LIGHT WEIGHT INTRUSION DETECTION SYSTEM FOR IOT BASED on MACHINE LEARNING

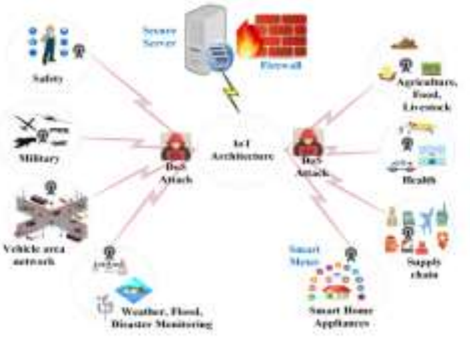
CH. AMBEDKAR, Assistant Professor, Department of CSE,
S.R.KINSTITUTEOFTECHNOLOGY, Enikepadu,Vijayawada–521108,,
Andhra Pradesh., India.

D.PUJITHA, P. KARTHIK, M. SATYAVANI, **K. PAVAN KUMAR,**
Student, Department of CSE, S.R.KINSTITUTEOFTECHNOLOGY,
Enikepadu,Vijayawada–521108,, Andhra Pradesh., India.

ABSTRACT: In the data collection stage, small, memory-constrained and low energy-consumption sensors with a short-range communications capability are employed to collect information about the physical environment. Ethernet, WIFI, ZigBee, and wire-based technologies are combined with Transmission Control Protocol/Internet Protocol to connect the objects and users across prolonged distances during data transmission. During the data processing and utilization stage, applications process the data to obtain useful information, and may initiate control commands to act on the physical environment after making decisions based on the collected information. The coordination of diverse technologies, the heterogeneity, and the distributed nature of communications technologies proposed for the IoT by different standards development organizations magnify the threat to end-to-end security in IoT applications.

INTRODUCTION

Internet of Things (IoT) is based on the integration of uniquely identifiable heterogeneous physical objects around us (humans, animals, sensors, instant cameras, vehicles etc.) and the cyber world with the ability to transfer data over a network without requiring humanto-human or human-to-computer interfaces. As illustrated in Figure 1, the applications of the IoT may range from simple appliance for a smart home to a complex apparatus in a smart grid. The IoT provides a tremendous opportunity for societiesaround the world. Even with different objectives, contrasting IoT applications have an intersectionset of characteristics. Broadly speaking, a primary node in IoT has capability to perform three distinct actions; data collection, data transmission, and data processing and utilization. In the data collection stage, small, memory-constrained and low energy-consumption sensors with a short-range communications capability is employed to collect information about the physicalenvironment. Ethernet, WIFI, ZigBee, and wire-based technologies are combined with Transmission Control Protocol/Internet Protocol to connect the objects and users across prolonged distances during data transmission. During the data processing and utilization stage, applications process the data to obtainuseful information, and may initiate control commands to act on the physical environment after makingdecisions based on the collected information. The coordination of diverse technologies, the heterogeneity and the distributed nature of communications technologies proposed for the IoT by different standards development organizations magnify the threat to end-to-end security in IoT applications. Numerous methods for improving data confidentiality, authentication, and access have been reported in the Literature however, even with these mechanisms, IoT networks are prone to multiple attacks aimed at disrupting the network. The growth, complexity, ubiquity, and diversity of the IoT expands the potential attacksurface. Therefore, intrusion prevention tools and signature-based intrusion detection methods cannot beeffective against modified attacks, and fundamentally new types of attacks, in the IoT. A defense mechanismaiming to detect novel and potential intrusions is required. Intrusion detection systems (IDSs) based onanomaly detection (a.k.a. statistically based) fulfill this purpose. Anomaly detection does notrequire prior identification of attack signatures.



PROPOSED SYSTEM

The cyber world with the ability to transfer data over a network without requiring tohumanto human or human-to-computer interfaces. As illustrated, the applications of the IoT may range from a simple appliance for a smart home to a complex apparatus in a smart grid. The IoT provides a tremendous opportunity for societies around the world. Even with different objectives, contrasting IoT applications have an intersection set of characteristics. Broadly speaking, a primary node in IoT has capability to perform three distinct actions; data collection, data transmission, and data processing and utilization.

In the data collection stage, small, memory-constrained and low energy-consumption sensors with a short-range communications capability are employed to collect information about the physical environment. Ethernet, WIFI, ZigBee, and wire-based technologies are combined with Transmission Control Protocol/Internet Protocol to connect the objects and users across prolonged distances during data transmission. During the data processing and utilization stage, applications process the data to obtain useful information, and may initiate control commands to act on the physical environment after making decisions based on the collected information. The coordination of diverse technologies, the heterogeneity, and the distributed nature of communications technologies proposed for the IoT by different standards development organizations [4] magnify the threat to end-to-end security in IoT applications.

DISADVANTAGES OF EXISTING SYSTEM:

1) Less accuracy

2)low Efficiency

The proposed classifier was obtained by combining a set of auto-encoders (AE) such that the output of an AE at (n − 1) th layer is the input to the AE at the nth layer. The results presented showed that the proposed DAE performed better in detecting intrusions in the systems, compared to the deep belief network (DBN) and a combination of AE+DBN. Shone et al. stepped forward and proposed a nonsymmetric deep auto-encoder (NDAE) to learn features in an unsupervised manner. A set of NDAEs is stacked to perform the learning and classification tasks.

