INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 5 - V8I5-1160)
Available online at: https://www.ijariit.com

DDoS Detection in Internet of Medical Things Approaches: Review

Reena Devi
sparky.fragy66@gmail.com
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

Avni Sharma
avnisharma910@gmail.com
Himachal Pradesh Technical University, Hamirpur, Himachal Pradesh

ABSTRACT

Health is a primary concern for every individual and to make it better all the resources should be available on one's hand. To make it practical manual supervision of healthcare tradition must be evaded. As various conventional healthcare practice, manual supervision in patient diagnosis, generating bills and maintains all medicine stock records, patient past records manually. Manual supervision of healthcare results to human error and the whole healthcare process becomes lengthy. To overcome these problems, a smart healthcare system enabled with Internet of Things (IoT) comes into sight, which lowers human error risk and also helps physician to diagnose the disease more effectively.

Keywords— *IoT, Medical, sensors, optimization*

1. INTRODUCTION

The collection of all medical devices and applications which is connected to a healthcare network and allows machine-to-machine (M2M) communication without any human interference is named as Internet of Medical Things (IoMT). IoMT system facilitates remote monitoring of patient, tracking patient medication and location of patient. With patient wearable medical devices, the information received by the healthcare providers, timely diagnosis of patient lowers the risk of patient's life during emergency. At the moment many healthcare providers started exploring IoMT, which provides ease to both patients and physicians in terms of patient record management, real time monitoring, early indication during emergency etc. In recent years, the growth of IoMT has been observed unmatched and seen providing room for development of many medical devices, which includes wearable sensors, implantable sensors, ambient sensors and stationary sensors [4] that aids healthcare providers to gather patient's information and also monitor.

These medical devices used very lightweight protocol for information transmission, such as CoAP [5] and gather data as shown in Figure 1.1 to transmit critical data to nearby sensors or gateways. While the data transmission is carried out through these sensors, the security and privacy of the sensors are crucial as the data collected by these sensors are patient's critical information and the data transferred are in bulk which raises new challenges to data security and privacy in IoMT. Any unauthorized access or leakage triggers patient's life at risk [6].

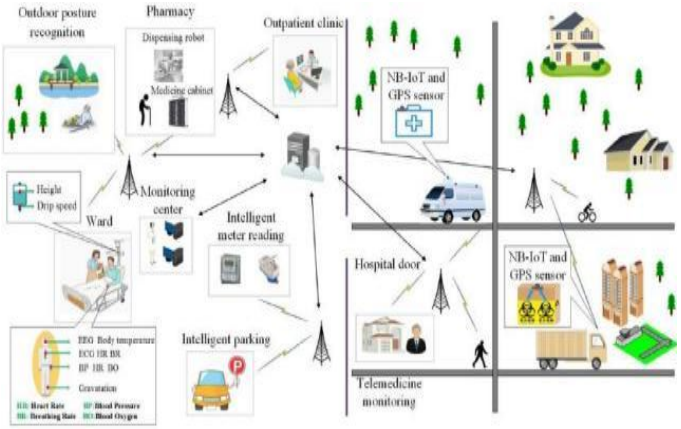

Figure 1.1: Smart Hospital Scenario

2. ARCHITECTURE OF INTERNET OF MEDICAL THINGS

An IoMT platform comprises of many interconnected sensors and electrical circuits which obtains biomedical signals from patient's body. A processing unit to process the signals gather from the medical devices, and a network layer device like gateway which transmits the information over the network. And to store those critical data, a volatile or non-volatile storage entity is employed and a presentation platform for physicians to take decision accordingly. The architecture of IoMT is displayed in Figure 1.2 below.

To compile the architecture of IoMT in a simple way, it consists of 3 main layers that are Things Layer, Intermediate Layer and Back-end Computing Layer [7].

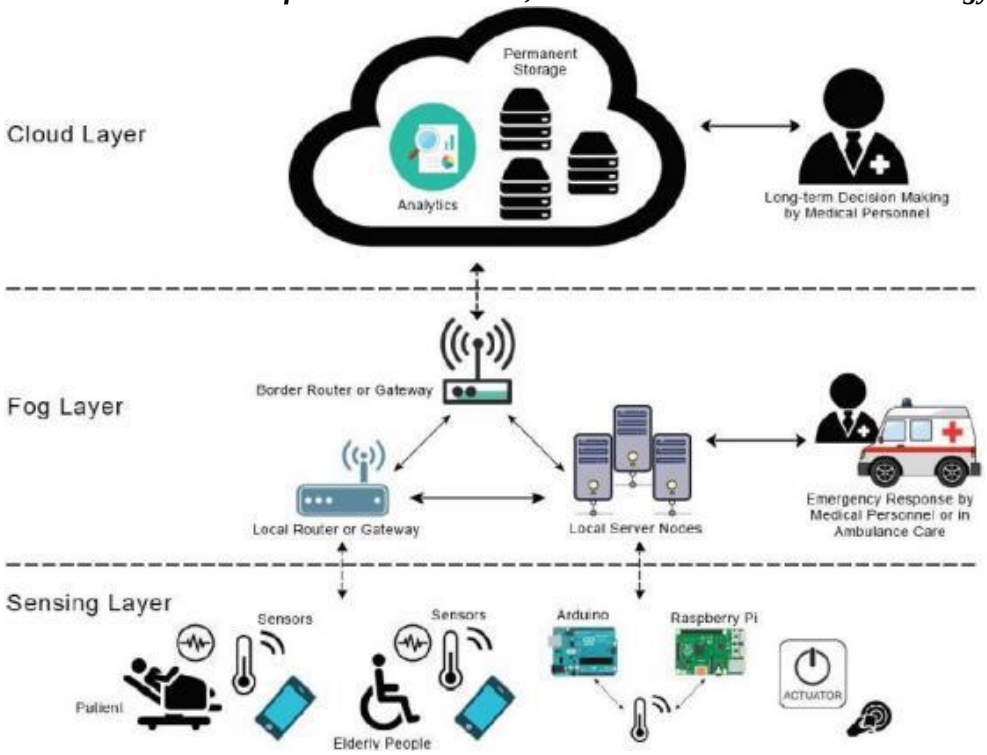

Figure 1.2: Architecture of Internet of Medical Things (IoMT) [8]

The three major layers of IoMT architecture is elaborated more below:

(a) Things Layer

This layer comprises with all the physical devices in IoMT such as pulse sensors, asthma monitoring sensors and other implantable sensors. All these medical devices communicate through their respective RFID and EPC coding. The sensors in things layer collect the data and communicate to the nearby Gateways which works in intermediate layer.

(b) Intermediate Layer

In intermediate layer the gateways are associated and is supposed to handle the bulk data coming from heterogeneous devices. Communication protocols like Bluetooth, Wi-Fi are used to connect with wide range of medical devices. The processing of bulk data and implementation of other technologies like fog computing are done in this layer. After processing, data are transferred to main server.

(c) Back-end Computing Layer

It is the server's role to collect data from the gateways, store huge amounts of data, and process it through many applications in order to control the healthcare system. Seeing massive data, high-performance computing, and Big Data analytics play a key part in this layer.

For past few years, DDoS attack prevention in Internet of Things (IoT) is one of significant challenge and is less addressed compared to other security issues. But then, many critical sectors like healthcare includes IoT for advancement of their services, it appealed research interest world-wide. In DDoS attack once the device gets infected, then it will start mutating throughout the network and for a service providers like healthcare sector it is leaving once life at stake. It is already known from literature review that there are many approaches to counter DdoS like statistical approach, machine learning approach etc.

In this chapter, we will discuss about the previous work done for detection of DDoS attack based on statistical approach and machine learning approach.

3. DDoS ATTACK DETECTION USING STATISTICAL APPROACH

Da Yin and Kun Yang [14] proposed an algorithm which compares the packet-in rate of real time traffic with the threshold value of cosine similarity of the vectors of packet-in rate at the ports. If any anomaly or inconsistency is detected from the packet-in rates, then it blocks source.

Seyed Mohammad and Marc St. Hilaire [15] proposed a method which is based on comparing entropy of repeated packet from the traffic which results in classifying the variations in their randomness. A threshold value is calculated to compare with the entropy of the traffic. The entropy is estimated based on the destination IP address of a window of 50 packets each and if the entropy is less than the threshold, the device is considered to be compromised and it is reported.

