


# Security Platform for Mobile OS

## Project ID :- 19-001

# Authors

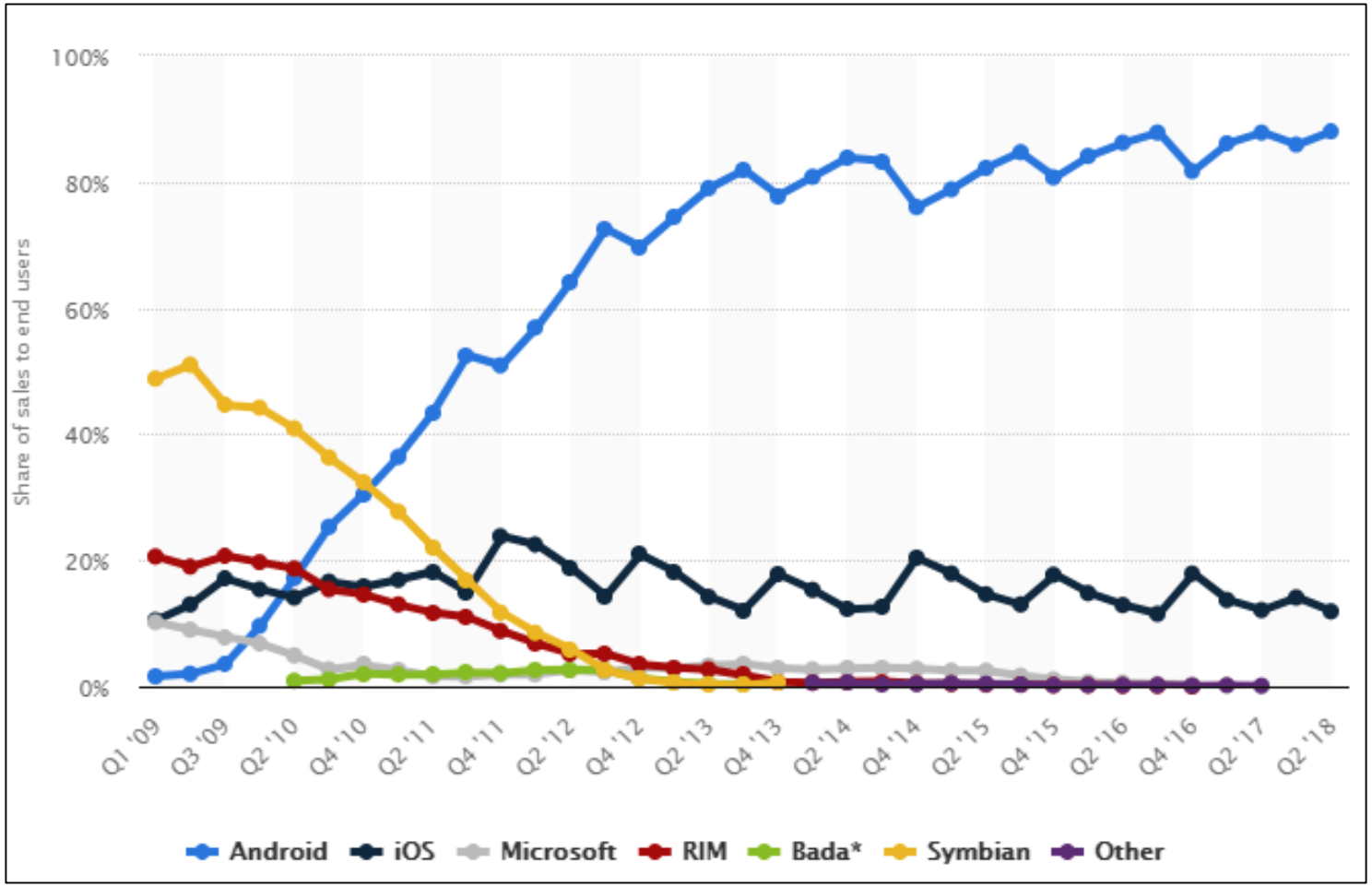
| Student ID | Name |
|---|---|
| **IT16009400** | **Brayan Benett A.S** |
| **IT16026544** | **Vinushanth K** |
| **IT16034396** | **Sam Abisherk R** |
| **IT16073399** | **Ranjitha L** |

Supervisor : Mr. Amila Nuwan Senarathne

Co Supervisor : Mr. Kavinga Yapa Abeywardena

# Introduction

- What are the information that matters?
- Importance of Mobile phones in day today life.
- Kaspersky Labs Statistics.
- Why android?



