iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** VII **Month of publication:** July 2021

DOI: https://doi.org/10.22214/ijraset.2021.36520

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 9 Issue VII July 2021- Available at www.ijraset.com

Insider Attack Detection in IoT devices using Data Analytics

Rashmi A G[1], Parvathi D S[2], Samarth C J[3], Mahesh K P[4], Shruthi N M[5]
[1, 2, 3, 4]*Student,* [5]*Guide, Department of Computer Science and Engineering, JSS Science and Technology University*

Abstract: ***In the recent years, the rate of theft of money being carried to ATM machines is increasing day by day. Each vehicle carrying money should be monitored at all times through communication protocol and the vehicle should have a GPS installed. This location information should be very confidential and accessible only to the authorized officials. Due to the advancement in the technology, there are numerous ways in which the attacks are happening. One such attack is accessing the confidential information (i.e., the GPS location of the vehicle in this case) by unauthorized means from the people within the same network and using it for various purposes. It's become a challenge to overcome these attacks and deposit the amount to ATM machines safely. There are other scenarios viz. carrying the witnesses to the court, shipping important materials like medicines or official documents where the GPS information is being misused. Providing security against insider attacks is the need of the hour. This paper mainly focuses on the development of an end-to-end system which detects the unauthorized access to the confidential information and gives analysis of the time and frequency of attack using data analytics.***
Keywords: IoT gateway, Authorized and unauthorized user, IoT System, Client machine

I. INTRODUCTION

There has been a marked increase in the number of incidents reported on network attacks in the recent years, where the network of the vehicles which are carrying ATM amount, or any important official documents or even the witness which are being produced to the court will be trapped by the unauthorized means. There exist many scenarios where these vehicles are trapped and the important items are stolen. Understanding this scenario and developing an application to prevent this from happening is the main aim of this paper. Internet of Things was mentioned by Kevin Ashton for the first time in 1999 for representing supply chain management aspects to the public. The Internet of Things (IoT) is the network of physical devices, home appliances, vehicles and other items embedded with software, electronics, sensors and connectivity which enables these objects to connect and exchange data. Each component is uniquely identifiable through its embedded computing system and is able to inter-operate within the existing Internet infrastructure. Applications of IoT include healthcare, finances, utilities, traffic etc. IoT comes in different shapes and sizes, ranging from small sensors to global structure covering entire countries.

With the recent spread of the IoT, the number of network-connected devices are increasing dramatically. Since these devices are responsible for generating and handling large amounts of sensitive data, the security of the IoT devices always pose a challenge. It is observed that a security breach could affect individuals and eventually the world at large.On the other hand, Artificial Intelligence(AI) has found many applications and is widely being explored in providing security specifically for IoT devices. IoT consists of various network connected devices and when one of the connected devices is infiltrated by malware, it becomes the starting point for the spread of infiltration to other devices. This could threaten the critical infrastructure that should be protected. One of the biggest security challenges associated with IoT devices is the insider attack.

II. RESEARCH METHODOLOGY

At present there exists a system where the network of the vehicles can be easily hacked i.e., there is no existing solution(application) to our problem domain. Started the work by reviewing literature, browsing on Google Scholar and other related websites and found relevant research done on network security in general but not IoT system as a whole. Thus, developing a methodology and an application became the main aim.

To overcome the problems of the existing system, introduction of a high network security system to protect the network from being attacked is done. Here IoT system will be communicate with the GPS module. This IOT system will only deliver the data to the authorized user. In order to enhance the security, usage of IOT gate way is done. The users who need to use this application should register before them logging in, and also, request for the authorization. When the user sends the request, IOT gate way will forward the request to IoT System. IoT system will differentiate between authorized and unauthorized user. Based on that the approval and the access will be provided for the authorized user.

Here the information will be fetched form the IoT system. Before providing the authorization, network capturing will be done so that all the details of the system including Ip address, protocols, and system id will be detected. If the system is considered as authorized system, then the authority will be given, if not then it is considered as a request from the fake user, and it will be maintained in the log. At the time of request from the unauthorized user IoT system will send him fake data (random number instead of geographical location) and it will be maintained in the log. This will help in order to identify the person who is trying to fetch data from the IoT system. Attacks are grouped by their types and maintained in a log which will be useful for further investigation in the Analytics module.

