

**AMRITA VISHWA VIDYAPEETHAM**  
**AMRITA SCHOOL OF ENGINEERING, COIMBATORE, 641112**



**BONAFIDE CERTIFICATE**

This is to certify that the project report entitled “**Enhancing Security of Bolt beats**” submitted by AKSHAY K (CB.EN.U4CSE15002), ARVIND. P. JAYAN (CB.EN.U4CSE15007) and GADKARI SHREYA SUNIL (CB.EN.U4CSE15115) in partial fulfillment of the requirements for the award of the **Degree of Bachelor of Technology in Computer Science and Engineering** is a bonafide record of the work carried out under our guidance and supervision at Amrita School of Engineering.

**PROJECT GUIDE**

Dr. N Harini  
Assistant Professor

**PANEL INCHARGE**

Ms. Vidya S  
Assistant Professor

Department of Computer Science and Engineering

**CHAIRPERSON**

Dr. Latha Parameswaran  
Dept. of Computer Science and Engg.

This project report was evaluated by us on : .....

INTERNAL EXAMINER

EXTERNAL EXAMINER

## ACKNOWLEDGEMENT

We would like to express our deep gratitude to our beloved **Satguru Sri Mata Amritanandamayi Devi** for providing the bright academic climate at this university, which has made this entire task appreciable. This acknowledgement is intended to be a thanks giving measure to all those people involved directly or indirectly with our project. We would like to thank our Vice Chancellor **Dr. Venkat Rangan. P** and Dr **Sasangan Ramanathan** Dean Engineering of Amrita Vishwa Vidyapeetham for providing us the necessary infrastructure required for the completion of the project.

We express our thanks to **Dr.Latha Parameswaran**, Chairperson of Department of Computer Science Engineering, Dr. P Bagavathy Sivakumar and Prof. Prashant R Nair, Vice Chairpersons of the Department of Computer Science and Engineering for their valuable help and support during our study. We express our gratitude to our guides, **/Internal Guide Name, External Guide Name/**, for his/her guidance, support and supervision.

We feel extremely grateful to **/Panel Mambbers/** for their feedback and encouragement which helped us to complete the project. We would like to thank **/Panel Incharge/** for scheduling and organising periodic reviews during the course of our project. We also thank the entire staff of the Department of Computer Science Engineering.

We would like to extend our sincere thanks to our family and friends for helping and motivating us during the course of the project. Finally, we would like to thank all those who have helped, guided and encouraged us directly or indirectly during the project work. Last but not the least, we thank **God** for His blessings which made our project a success.

## **ABSTRACT**

Today there are thousands of IoT based wearable devices available in the market. Most wearables collect data and send this data to a connected device mostly a smartphone over Bluetooth. The smartphone then collects all this data and may do a preliminary analysis for immediately warning the user for abnormalities in the readings. Apart from this the smartphone also sends all this collected data to the users doctor so that he can keep track of this patients vitals on the long run. However the feature for sending data to the doctor may be accessible to only users in major cities where their hospitals have the added facilities to collect, consolidate and maintain all this data. This work proposes a solution to enhance the security of the data collected during transmission on Wi-Fi and Bluetooth networks.

# LIST OF FIGURES

<b>Figure Number</b>	<b>Figure Caption</b>	<b>Page Number</b>
4.1	Proposed Architecture Diagram PHASE 1	10
4.2	Proposed Architecture Diagram PHASE 2	12
5.1	Data extracted found to be in plain text	14
5.2	Wi-Fi Pineapple – Evil Twin Attack	15
5.3	Wi-Fi Pineapple device	15
5.4	Compromised device configurations	16
5.5	Data Packets monitored	16

# LIST OF TABLES

Table Number	Table Caption	Page Number
1.1	Different IoT wearable configurations	2

## LIST OF ABBREVIATIONS

SNO	Abbreviations	Meaning
1	IoT	Internet of Things
2	RFID	Radio Frequency Identification
3	WT	Wearable Technology
4	XSS	Cross Site Scripting
5	NFC	Near Field Communication
6	Wi-Fi	Wireless Fidelity
7	WAP	Wireless Access Point
8	AP	Access Point
9	WEP	Wired Equivalent Privacy
10	WPA	Wi-Fi Protected Access
11	MITM	Man In The Middle
12	RSSI	Received Signal Strength Indication
13	SSID	Service Set Identifier
14	API	Application Programmer Interface
15	App	Application

