Critical Review of Various Intrusion Detection Techniques for Internet of Things

Priyamwada Sharma
PhD Scholar
Rabindranath Tagore University
Bhopal, India
priyamwada14@gmail.com

ABSTRACT

Technology is rapidly moving towards the systems enabling maximum comfort to human being. IoT scenario has evolved into a technology for developing such comfortable eco system and became popular day by day, and at the point of attraction for the researchers world-wide who are involved in developing technology for creating comfortable and sustainable eco system for human being. Now a days IoT has shown a strong technological presence globally which embraced humanity in many ways, spread from home automation, smart city, industry and healthcare. These applications is endless and imaginable. A number of challenges and issues perceived by the system in which security and privacy are key issues. This security and vulnerability in IoT based system implies security threats which affects the overall performance of the system. In majority system related attacks could be addressed by an effective Intrusion detection system (IDS).

Due to limited resources like computing, energy, storage and specially designed protocols for operations, common Intrusion detection system those are well suited for conventional network are not enough for the intrusion detection in IoT. A well designed mechanism is needed for addressing the specific challenges and issues IoT faces. This paper surveys some suitable mechanism designed for detection of intrusions in an IoT system. As a result of the survey, this paper highlights the various issues and challenges associated with IDS of IOT

Keywords— Internet of things, Intrusion Detection System, Cyber-attack, Machine Learning, Anomaly Detection

INTRODUCTION

Pervasiveness of technology is imperative now a days for global economy, IoT now become the prime mover for global shift from the human operated technology to the automated human environment for the comfortable and sustainable human life. The advancement of material and sensor technology make it more effective to utilize it in various life domain. This also enable technology to develop intelligent system in which human involvement in taking decisions could be minimize. Even a tiny sensors embedded on a small chip could be capable to acquire data, process data and store data and even capable of taking decision.

Modern era of technology is dependent on the automated system for human comfort as well as for industrial automation, this tends to develop new technology called IOT the internet of things mainly concern to the interconnected devices equipped with some sensors and data acquisition system. The overall ecosystem of interconnected devices enable automatic and autonomous solution for various day to day and industrial problems. These mainly focuses on the automation preventive maintenance and other activities that are not very easy before this technology. The thing in IOT could be a sensor device for the CNC machine [1] which monitors the wear and tear losses, health monitoring system data acquisition system etc which are equipped with the embedded technology in the object help to communicate with the user for internal and external state of the system for which it has connected. With each innovation IOT receive more attention in terms of its vast usability and application. IOT system is a system of interconnected ting devices communicated wirelessly or and with internet. Communication itself perceived several security threats viz, intrusion, authentication. DOS etc which can affect overall performance of the system [2]. This paper present the contribution that spam the various intrusion detection technology and methods used by various researcher in IOT, also comprehensive analysis of various system has been done.

INTERNET OF THING ARCHITECTURE

With the development of the IoT technology and growing number of its deployment various architecture of IoT system has been introduced, most of them are based on their specific requirement depending upon the scope of the services rendered by this system. Some are focused on service layers while some are concerned about the sensing layer. This section presents an overview of the architectures proposed for IoT by various researchers.

[3] Defined may key challenges while designing an efficient IoT system equipped with embeds intelligence in the sensor devices capable of autonomous communications, exchange

of information, taking intelligent decisions, like Naming and Identity Management, Interoperability and Standardization, Information Privacy, Objects safety and security, Data confidentiality and encryption, Network security, Spectrum and Greening of IoT.

[4] Outlined the generic architecture of an IoT system which is consisting of three layers with specific services embedded in it like as application layer providing services for intelligent computing support range from data processing, data mining, security and analytics for huge data generated from the IoT system to efficiently interaction with the user. Transportation addresses issues related to the networking functions like routing, packet handling, gateways etc. whereas sensing layer deals with the issues related to the data acquisition and collection of information.

[5] Authors suggested some architectural requirements, which is an important aspect for developing technologies of future IoT defining the intrinsic and basic architectural requirement for IoT, they suggested, while designing the architecture of the IoT systems it should be able to handle millions of objects over network drawing traces and controls, having ubiquities capability with its high level compatible with the network, providing intelligent facility for taking decisions is an added advantage. They also identified the important issues like interconnections, intra connection and compatibility with a set of design standard.

[6] Suggested a IoT architecture for large scale composition based on capable of communication peer to peer and self-configuration. The aim of this proposed architecture is mutual independence of nodes with service discovery at global and local level for successful interaction among the network. Authors are tested their proposed model with an experiment on real world devices with reliable results.

[7] Discussed foundations for a generic IoT distributed architecture DIAT, which works on several abstraction levels capable to address most relevant issues such as heterogeneity, scalability, interoperability which are very important features such as automation, intelligence and zero configuration are the inherent part of the architecture. Satisfies the key characteristics and goals like Automation, Intelligence, Dynamicity and Zero-configurations. They have suggested an architecture where each layer and some of their cognitive features, virtualization of physical entities is the responsibility of the Virtual Object Layer (VOL), this layer also provide the service to act as a translator which bridges the gap between real world and cyber world and also helps to address heterogeneity issues. It also ensures the interoperability and reusability of entities. Automatic service deployment is done at Service Layer by initiating service requests by its own and this layer also tackles all service requests from users. Overall creation and management of services is the responsibility of this layer.

SECURITY OF IOT SYSTEMS

Exponential growth in number of IoT based services deployment and the future prediction, there is a need to utilize and researched on the secured integration of services as they are sensitive in nature directly related to automation and comfort of mankind. Several researchers have outlined the limitations of IoT devices like little energy level leads it to small life time and a very limited computational capability, accordingly suggested mechanism suitable to them, most of them are pointed out the need of a lightweight cryptographic mechanism which could be embedded on a small chip. Authorization and authentication are also important aspect for the secured IoT system here we present a survey of various security issues and challenges related to Secured IoT system deployment.

[8] Outlined the areas and challenges on which research on IoT security is imperative. This article suggested the importance and necessity of research in IoT security in the areas which need to address. One of them is Object identification and locating which is prime as identify an object came before other security issues. IoT architecture is resource constraint so that conventional Authentication and Authorization do not efficiently work on it so that research on Authentication and Authorization in IoT is needed. The case is same in the privacy, Cryptosystems and security protocols issues. Issues related to Android Platform and Malware in IoT

[9] Presented a security model for IoT which consisting four nodes responsible for different tasks, they are defined by person, process and technological ecosystem and Intelligent Object communicating in IoT ecosystem and work as basic actor in security mechanism. Intelligent Object has an important responsibility and works as a central agency for interactions among the other nodes.

This model proposes the service to be provided by Person which defines various rules, protocols, auditing practices while the system is in operational mode. Information security risk assessment, strategy, control implementation, monitoring and updating is the responsibility of Process and for sharing and exchanging information is the responsibility of intelligent object.

Technological ecosystem node is meant for the choices made for ensuring IoT system security they are categorized as Security Design and Configuration, Identification and Authorization, Enclave internal, Enclave boundary and Physical and environmental.

[10] Presented network architecture of cloud based IoT with an assumption that the users groups are formed based on the user pattern. They also addressed security and privacy requirements in cloud-based IoT on which they have proposed a security architecture; those are identity and location privacy, node compromise and layer, removing

/adding Attack, forward and backward security, malicious cloud security which mainly focuses on fine-grained cipher text access control, data confidentiality, location privacy and query privacy. They also introduced one-way trapdoor permutation as privacy preserving technique for secure data aggregation.

INTRUSION DETECTION SYSTEMS

Pervasiveness and ubiquitous capability of IOT has brought several benefits but also various security concern of interoperability and privacy. The major issue is there is no standard specifically designated for devices with limited resources and heterogeneity.

We can categorize attacks on an IOT system on various service layers. The important attack is the physical attack which mainly experience by the hardware associated with the IOT system. This attack can only be possible when an attacker is chase or inside the system. The most services attack on the IOT system is DOS (Denial of services) is which an attacker perform such operation on the system which jam the system and services are unavailable to the interconnected system which utilize the routing process for communication also perceived several security threats in which an attacker could modify the predefined route on which data as travelling and resulting wastage of data and resources – Data transmit attack is also a serious type of attack in which the confidentiality and integrity of the system affected during the data transit. In most of the application IoT system acquires important data and communicate to the user for processing this data is prone to theft which generally happen by using authentic credentials of the legitimate user. To affect the overall performance and result an attacker can upload malicious code through the known vulnerability leading to software malfunctioning and services.

It is imperative to find out the ways to address various issues of the IoT technology, mainly focused on open security environment, protection of individual privacy, functions related to terminal security of the system and laws related to the security of such an open environment. The security in Internet of thing could be precisely handled by deployment of complete regulation policies, laws and regulations and the stable and efficient management system. [11] Like all network system IOT is also vulnerable to cyber-attack because of the interconnection through wireless and internet. Insider attacks are more serious as the devices are configured to access the internet without intrusion detection system or firewall in place. [12] Focuses on the study of three insider attacks namely black hole, wormhole and sinkhole attack authors uses trust score to evaluate and compare with the existing in immutable ledger and used to take decision the node could be or not the part of the network. There are various researchers proposed highly scalable for intrusion detection which consider quality of service trust and social trust statistical method and stochastic petri nets for identifying the malicious behavior of any individual or group of nodes.

[13] Addresses the intrusion detection closely on the application layer of the IOT system to identify further attack against the normal operation rule of COAP protocol. In its solution Block chain is the distribution computing and storage environment utilizing the power of Hash function to authenticate each and every block of the chain, which can't be modified as the copy of every block resides at every node of the network. The power of block chain for developing intrusion detection system of IOT has been the network, BAD has designed to identify anomalous transections in the network and stopped them to spread further is the network. Machine learning techniques are associate with the BAD architecture to make it predictive for IOT heterogeneous malicious transaction.

It this solution the attack logs create a threat database which enable other victim node for safeguard against zero day attacks which was already discovered by the network. [14] Proposes generic architecture for the intension of block chain technology into intrusion detection system utilizing collaboration mechanism by combining knowledge of large no of monitors to populate historical data of monitored network. The major challenge of maintain trust among the collaboration nodes are addressed by taking advantage of distributed ledger technologies which help to improve trust significantly between monitors.

Author proposed collaborative intrusion detection system in which they used block chain as a mean of collaboration. In their Intrusion detection architecture authors assign every participating node in block chain network could work as either for monitoring, analysis or performing both work simultaneously. Without a secret key any node could not see alert data exchanged and processed among certified participating nodes, which leads to develop a mechanism in which participating peer shall be in position to collaborate in multiple groups without disseminating any confidential alert information to non- participating external node.

Most of the signature based Intrusion detection system work on the principal of similarity as the signatures are already available with the database, these system are efficient for detecting known attacks, make this system more popular and acceptable in the industry.

[15] Proposed a signature-based intrusion detection system for the detection of denial of service attack and routing attacks utilizing a hybrid placement strategy for intrusion detection system modules at centralized and distributed components. Detection module is being deployed on main router and other module comparably having lower computing complexity be deployed over the network which is nearly located to IoT device, which only perform the task of traffic monitoring and reporting, which does not affect the software configuration of existing device. Proposed

method involve centralized and distributed deployment strategies for detection of intrusion from initiated form participating compromised IoT device and the external network. The disadvantage of the proposed method is their negative impact of power consumption by IoT Node which could cause dis connectivity of node to the network due to less power.

[16] Proposed IDS based on clustering featuring patterns and Gaussian dissimilarity measure. Incremental feature clustering performed by distance measure to find dimensionally reduction and approach threshold selection. Here allowable user threshold or dissimilarity limit defines the number of clusters generation in which both of them are related in inverse function. The limitation of this method is that the user has to specify the value of deviation as the number of clusters will be formed on the basis of value of deviation, which shall be performed in an incremental manner.

Author have proposed there separate algorithms for incremental feature clustering, dimensionality and feature representation and for anomaly detection. Here anomaly detection algorithm is based on evolutionary clustering and feature transformation. The performance of the proposed method accuracies for U2R and R2L attack classes, for KNN and J48 classes but lowest classification and detection accuracies for SVM classifiers. [17] User behavioral based algorithm which is based on immunity inspired algorithms to find the patter for matching the similarity from the desired pattern and the deviated pattern. This techniques acquire behavioral pattern by capturing IOT sensor data activity as a set of event sequences and develop a numerical representation of ambiguity associated with the one behavior to many behavioral scripts. [18] Propose automata model for getting complete intrusion view is an IOT network. I this scheme intrusion is an IOT network will be detected by collecting data from network and analyzing the transmitted packets which shall further translated to formal format of automata, then by comparing real- time action flows to the anomalous flow or standard libraries.

[19] Author proposed trust based intrusion detection method in which the trust score is measured by the comparison with the score existing in immutable distributed ledger in block chain which could be the base for making decision whether the network should exclude or include such node on the account of trustworthiness of nodes. Initial trust score is stored in the device at the time of its manufacturing to act as monitoring node which help it to calculate trust score of all the neighbor nodes based on its honestly observation on the cooperative behavior of reception and forwarding of packets by neighbor nodes as every node in the network has to keep a neighborhood table which the information of node ID is maintained and act as monitor node to prepare a transaction record, which is shared to all the neighboring nodes at a specific interval. Trust score created by un-cooperative behavior of neighboring node help to detect malicious packet forwarding and dropping. The method utilize a trust management system in which trust score is stored in the distributed ledger by ledger election. The node with highest trust score at that moment of time shall be elected as the leader.

This proposed scheme can detect three types of intrusion attacks on IOT viz Jam – attack false attack and reply attack. Mapping of IOT system to an abstract space for uniform security mechanism using automata, which is a combinations of heterogeneous networks with terms and graphs. Automata based IDS has four major components ie Event monitor, Event Database, Event Analyzer and Response unit. Event monitor collect the data at the gateway of the network in terms of a digital file and send the file to IDS event analyses. Event database is collection of standard protocol libraries, abnormal action library and normal action libraries. As the network event is described as the abstract action flows the comparison of real time abstract action flow with the protocol libraries gives the view of attack. Event analyzer consisting Network structure learning model, Action flow abstraction model and intrusion detection model.

Network structure learning model give the general view of network topologies. Action flows abstraction model classify network traffics into message sequences. Which shall allocate the packets to be message into abstract action flows using Standard Protocol library. Which is now the list of automata transition sequence of the target system. Which is sent to the input to intrusion verification for intrusion detection.

[20] Proposed a model for detection intrusion in IoT at its network layer based on dimension reduction model Principal Component Analysis and a classifier based on soft max regression which is that it is suitable for dealing with the data flow instantly shows better time performance for labelling benign behaviours and identifying malicious behaviours. This proposed method is designed for Probing Attack, Denial of Service Attack, and Users to Root Attack and Remote to Local Attack. High dimensional data reduce the performance of fault diagnosis as there are lot of dimensions which are not only irrelevant for fault identification but creates noise but also, for that authors have used high dimensional data reduction algorithm.

For addressing the issues related to complexity of data as the data which is to be analyzed is having a lot number of dimensions in which many of them are irrelevant, author suggested to reduce dimension which are irrelevant for analyzing to improve performance of fault diagnosis. This mechanism also reduces noisy data and computational

complexity, which is a necessary requirement for real time system.

CONCLUSION

This paper presents the survey about various aspect of IoT technology start from various architecture proposed in time and the issues and the challenges on which the architecture have been proposed also presented a taxonomy to classify these architectures, which is based on the attributes like layered structure, physical attributes and the scope of the requirements. Security in IoT is also studied in this paper underlined various issues and challenges in IoT system deployments. Various security requirements and parameters were also discussed in general IoT environment and at the cloud based environment. Scope of this paper is to survey various intrusion detection system for IoT system, so that a critical study also done in the area and presented some research outcome of various researchers who proposed Intrusion detection system for IoT on various system deployments. They all are categorized in the categories on the basis of the type of the deployment and the security threats perceived by the IoT system.

