Enhancing Cyber Space Security in Modern Internet of Things (IoT) with the use of Intrusion Prevention Algorithm for IoT (IPAI)

[1] Nadiya Begum, [2] Nousheen Sulthana, [3] Mohammadi Aliya,[4] Mr.Mohammed Rahmat Ali

[1] BE Student, Dept. of Computer Science Engineering, ISL Engineering College

[2] BE Student, Dept. of Computer Science Engineering, ISL Engineering College

[3] BE Student, Dept. of Computer Science Engineering, ISL Engineering College

[4] Assistant Professor, Dept. of Computer Science Engineering, ISL Engineering College

Article Info
Page Number: 1398-1405
Publication Issue:
Vol. 72 No. 1 (2023)

Article History
Article Received: 15 October 2022
Revised: 24 November 2022
Accepted: 18 December 2022

ABSTRACT

These Internet of Things (IoT) is a swiftly evolving paradigm having potential to transform the physical interaction between the individuals and organizations. IoT network aims to exchange ‘‘things’’ in secure and reliable way through IT infrastructure. This technology has found application in multiple fields such as, healthcare, learning and training, resource management, information processing to name a few.A prevention technique is proposed to enhance cyber security of IoT devices and networks against DDoS attacks which consume the bandwidth in modern Internet of things (IoT) devices.DDoS includes a group of attacker nodes and targets the victim to prevent the legitimate users from accessing the network services and resources. Intrusion prevention system in IoT devices are the procedures that are treated as Add-ons’ of the intrusion detection system to actively defend and prevent the intrusions, that are detected by the detection procedures of the IDS. The report that is generated by the IDS after analyzing the report of the forensic analysis is the base of the proposed procedure. As extension in this project to increase network performance and to reduced packet transmission time we are employing packet compression technique.

Keywords: *IoT, DDoS, Cyber Security, IDS, IPS.*

1. Introduction

The Internet of Things (IoT) is a rapidly growing trend that involves connecting various devices and objects through wireless sensors and the internet. It enables seamless communication and interaction between physical objects, users, and the virtual world. The primary objective of IoT is to facilitate the exchange of data and services within the global supply chain network. It is an active IT infrastructure with self-configuring capabilities that allow different devices to communicate through intelligent interfaces.

However, one of the significant challenges faced by IoT is security. Unlike traditional wired networks, wireless IoT networks are more vulnerable to attacks. In wired networks, traffic passes through secure routing devices equipped with firewalls and other security measures. In contrast, IoT networks, being peer-to-peer and ad-hoc in nature, lack centralized control, and the communication links between nodes are wireless. The dynamic and decentralized nature of

IoT networks makes it necessary for each node to incorporate security mechanisms to preventattacks.

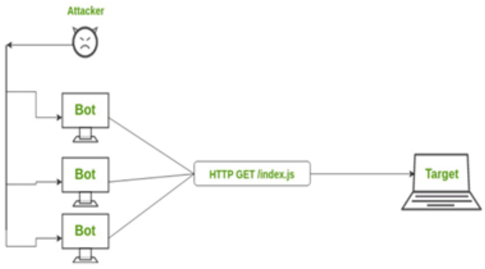


Fig.1: Example figure

2. Literature Review

Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms:

AUTHORS: T. A. Ahanger and A. Aljumah.

The Internet of Things (IoT) is an evolving global trend in Web-based information architecture aiding in the exchange of services and goods over a network without necessitating human-to-human or human-to-computer interaction. It has the potential to revolutionize physical world interaction of individuals and the organizations. The application of IoT can be recognized significantly in many areas such as in healthcare, resource management, learning, knowledge processing, and many more. The practical realization of IoT is met with a plethora of security and privacy challenges that need to be tackled for IoT's successful deployment on a commercially viable large scale. This paper analyzes the security issues related to IoT networks through an analysis of the existing empirical researches to get an insight on the security requirements of the IoT networks. The findings of the study revealed that security threats are one of the biggest and ever-growing challenges for IoT, and it is essential to substantially mitigate them for the success of this platform.