# TABLE OF CONTENTS

CHAPTER	TITLE	PAGE NO
	<b>ABSTRACT</b>	<b>i</b>
	<b>LIST OF FIGURES</b>	<b>ii</b>
	<b>LIST OF TABLES</b>	<b>iii</b>
	<b>LIST OF ABBREVIATIONS</b>	<b>iv</b>
<b>1.</b>	<b>INTRODUCTION</b>	<b>01</b>
	1.1 Background	01
	1.2 Problem statement	01
	1.3 Purpose of Study	01
	1.4 Specific Objective	02
	1.5 Scope and Importance of Study	02
	1.6 Limitations	02
<b>2.</b>	<b>LITERATURE SURVEY</b>	<b>03</b>
	2.1 IoT Devices	03
	2.2 Issues in IoT	03
	2.3 Rogue Access Point	05
	2.4 IoT Security	07
	2.5 Bolt Health and Fitness Application	07
<b>3.</b>	<b>SYSTEM SPECIFICATIONS</b>	<b>09</b>
<b>4.</b>	<b>PROPOSED SCHEME – ARCHITECTURE</b>	<b>10</b>
<b>5.</b>	<b>PRELIMINARY RESULTS</b>	<b>14</b>
<b>6.</b>	<b>CONCLUSION</b>	<b>17</b>
	<b>REFERENCES / BIBLIOGRAPHY</b>	<b>18</b>

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 Background**

Today there are thousands of IoT based wearable devices available in the market. Most wearables collect data and send this data to a connected device mostly a smartphone over Bluetooth. The smartphone then collects all this data and may do a preliminary analysis for immediately warning the user for abnormalities in the readings. Apart from this the smartphone also sends all this collected data to the users doctor so that he can keep track of this patients vitals on the long run. However the feature for sending data to the doctor may be accessible to only users in major cities where their hospitals have the added facilities to collect, consolidate and maintain all this data. The leak of such important data can lead to the misuse of personal data. Moreover the adversary could modify the data that is being sent. This can lead to the doctors misinterpreting important sensitive data.

### **1.2 Problem Statement**

The work intends to test the data security of the IoT system since extremely sensitive data is being sent. Vulnerabilities that can lead to the leak of this personal data is found. This project illustrates a process for identifying a vulnerability and proposes a solution for mitigating the same.

### **1.3 Purpose of Study**

IoT wearable devices have revolutionised the way people monitor their biological parameters. People can monitor their vitals on the wrist of their hand without visiting the hospital for primary analysis. However this is not advisable for sophisticated and complex measuring. Since such wearables are compact they do not contain the necessary storage for storing large amounts of data over a period of time. This problem is overcome by connecting the device to a smartphone and transferring the collected data to it which is then later sent to the hospital over the Internet. This leads to compromise of the security of the data being sent and it being subject to attacks.



Sensitive data can be leaked due to such compromises. In industries such as the sports industry, companies invest huge amount of money in IoT wearables to continuously monitor the progress and the overall health of the athlete. Compromises in such scenarios can lead to huge losses in money.

## 1.4 Specific Objective

This project proposes to observe the working of *Boltt beat* and with a focus of finding existing security vulnerabilities in the system. The following observations were made:

- The device transmits data over Bluetooth
- Data was transmitted in plain text by the device.

## 1.5 Scope and Importance of the study

IoT devices that monitor the health parameters help users predict various information about their health conditions. In the sports industries this help to monitor and improve an athletes progress. A leak in such data would help the rival know more about their opponents and prepare better and put the athlete at a disadvantage. Moreover a modification in the data sent can put the user at a major risk with him being led to think his that he is in perfectly good health.