III.THEORY AND IMPLEMENTATION

There are 4 modules in the proposed system: Client module, IoT Gateway module, IoT system module and the Analytics module.

A. Client-side view

The system is designed in such a way that the clients are not aware of the pre-processing happening in the system. For the clients, it appears as if it is directly connected to the IOT environment rather than the IoT gateway. Hence abstraction is achieved.

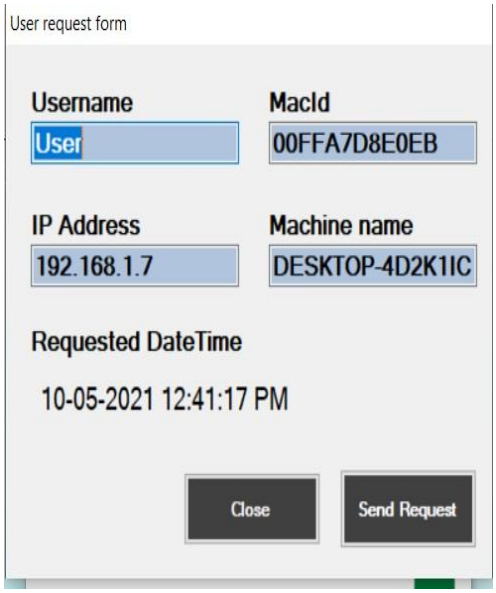


Figure 1: Client sending authorization request

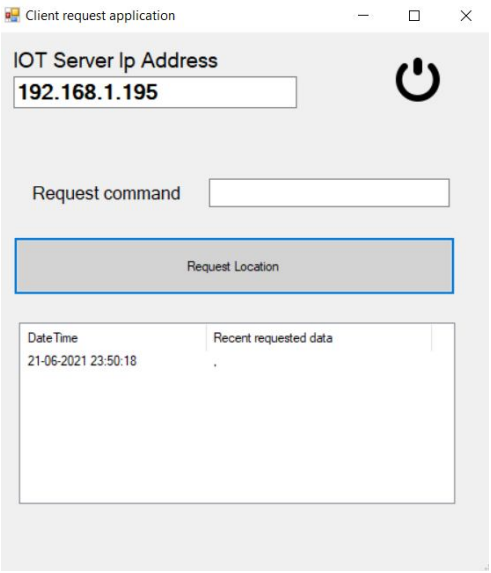


Figure 2: Client requesting GPS location

B. IoT Gateway

The first function here is capturing the packets. When 'n' number of clients sends requests, the gateway should be in a position to capture all the packets. The packets are captured and the information is kept in byte array called raw.

The second function is analysing of packets. The array is then analysed byte by byte in order to retrieve information such as version of the Ip packet, header length, time to live, source port address, destination port address etc.,

The next function is consistency classification. This function generates a classification which is an Ip v/s type of sensor matrix. It gives information regarding which Ip has requested for accessing GPS location with request command.

The fourth function is to identify the IOT request and maintain a log which contains information such as Ip address, requested timestamp, physical address, source and destination port, protocol, username, request command and the expected command. This log will be used in Machine learning module for analysing and identifying the internal attack. Then the request will be forwarded to the IOT server.

