
SLIIT

*Discover Your Future*

# Security Platform for Mobile OS

## Project ID :- 19-001

## Project Proposal

**B.Sc. Special (Honors) Degree in Information Technology**

**Submitted on 2019-03-12**

# SECURITY PLATFORM FOR MOBILE OS

**Project ID :- 19-001**

**Authors:**

| Student ID | Name | Signature |
|---|---|---|
| **IT16009400** | **Brayan Benett A.S** | |
| **IT16026544** | **Vinushanth K** | |
| **IT16034396** | **Sam Abisherk R** | |
| **IT16073388** | **Ranjitha L** | |

## Supervisor

**…….**

**Mr. Amila Nuwan Senarathne**

## Co Supervisor

**…….**

**Mr. Kavinga Yapa Abeywardena**

## DECLARATION

We declare that this is our own work and this project proposal does not incorporate with acknowledge any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of our knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

| | |
|---|---|
| …… | …… |
| Brayan Benett A.S | Vinushanth K |
| …… | …… |
| Sam Abisherk R | Ranjitha L |

# ABSTRACT

Evolution of human is the corner stone for everything that we see, feel and use today. History of Phone is the greatest living example we can see. All started from devices which transmitted signals from one place to another followed by wired devices which transmitted voice to a limited distance. With the invention of new technologies and improved mechanisms wireless signals helped in the field of telecommunication. Mobile phones aka hand held phones are the epitome of telecommunication is a true statement now than ever before.

In the 21st century mobile phones are the extended arms of almost every human being. Nowadays mobile phones are not only used in voice communication or text messages. It acts as a palmtop computer with almost all the capabilities. Modern devices have all the features that helped it to become the ultimate source of data for an individual. It was easy for an individual to keep all his data intact with him in his hands. But with great power comes the great responsibility. Almost all the details about the person is saved in his/her mobile phone which act as a single point of failure.

There are vulnerable points which can be exploited to acquire the personal and sensitive data from the device in order to gain unethical advantage over an individual. Bluetooth, Wi-Fi and human errors are some of those vulnerable points which can give out sensitive data to the perpetrator. In our research we intend to propose solutions for the main above-mentioned issues which will result in a secure trustable Android platform for secure operating system that can be very much helpful for the general public and professionals to safeguard their information.

# TABLE OF CONTENT

# LIST OF FIGURES

# LIST OF TABLES

# 1 INTRODUCTION

## 1.1 Background

Mobile phones are one of those inventions that helps human being in every possible way. In present days mobile phone act as a single go to point for all the important needs. Whether it could be communication or data storing. All the most important details such as personal health information, Credit card or Bank account details, addresses, email addresses and so on. And it needs to be understood that loss of assets these days are not only refers to the loss of money and properties it also refers to the sensitive data that we possess.

When we consider security breaches and data loss in mobile phones it needs to be noted that Bluetooth and Wi-Fi are a concern to our data. In the meantime, sensitive data can be disclosed to unauthorized individuals through insecure internet or wireless connection and even accidental transportation of data. In particular it has to be taken as a serious issue that an attacker can gain many important data through exploiting vulnerabilities in Bluetooth and wireless connectivity which will result in the loss of privacy and valuable assets. There have been several techniques been used in the past to decrease the possibility of these attack. Even though if we consider android platform which is used by majority have only a basic level of protection given to these channels.

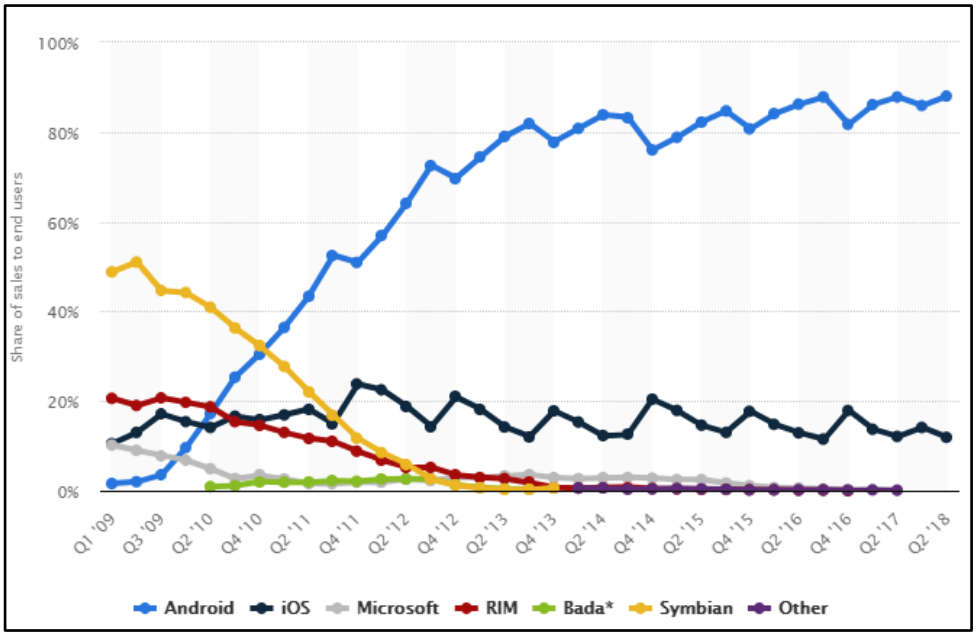


Figure 1– Global mobile OS market share

According to Kaspersky lab, number of android users at the time of the proposal presentation is 4,480,971,997 and increasing every second. Almost 88% of the total mobile OS market share belongs to android. As android kernel is a modified version of Linux kernel and Linux being an open source the security measures that have been taken in android platform for Bluetooth security, Wi-Fi access points security, Wi-Fi direct security and accidental data leakage prevention is very minimum to none.


We propose to secure Android Mobile OS by implementing Machine learning technology in certain aspects of Wireless connectivity, Bluetooth connectivity and Keyboard system which will result in a secure connection via Wireless access points, Secure file transection and connectivity via Bluetooth and prevent the accidental leakage of sensitive details to an unauthorized individual. On the whole our research product can be a comprehensive secure platform for mobile OS.

## 1.2 Literature Review

We did an inside Literature survey on already existing security measures and the inside architecture of Bluetooth, Wi-Fi connectivity, Rogue access point detection, Data leakage prevention and Wi-Fi direct. The outcome of our in-depth search for the knowledge of underlying technologies and their security levels as follow.

### I. Data Leakage prevention

There have been several researches conducted on the topic of data leakage and its prevention. Even though there are no much researches done on accidental data leakage to unauthorized parties, general concept of data leakage prevention has been discussed widely. Most of them are industrial level standards.

#### A. Detecting Data semantic: A data leakage prevention approach [10]

The leakage of sensitive files and data to outsiders can be a disastrous thing for a multinational organization or to an individual. The leakage in data such as trade secret, company banking details, individual ID numbers and health records can affect the stake of a company, the privacy of an individual and the security of the assets.

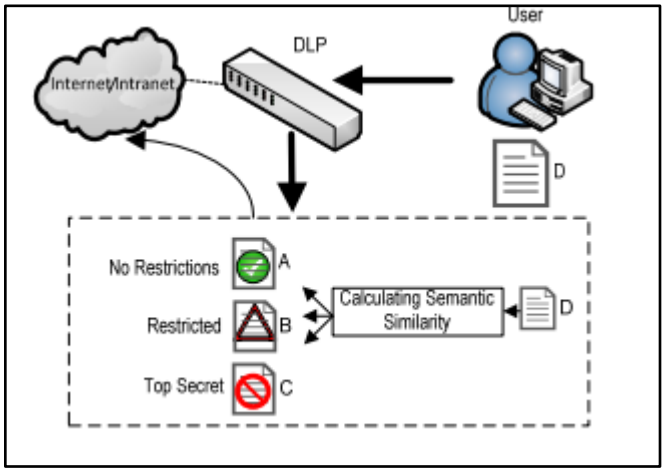


Figure 2 - DLP model

In this DLP model they use statistical data analysis to identify the sensitive data semantics. They use a very famous weighting function Term Frequency- Inverse Document Frequency (TF-IDF) which is used to retrieval of information and text mining to measure the amount of information in a document or a file. They are aiming to separate the details in the document according to pre-defined topics which has a predefined secrecy level. And once the detected, it can be blocked, quarantined

or alerted according to the predefined set of instructions. And they propose to implement the DLP as a hardware appliance or a software agent which can be installed in the clients Device.