## 1.6 Limitations

The project is restricted to the use of Bolt Beat wearable. Implementing this on a larger scale would require getting to know the specifics of each wearable device such as:

SNO	DEVICE NAME	CONNECTIVITY	DATA
1	Boltt Beats 2.0	Bluetooth	Unencrypted
2	Apple Watch series 4	Bluetooth	Encrypted
3	Mi Band 3	Bluetooth	Unencrypted

Table 1.1 Different IoT wearable devices

## **Chapter 2**

### **Literature Survey**

#### **2.1 IoT devices:**

The Internet of Things (IoT) is regarded as a technology and economic wave in the global information industry after the Internet. The IoT is an intelligent network which connects all things to the Internet for exchanging information and communicating through the information sensing devices in accordance with agreed protocols. It achieves the goal of intelligent identifying, locating, tracking, monitoring, and managing things. It is an extension and expansion of Internet-based network, which expands the communication from human and human to human and things or things and things. In the IoT paradigm, many objects surrounding us will be connected into networks in one form or another. RF identification (RFID), sensor technology, and other smart technologies will be embedded into a variety of applications [1].

Wearable Technology (WT) or called as wearable is a computing technology device that can be worn on the human body, either a computer that are incorporated as an accessory or as part of material used in clothing. These devices come in many different forms such as watches, glasses, wristbands or even jewellery items. Wearable devices are defined by six main characteristics which are un monopolizing, unrestrictive, observable, controllable, attentive and communicative. The development of the applications that can work with WT cover a broad field from those focused-on healthcare and fitness, to industrial applications, and even entertainment and arts [2].

The scope of wearable technologies is very broad and amorphous, and determining the characteristics and specifications of wearable technologies is very difficult. Therefore, to understand the classification of wearable technologies based on the basic characteristics will be very beneficial. According to the literature, the wearable technologies may be divided into three main categories. These categories can be called as wearable health technologies, wearable textile technologies and wearable consumer electronics [1,2,3].

## **2.2 Issues in IoT:**

As the use of wearable services increases, the concern about their security becomes critical. According to HP research, most of smartwatches are vulnerable to security attacks, having a risk to leak personal data. Several studies demonstrate that firmware update vulnerability in wearable devices allows attackers to inject malicious codes. As smartphone apps and web services make use of open interfaces for interoperability, they are susceptible to attack, becoming a weak point for a security threat [6]. For instance, web services suffer from the notorious vulnerabilities such as SQL injection and XSS (Cross-Site Scripting) attacks [4].

### **2.2.1 Easy Physical Access to Data:**

The fact that many wearables store data on the local device without encryption is a real issue. There's often no PIN or password protection, no biometric security and no user authentication required to access data on a wearable. If it falls into the wrong hands, there's a risk that sensitive data could be accessed very easily [5].

### **2.2.2 Insecure Wireless Connectivity:**

The fact that the wearable devices tend to connect to one's smartphone or tablet wirelessly using protocols such as Bluetooth, NFC and Wi-Fi, create another potential point of entry. One may have features like Bluetooth, hotspot connectivity turned ON 24/7 for the need to synchronize with the device. Many of these wireless communications are insufficiently secure to guard against a determined brute-force attack [5]. The data transmission is sometimes not encrypted, which leads a lot of malicious attacks like eavesdropping, evil twin etc.

### **2.2.3 Lack of Encryption:**

Many research work report the lack of encryption on many wearable devices, but there are also serious issues with data in transit when it's being synced and with data being stored on manufacturer's or service provider's cloud servers. Some third-party apps neglect

basic security standards and send or store information that's not encrypted. The kind of data that's automatically being collected by wearables is very valuable to the right people [5].

## **2.3 Rogue Access Point / Evil Twin Attack:**

Nowadays, common places such as airports, coffee shops and hotels have Wireless access points (WAP) or in general Access Points (AP) that allows the people to connect to the Internet at ease. Access point supports security settings such as WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2 (Wi-Fi Protected Access 2). An Access Point can also be configured with no security, which means any client can connect to the Access point without any authentication and it is called as open access point. According to the recent survey, 60% of access points are open, 30% of them are partially configured and remaining 10% are properly configured [6].

Evil Twin is a stealthier attack which makes the attacker to perform Man In The Middle attack (MITM) to steal sensitive credentials. It is easy for adversaries to launch an evil twin attack successfully at public places. First, attackers can configure an evil twin on a laptop in the wireless network by using specific software. To masquerade as a legal AP and lure users to connect it, attacker configures the laptop with the same SSID like legitimate AP. Then, malicious adversaries improve the RSSI of evil twins by deploying them closer to the victim users than a legitimate one or using a directional antenna. Consequently, users may be cheated to connect the evil twin when they attempt to surf the Internet through a legitimate AP. Finally, attackers can sniff the users' network traffic through evil twins. Even worse, if users' data are not encrypted, sensitive information like passwords, credit card information can be captured by attackers [6, 7].