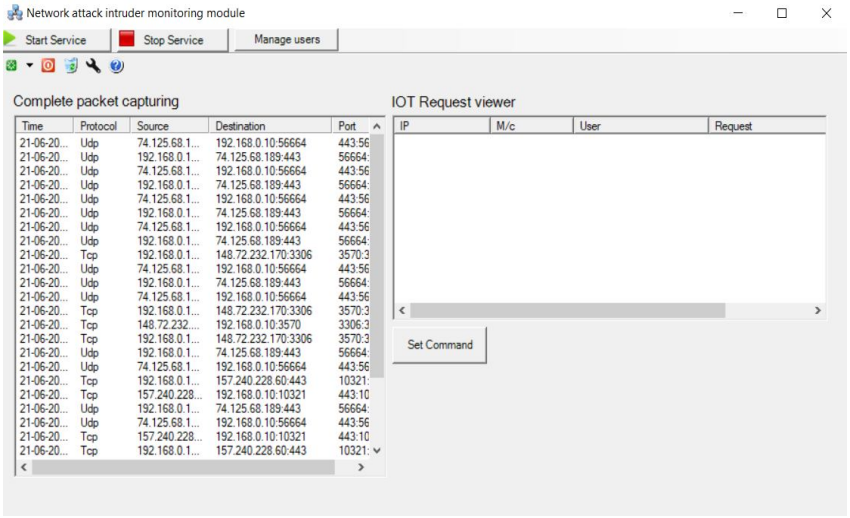


Figure 3: List of all the services running on a particular IP in IoT gateway

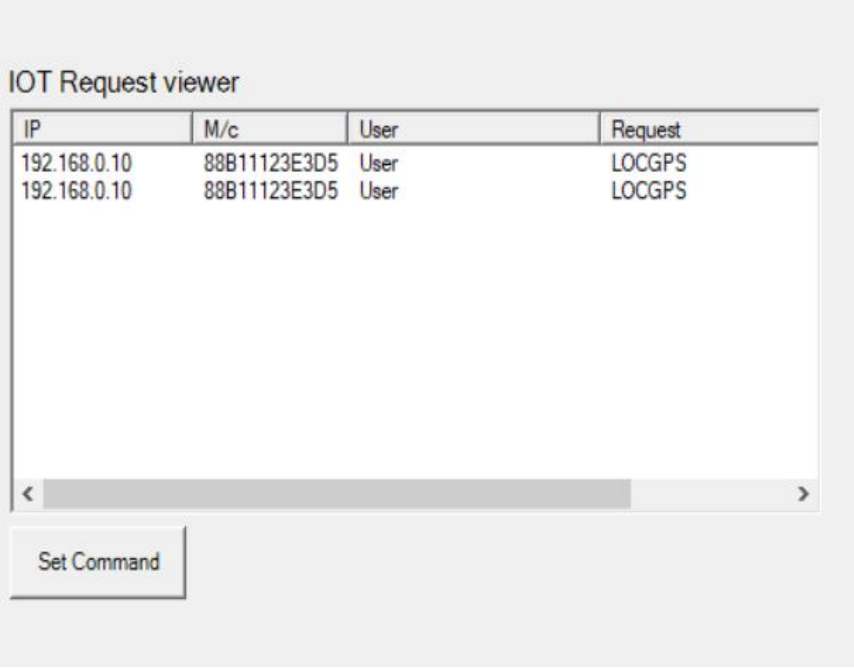


Figure 4: List of Clients requesting GPS location

C. IoT System

The IoT system consists of hardware (GPS module, Arduino UNO) connected to the system and the User Interface.

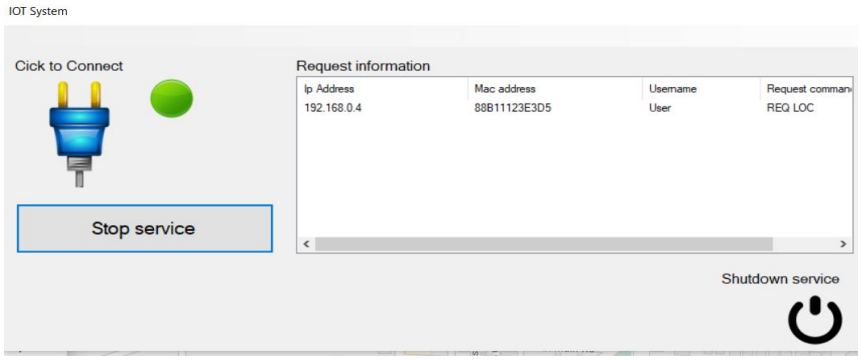


Figure 5: The IoT system UI, connected to the hardware

IV. RESULTS AND DISCUSSIONS

The generated data is analysed using the Analytics module and the results are obtained. Insider attack analysis is a module to find intruder machine based on various groups and summarizing them from the log created through the IoT gateway. Alternately IDS can be classified into two methodologies: Anomaly detection and misuse (signature-based) detection. In Anomaly detection, user behaviour profile is created and, if some difference occurs in style of execution of user i.e., consuming more bandwidth, more resources, key stroking speed etc, this deviation from normal behaviour is observed and the user or system is considered as an intruder. In order to find the attacker, this module uses LINQ (Language integrated query) which works on dataset collected from the log file and groups it based on the timestamp, count of request and load from the same IP address machine whose count is more than certain threshold and can be classified as machines which impact server performance