An IoT-Aware Architecture for Smart Healthcare Systems:

AUTHORS: L. Catarinucci et al.

Over the last few years, the convincing forward steps in the development of Internet of Things (IoT)-enabling solutions are spurring the advent of novel and fascinating applications. Among others, mainly radio frequency identification (RFID), wireless sensor network (WSN), and smart mobile technologies are leading this evolutionary trend. In the wake of this tendency, this paper proposes a novel, IoT-aware, smart architecture for automatic monitoring and tracking of patients, personnel, and biomedical devices within hospitals and nursing institutes. Staying true to the IoT vision, we propose a smart hospital system (SHS), which relies on different, yet complementary, technologies, specifically RFID, WSN, and smart mobile, interoperating with each other through a Constrained Application Protocol (CoAP)/IPv6 over low-power wireless personal area network (6LoWPAN)/representational state transfer (REST) network infrastructure. The SHS is able to collect, in real time, both environmental conditions and patients' physiological parameters via an ultra-low-power hybrid sensing network (HSN) composed of 6LoWPAN nodes integrating UHF RFID functionalities. Sensed data are delivered to a control center where an advanced monitoring application (MA) makes them easily accessible by both local and remote users via a REST web service. The simple proof of concept implemented to validate the proposed SHS has highlighted a number of key capabilities and aspects of novelty, which represent a significant step forward compared to the actual state of the art.

Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios:

AUTHORS: E. Oriwoh, H. M. al-Khateeb, and M. Conrad.

The proliferation and popularity of smart autonomous systems necessitates the development of methods and models for ensuring the effective identification of their owners and controllers. The aim of this paper is to critically discuss the responsibility of Things and their impact on human affairs. This starts with an in-depth analysis of IoT Characteristics such as Autonomy, Ubiquity and Pervasiveness. We argue that Things governed by a controller should have an identifiable relationship between the two parties and that authentication and non-repudiation are essential characteristics in all IoT scenarios which require trustworthy communications. However, resources can be a problem, for instance, many Things are designed to perform in low-powered hardware. Hence, we also propose a protocol to demonstrate how we can achieve the authenticity of participating Things in a connectionless and resource-constrained environment.

Integration of Agent-based and Cloud Computing for the Smart Objects-oriented IoT:

AUTHORS: G. Fortino, A. Guerrieri, C. Savaglio, and W. Russo.

In In the future Internet of Things (IoT), smart objects will be the fundamental building blocks for the creation of cyber-physical smart pervasive systems in a great variety of application domains ranging from health-care to transportation, from logistics to smart grid and cities. The implementation of a smart objects-oriented IoT is a complex challenge as distributed, autonomous, and heterogeneous IoT components at different levels of abstractions and granularity need to cooperate among themselves, with conventional networked IT infrastructures, and also with human users. In this paper, we propose the integration of two complementary mainstream paradigms for large-scale distributed computing: Agents and Cloud. Agent-based computing can support the development of decentralized, dynamic, cooperating and open IoT systems in terms of multi-agent systems. Cloud computing can enhance the IoT objects with high performance computing capabilities and huge storage resources. In particular, we introduce a cloud-assisted and agent-oriented IoT architecture that will be realized through ACOSO, an agent-oriented middleware for cooperating smart objects, and BodyCloud, a sensor-cloud infrastructure for large-scale sensor-based systems.

3. METHODOLOGY

However, practical realization of this technology is met numerous security and privacy concerns, which are to be mitigated for large scale successfully deployment of IoT technology. A prevention technique is proposed to enhance cyber security of IoT devices and networks against DDoS attacks which consume the bandwidth in modern Internet of things (IoT) devices. Since these networks are wireless and self configuring and doesn't need a pre-existing infrastructure and have a large unpredictable node movements, security becomes one of the most vital issue to be raised into the account.