### **2.3.1 Wi-Fi Pineapple:**

The Wi-Fi Pineapple is more than hardware or software — its home to a helpful community of creative penetration testers and IT professionals. Wi-Fi Pineapple is a powerful and flexible wireless auditing platform. The project is a combination of continuously evolving hardware, software and modules. It caters to and is supported by a passionate and creative community of penetration testers, systems administrators and wireless enthusiasts.

With each generation, the hardware is designed to take advantage of the best available wireless components of the day. The hardware continues to grow as the user experience is refined and components are updated to respond to the ever changing wireless landscape. The firmware is engineered alongside the hardware to fully exploit 802.11 protocols. Comprising both the embedded Linux base as well as the web-based user interface, it's in continuous development with free updates delivered over the air.

To further enhance the platform the firmware is designed with an API which enables add-on modules. Modules extend the functionality by providing additional tools and exploits to take advantage of the platform. They can be downloaded and installed over the air from the web interface. In fact, every Wi-Fi Pineapple component is a module which can be updated from the web interface [8].

## **2.4 IoT Security:**

System or Device should be configured beforehand when anyone who want to use it and it is obvious in service and security aspect. Therefore, configuration management and security is essential to a system administrator and a user who just use a service of the system[8]. The fact that there is an exponential growth in the number and type of IoT devices being used today for data collection and monitoring process brings out a clear need for looking at security aspects in detail [9].

## **2.5 Bolt Health & Fitness Application:**

Bolt is a Health and Fitness platform that captures data from a wide range of devices, apps and a collection of Bolt Wearables. The data is analysed to give personalised and automated health feedback, by the Bolt Mobile App. Bolt does not just track a person's data, but converts it into actionable feedback using Artificial Intelligence [10].

The Bolt Mobile App brings together the most important fundamentals effecting one's health and fitness. It analyses the data and gives real time AI based coaching. Bolt uses Data Science, Machine Learning and Cognitive Computation to advance health & fitness levels of this generation. Machines that

perform voice recognition and respond to human prompts, are routine in today's society. The wearable AI advancement at Bolt is exploring the future capabilities of machines, the limits and extremes of their "intelligence" and their ability to replicate human thinking [10].

## **Summary of Findings:**

The IoT computing process equipped with sensors, micro controllers is built with suitable protocol stack for communicating with other devices and users. The IoT device to monitor healthcare could be used to collect physiological parameters of users that could serve as a parameter for doctors to regularly monitor and provide medication for users. The quality, cost of the device determines the level to which the data collection and analysis is facilitated. The IoT eliminates the need for the professional to come in person for monitoring the user. The fact that the system uses sensitive data brings out the need to perform penetration testing to detect possible vulnerabilities.

## **CHAPTER 3**

# **SYSTEM SPECIFICATIONS**

The proposed system requires a mobile phone with the following specifications.

- Android operating system (Jelly Bean or KitKat)
- 91 MB of storage for the installation of the Bolt health app
- Packet data facility (minimum of 30 kbps)
- Wi-Fi facility
- Bluetooth facility

The following permissions are requested before installing the application in the mobile phone.

- Approximate location (network based)
- Precise location (GPS and network based)
- Read Google service configuration
- Full network access
- View network connections

The project makes use of the Bolt beat wearable device with the given specifications:

- Bluetooth
- Step counter
- Calorie counter
- Heartbeat detection

## CHAPTER 4

### PROPOSED SCHEME - ARCHITECTURE

The proposed scheme for identifying and mitigating vulnerability that exists in Boltt Beat operates in two phases.

Phase 1 - Communication between IoT wearable device and Mobile device.

Phase 2 - Communication between Mobile device and external server.

Phase 1 involves data collection from the user by the Boltt Beat and communicating the same to the authorized mobile phone

Phase 2 involves monitoring of the collected data from a remote location by an authorized user (example a doctor to monitor the health of the athlete).