Our approach of post-Attack intrusion detection is an Anomaly, learning-based, host-based intrusion detection model depending on the number of requests received from authorized and unauthorized machines. The theory behind it is, the attack takes the form of an abnormal sequence of IoT request to access GPS data. In our assumption the attacker has bypassed the online intrusion detection system without process of registration, if any and there is a set of logs, where activities of the intrusion have been recorded by sending too many requests from unauthorized machine to impact internal server performance, which is traced by IoT gateway from the packets captured. We developed a method that is capable of pinpointing in one such log where the execution of an exploit should exist. Our Analytics model generated o/p is a successful post-attack intrusion detection system to generate IP list, Identify Authenticated and Unauthenticated client list.

Signature-based IDS may detect an attack/intrusion if the attack's signature is already stored in the internal command settings by IoT Gateway admin. These systems can detect known attacks very accurately by identifying user sending invalid commands and trying to build communication with trial and error by invoking different IoT commands to get data or build communication bridge.

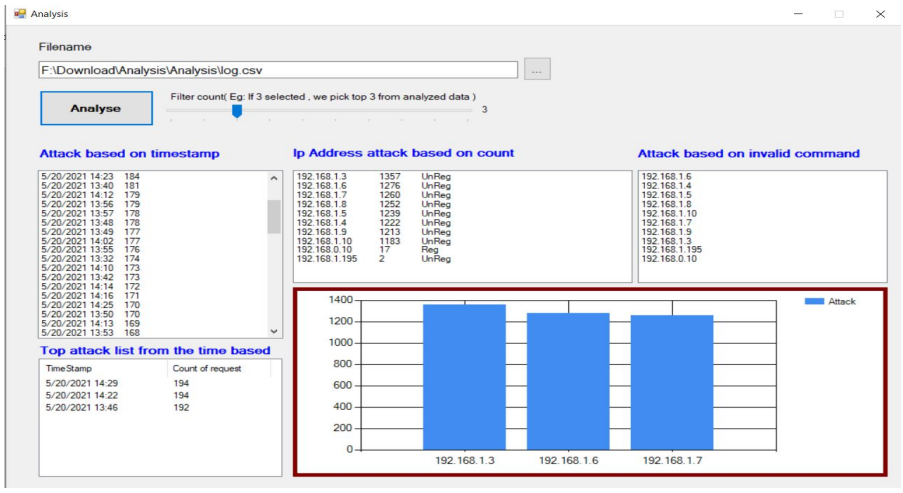


Figure 6: Analysis based on parameters like timestamp, Ip address and invalid command