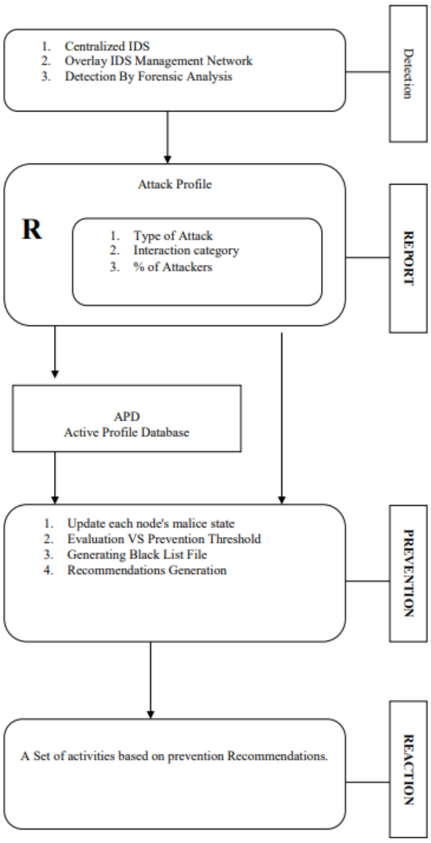

1. Centralized IDS
2. Overlay IDS Management Network
3. Detection By Forensic Analysis
Detection
Attack Profile
R
1. Type of Attack
2. Interaction category
3. % of Attackers
REPORT
APD
Active Profile Database
1. Update each node's malice state
2. Evaluation VS Prevention Threshold
3. Generating Black List File
4. Recommendations Generation
PREVENTION
A Set of activities based on prevention Recommendations.
REACTION

Fig.2: System architecture

4. Implementation

IOT (Internet of Things) are small devices which can send or receive data through internet and this devices are using in various fields such as health care (doctors will embed IOT devices in patient body or can be used as watch to monitor patient BP, Heart Rate etc and send that information to hospital server for monitoring), agriculture fields, military area etc. This small devices runs on batteries and infrastructure less as it can configure themselves by finding neighbours to send or receive data. Due to infrastructure less (require no monitoring of human) this small devices security is at risk as we cannot include heavy computation security algorithms in small devices due to battery power.

Attackers can intrude any devices and monitor all data and then perform mischievous activities by making himself as neighbour and then collect all packets and drop them or continuously send dummy packet to jam the network. This attacks are of two types INSIDER and OUTSIDER in INSIDER attack attacker steal information from genuine node and misuse it and in OUTSIDER attack attacker becomes neighbour of genuine node and perform mischievous activities.

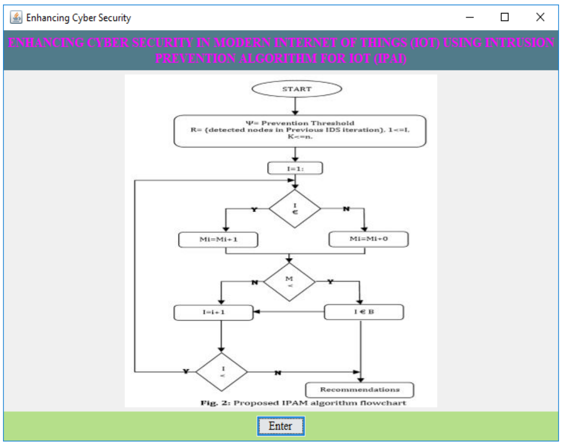
As we cannot include intrusion detection system in small devices so to provide security to IOT devices author of this paper introduce simple concept called LOG monitoring. In this propose approach two types of nodes work together called NORMAL NODES and IDS NODES. Normal nodes will send and receive packets and all this activities will be monitor by IDS node and generate a report. In this report we will have Node id, event type (whether nodes perform proper communication or drop the packets this we can now by receiving ACK from nodes) and time stamp. Generated log report will be send to STATION and STATION will analyse this report to know which nodes are performing well and which nodes are doing malicious activities. By using this information station will remove such IOT nodes from networks. If attacker node drop/jam packets more than given threshold than that IOT node will be consider as attacker.