#### PHASE 1

Fig 4.1 shows the architecture diagram of Phase 1. The communicating components in the module includes – Boltt Beats, smart phone and the database installed in the smart phone.

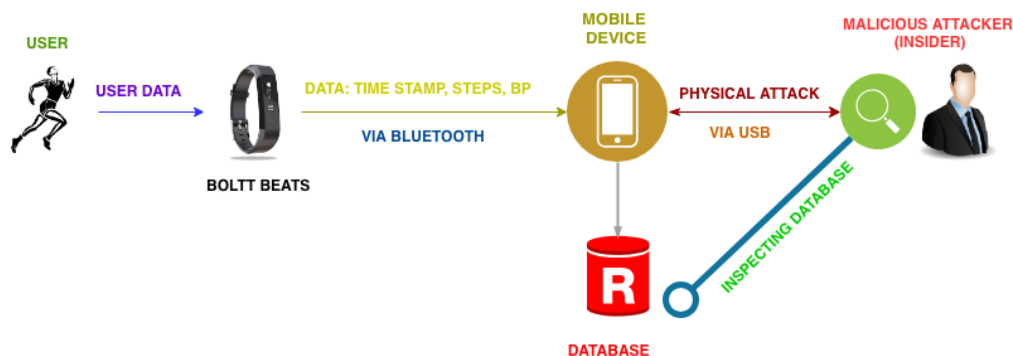


Fig. 4.1 Proposed Architecture PHASE 1

Considering a scenario where data transmission occurs from IoT wearable device Boltt Beats to the mobile device. The data from the device from could be accessed by an insider attacker. Upon physical access to the mobile device, a vulnerability of data transmitted in plain text was observed. The data the IoT wearable device sends is recorded on the mobile device and this can be accessed through an



inspection of the mobile device directories. The same is illustrated in figure 4.1 where an insider access the phone to obtain the unencrypted data from the appropriate database.

The internal storage of the mobile device accessed using an USB connection or otherwise. After which the appropriate database which holds the data sent from the IoT wearable device is located. The database content is explored to understand how data was stored and what is the possible next step for exploitation and for enhancing security through that. The working of the Phase 1 is as follows:

1. The IoT device sends data collected through its sensor to the authorized mobile device connected, in this case using Bluetooth.
2. The mobile device stores the data locally in its own internal storage.
3. An adversary can physically access the mobile device through USB connection for inspecting the internal storage.
4. The database related to the IoT wearable device is located for further exploitation based on storage characteristics, if data is not found to be in plain text, he/she can using cracking tools to decipher the sensitive data.

## PHASE 2

Fig 4.2 shows the architecture diagram of Phase 2. The communicating components include – Bolt Beats device, mobile device, Wi-Fi Pineapple and external server.

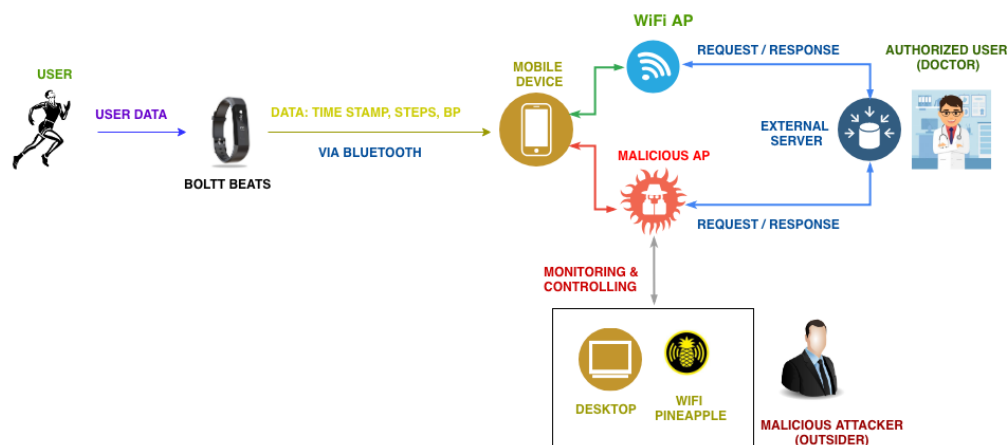


Fig. 4.2 Proposed Architecture PHASE 2

Assuming that there is a need for remote monitoring of data by a legitimate user, the collected data from the smart phone is to be transmitted in the public network.