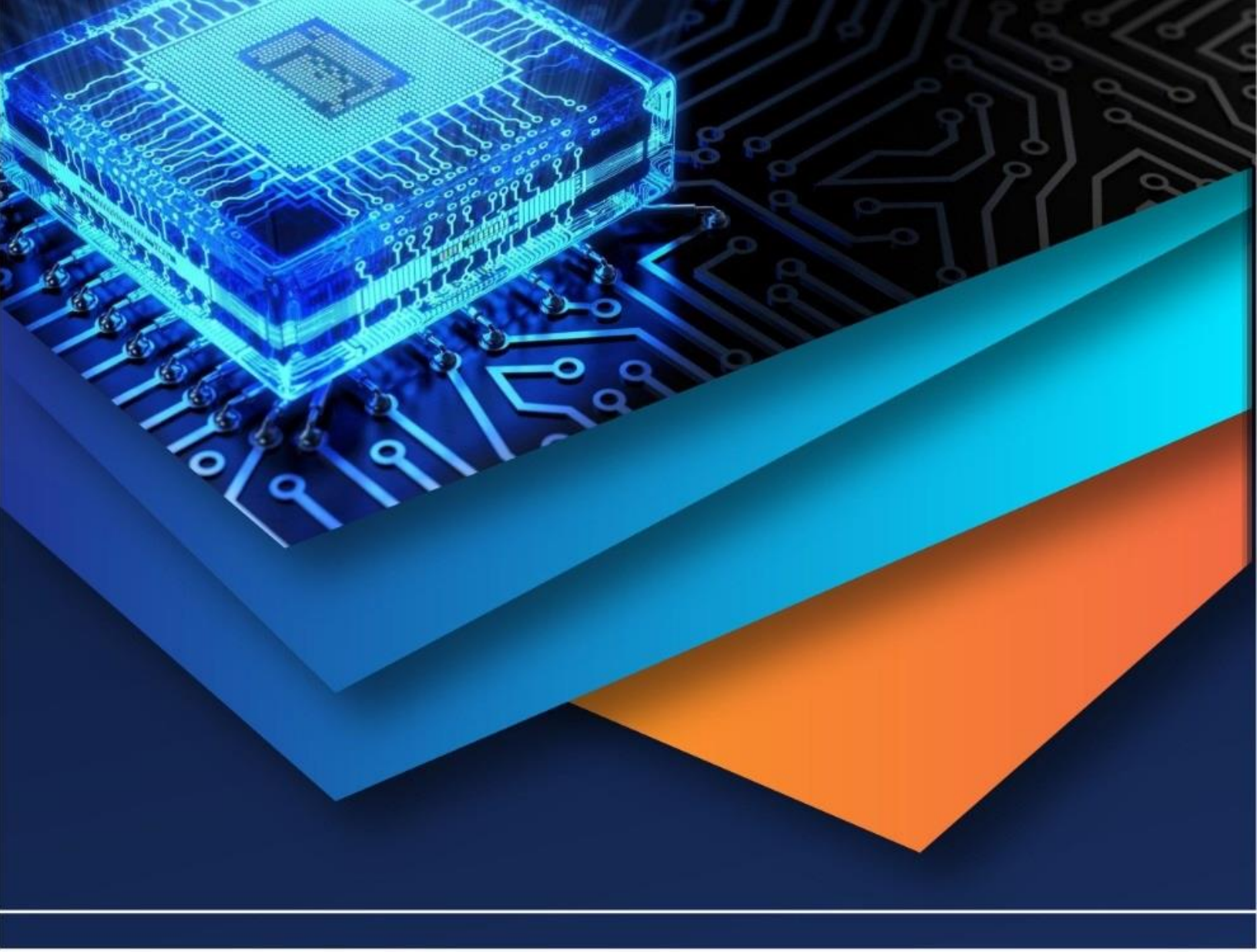
V. CONCLUSION AND FUTURE WORK

The application developed acts as a security barrier for the unauthorized actors who are trying to fetch the network data, with the help of IoT gateway. Hence, the network of the vehicle which will be carrying ATM money will not be trapped. Load balancing is an important technique for improving IoT environment performance by considering the group of sensors in the system to share their workloads. This results in a better utilization of sensors resources, a high system throughput and quick response time of user requests. In load sharing, the incoming client requests are evenly distributed among the participating sensors. The load on an overloaded host is transferred to an under loaded host to enhance the system throughput. Effective load balancing among the group of sensors in an IoT environment relies on accurate knowledge of the state of the individual host. This knowledge is used to judiciously assign incoming computational tasks to appropriate sensors, by using specific load distribution policies so that the requests can be processed quickly. This is achieved by allowing the sensors cooperatively monitor the global system load and distribute/re-distribute the load according to the load sharing algorithms which can be static or dynamic and can have either centralized or distributed control.

For future enhancements, instead of dropping the packets sensors can be added dynamically and forward the request packets to this new sensor thereby no packets are lost. Next level security can be introduced by giving login credentials to Admin (IoT Gateway device like system id, user id and password for login) and also encrypt this data using advanced encryption algorithms and store it in database for effective login and verification purposes. Can include parallel processing as well.

REFERENCES

[1] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997. [1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future Generation Computer Systems, vol. 29, issue 7, 2013, pp. 1645–1660.
[2] “Wearable Sensors for Human Activity Monitoring: A Review” Subhas Chandra Mukhopadhyay Publication Year: 2015, Page(s):1321 – 1330.
[3] “Sensor and different types” by Margaret Rouse, updated in July 2012.
[4] “Analysis of types and importance of sensors in smart home services” published in IEEE international conference on smart city 12- 14th December, 2016.
[5] “Malicious Insider attack detection in IoTs using Data Analytics”, published in IEEE Xplore in December 2019.
[6] “Privacy and authentication in the Internet of Things” published in march 2015, sourced from Manfred Kube, Gemalto.
[7] “Proposal of a secure, deployable and transparent middleware for Internet of things”, published in Information system and technology, 2014 9th Iberian Conference on 21 June 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY