen a meteoric rise in the variety of IoT use cases, from smart homes and VANETs to healthcare and smart cities to wearables. According to IHS Markit 1, the number of connected devices is expected to increase from 27 billion in 2017 to 125 billion in 2030, an average yearly increment of 12 percent. Due to the diversity of IoT architecture, devices, and communication channels (most notably wireless) and the sheer volume of data being transferred over these channels, security has become an urgent concern in the IoT space. As the number of IoT-enabled gadgets grows, so does the significance of ensuring their safety. We propose a novel Deep Learning-based Intrusion Detection System (DLIDS) to identify security threats in IoT environments and thereby help address the aforementioned problems with protecting IoT devices. The accuracy of attack detection is negatively impacted by the fact that many IDSs in the literature do not have optimal feature learning and dataset management. Many signature-based and machine learning/deep learning AUTO ENCODER-based CNN algorithms have been proposed to try and detect such attacks, but their success rate has been less than stellar. We introduce Deep Learning IDS based on the Convolution2D Deep Learning algorithm, which employs many layers to filter IOT data and, as a consequence, obtains optimised features that enable the detection of IOT attacks with a prediction accuracy of 99%.

Key words:-Image search, image re-ranking, semantic space, semantic signature, keyword expansion.

INTRODUCTION

The proliferation of Internet of Things applications has accelerated in recent years. There are many distinct kinds of physical endpoints or sensors that make up the Internet of Things. Because of their interconnectedness and Internet access, they may gather information from their surrounds and share it with one another. IoT gateways collect data from a wide variety of low-powered and resource-constrained devices and forward it on to Internet-connected endpoint networks. As the Internet of Things (IoT) market develops, security concerns become increasingly complex. The sheer volume of data being transferred over the network is only one factor; the complexity also stems from the diversity of the IoT's underlying architecture, the variety of devices that can be accessed, the variety of methods used to communicate, and so on. According to SonicWall's 2019 Cyber Threat Report, the number of attacks against the internet of things (IoT) surged by 217.5 percent between 2017 and 2018, from 10.3 million to 32.7 million. Authentication, data privacy, availability, confidentiality, integrity, energy efficiency, verifying single-point failures, and so on are all common components of security problems. High-level threats include things like unsecured interfaces and software/firmware/middleware; intermediate-level threats include things like routing disruptions, replay attacks, insecure neighbour discovery, buffer reservation, sinkholes, authentication, session establishment, and privacy violations; and low-level threats include things like jamming, Sybil, spoofing, insecure initialization, and sleep deprivation attacks.

A plethora of Intrusion Detection Systems (IDSs) have been published to address the security issue in the IoT. In conventional IDS, sensors collect data, which is then forwarded to an analysis engine, which analyses the data and looks for signs of intrusion. The reporting mechanism will notify the system administrator of any identified intrusions. Depending on whether the observed system or network behaviours match an attack signature or exceed a threshold, IDS methodologies can be further categorised as signature-based or anomaly-based methods. However, the accuracy of attack detection cannot be ensured using conventional methods due to the possibility of over-fitting caused by dealing with irrelevant aspects in the high dimensional data generated from hundreds of IoT sensors and devices. and lengthens the period of preparation.

RELATED WORK

This Sensitive Data Perturbation scheme is an improved heuristic data perturbation approach in which the degree of privacy is maximally preserved by the computation of tuple values corresponding to each user defined sensitive drift value [3, 4, 5].

A Geometric data perturbation scheme with variant perturb functions was proposed for effective privacy preserving data mining task [9].

The precision and recall of this tree-based ensemble classification scheme was determined to be excellent independent to the base classifiers used in the effective classification process.

We therefore had to carefully calibrate the methods used for measuring risks as well as the

transformations applied, to ensure that the PUF remains useful and at the same time complies with GDPR-specific requirements for publishing an open dataset.

LITERATURE REVIEW

Atzori, L., Iera, A., Morabito, G. (2010). The Internet of Things: A survey. *Computer Network*, 54(15): 2787-2805. <https://doi.org/10.1016/j.comnet.2010.05.010>

The concept of "the Internet of Things" is the focus of this paper. The convergence of many technological and linguistic approaches is the primary enabler of this promising paradigm. Among the most pertinent are identification and tracking methods, wired and wireless sensor and actuator networks, improved communication protocols (which are also used in the Next Generation Internet), and decentralised intelligence for smart things. Any significant advancement in the Internet of Things, it is easy to see, must be the outcome of synergistic operations undertaken in different domains of knowledge, such as telecommunications, informatics, electronics, and social science. This poll is intended for anyone who are interested in tackling this difficult field and helping to shape its future. Several scenarios for the future of the Internet of Things are discussed, and the technologies that will make them possible are analysed. Evidently, the research community still has some serious problems to solve. The most important ones are discussed at length below.

Sedjelmaci, H., Senouci, S.M., Al-Bahri, M. (2016). Lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. *IEEE ICC - Mobile and Wireless Networking Symposium*. <https://doi.org/10.1109/ICC.2016.7510811>

In the IoT, tiny sensors and devices with little resources may be linked to shady networks. However, due to the importance of the data handled by IoT devices, it is essential that they be protected. With encryption compromised, the most effective method for detecting intruders with a high degree of accuracy is an Intrusion Detection System (IDS). The high detection and low false positive rates of anomaly detection and signature detection are combined to accomplish this. The anomaly detection method models a node's usual activity with a learning algorithm, and when a new attack pattern (also called a signature) is found, it is also modelled with rules in order to obtain a high detection rate. The latter is what the signature detection method use to verify an assault. Anomaly detection, when enabled permanently on low-resource IoT devices, might result in significant energy waste.

Summerville, D.H., Zach, K.M., Chen, Y. (2015). Ultralightweight deep packet anomaly detection for Internet of Things devices. *2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC)*. <https://doi.org/10.1109/PCCC.2015.7410342>

Small embedded devices are progressively becoming network-enabled as we rush toward the Internet of Things (IoT). Many Internet of Things (IoT) devices are susceptible to attack because they either lack the processing power to run current intrusion prevention techniques or because their designers placed the addition of features and services above the need for protection. We've created a lightweight deep packet anomaly detection method that works well in differentiating between regular and abnormal payloads, and it can be deployed on resource-constrained IoT devices. In order to pick features, a bitwise AND operation and a conditional counter increment are all that is needed for efficiency. To facilitate quick assessment and adaptable feature space representation, the discriminating function is designed as a lookup table. The approach's inherent simplicity makes it amenable to efficient hardware or software implementation, allowing its use anywhere from network appliances and interfaces to the protocol stack of a given device. Using data collected from commercially available Internet of Things devices, we show that it is possible to distinguish payloads with a high degree of accuracy.

PROPOSED METHODOLOGY

IOT devices are small sensors which can be deployed in any environment such as Road Traffic Monitoring, patient health monitoring, home CCTV monitoring and many more. IOT devices are used to sense data from its environment and then using Internet connection will send that sense data to centralized server for monitoring. Sometime some malicious user can alter IOT network data to report false information for example they can later traffic sensor IOT to report false traffic data and this false information will be spread in to entire network.

To detect such attack many signature based and machine learning and deep learning AUTO ENCODER based CNN algorithms are introduced but their detection rate is not satisfactory. To increase detection performance we are introducing Deep Learning IDS based on Convolution2D Deep Learning algorithm which contains multiple layers to filter IOT data and this filtration helps in obtaining optimize features which result into IOT attack detection with a prediction accuracy of 82%.