EXTENSION:

In this project to reduced packet transmission time we are employing packet compression technique which will monitor all packets in a period of time and if redundant packet sense or generated then those packets will be ignored from transmission and packet sending size will get reduce and can improve or reduce packet transmission time.

Normally IOT sensor always sense data from its environment and there is a chance that IOI will sense redundant or similar data and sending such data will consume network resources and take more transmission time and by avoiding such packets we can improve network performance.

5. Experimental Results

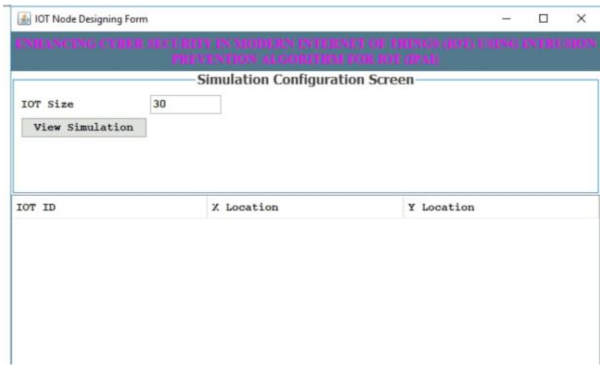


Enhancing Cyber Security

ENHANCING CYBER SECURITY IN MODERN INTERNET OF THINGS (IOT) USING INTRUSION PREVENTION ALGORITHM FOR IOT (IPAI)

Fig. 2: Proposed IPAM algorithm flowchart

Fig.3: Home screen



IOT Node Designing Form

ENHANCING CYBER SECURITY IN MODERN INTERNET OF THINGS (IOT) USING INTRUSION PREVENTION ALGORITHM FOR IOT (IPAI)

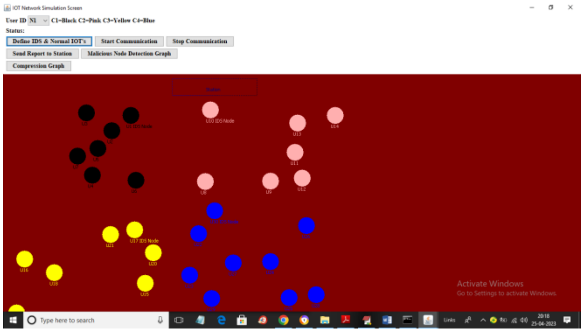
Simulation Configuration Screen

IOT Size: 30

View Simulation

IOT ID	X Location	Y Location

Fig.4: Simulation configuration screen



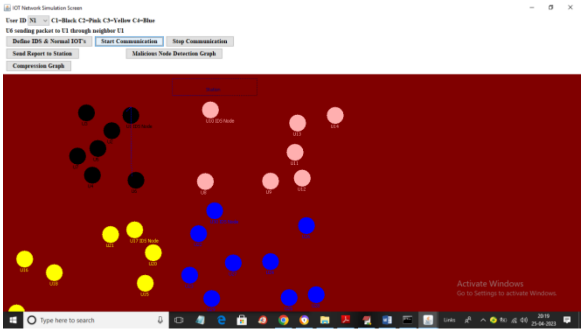
IOT Network Simulation Screen

User ID N1 C1=Black C2=Pink C3=Yellow C4=Blue

Status:

Define IDS & Normal IOT's | Start Communication | Stop Communication | Send Report to Station | Malicious Node Detection Graph | Compression Graph

Fig.5: Define IDS & normal IOTs



IOT Network Simulation Screen

User ID N1 C1=Black C2=Pink C3=Yellow C4=Blue

U6 sending packet to U1 through neighbor U1

Define IDS & Normal IOT's | Start Communication | Stop Communication | Send Report to Station | Malicious Node Detection Graph | Compression Graph