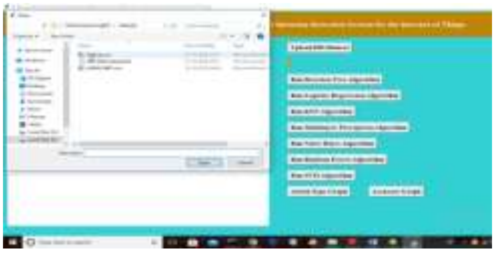
A malicious pattern detection mechanism was proposed by Oh et al. to secure networks in the IoT. They reduced memory usage in a pattern-matching process by proposing an auxiliary shifting method and an early decision scheme. They reported efficient results in early detection of a malicious pattern; however, they failed to detect and classify other attacks, such as denial of service (DoS), false data injection, etc. Furthermore, an attacker may try a unique pattern each time, making it difficult for the node to detect an attack.

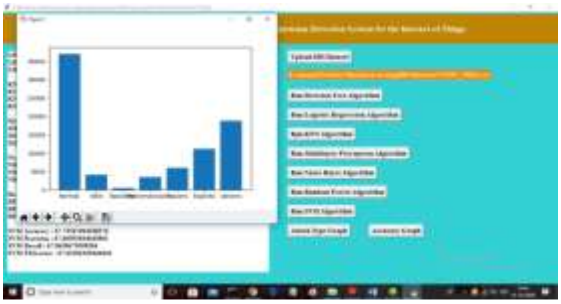
ADVANTAGES OF PROPOSED SYSTEM:

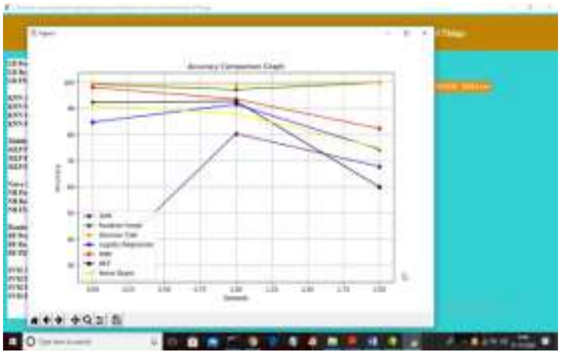
1) High accuracy

2)High efficiency

SAMPLE RESULTS







CONCLUSION

In this project The IoT is a promising technology developed for applications ranging from small smart-home systems to large networks, such as smart grids. However, this vast network is exposed to different types of attacks, compromising its reliability.

Furthermore, the limitations in the nodes, including memory, computational resources, and battery capacity, challenge network security. It is necessary to design a lightweight system that can efficiently improve the security of the IoT with the available resources.

This paper focuses on designing a lightweight IDS for anomaly detection in the IoT. A common type of attack, known as DDoS, is the target. The proposed IDS is focuses on two major issues; the attribute of the receiving data used to classify the signal and the machine learning based classifier. The only attributed considered in this paper is the packet arrival rate to the node. For classification purpose, an SVMbased classifier with input given in the form of two or three incomplex features is utilized. Through a series of experiments, we prove that these two factors (the packet arrival rate attribute and an SVM-based classifier) can be enough to detect the intrusion in IoT network.

FUTURE WORK: Furthermore, we presented a comparative analysis of SVM-based classifier with other machine learning-based classifiers including NN, k-NN and DT to show the advantage of utilizing SVM in terms of accuracy over other techniques. For further proof, we also presented a comparison of proposed algorithm with other IDS proposed in literature. The results show that an SVM-based IDS can perform satisfactorily in detection of attacks. Also, the lightweightness measure of proposed algorithm is proven in terms of CPU time execution.

An investigation of various concomitant effects of attacks and increase in the scope of this IDS system to encompass other types of intrusions, where the effect of changing traffic intensity is not clearly pronounced or masked by intruders, is reserved for future works.

REFERENCES

[1] Bruno BogazZarpelão, Rodrigo SanchesMiani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. A survey of intrusion detection in internet of things. Journal of Network and Computer Applications, 84:25–37, 2017.

[2] Sabrina Sicari, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. Security, privacy and trust in internet of things: The road ahead. Computer networks, 76:146–164, 2015.

[3] Dhananjay Singh, Gaurav Tripathi, and Antonio J Jara. A survey of internet-of-things: Future vision, architecture, challenges and services. In Internet of things (WF-IoT), 2014 IEEE world forum on, pages 287–292. IEEE, 2014.

[4] ArefMeddeb. Internet of things standards: who stands out from the crowd?

IEEE Communications Magazine, 54(7):40–47, 2016.

[5] Hichem Sedjelmaci, Sidi Mohamed Senouci, and Tarik Taleb. An accurate security game for low-resource iot devices. IEEE Transactions on Vehicular Technology, 66(10):9381–9393, 2017.

[6] Yulong Fu, Zheng Yan, Jin Cao, Ousmane Koné, and Xuefei Cao. An automata-based intrusion detection method for internet of things. Mobile Information Systems, 2017, 2017.

[7] Martin Roesch et al. Snort: Lightweight intrusion detection for networks. In Lisa, volume 99, pages 229–238, 1999.

[8] Tran Hoang Hai, Eui-Nam Huh, and Minho Jo. A lightweight intrusion detection framework for wireless sensor networks. Wireless Communications and mobile computing, 10(4):559–572, 2010.

[9] Yassine MALEH and AbdellahEzzati. Lightweight intrusion detection scheme for wireless sensor networks. IAENG International Journal of Computer Science, 42(4), 2015.

[10] Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari, and Ali A Ghorbani. Towards a reliable intrusion detection benchmark dataset. Software Networking, 2018(1):177–200, 2018.