**B. Automatic detection of sensitive attribute in PPDM** [11]

Here they propose to suppress the sensitive data by data mining in order to prevent it from being leaked. They propose to do the data mining to find out the sensitive attributes in a database and hide the values in order to protect the privacy.

A SAMPLE EMPLOYEE DATABASE TABLE

| S.No. | Name | Mobile no. | Salary | Age |
|---|---|---|---|---|
| 1 | Awera | 9112345987 | 25000 | 25 |
| 2 | Bokln | 9871234567 | 40000 | 40 |
| 3 | cyrus | 9876754567 | 80000 | 60 |
| 4 | Kinili | 8834231133 | 34560 | 35 |

Completely modified table to protect the employee privacy

| S.No. | Mobile no. | Salary | Age |
|---|---|---|---|
| 1 | 91********* | 2***** | 2* |
| 2 | 98********* | 4***** | 4* |
| 3 | 98********* | 8***** | 6* |
| 4 | 88********* | 3***** | 3* |

Figure 3 – Sample Database Table

First client query is thoroughly analyzed to find out the sensitive attributes. Attributes can be defined as sensitive with regards to the previously defined threshold value by the data owner. When considering a database sensitivity weight will be assigned to every attribute and the query will be analyzed for the total sensitivity value. If the total of the sensitivity of the required attributes exceed the threshold it will carry out the operations which were pre-defined. By this method they propose to eliminate the accidental leakage of sensitive data from a database to an outside unauthorized party.

### C. Sensitive data leakage detection in pre-installed applications of custom Android firmware. [12]

In this research study they came up with a sensitive information leakage analysis system for android based devices by analyzing the over 290 custom ROMs which are already existing. The system has three main modules.

- APK extractor: - This extractor helps to extract the pre-installed applications from the custom ROMs. To extract, a batch script is being used to get all the applications which can be pre-installed in any formats such as zip.
- APK analyzer: - This particular module first analyzes every extracted application for sensitive paths and their entry and exit points. It checks the entry point and exit point in order to be used by the path matcher later. And also, this APK analyzer analyze the data flow of each applications and filter out the flows that relates to sensitive sources and critical sinks. These source-sink methods help to find out the actual sensitive data.
- Path Matcher: - In this module path matcher builds all the possible links for the entry points and exit points which were found by APK Analyzer to detect the availability of data leakage in the flow. These flows can be present anywhere.

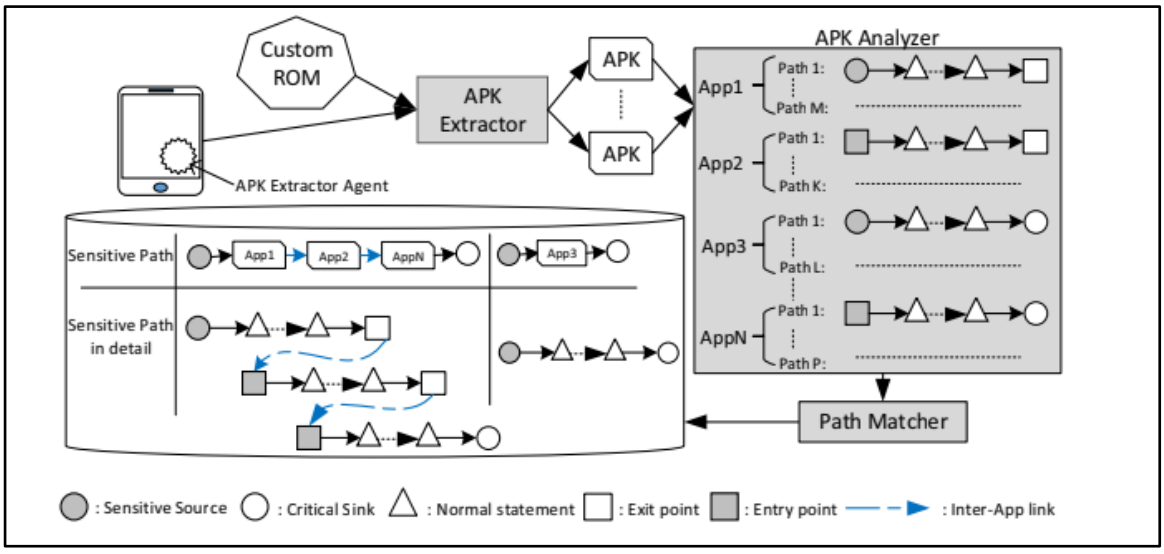


Figure 4 - Information leakage analysis system

As a result of these research they found 4 out of 290 custom ROMs had data leakage in the pre-installed system applications.

## II. Rogue access point detection

### A. Active User-side Evil Twin Access Point Detection Using Statistical Techniques (TMM, HDT). [4]

This research proposes a new lightweight end user based evil twin detection solution. This technique does not rely on fingerprint checking of suspect devices nor require a known authorized AP/host list. Thus, this solution is most beneficial for user who are in the move or has high mobility outside the organization.

This research focuses mainly on accomplishing most from Intrinsic communication and to identify the properties of the evil twin attacks. Furthermore, we propose two statistical anomaly detection algorithms for evil twin detection that is Trained Mean Matching (TMM)and Hop Differentiating Technique (HDT). In particular, our HDT improves TMM by removing the training requirement. HDT is resistant to the environment change such as network saturation and RSSI fluctuation.

### B. CETAD: Detecting Evil Twin Access Point Attacks in Wireless Hotspots [13]

In this paper, we propose a mechanism CETAD leveraging public servers to detect such attacks. CETAD only requires installing an app at the client device and does not require to change the hotspot APs. CETAD explores the similarities between the legitimate APs and discrepancies between evil twin APs, and legitimate ones to detect an evil twin AP attack. Through our implementation and evaluation, we show that CETAD can detect evil twin AP attacks in various scenarios effectively. As most of the most solutions are designed for infrastructure network rather than for client devices. This research mainly focuses on developing a solution on client side. Thus, this research focus on designing a plug-and-play mechanism to detect evil twin AP attacks that only requires to install software at the client device.

There are many challenges that has to be faced when designing a client-side mechanism to detect evil twin AP attacks. First, the client has no information or access about the hotspot architecture as it has only limited resources. Second, many scenarios have to be considered while developing as all the hotspots use various Wi-Fi setup. Third, adding custom hardware, e.g., routers or servers, is not an option as it would limit the applicability and universal acceptance. We overcome these challenges and design a detection mechanism that we call CETAD (Client end Evil Twin Access point Detector).

When multiple AP's connect to the same ISP when they are legally configured to form a hotspot. Thus, they share same SSID and similar network parameters such as ISP names, Global IP address, Round trip timer, temporal network behavior. But a evil twin AP will use a different network setup. This research mainly focuses on these parameters to identify whether the APs belong to same group or not. Even though CETAD is designed for client devices, it can be extended to detect evil twin APs in an infrastructure network as well.