Fig.6: Start communication

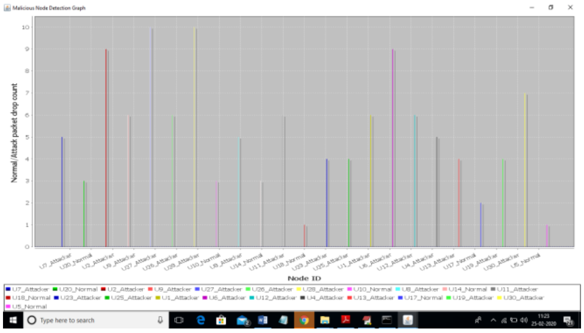
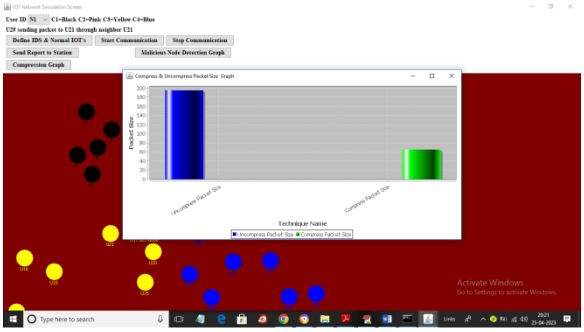


Fig.7: Malicious node detection graph



User ID N1 C1=Black C2=Pink C3=Yellow C4=Blue

U29 sending packet to U21 through neighbor U21

Fig.8: Compression graph

6. Conclusion

This article highlights the increasing threat of DDoS attacks in IoT networks and the potential harm they can cause to security and performance. It emphasizes the need for effective security techniques and proposes a prevention scheme suitable for vulnerable IoT networks. The proposed algorithm is based on existing IDS structures and functions, providing adaptability and adjustability to meet various security needs. It includes a simultaneously updatable blacklist table and can generate recommendations for reaction modules to ensure network performance, security, and survivability during attacks. Additionally, packet compression is employed to reduce packet size, enabling faster transmission and enhancing network lifetime.

7. Reference

1. G. Fortino, A. Guerrieri, C. Savaglio, and W. Russo, “Integration of Agent-based and Cloud Computing for the Smart Objects-oriented IoT,” researchgate, 2014.
2. Ahamad Ahanger, Tariq. (2018). Defense Scheme to Protect IoT from Cyber Attacks using AI Principles. International Journal of Computers Communications & Control. 13. 915-926. 10.15837/ijccc.2018.6.3356.
3. Umbarkar, A. M., Sherie, N. P., Agrawal, S. A., Kharche, P. P., & Dhabliya, D. (2021). Robust design of optimal location analysis for piezoelectric sensor in a cantilever beam. Materials Today: Proceedings, doi:10.1016/j.matpr.2020.12.1058
4. Vadivu, N. S., Gupta, G., Naveed, Q. N., Rasheed, T., Singh, S. K., & Dhabliya, D. (2022). Correlation-based mutual information model for analysis of lung cancer CT image. BioMed Research International, 2022, 6451770. doi:10.1155/2022/6451770
5. Veeraiah, D., Mohanty, R., Kundu, S., Dhabliya, D., Tiwari, M., Jamal, S. S., & Halifa, A. (2022). Detection of malicious cloud bandwidth consumption in cloud computing using machine learning techniques. Computational Intelligence and Neuroscience, 2022 doi:10.1155/2022/4003403
6. Veeraiah, V., Anand, R., Mishra, K. N., Dhabliya, D., Ajagekar, S. S., & Kanse, R. (2022). Investigating scope of energy efficient routing in adhoc network. Paper presented at the PDGC 2022 - 2022 7th International Conference on Parallel, Distributed and Grid Computing, 681-686. doi:10.1109/PDGC56933.2022.10053344 Retrieved from www.scopus.com
7. Kouicem, D. E., Bouabdallah, A., & Challal, Y. (2016). Security in the Internet of Things: A review. Computers & Security, 56, 1-27.