REFERENCES

[1] Ibtesam R. K. Al-Saedi, Farag Mahel Mohammed and Saif Aldeen Saad Obayes, CNC Machine Based on Embedded Wireless and Internet of Things for Workshop Development, International Journal of Computing and Digital Systems, 6(4), (2017) pp 205-211

[2] Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network Intrusion Detection for IoT Security based on Learning Techniques. IEEE Communications Surveys & Tutorials, 1–1.

[3] Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. 2012 10th International Conference on Frontiers of Information Technology.

[4] Yaqoob, I., Ahmed, E., Hashem, I. A. T., Ahmed, A. I. A., Gani, A., Imran, M., & Guizani, M. (2017). Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges. IEEE Wireless Communications, 24(3), 10–16.

[5] Ning, H., & Wang, Z, . Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework? IEEE Communications Letters, 15(4), 461–463, 2011

[6] S. Cirani et al., "A Scalable and Self-Configuring Architecture for Service Discovery in the Internet of Things," IEEE Internet of Things J., vol. 1, no. 5, 2014, pp. 508–21.

[7] Sarkar, C., Nambi, S. N. A. U., Prasad, R. V., & Rahim, A. (2014). A scalable distributed architecture towards unifying IoT applications. 2014 IEEE World Forum on Internet of Things.

[8] Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K., & Shieh, S. (2014). IoT Security: Ongoing Challenges and Research Opportunities. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications

[9] Yacine Challal, Internet of Things Security: towards a cognitive and systemic approach, HDR Thesis, Université de Technologie de Compiègne, 2012.

[10] Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and Privacy for Cloud-Based IoT: Challenges. IEEE Communications Magazine, 55(1), 26–33.

[11] Lan Li, Study on Security Architecture in the Internet of Things, Intemational Conference on Measurement, Information and Control (MIC), pp 374-377, 2012

[12] Ambili, K. N., & Jimmy Jose. (2019). Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems. Information Science and Applications, 631–638.

[13] Granjal, J., & Pedroso, A. (2018). An Intrusion Detection and Prevention Framework for Internet-Integrated CoAP WSN. Security and Communication Networks, 2018, 1–14.

[14] Alexopoulos, N., Vasilomanolakis, E., Ivánkó, N. R., & Mühlhäuser, M. (2018). Towards Blockchain-Based Collaborative Intrusion Detection Systems. Lecture Notes in Computer Science, 107–118.

[15] Philokypros P. Ioulianou, Vassilios G. Vassilakis, Ioannis D. Moscholiosy, Michael D. Logothetis, A Signature-based Intrusion Detection System for the Internet of Things, Information and Communication Technology Form, 2018

[16] Aljawarneh, S. A., & Vangipuram, R. (2018). GARUDA: Gaussian dissimilarity measure for feature representation and anomaly detection in Internet of things. The Journal of Supercomputing.

[17] Arrington, B., Barnett, L., Rufus, R., & Esterline, A. (2016). Behavioral Modeling Intrusion Detection System (BMIDS) Using Internet of Things (IoT) Behavior-Based Anomaly Detection via Immunity-Inspired Algorithms. 2016 25th International Conference on Computer Communication and Networks (ICCCN).

[18] Fu, Y., Yan, Z., Cao, J., Koné, O., & Cao, X. (2017). An Automata Based Intrusion Detection Method for Internet of Things. Mobile Information Systems, 2017, 1–13.

[19] Ambili K.N., Jimmy Jose Trust Based Intrusion Detection System to Detect Insider Attacks in IoT Systems. In: Kim K., Kim HY. (eds) Information Science and Applications. Lecture Notes in Electrical Engineering, vol 621. Springer, Singapore, 2020

[20] Shengchu Zhao, Wei Li, Tanveer Zia and Albert Y. Zomaya, A Dimension Reduction Model and Classifier for Anomaly-Based Intrusion Detection in Internet of Things, IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, pp 1836-843, 2017