### C. A Hidden Markov Model Based Approach to Detect Rogue Access Points[3]

This research focuses on using Hidden Markov Model to detect the Rogue Access Points in a WLAN. This approach identifies a RAP by observing the traffic characteristics of the end hosts in a network. Hidden Markov Model represents the probability of transitions between the different security states of an access point. HMM functions as follows, HMM is trained based on some training data set which consists of information obtained from related to packet traces. These packet traces are gleaned from traffic which includes normal internet activities.
Once the HMM is trained different traffics are monitored in the end user side. By observing the inter arrival time of the packets HMM decides whether an access point is authorized or not.

## III. Secure Bluetooth

### A. Bluetooth Security Protocol Stacks

Protocol stacks are defined as the combination and implementation of security protocols of hardware/software. Protocol stacks defines the connectivity between devices according to the standards. [9]

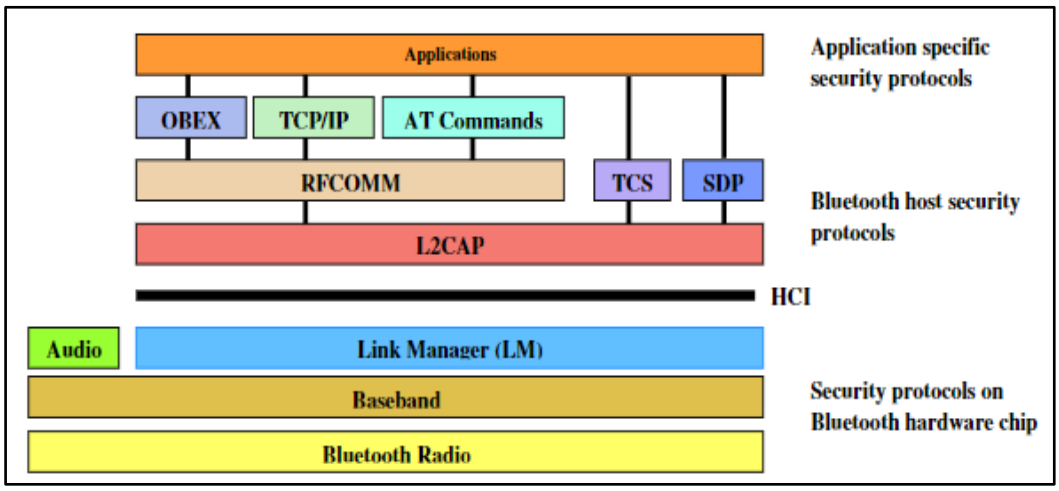


Figure 5 - Bluetooth Security Protocol Stacks

OBEX- Object Exchange Protocol used to transfer objects such as files, contacts and calendars as client-server model.
SDP- Service Discovery Protocol discovers all the services that are around the RF range proximity and it validate the characteristics of the available discoverable device services.
The above-mentioned protocols are limited to some security extends according to their requirements. We are proposing a solution for the protocol stacks with an overall security of the inbound and outbound connectivity of the Bluetooth technologies by implanting a firewall which will contain the below stated features,

- Considering all the protocols in Bluetooth channels which will monitor and filter the inbound traffic for malicious packets with signature and behavioral based detections.
- Alerting the user for malicious behaviors of incoming files and automatically quarantine them.
- User confirmation will be granted for the particular device to permanently block the attacker device from being connected again

- Logs all Bluetooth events.
- We have the choice to decide on the trusted remote devices.
- Ability to validate the device types with the Bluetooth addresses.

### B. Bluetooth Improved Link Key Generation

Several protection measures have been implemented at one of a kind protocol degree, however the safety of the protocols depends on the configuration of the user's device according to their decision of Turing one the discoverable and connectivity options. We can divide the discoverability and connectivity into three modes of operations for the security purposes,

**Silent:** In this more only the traffics will be monitored and no data connection will be accepted.

**Private:** According to this mode the device will be only discoverable for the devices which is already having the Bluetooth device address of the requested device. The Bluetooth device address is unique for the particular device.

**Public:** It is a discoverable device which is open for connectivity.

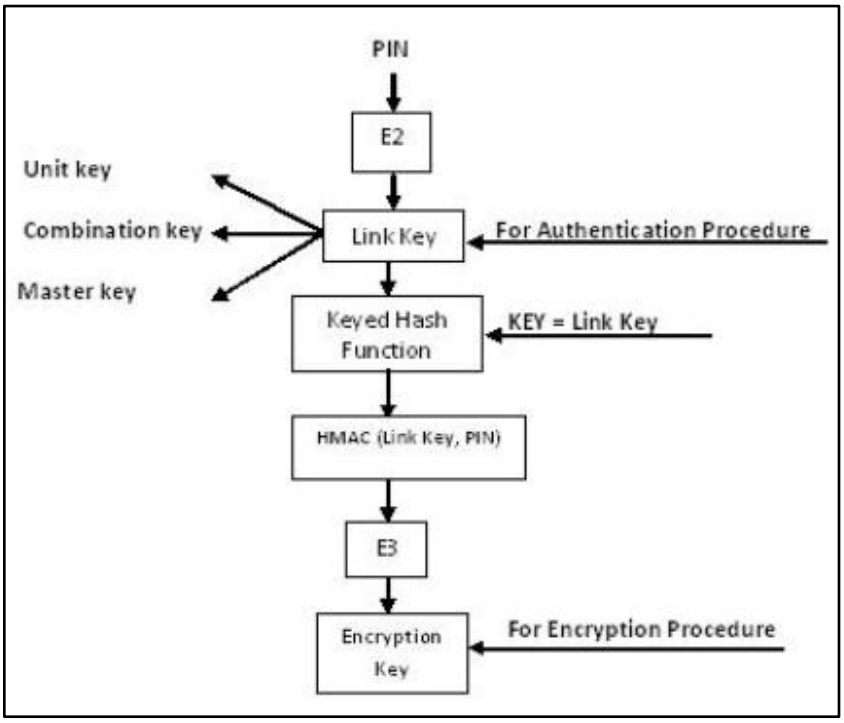


Figure 6- Link Key Generation

By discovering the unit key of the devices Man-in-the-Middle attack is possible. According to the researcher perspective the two devices connected with the unit key has to enter the PIN for the authentication purposes, considering that the file traffic will have a secure connection with the aid of Keyed Hash Function/Algorithm. The is known to the specific devices which is considered as Link Key by them. Then the Link key will go through the Keyed Hash Algorithm and PIN will be combined as E3 algorithm to obtain the Encryption key. The PIN also know to the only the connected devices so the untrusted and fake devices can be eliminated and cannot generate the Encryption Key for accessing the devices the each other. By this process the Man-in-the-Middle attack will be eliminated according the researcher's perspective. [7]

This paper proposes the encryption architecture of the Bluetooth key management technique, with above mentioned PIN encryption method and by validating the Bluetooth addresses with the aid of the embedded inbuilt Bluetooth firewall technology. Bluetooth addresses which is displayed in as 6 bytes and written in hexadecimal format and separated with colons. It will eliminate fake devices more accurately than previous method and the Man-in-the-Middle attack will be failed to exploit for the attacker.

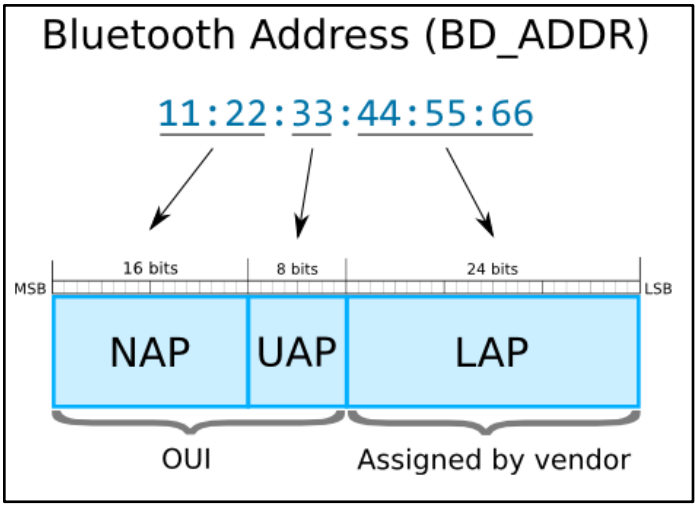


Figure 7 – Bluetooth Address

NAP- Non-significant Address Part value is used in Frequency-hopping spread spectrum (FHSS) frames.