8. K. Rose, S. Eldridge, and L. Chapin, “THE INTERNET OF THINGS: AN OVERVIEW, Understanding the Issues and Challenges of a More Connected World,” 2015.
9. R. H. Weber, “Internet of Things – New security and privacy challenges,” Comput. law Secur. Rev., vol. 26, pp. 23–30, 2010.
10. L. Catarinucci et al., “An IoT-Aware Architecture for Smart Healthcare Systems,” IEEE, 2015.
11. IEEE, “Towards a definition of the Internet of Things (IoT),” 2015.
12. J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and Privacy for Cloud-Based IoT: Challenges,” IEEE Commun. Mag., vol. 55, no. 1, pp. 26–33, Jan. 2017.
13. NISTIR 8259: "IoT Device Cybersecurity Capability Core Baseline"
14. H. Lin and N. W. Bergmann, “IoT Privacy and Security Challenges for Smart Home Environments,” MDPI, 2016.
15. R. Petrolo, V. Loscri, and N. Mitton, “Towards a Smart City based on Cloud of Things,” Int. ACM MobiHoc Work. Wirel. Mob. Technol. Smart Cities, 2014.
16. Syed Shehriyar Ali, Mohammed Sarfaraz Shaikh, Syed Safi Uddin, Dr. Mohammed Abdul Bari, “Saas Product Comparison and Reviews Using Nlp”, Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022.
17. Hafsa Fatima, Shayesta Nazneen, Maryam Banu, Dr. Mohammed Abdul Bar,” Tensorflow-Based Automatic Personality Recognition Used in Asynchronous Video Interviews”, Journal of Engineering Science (JES), ISSN NO:0377-9254, Vol 13, Issue 05, MAY/2022.
18. Mohammed Shoeb, Mohammed Akram Ali, Mohammed Shadeel, Dr. Mohammed Abdul Bari, “Self-Driving Car: Using Opencv2 and Machine Learning”, The International journal of analytical and experimental modal analysis (IJAEMA), ISSN NO: 0886-9367, Volume XIV, Issue V, May/2022.
19. Mr. Pathan Ahmed Khan, Dr. M.A Bari,: Impact Of Emergence With Robotics At Educational Institution And Emerging Challenges”, International Journal of Multidisciplinary Engineering in Current Research(IJMEC), ISSN: 2456-4265, Volume 6, Issue 12, December 2021,Page 43-46.
20. Mohammed Abdul Bari, Shahanawaj Ahamad, Mohammed Rahmat Ali,” Smartphone Security and Protection Practices”, International Journal of Engineering and Applied Computer Science (IJEACS) ; ISBN: 9798799755577 Volume: 03, Issue: 01, December 2021.
21. Ijteba Sultana, Mohd Abdul Bari and Sanjay,” Impact of Intermediate Bottleneck Nodes on the QoS Provision in Wireless Infrastructure less Networks”, Journal of Physics: Conference Series, Conf. Ser. 1998 012029 , CONSILIO Aug 2021.
22. M.A.Bari & Shahanawaj Ahamad, “Code Cloning: The Analysis, Detection and Removal”, in International Journal of Computer Applications(IJCA),ISSN:0975-887, ISBN:978-93-80749-18-3,Vol:20,No:7,pp:34-38,NewYork,U.S.A.,April 2011.
23. Dr. M.A.Bari, ”Effective IDS To Mitigate The Packet Dropping Nodes From Manet “, JACE, Vol -6,Issue -6,June 2019.
24. Sun, Y., Zhang, Y., Wang, X., & Gui, C. (2020). A survey of anomaly detection in Internet of Things. Future Generation Computer Systems, 108, 820-832.