IMPLEMENTATION

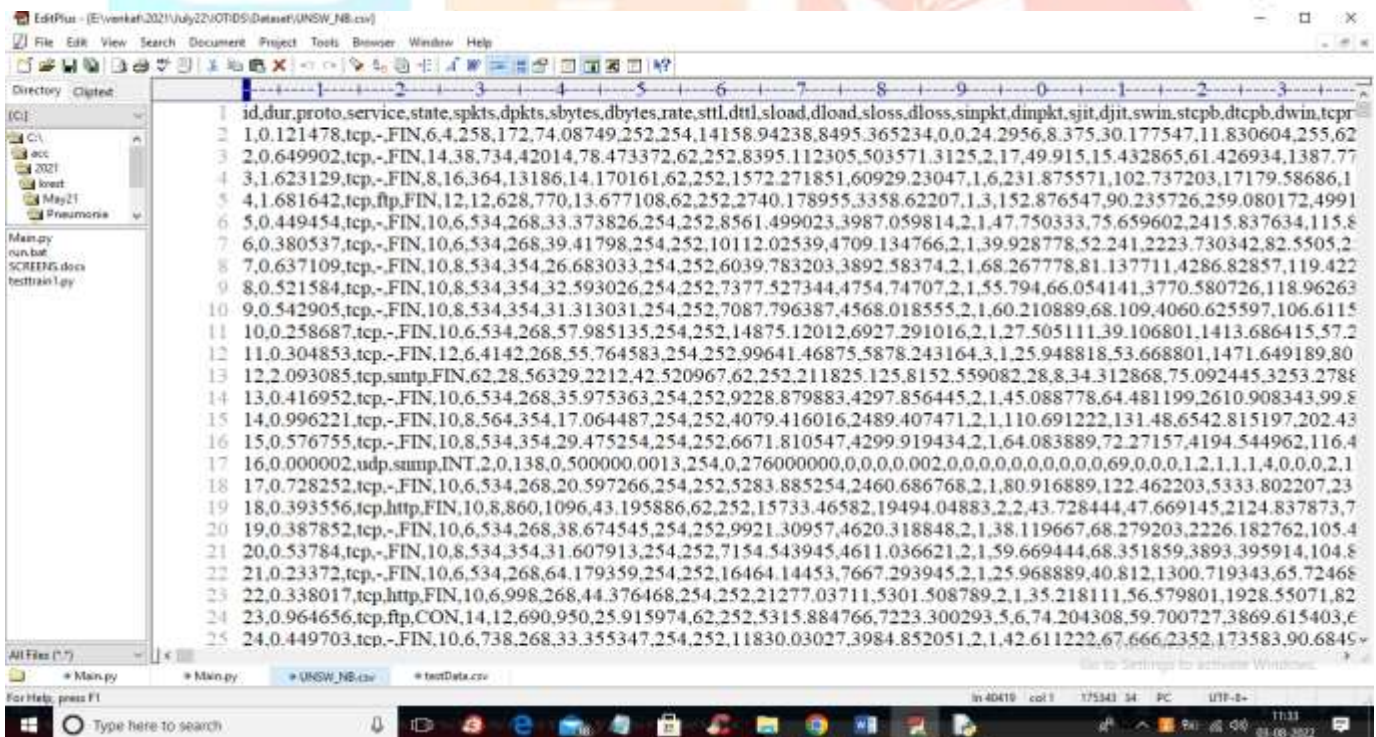
- 1) Upload UNSW-NB15 Dataset: using this module we will upload and read dataset values and then plot graph with normal and attack records
- 2) Preprocess Dataset: dataset contains missing and non-numeric values but deep learning algorithms only accept numeric values so by applying Preprocessing technique we are replacing missing values with 0 and then converting non-numeric data to numeric data by applying Label Encoding algorithm which will assigned unique Integer ID to each non-

numeric values. After processing dataset we are splitting into train and test where application using 80% dataset for training and 20% dataset for testing

- 3) Run AutoEncoder-CNN Algorithm: using this module we will input 80% training data to Auto Encoder algorithm and then trained a model and this trained model applied on 20% test data to calculate prediction accuracy
- 4) Run Propose Deep Learning-IDS: using this module we will input 80% training data to Propose Deep Learning Convolution2d algorithm and then trained a model and this trained model applied on 20% test data to calculate prediction accuracy
- 5) Detect Attack from Test Data: using this module we will upload test data and then Propose DL-IDS will predict whether test data is normal or contains attack
- 6) Comparison Graph: using this module we will plot comparison graph between existing and propose algorithms
- 7) Comparison Table: using this module we will display both algorithms performance in tabular format.