Surender Singh and Sandeep Jain [16] proposed a distributed framework, to analyse the behaviour of the packets in traffic. To distinguish between the malicious traffic and legitimate traffic from network traffic, this method uses traceback algorithm and entropy.

Mohan Dhawan et al. [17] proposed a SPHINX framework which detects DDoS attack in SDN with less perfomance overheads. This framework spots both known and potential attacks on network. This is based on approximation of real time network traffic into a flow graph to detect threats in a network traffic.

Haopei Wang et al. [18] proposed a Flood Guard system which focuses on a SDN attacks. It has two modules proactive flow rule analyzer, which maintians network policy enforcement, and packet migration, which prevents the controller from becoming overloaded.

Yair Meidan et al. [19] used deep auto encoders for each

device, and proposed a model which is trained on a feature extracted from benign and junk traffic data and also captures the behavior snapshots. Once the model is trained, it is encapsulated into auto encoders. When the fresh data is employed on an IoT device, auto encoders extract the features from the network traffic and tries to reconstruct the snapshots. When the auto encoder fails to reconstruct, then it will tag as unusual anomalies which indicate that the device is compromised.

Keisuke Kato and Vitaly Klyuev [20] proposed an intelligent DDoS attack detection system with Support Vector Machine. In this system SVM with a Radio Basis Function (RBF) is used and the dataset is collected from CAIDA for DDoS attack 2007, experiments and results are done with this dataset.

Lingfeng Yang and Hui Zhao [21] proposed a SDN based framework to counter DDoS attack using machine learning. The framework is divided into three modules, that is traffic collection module, identification module and flow table delivery module. The traffic collection module extracts the features and prepares traffic identification to update in flow table. With the help of controller in SDN, the features are extracted from flow table and employed to Support Vector Machine (SVM) classifier to detect the attack. The dataset is collected from KDD99 and all experiment is conducted using KDD99 dataset.

Saurav Nanda et al. [22] proposed a machine learning algorithm to identify the potential malicious connection and in addition the algorithm also discovers the attack destinations using historical network attack data. The paper proposed four machine learning algorithms: C4.5, Bayesian Network (BayesNet), Decision Table (DT) and Naïve-Bayes to predict the destination that can be attacked. The accuracy of the algorithms are compared and concluded that Bayesian network attained highest accuracy of 91.68%.

Alpna and Sona Malhotra [23] uses Random Forest (RF) to detect the DDoS attack and the results of RF is compared with K-nearest neighbor (KNN) algorithm. The experiment was conducted through UCLA dataset. The packets in network flow is only TCP packets and 20 packets are collected per seconds. Features like packet size, no. of packets, time interval etc. are considered for DDoS attack detection. For packet classification packet is tagged as 'non attack' and 'attack' based on the comparison of packets features with the threshold. The experiment declares that RF has more accuracy then KNN with less error.

4. CONCLUSION

IoMT in Healthcare System facilitates many exclusive services to both patients and physicians through patient record management, real-time monitoring, fast response during emergencies situation etc. There is another advancement in IoMT in terms of body sensors which captures patient's medical data and transmits data through gateways to the main server. However, there are enormous heterogeneous medical devices connected in IoMT through internet and the critical data transferred are massive in volume which raises new security challenges in IoMT.

According to a review paper report [4], DDoS attack is the most dominant attack in IoT Healthcare System which takes advantage of insure devices and gets infected by a malware. DDoS attack attempts to disrupt normal traffic of the network by utilizing the compromised device and can shut down the server by flooding internet traffic. Considering, IoMT Healthcare System

REFERENCES

[1] S. Vishnu, S.R Jino Ramson and R. Jegan, "Internet of Medical Things (IoMT) - An overview, 2020 5th International Conference on Devices," in *Circuits and Systems (ICDCS)*, 2020.

[2] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, and S. Guizani, "Internet-of- Things-Based Smart Cities: Recent Advances and Challenges," *IEEE Communications Magazine*, vol. 55, pp. 16-24, 2017.

[3] A. S. El-Wakeel, J. Li, A. Noureldin, H. S. Hassanein, and N. Zorba, "Towards a Practical Crowdsensing System for Road Surface Conditions Monitoring," *IEEE Internet of Things Journal*, vol. 5, p. 4672–4685, 2018.