Considering this scenario, the data transmission happens from authorized mobile device to external server. It is obvious that any network monitoring tools can be used by an attacker to collect the data for misuse.

The adversary will be able to hack the mobile with the aid of a false evil twin Access Point created using Wi-Fi Pineapple device. After which the appropriate data packets sent from the IoT wearable device is monitored and controlled using network monitoring tools like Wireshark. An ethical hacking procedure is carried out with the proposed setup to understand the vulnerabilities which would in turn pave way for proposing schemes to enhance the existing security mechanisms. The monitoring of data packets revealed the fact that it was done in plain text mode. The working of the Phase 2 is as follows:

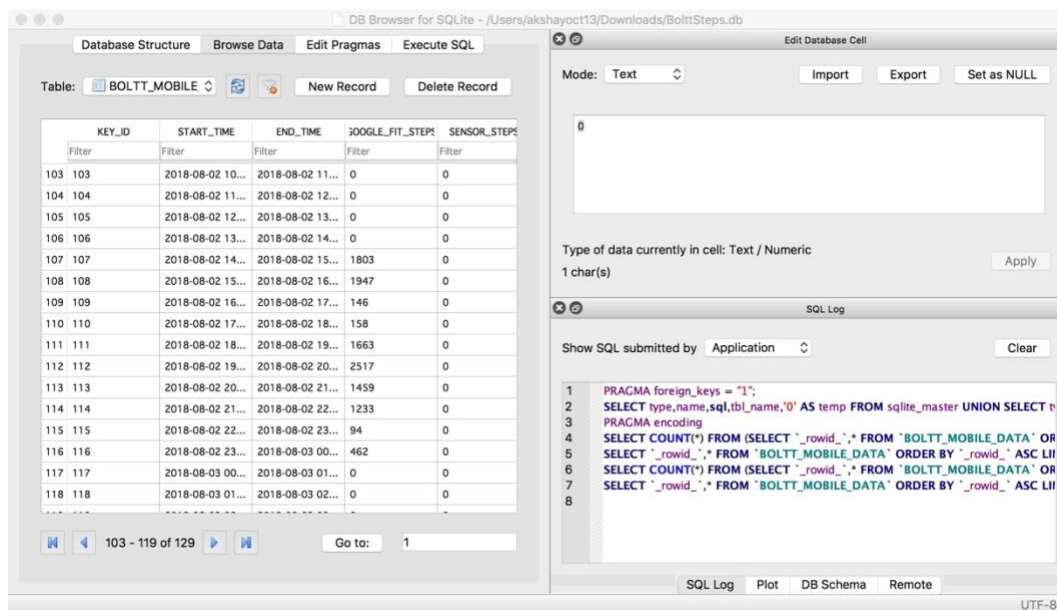
1. The IoT device sends data from collected through its sensor to the mobile device connected, in this case using Bluetooth (Phase 1).
2. The mobile device which was initially connected to non-malicious Wi-Fi AP will be de-authenticated and made to connect to a malicious AP with the help of Wi-Fi Pineapple Nano.
3. From this point onwards, all the data packets of the mobile device can be monitored using the Wi-Fi Pineapple Nano's interface and also other network monitoring tools like Wireshark.
4. The data packets related to the IoT wearable device is monitored and sensitive information is obtained by the adversary.

## CHAPTER 5

### PRELIMINARY RESULTS

The experimental setup of the proposed system was created to carry out ethical hacking. The device was connected to a registered android phone.

The data was extracted from the database created by Bolt beat on the local storage from the smartphone. Evil twin exploit has been used to compromise the Wi-Fi network and extract the data being sent to the hospital.