UAP- Upper Address Part value is used for seeding the various Bluetooth specification algorithms.

LAP- Lower Address Part value uniquely finds a Bluetooth device as part of the Access Code in all transmitted traffics.

OUI- Organizationally Unique Identifier

There is an open source tool available for Bluetooth address lookup which provide the information of the vendor, the device type and manufacturing details. The tool can used by inputting the Bluetooth addresses. Our study will sum up by embedding this information gathering tool with the address of Bluetooth, which will be added alongside with our Bluetooth firewall technology for validating the device details and logging purposes.

## IV. Secure Wi-Fi Direct

There have been no many researches done regarding the security issues of peer-to-peer technology connection and contingencies done. Some of the similar research topics and their abstracts are below.

### A. Secure Device-to-Device Communications over Wi-Fi Direct- A Short-Authentication-String-Based Key Agreement Protocol [14]

This research mainly focused on designing protocol for pair wise key agreement to involve minimal mutual authentication or human interaction. This protocol basically provides an ideal security level in regarding to the required bits that must be mutually authenticated.

Short Authentication based key agreement protocol utilizes a cryptography commitment scheme. This commitment scheme allows to hide a chosen value through a single commit action. Any device which obtains the pair of value is able to reveal the committed value via an open operation. This commitment value doesn't leak any information about the hidden value. This cryptographic function helps to achieve an efficient commitment scheme.

The main goal of this research is to implement an Android application by involving Secure Key establishment functionality into a conventional Wi-Fi Direct application. This solution would allow the user to establish pairwise secret keys which can be used to encrypt the data transmitted through Wi-Fi direct connection.

## B. Wi-Fi protected Service (WPS) [15]

Wi-Fi Direct devices are required to implement Wi-Fi Protected Setup (WPS) to support a secure connection with minimal user intervention. In particular, WPS allows to establish a secure connection by introducing a PIN in the P2P Client, or pushing a button in the two P2P Devices. Following WPS terminology, the P2P GO is required to implement an internal Registrar, and the P2P Client is required to implement an Enrollee. The operation of WPS is composed of two parts. The first part which is referred as “Phase 1”, the internal Registrar is in charge of generating and issuing the network credentials such as security keys, to the Enrollee. WPS is based on WPA-2 security and uses Advanced Encryption Standard (AES)-CCMP as cypher, and a randomly generated PreShared Key (PSK) for mutual authentication. The second part, denoted as “Phase 2”, the Enrollee (P2P Client) disassociates and reconnects using its new authentication credentials. In this way, if two devices already have the required network credentials (this is the case in the Persistent group formation), there is no need to trigger the first phase, and they can directly perform the authentication.

### 1.2.1 Solutions available in the current market.

#### A. Data Leakage Prevention [1]

##### a. Symantec Data Loss Prevention

- Compatible with Desktop PC
- Cloud compatibility
- Scalable to a vast area.
- Too much enterprise oriented

##### b. SecureTrust Data Loss Prevention

- Compatible with Desktop PC.
- Cloud compatibility
- Large range of predefined settings available
- Automatic blocking of threats
- Too much of settings which can overwhelm general user.

##### c. Digital Guardian Endpoint DLP

- Desktop Oriented Protection
- Cross platform compatibility
- Can be deployed on premises, cloud or hybrid.
- Very Expensive as it is enterprise oriented.

## 1.3 Research Gap and Research Problem

### 1.3.1 Research Problem

#### A. Accidental Data Leakage

The unauthorized transfer of classified information from a computer, mobile phone or datacenter to the outside world is known as data loss. Data leakage can be accomplished by simply mentally remembering what was seen, by physical removal of tapes, disks and reports or simply sending sensitive data accidentally to a recipient that is not authorized.

Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network if it's a corporate environment or preventing from sending sensitive personal information accidently. The term is also used to describe software products that help a network administrator control what data end users can transfer.

There have been many techniques adopted to prevent the data loss in both computers and mobile phones. But preventing a user from accidently exposing his sensitive data in a mobile phone has always been a tough ask as of now.

#### B. Rogue Access points

With the proliferate growth of WIFI usage which has triggered the increase in the deployment of WIFI equipment in an organization or in anywhere else where users require it most. However, there is an emerging threat that can severely compromise the security of wireless users which is an evil twin attack. These attacks can be a high thread for the organizations compared to other scenarios. Rough Access point or an Evil twin is an access point in a local WAN network inside of an organization which is most likely to be published by the employee of that organization itself. An evil twin is essentially a phishing Wi-Fi access point that has the same SSID like the legitimate one, which lead to the user to join these AP's without knowledge which will result in leaking the confidential information or even in launch of Denial of service.

## C. Bluetooth

Before we going deep into the present Bluetooth security, we have to go back a bit time and check the statuses of the security in old days. Bluetooth was invented during then end of 1989s by Dr. Jaap Haartsen while working at Ericsson, but it really came into hands of use during the beginning of 2000s. Bluetooth is not a single protocol, it is the collection of protocols together according to the one single specification. Bluetooth Special Interest Group (SIG) is the organization which is currently managing doing all the implementations in Bluetooth.

The first few iterations in the beginning of implementation served as draft/test versions until the first successful release of v1.0. Since then there were major releases of the Bluetooth versions as 1.2, 2.0, 2.1, 3.0, 4.0, 4.1, 4.2, and the latest Bluetooth 5 which was recently in December 2016. Each version has increased in significant enhancements and easiness for the use.

Figure 8 gives a summary of the all currents versions. [5]

| Version | Year | Features |
|---|---|---|
| 1.1 | | Support for non encrypted channels<br>Received Signal Strenght Indicator (RSSI) |
| 1.2 | | Faster connection<br>Adaptive frequency hopping<br>Enhanced error detection and flow control<br>Enhanced synchronization capability |
| 2.0+EDR | 2004 | Enhanced Data Rate |
| 2.1+EDR | 2007 | Erroneous Data Reporting<br>Encryption Pause and Resume<br>Extended Inquiry Response<br>Link Supervision Timeout Changed Event<br>Non-Automatically-Flushable Packet Boundary Flag<br>Secure Simple Pairing<br>Sniff Subrating<br>Security Mode 4 |
| 3.0+HS | 2009 | AMP Manager Protocol (A2MP)<br>Enhancements to L2CAP including<br>Enhanced Retransmission Mode and Streaming Mode<br>Improvements to the L2CAP state machine for AMP channels<br>Fixed channel support<br>Enhancements to HCI for AMP<br>Enhancements to Security for AMP<br>802.11 Protocol Adaptation Layer<br>Enhanced Power Control<br>Unicast Connectionless Data<br>HCI Read Encryption Key Size command<br>Generic Test Methodology for AMP<br>Enhanced USB and SDIO HCI Transports |
| 4.0 | 2010 | Bluetooth Low Energy including<br>Low Energy Physical Layer<br>Low Energy Link Layer<br>Enhancements to HCI for Low Energy<br>Low Energy Direct Test Mode<br>AES Encryption (128 bit)<br>Enhancements to L2CAP for Low Energy<br>Enhancements to GAP for Low Energy<br>Attribute Protocol (ATT)<br>Generic Attribute Profile (GATT)<br>Security Manager (SM) |

Figure 8 – Features and Versions of Bluetooth Technology

According the wireless nature of Bluetooth, most of the wireless connectivity is subject to many different threats such as eavesdropping, denial of service, impersonation and man-in-the-middle. The above-mentioned threats are common for all wireless connectives. But there are specific threats for Bluetooth connectivity as well. They are,