EXPERIMENTAL RESULTS

DATASET INFORMATION:



id	dur	proto	service	state	spkts	sbytes	dbytes	rate	sttl	dttl	sload	dload	sloss	dloss	simpkt	dimpkt	sjit	djit	swin	stcpb	dtcpb	dwin	tcpr	
1	0.121478	tcp	-	FIN	6.4	258.172	74.08749	252.254	14158.94238	8495.365234	0.0	24.2956	8.375	30.177547	11.830604	255.62								
2	0.649902	tcp	-	FIN	14.38	734.42014	78.473372	62.252	8395.112305	503571.3125	2.17	49.915	15.432865	61.426934	1387.77									
3	1.623129	tcp	-	FIN	8.16	364.13186	14.170161	62.252	1572.271851	60929.23047	1.6	231.875571	102.737203	171.79	58686.1									
4	1.681642	tcp	ftp	FIN	12.12	628.770	13.677108	62.252	2740.178955	3358.62207	1.3	152.876547	90.235726	259.080172	4991									
5	0.449454	tcp	-	FIN	10.6	534.268	33.373826	254.252	8561.499023	3987.059814	2.1	47.750333	75.659602	2415.837634	115.8									
6	0.380537	tcp	-	FIN	10.6	534.268	39.41798	254.252	10112.02539	4709.134766	2.1	39.928778	52.241	2223.730342	82.5505	2								
7	0.637109	tcp	-	FIN	10.8	534.354	26.683033	254.252	6039.783203	3892.58374	2.1	68.267778	81.137711	4286.82857	119.422									
8	0.521584	tcp	-	FIN	10.8	534.354	32.593026	254.252	7377.527344	4754.74707	2.1	55.794	66.054141	3770.580726	118.96263									
9	0.542905	tcp	-	FIN	10.8	534.354	31.313031	254.252	7087.796387	4568.018555	2.1	60.210889	68.109	4060.625597	106.6115									
10	0.258687	tcp	-	FIN	10.6	534.268	57.985135	254.252	14875.12012	6927.291016	2.1	27.505111	39.106801	1413.686415	57.2									
11	0.304853	tcp	-	FIN	12.6	4142.268	55.764583	254.252	99641.46875	5878.243164	3.1	25.948818	53.668801	1471.649189	80									
12	2.093085	tcp	smtp	FIN	62.28	56329.2212	42.520967	62.252	211825.125	8152.559082	28.8	34.312868	75.092445	3253.278										
13	0.416952	tcp	-	FIN	10.6	534.268	35.975363	254.252	9228.879883	4297.856445	2.1	45.088778	64.481199	2610.908343	99.8									
14	0.996221	tcp	-	FIN	10.8	564.354	17.064487	254.252	4079.416016	2489.407471	2.1	110.691222	131.48	6542.815197	202.43									
15	0.576755	tcp	-	FIN	10.8	534.354	29.475254	254.252	6671.810547	4299.919434	2.1	64.083889	72.27157	4194.544962	116.4									
16	0.000002	udp	sump	INT	2.0	138.0	500000.0013	254.0	276000000.0	0.0	0.002	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
17	0.728252	tcp	-	FIN	10.6	534.268	20.597266	254.252	5283.885254	2460.686768	2.1	80.916889	122.462203	5333.802207	23									
18	0.393556	tcp	http	FIN	10.8	860.1096	43.195886	62.252	15733.46582	19494.04883	2.2	43.728444	47.669145	2124.837873	7									
19	0.387852	tcp	-	FIN	10.6	534.268	38.674545	254.252	9921.30957	4620.318848	2.1	38.119667	68.279203	2226.182762	105.4									
20	0.53784	tcp	-	FIN	10.8	534.354	31.607913	254.252	7154.543945	4611.036621	2.1	59.669444	68.351859	3893.395914	104.8									
21	0.23372	tcp	-	FIN	10.6	534.268	64.179359	254.252	16464.14453	7667.293945	2.1	25.968889	40.812	1300.719343	65.72468									
22	0.338017	tcp	http	FIN	10.6	998.268	44.376468	254.252	21277.03711	5301.508789	2.1	35.218111	56.579801	1928.55071	82									
23	0.964656	tcp	ftp	CON	14.12	690.950	25.915974	62.252	5315.884766	7223.300293	5.6	74.204308	59.700727	3869.615403	6									
24	0.449703	tcp	-	FIN	10.6	738.268	33.355347	254.252	11830.03027	3984.852051	2.1	42.611222	67.6662352	173583.90	68.45									