KEY_ID	START_TIME	END_TIME	GOOGLE_FIT_STEPS	SENSOR_STEPS
103	2018-08-02 10...	2018-08-02 11...	0	0
104	2018-08-02 11...	2018-08-02 12...	0	0
105	2018-08-02 12...	2018-08-02 13...	0	0
106	2018-08-02 13...	2018-08-02 14...	0	0
107	2018-08-02 14...	2018-08-02 15...	1803	0
108	2018-08-02 15...	2018-08-02 16...	1947	0
109	2018-08-02 16...	2018-08-02 17...	146	0
110	2018-08-02 17...	2018-08-02 18...	158	0
111	2018-08-02 18...	2018-08-02 19...	1663	0
112	2018-08-02 19...	2018-08-02 20...	2517	0
113	2018-08-02 20...	2018-08-02 21...	1459	0
114	2018-08-02 21...	2018-08-02 22...	1233	0
115	2018-08-02 22...	2018-08-02 23...	94	0
116	2018-08-02 23...	2018-08-03 00...	462	0
117	2018-08-03 00...	2018-08-03 01...	0	0
118	2018-08-03 01...	2018-08-03 02...	0	0

Fig 5.1 Data extracted found to be in plain text

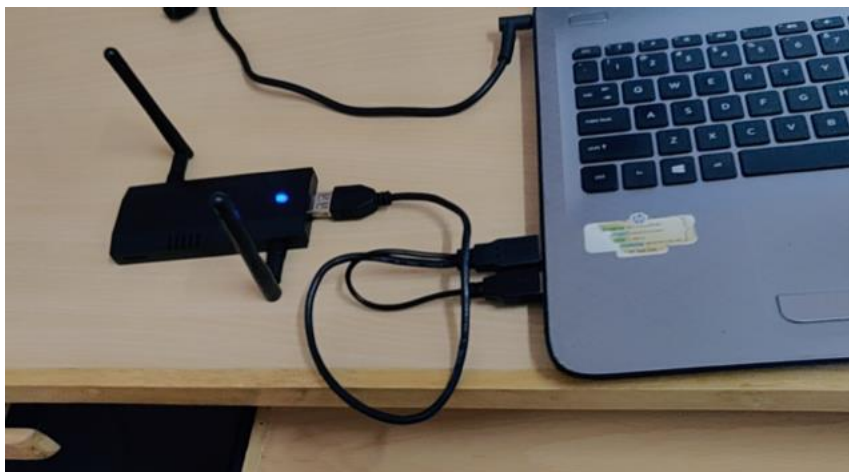


Fig. 5.2 Wi-Fi pineapple used to carry out evil twin attack on the system



Fig 5.3 Wi-Fi pineapple device

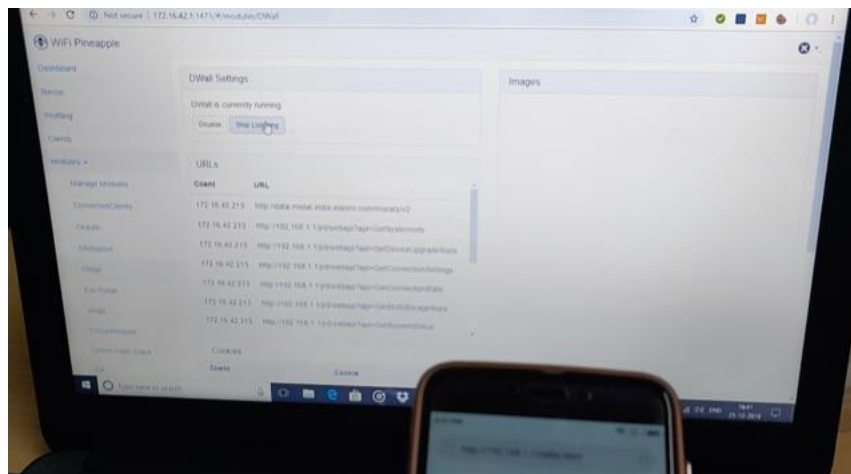


Fig. 5.4 Configuration of compromised Wi-Fi network on Wi-Fi pineapple

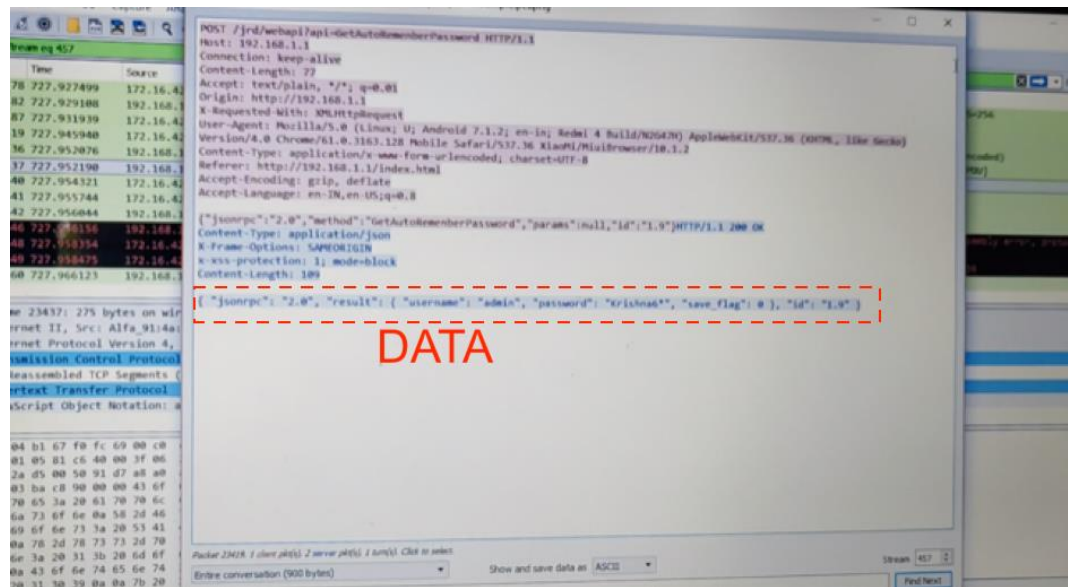


Fig. 5.5 Data sent over the network monitored captured using a packet tracer

# **CHAPTER 6**

## **CONCLUSION**

A vulnerability in the IoT device was detected and various ways to exploit the system was tested.

### **6.1 Future Work**

The project can be further developed by fixing the vulnerabilities that are identified. Various potential fixes were identified as:

- Data packets transmitted could be encrypted
- The underlying data channel for transmission could be encrypted.
- The smartphone permission “Automatically connect to open networks” should not be granted.