- **Bluesnarfing-** It is an attack which a successful exploitation will give attacker for Any unauthorized access and which can be used for theft of information such as emails, contacts, messages, schedules and more.
- **Bluebugging**- It gives an attacker to take over the phone and let them listen phone conversations, forwarding calls, sending text messages.
- **Bluejacking-** It sends fake messages and creates confusion among the users. It can also send fake audio files and create diversion of the devices.
- **Location tracking-** With enabled GPS devices it possible to discover the location of the devices.
- **Key management-** Key management which involves in the distribution, storage, and usage of the cryptography keys.
- **Denial of Service (Dos)-** Interruption of the services of the devices, an attacker can cause it with the malicious content. [8]

### D. Wi-Fi Direct

Peer to Peer technology is where users share the files that are housed in their local system with others. P2P is one of the fastest growing technologies in the recent years, as an evident for this statement it is reported in a recent survey that Peer-to-Peer applications generate one-fifth of the total Internet traffic, and it is believed that it will continue to grow. Indeed, given the recent advances of high-speed wireless communication technologies, including 3G, post-3G and WLAN, it is widely envisioned that file sharing over a wireless P2P network will naturally be the next step. However, P2P applications introduce security risks that may put your information or your computer in jeopardy.

Once two devices are connected to each other through P2P technology any data can be transmitted between them. When attacker decides to send a malicious file, which contain harmful data like Viruses, Malicious code, Malware and Trojan they can be received and downloaded by the other end user and data in recipient device can be exposed to the attacker. Currently there are some third-party mobile antivirus solution to hunt the Viruses and Firewalls to prevent malicious objects from attacking the device.

### 1.3.2 Research Gap

#### A. Accidental Data Leakage Prevention

Although there were many DLP systems have been implemented as of our knowledge there are no prevention mechanisms implemented in mobile phones to prevent accidental leakage of sensitive data. And preventing the leakage by notifying the sensitive details to the user at the point of creation itself is an advanced way of prevention

There has been a shortage of solutions which can be a real-time data loss detection. And also, with the effectiveness of machine learning, no solutions have been produced previously.

#### B. Rogue access point / Evil twin access point Detection

It can be noticed that there are rogue access point and Evil twin access point detection methods which have been already proposed and implemented none of them has the efficiency of a Machine learning Model. And also, no android mobile platform has accompanied the detection process before connecting.

#### C. Bluetooth

The following describes the Bluetooth Vulnerabilities which is mapped with their versions. According to the identified threats it is addressable in future for further recommendations in security upgrades and improve Bluetooth security. Mentioned common vulnerabilities which is for all versions has been filtered are mentioned at the bottom. [6]

| | Security Issue or Vulnerability | Remarks |
|---|---|---|
| **Versions Before Bluetooth v1.2** | | |
| 1 | **Link keys based on unit keys are static and reused for every pairing.** | A device that uses unit keys will use the same link key for every device with which it pairs. This is a serious cryptographic key management vulnerability. |
| 2 | **Use of link keys based on unit keys can lead to eavesdropping and spoofing.** | Once a device's unit key is divulged (i.e., upon its first pairing), any other device that has the key can spoof that device or any other device with which it has paired. Further, it can eavesdrop on that device's connections whether they are encrypted or not. |
| **Versions Before Bluetooth v2.1** | | |
| 3 | **Security Mode 1 devices never initiate security mechanisms.** | Devices that use Security Mode 1 are inherently insecure. For v2.0 and earlier devices, Security Mode 3 (link level security) is highly recommended. |
| 4 | **PINs can be too short.** | Weak PINs, which are used to protect the generation of link keys during pairing, can be easily guessed. People have a tendency to select short PINs. |
| 5 | **PIN management is lacking.** | Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems. The best alternative is for one of the devices being paired to generate the PIN using its random number generator. |
| 6 | **The encryption keystream repeats after 23.3 hours of use.** | As shown in Figure 3-5, the encryption keystream is dependent on the link key, EN_RAND, Master BD_ADDR, and Clock. Only the Master's clock will change during a particular encrypted connection. If a connection lasts more than 23.3 hours, the clock value will begin to repeat, hence generating an identical keystream to that used earlier in the connection. |
| **Bluetooth v2.1 and v3.0** | | |
| 7 | **Just Works association model does not provide MITM protection during pairing, which results in an unauthenticated link key.** | For highest security, devices should require MITM protection during SSP and refuse to accept unauthenticated link keys generated using Just Works pairing. |
| 8 | **SSP ECDH keypairs may be static or otherwise weakly generated.** | Weak ECDH keypairs minimize SSP eavesdropping protection, which may allow attackers to determine secret link keys. All devices should have unique, strongly-generated ECDH keypairs. |
| 9 | **Static SSP passkeys facilitate MITM attacks.** | Passkeys provide MITM protection during SSP. Devices should use random, unique passkeys for each pairing attempt. |
| 10 | **Security Mode 4 devices (i.e., v2.1 or later) are allowed to fall back to any other security mode when connecting with devices that do not support Security Mode 4 (i.e., v2.0 and earlier).** | The worst-case scenario would be a device falling back to Security Mode 1, which provides no security. NIST strongly recommends that a Security Mode 4 device fall back to Security Mode 3 in this scenario. |

| | | |
|---|---|---|
| **Versions Before Bluetooth v4.0 (Low Energy)** | | |
| **11** | **Attempts for authentication are repeatable.** | A mechanism needs to be included in Bluetooth devices to prevent unlimited authentication requests. The Bluetooth specification requires an exponentially increasing waiting interval between successive authentication attempts. However, it does not require such a waiting interval for authentication challenge requests, so an attacker could collect large numbers of challenge responses (which are encrypted with the secret link key) that could leak information about the secret link key. |
| **12** | **The master key used for broadcast encryption is shared among all piconet devices.** | Secret keys shared amongst more than two parties facilitate impersonation attacks. |
| **13** | **The E0 stream cipher algorithm used for Bluetooth BR/EDR encryption is weak.** | FIPS-approved encryption can be achieved by layering application-level FIPS-approved encryption over the Bluetooth BR/EDR encryption. Note that Bluetooth LE uses AES-CCM. |
| **14** | **Privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.** | Once the BD_ADDR is associated with a particular user, that user's activities and location could be tracked. |
| **15** | **Device authentication is simple shared-key challenge–response.** | One-way-only challenge–response authentication is subject to MITM attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that devices and the network are legitimate. |
| **Bluetooth v4.0 (Low Energy)** | | |
| **16** | **LE pairing provides no eavesdropping protection. Further, the Just Works pairing method provides no MITM protection.** | If successful, eavesdroppers can capture secret keys (i.e., LTK, CSRK, IRK) distributed during LE pairing. Further, MITM attackers can capture and manipulate data transmitted between trusted devices. LE devices should be paired in a secure environment to minimize the risk of eavesdropping and MITM attacks. Just Works pairing should not be used. |
| **17** | **LE Security Mode 1 Level 1 does not require any security mechanisms (i.e., no authentication or encryption).** | Similar to BR/EDR Security Mode 1, this is inherently insecure. LE Security Mode 1 Level 3 (authenticated pairing and encryption) is highly recommended. |
| **All Versions** | | |
| **18** | **Link keys are stored improperly.** | Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls. |
| **19** | **Strengths of the pseudo-random number generators (PRNG) are not known.** | The Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the security mechanisms. Bluetooth implementations should use strong PRNGs based on NIST standards. |
| **20** | **Encryption key length is negotiable.** | The v3.0 and earlier specifications allow devices to negotiate encryption keys as small as one byte. Bluetooth LE requires a minimum key size of seven bytes. NIST strongly recommends using the full 128-bit key strength for both BR/EDR (E0) and LE (AES-CCM). |
| **21** | **No user authentication exists.** | Only device authentication is provided by the specification. Application-level security, including user authentication, can be added via overlay by the application developer. |
| **22** | **End-to-end security is not performed.** | Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by use of additional security controls. |
| **23** | **Security services are limited.** | Audit, non-repudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer. |
| **24** | **Discoverable and/or connectable devices are prone to attack.** | Any device that must go into discoverable or connectable mode to pair or connect should only do so for a minimal amount of time. A device should not be in discoverable or connectable mode all the time. |