Fig 1: In above screen first row contains dataset column names and remaining rows contains dataset value and in last column we have class label as Normal or ATTACK which means IOT request record contains normal signature or attack

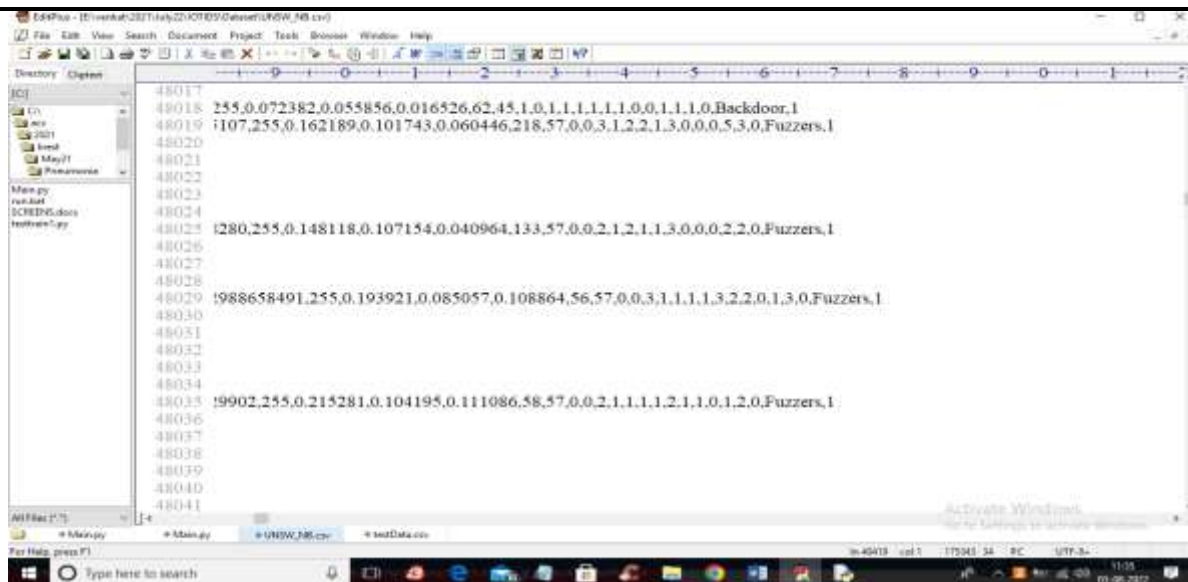


Fig 2: In above screens in last column we can see label as 0 or 1 where 0 means Normal and 1 means attack. By using above dataset we are training both existing and propose algorithm and then calculating their performance in terms of accuracy and precision and confusion matrix.