### **6.2 Limitations**

The project is restricted to the use of Bolt Beat wearable. Implementing this on a larger scale would require getting to know the specifics of each wearable device. The encryption of the database can lead to a formidable increase in size of the data being stored and hence may take up a large amount of storage space.

## REFERENCES

- [1] Shanzhi Chen , Hui Xu , Dake Liu , Bo Hu , Hucheng Wang, *"A Vision of IoT: Applications, Challenges and Opportunities with china Perspective"*. IEEE Internet of Things Journal, 2014.
- [2] Ke Wan Ching and Manmeet Mahinderjit Singh, *"Wearable Technology Devices Security and Privacy Vulnerability Analysis"*. International Journal of Network Security & Its Applications (IJNSA), May 2016.
- [3] Mesut Çicek, *"Wearable Technologies and Its Future Applications"*, International Journal of Electrical, Electronics and Data Communication, April-2015.
- [4] Mario Frustaci, Pasquale Pace, Gianluca Aloï, Giancarlo Fortino, *"Evaluating Critical Security Issues of the IoT World: Present and Future Challenges"*, IEEE Internet of Things Journal, Aug. 2018 .
- [5] Michelle Drolet, *"Potential Security Concerns for Wearables"*, [www.csoonline .com](http://www.csoonline.com), April 11.
- [6] Aswin Kumar A, Ashok Kumar Mohan, and Amritha P.P, *"Deceiving Attackers in Wireless Local Area Networks using Decoys"*, TIFAC-CORE in Cyber Security, Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India.
- [7] Qian Lu ; Haipeng Qu ; Yuan Zhuang ; Xi-Jun Lin ; Yanyong Zhu ; Yunzheng Liu, *"A Passive Client-based Approach to Detect Evil Twin Attacks"*, 2017 IEEE Trustcom/BigDataSE/ICCESS.
- [8] *"Wi-Fi Pineapple"*, [www.hack5.org](http://www.hack5.org) .

- [9] Boheung Chung ; Jeongyeo Kim ; Youngsung Jeon, *"On-demand security configuration for IoT device"*, 2016 International Conference on Information and Communication Technology Convergence (ICTC).
- [10] *"Bolt Health & Fitness Application"*, [www.boltt.org](http://www.boltt.org)