Table 1 – Bluetooth Vulnerabilities

### D. Wi-Fi Direct

Once the connection is made no trace for incoming and outgoing data. The connection mechanism is also vulnerable.

| | Current Mobiles with Android OS | Secure Mobile OS |
|---|---|---|
| Data Leakage Prevention Mechanism | | ✓ |
| Bluetooth Connectivity | ✓ | ✓ |
| Bluetooth Logs | | ✓ |
| Bluetooth Firewall | | ✓ |
| Wireless Connection | ✓ | ✓ |
| Rogue Access point detector | | ✓ |
| Wi-Fi Direct Logs | | ✓ |
| Wi-Fi Direct Firewall | | ✓ |
| Outgoing data manager | | ✓ |

Table 2 – Research Gap

# 2 OBJECTIVES

## 2.1 Main Objectives

**Objective 1: Implementation of Accidental DLP methodology in Keyboard**

Data Leakage prevention will be implemented with the help of a systemized keyboard which will help to notify the user before transferring any sensitive information.

- Implementing machine learning mechanism to find out the sensitive data in the text.
- Implementing it to a keyboard which will give response in real time.

**Objective 2: Implementing Rogue access point detector**

Implementing a method in mobile phones to detect whether the wireless network is a genuine one or Evil twin/Rogue wireless access point and filtering at the time of connectivity (Rogue wireless network Detection). Validating details from the access points with the help of Machine learning.

**Objective 3: Implementing a Bluetooth Firewall**

- Implanting a firewall in Bluetooth channels which will monitor the incoming traffic for malicious files with the help of Machine learning algorithm.
- Alerting the user for incoming connections and files.
- Validating Bluetooth Address.
- Keeping the logs for all the activities done through Bluetooth channels.

**Objective 4: Implementing Wi-Fi Direct Firewall**

- Implanting a firewall in Wi-Fi direct which will monitor the incoming traffic for malicious files with the help of Machine learning algorithm.
- Keeping the logs for all the activities done through Bluetooth channels.

## 2.2 Specific Objectives

**Objective 5: Ease of use**

The above-mentioned implementation has to be done in the system level itself so as the user experience will be easy.

**Objective 6: Minimum use of available resources.**

Implemented new methodologies are forced to use minimum amount of resources which won't affect the usual system process.

**Objective 7: Analyzation of data**

Intended to analyze most of the currently available malware signatures and behaviors to create a data set which will result in a more optimized output.

**Objective 8: Knowledge acquisition**

As we step into an unknown territory, at the end all the members could gain a full knowledge about android architecture and modern technologies.

# 3 RESEARCH METHODOLOGY

This particular part of our proposal gives out the idea of how we are going to carry out our research. An idea about what are the technologies and tools that we are going to use is also mentioned in this part.

## 3.1 Pre-requirements

We need a set of devices and tools as the pre-requirements in order to carry out our process.

- Machine with Linux or Mac (64-bit environment): - In order to compile Android
- Sandbox: - It needs to be precaution to safeguard the running system from malwares as we have to work with malwares to get data set.
- Machine Running Windows 7 or latest: - To run an emulator
- Android Emulator: - To check for the capabilities and every build should be checked.
- Mobile Phone with Android OS: - To check the customized ROM
- Network Simulator: - In order to create fake access points.

We have planned to get the samples of behavior and signatures from more than 100 malware files in order to create our data set.

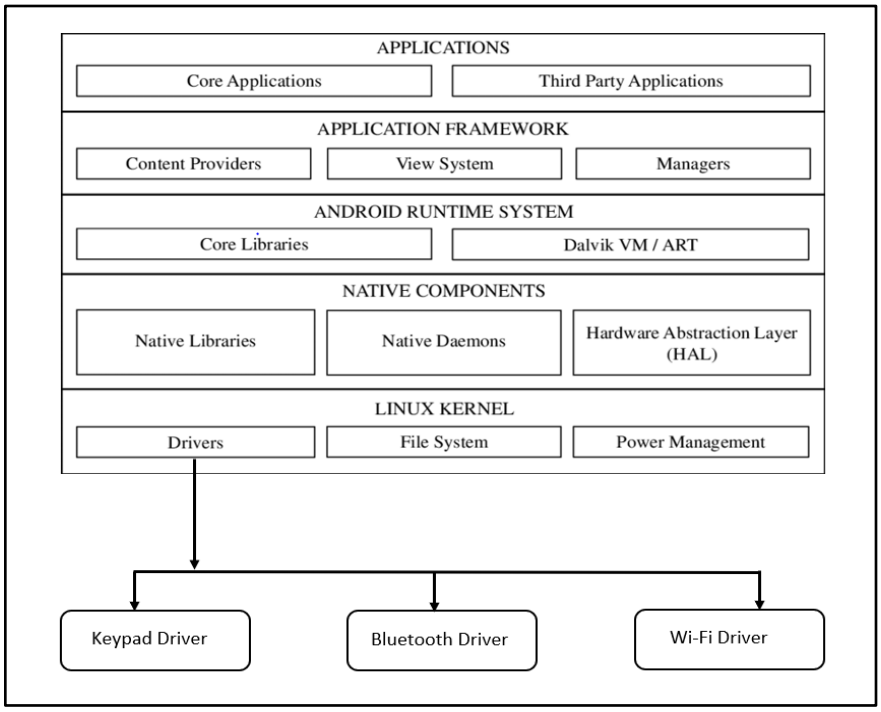


Figure 9 – System Diagram

### 3.2 Research Architecture

I. Create data set for each process.
    a. Data set for Accidental DLP
    b. Data set of Rogue access point/Evil twin access point details.
    c. Data set from samples of malicious files for Bluetooth security
    d. Data set from samples of malicious files for Wi-Fi Direct security
II. Train the ML algorithm.
III. Develop the keyboard to implement trained machine learning algorithm.
IV. Implement detection part for wireless connectivity in order to detect Rogue access points with the help of trained machine learning algorithm.
V. Implement a firewall system for the Bluetooth channel with trained machine learning algorithm to detect malicious files.
VI. Implement a firewall system for the Wi-Fi direct channel with trained machine learning algorithm to detect malicious files.
VII. Configure Implemented firewall to maintain logs.
VIII. Integrate all modules to a customized ROM.