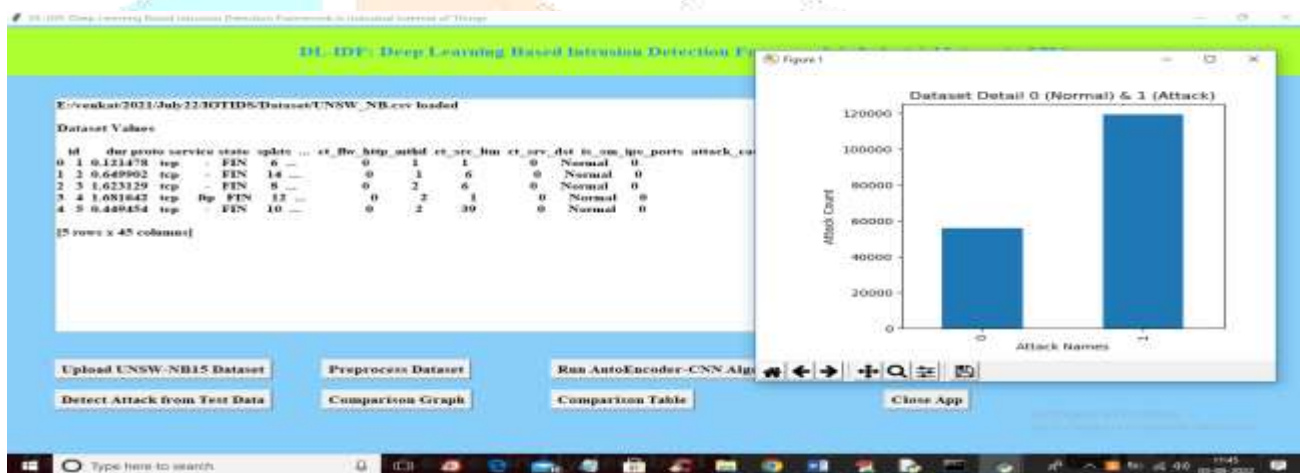


Fig 3: In above screen dataset loaded and in above graph x-axis contains class labels y-axis represents count of that class label where 0 means normal and 1 means attack. In above dataset we can see it contains non-numeric data so close above graph and the click on 'Preprocess Dataset' button to convert non-numeric to numeric and get below output



Fig 4: In above graph x-axis represents algorithm names and y-axis represents accuracy and other metrics such as precision, recall etc. In above graph different bar colour represents different metrics. Now close above graph and then click on 'Comparison Table' button to get below output

CONCLUSION

In this research, we present a novel intrusion detection system (IDS) based on deep learning for rapidly expanding IoT-based networks, with the goal of identifying critical abnormalities. Extracting the most important features from a dataset is the goal of the Deep Learning-IDS algorithm, which is a proposed replacement for the AutoEncoder-CNN Algorithm. In addition, these algorithms are utilised to learn the best attributes for classifying data as either normal or suspicious, indicating a cyber attack. With the NSL-KDD dataset as an evaluation ground, we found that our DL-IDS system outperformed the state-of-the-art methods in terms of accuracy (96.4%), precision (97.28%), recall (97.36%), and F1-score (97.32%).

REFERENCES

1. Howell. Number of Connected IoT Devices Will Surge to 125 Billion by 2030, IHS Markit Says. <https://technology.ihs.com>, Accessed June 2019.
2. V. Balasubramanian, et al. . A Mobility Management Architecture for Seamless Delivery of 5G-IoT Services. ICC 2019 - IEEE International Conference on Communications (ICC). 2019; 1-7.
3. Al Ridhawi, Ismaeel, et al. . A Profitable and Energy-Efficient Cooperative Fog Solution for IoT Services. IEEE Transactions on Industrial Informatics. (2019).
4. N. Abbas, et al. .A Mechanism for Securing IoT-enabled Applications at the Fog Layer. J. Sens. Actuator Netw. 2019; 8(1):16.
5. SonicWall Inc. . 2019 SonicWall Cyber Threat Report (2019). <https://www.sonicwall.com>, Accessed June 2019.
6. D.E. Kouicem, A. Bouabdallah, H. Lakhlef. Internet of things security: A top-down survey. Computer Networks.2018;141:199-221.
7. N. Tariq, et al. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey.2019;19(8): 1788.
8. J. Canedo, A. Skjellum. Using machine learning to secure IoT systems, in Proc. 14th IEEE Annu. Conf. Privacy Security Trust (PST). 2016:219-222.
9. M. AL-Hawawreh, N. Moustafa, E. Sitnikova. Identification of malicious activities in industrial internet of things based on deep learning models. Journal of Information Security and Applications. 2018;41:1-11.
10. M. Asad, et al. . DeepDetect: Detection of Distributed Denial of Service Attacks Using Deep Learning. The Computer Journal. 2019;0(0).
11. M. Aloqaily, S. Otoum, I. AlRidhawi, Y. Jararweh. An intrusion detection system for connected vehicles in smart cities. Ad Hoc Networks. 2019.
12. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. IEEE Internet of Things J.2017;4(5):1125-1142.