[4] Nipuni Nanayakkara, Malka N. Halgamuge and Ali Syed, "Security and Privacy of Internet of Medical Things (IoMT) Based Healthcare Applications: A Review," in *International Conference on Advances in Business Management and Information Technology, Research Gate*, 2019.

[5] K. Ngo Manh, S. Saguna, M. Karan and A. Christer, "IReHMo: An efficient IoT-based remote health monitoring system for smart regions," in *2015 17th International Conference on E-health Networking, Application & Services (HealthCom), IEEE*, Boston, 2015.

[6] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE Sensors Journal*, vol. 16, pp. 1368-1376, 2016.

[7] Mohammed Irfan, Naim Ahmad, "Internet of Medical Things: Architectural Model, Motivational Factors and Impediments," in *2018 15th Learning and Technology Conference (L&T) IEEE*, 2018.

[8] Vankamamidi S. Naresh, Suryateja S. Pericherla, Pilla Sita Rama Murty and Sivaranjani Reddi, "Internet of Things in Healthcare: Architecture, Applications, Challenges and Solutions," *Computer Syst Sci & Eng*, vol. 6, pp. 411-421, 2020.

[9] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "Ube-Health: A Personalized Ubiquitous Cloud and Edge-Enabled Networked Healthcare System for Smart Cities," *IEEE Access*, vol. 6, p. 32258–32285, 2018.

[10] Bahar Farahani, Farshad Firouzi, Victor Chang, Mustafa Badaroglu, Nicholas Constant, Kunal Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Future Generation Computer Systems*, vol. 78, p. 659–676, 2018.

[11] Hilaire, Seyed Mohammad Mousavi and Marc St., "Early Detection of DDoS Attacks against SDN Controllers," in *International Conference on Computing, Networking and Communications, Communications and Information Security Symposium*, 2015.

[12] V. Matta, M. D. Mauro and M. Longo, "DDoS attacks with randomized traffic innovation: botnet identification challenges and strategies," *IEEE Transactions on Information Forensics and Security*, vol. 2017, pp. 1844-1859, 2017.

[13] T. Booth and K. Andersson, "Network Security of Internet Services: Eliminate DDoS Reflection Amplification Attacks," *Journal of Internet Services and*

Information Security (JISIS), vol. 5, pp. 58-79, 2015.

[14] Da Yin, Lianming Zhang and Kun Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," *IEEE Access*, 2018.

[15] Seyed Mohammad Mousavi and Marc St. Hilaire, "Early Detection of DDoS Attacks against SDN Controllers," in *International Conference on Computing, Networking and Communications, Communications and Information Security Symposium*, 2015.

[16] Jain, Surender Singh and Sandeep, "A Review of Detection of DDoS Attack Using EntropyBased Approach," in *IJCST*, 2013.

[17] Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan and Vijay Mann, "SPHINX: Detecting Security Attacks in Software-Defined Networks," in *BM Research*, 2009.

[18] Haopei Wang, Lei Xu and Guofei Gu, "FloodGuard: A DoS Attack Prevention Extension in Software-Defined Networks," in *45th Annual IEEE/IFIP International Conferenceon Dependable Systems and Networks (DSN'15*, 2015.

[19] Yair Meidan, Michael Bohadana, Yael Mathov, Yisroel Mirsky. Dominik Breitenbacher, Asaf Shabtai, and Yuval Elovici, "N-BaIoT: Network-based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE PERVASIVE COMPUTING,* vol. 13, 2018.

[20] Keisuke Kato and Vitaly Klyuev, "An Intelligent DDoS attack Detection System Using Packet analysis and Support Vector Machine," *IJICR*, vol. 5, 2014.

[21] Zhao, Lingfeng Yang and Hui, "DDoS Attack Identification and Defense Using SDN Based on Machine Learning Method," *IEEE*, 2018.

[22] Saurav Nanda, Faheem Zafari, Casimer DeCusatis, Eric Wedaa and Baijian Yang, "Predicting Network Attack Patterns in SDN using Machine Learning Approach," *IEEE*, 2016.

[23] Alpna and Sona Malhotra, "DDoS Attack Detection and Prevention Using Ensemble Classifier (RF)," *IJARCSSE*, 2016.