### 3.3 Machine learning Architecture

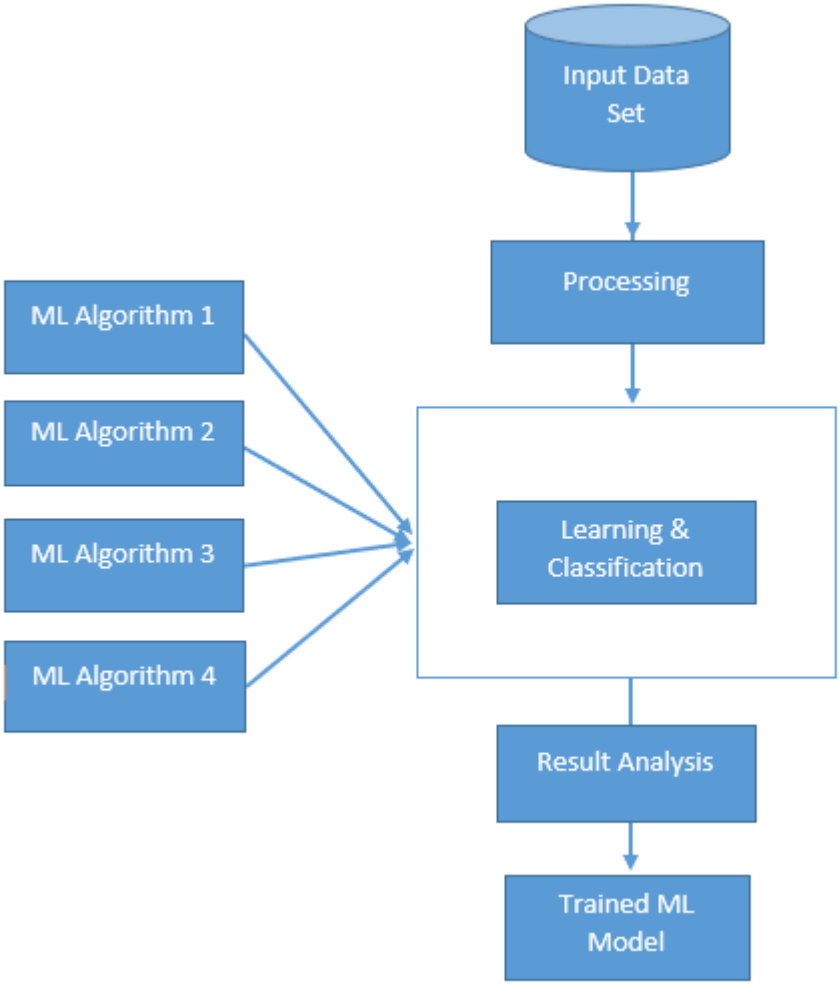


Figure 10 - Machine Learning Architecture

In the Machine learning architecture as the figure depicts, all the finalized data set will be taken to processing state where critical attributes will be assigned for learning process. All processed data will undergo any of four machine learning algorithms (Eg: -Linear Discriminant Analysis, Classification and Regression Trees, K-Nearest Neighbors, Learning Vector Quantization, Support Vector Machines) and the learning outcome will be analyzed in Result analysis phase. In result analysis phase it will be decided whether the outcome is reliable or not and the finally the highest accurate algorithms will be selected to be used in every respective modules. [2]

## 3.4 System Architecture

### I. Accidental data leakage prevention

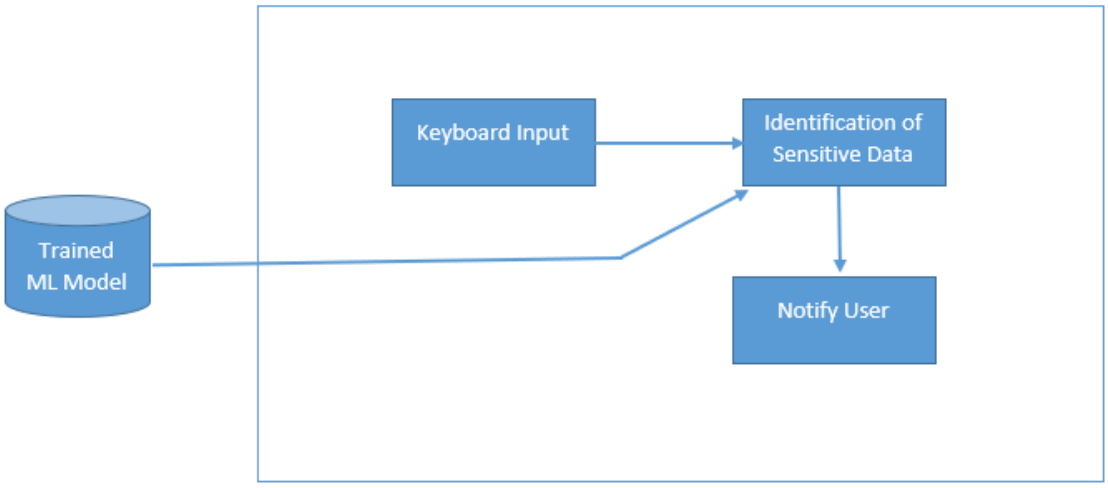


Figure 11 - DLP architecture

Above figure shows the flow of the process of accidental data leakage prevention in keyboard level. As the figure depicts Inputs will be given from keyboard and system will go through the text to find out sensitive details. And if found any, it will notify the user about the sensitive data.

## II. Rogue access point/Evil twin access point detection

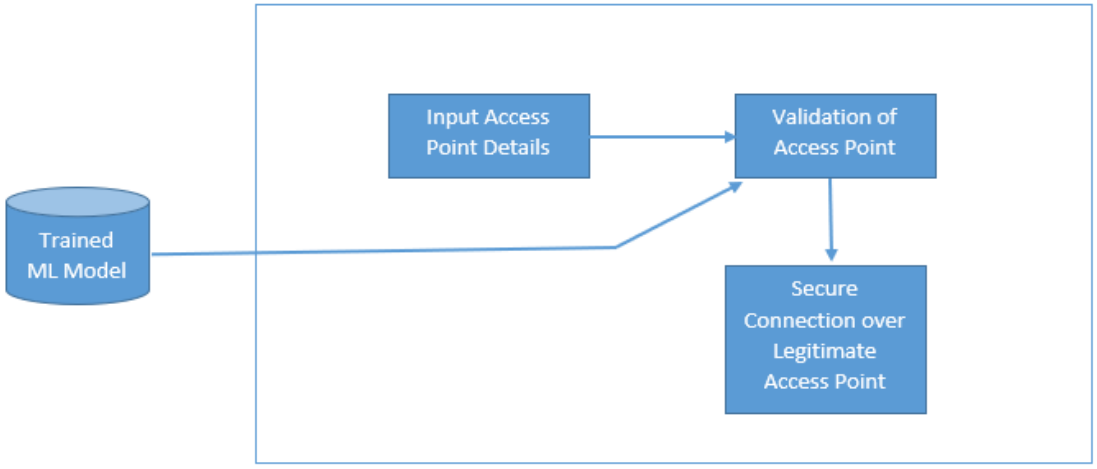


Figure 12 - RAP detection Architecture

In Rogue access point detection process wireless antenna will detect the access point and get the necessary details to make the connection. Those details will be sent to the trained machine learning algorithm in order to verify its legitimacy. If validated, connection is made. If not the connection is refused.

## III. Secure Bluetooth

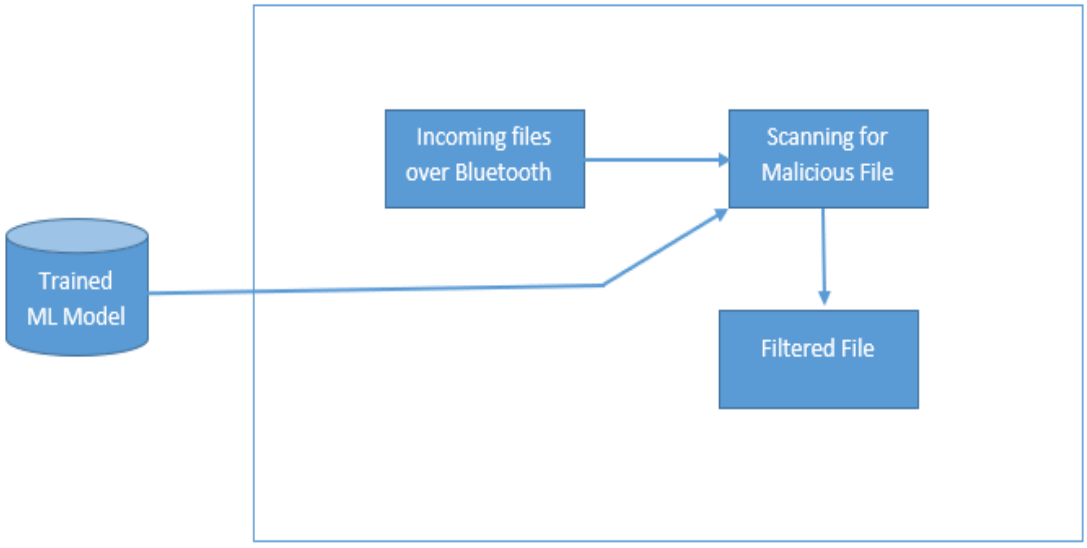


Figure 13 - Secure Bluetooth Architecture

As the image shows incoming files will be sent for scanning. In the scanning process Trained ML Model will check for the malicious files. And if found it will be notified to the user.

## IV. Secure Wi-Fi Direct

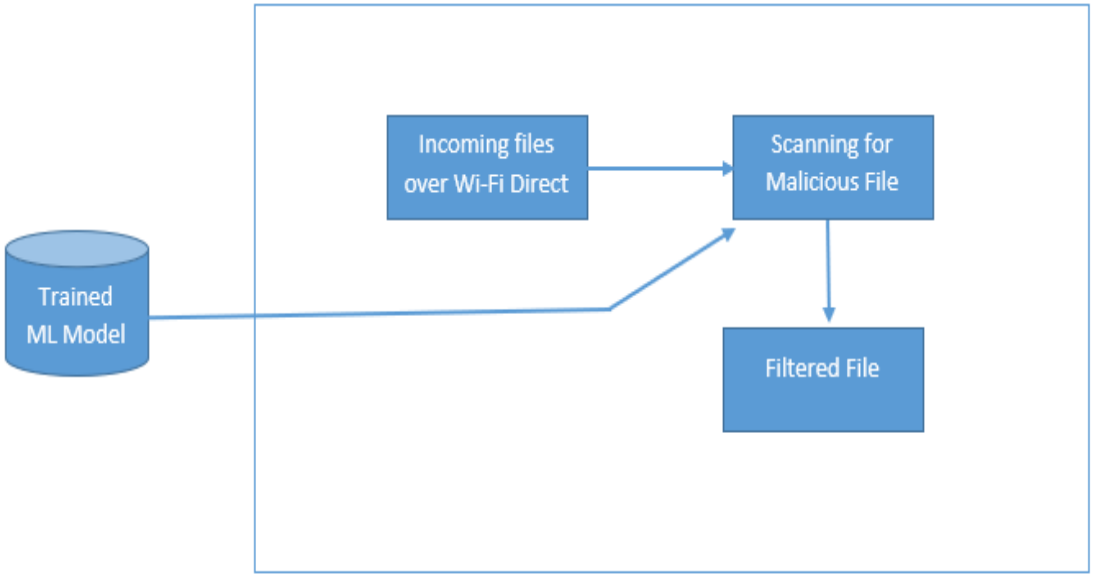


Figure 14 - Secure Wi-Fi direct architecture

As the image depicts incoming files will be sent for scanning. In the scanning process Trained ML Model will check for the malicious files. And if found it will be notified to the user.

# 4 DESCRIPTION OF PERSONAL AND FACILITIES

| Member | Component | Tasks |
|---|---|---|
| Brayan Benett A.S<br>IT 16009400 | Implementing Data Leakage prevention in the Keyboard. | • Collect data set about sensitive Information.<br>• Preprocess the data for Machine learning.<br>• Define an algorithm to use in the final product by learning and classification using multiple machine learning algorithms.<br>• Create optimized Machine Learning Model at the end of Result analysis.<br>• Build a Keyboard with finalized ML model.<br>• Deploy it into the custom ROM.<br>• Build the final version of the custom ROM. |
| Ranjitha L<br>IT 16073399 | Implementing Rogue access point/ Evil twin access point detection in mobile. | • Collect data set about Rogue access points.<br>• Preprocess the data for Machine learning.<br>• Define an algorithm to use in the final product by learning and classification using multiple machine learning algorithms.<br>• Create optimized Machine Learning Model at the end of Result analysis.<br>• Build a RAP detection system with finalized ML model.<br>• Deploy it into the custom ROM. |
| Sam Abisherk R<br>IT 16034396 | Implementation of Bluetooth firewall. | • Collect data set about malware files.<br>• Preprocess the data for Machine learning. |

| | | |
|---|---|---|
| | | • Define an algorithm to use in the final product by learning and classification using multiple machine learning algorithms.<br>• Create optimized Machine Learning Model at the end of Result analysis.<br>• Build a Bluetooth firewall system with finalized ML model.<br>• Configure firewall to maintain Log.<br>• Configure firewall to notify for outgoing data. |
| Vinushanth K<br>IT 16026544 | Implenetation of Wi-Fi Direct firewall. | • Collect data set about malware files.<br>• Preprocess the data for Machine learning.<br>• Define an algorithm to use in the final product by learning and classification using multiple machine learning algorithms.<br>• Create optimized Machine Learning Model at the end of Result analysis.<br>• Build a Wi-Fi Direct firewall system with finalized ML model.<br>• Configure firewall to maintain Log.<br>• Configure firewall to notify for outgoing data |

Table 3 - Description of personal and facilities

# 5 BUDGET

| Description | Estimated Cost (LKR) |
|---|---|
| Windows 10 OS | 7500.00 |
| Android Device | 50000.00 |
| Android Platform | 5000.00 |
| Miscellaneous | 3500.00 |
| Total | 66000.00 |

Table 4 - Budget

# 6 REFERENCES


[1]N. Fearn, "Best data loss prevention service of 2019: Choose the right DLP to protect your assets", *TechRadar*, 2019. [Online]. Available: https://www.techradar.com/best/best-data-loss-prevention-service. [Accessed: 08-Mar- 2019].

[2]J. Le, "A Tour of The Top 10 Algorithms for Machine Learning Newbies", *Towards Data Science*, 2019. [Online]. Available: https://towardsdatascience.com/a-tour-of-the-top-10-algorithms-for-machine-learning-newbies-dde4edffae11. [Accessed: 09-Mar- 2019].

[3] SHIVARAJ, G., SONG, M. AND SHETTY, S. *A Hidden Markov Model Based Approach to Detect Rogue Access Points.*

[4] CANG, C., SONG, Y. AND GU, G. *ACTIVE USER-SIDE EVIL TWIN ACCESS POINT DETECTION USING STATISTICAL TECHNIQUES*

[5]P. Stirparo, J. Loeschner and M. Cattani, *Bluetooth technology: security features, vulnerabilities and attacks*. 2015.

[6]J. Padgette and K. Scarfone, *Guide to Bluetooth Security*. NIST, 2011.

[7]W. Iqbal, F. Kausar and M. Arif, *Attacks on Bluetooth Security Architecture and Its Countermeasures*. 2017.

[8]J. Alfaiate and J. Fonseca, *Bluetooth Security Analysis for Mobile Phones*. 2012.

[9]N. Minar and M. Tarique, *BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY*. 2012.

[10]S. Alneyadi, E. Sithirasenan and V. Muthukkumarasamy, *Detecting data semantic: A data leakage prevention approach*. 2015.

[11]P. Kamakshi and D. Babu, *Automatic Detection of Sensitive Attribute in PPDM*. 2012.

[12]N. Tan Cam, V. Pham and T. Nguyen, *Sensitive data leakage detection in pre-installed applications of custom Android firmware*. 2017.

[13] MUFASA, H. AND XU, W.CETAD: *Detecting Evil Twin Access Point Attacks in Wireless Hotspots*

[14] SHEN, W., YIN, B., COO, X. AND CHENG, Y.*Secure Device-to-Device Communications Over Wi-Fi Direct*

[15] CAMPS-MUR, D., GARCIA- SAAVEDRA, A. AND SERRANO. *Device to Device communication with WiFi Direct:Overview and experimentation*

# 7 APPENDICES

## 7.1 Gantt Chart

## 7.2 Work Breakdown Structure