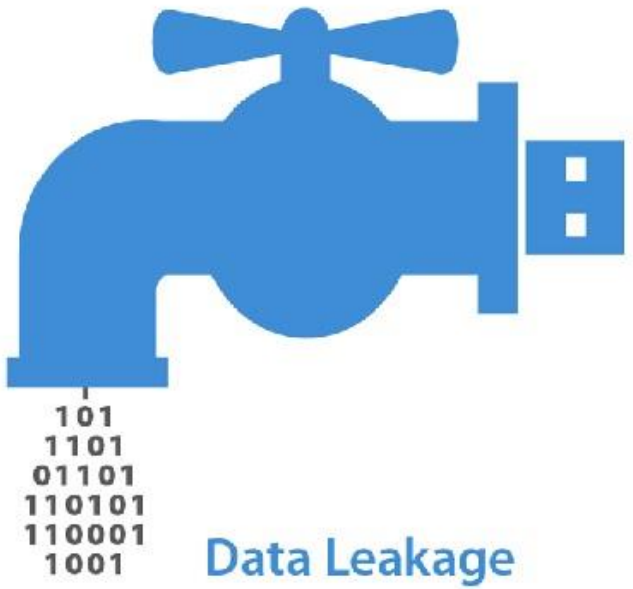

**Global mobile OS market share in sales to end users from 1st quarter 2009 to 2nd quarter 2018 by www.statista.com**

# Research Components.

- Accidental Data Leakage Prevention
- Rogue Access point Detector
- Secure Bluetooth
- Secure Wi-Fi Direct

# Accidental Data Leakage Prevention.

- What is a data leakage?
- How does it affects an Organization?
- How does it affects an Individual?
- What is an accidental Data leakage?

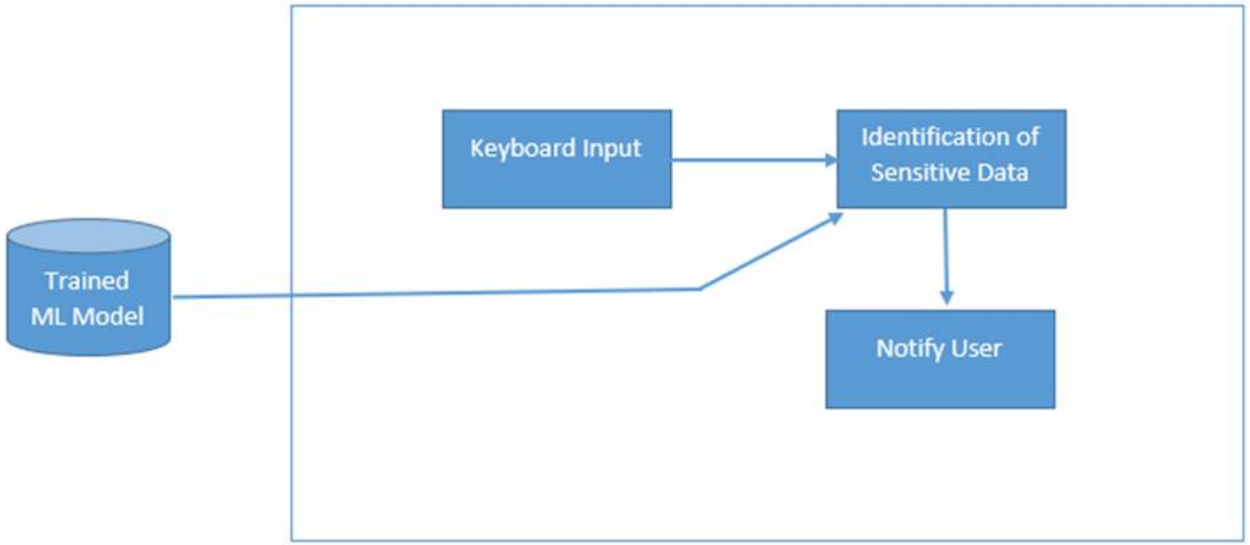


# Existing Security Measures

- Detecting Data semantic: A data leakage prevention approach.
  - Term Frequency-Inverse Document Frequency (TF-IDF) for text mining.
  - Separate details into predefined topics.
  - Secrecy Level.
- Automatic detection of sensitive attribute .
  - Suppress the data by data mining.
  - Query analysis.
- Sensitive data leakage detection in pre-installed applications of custom Android firmware.
  - APK extractor
  - APK analyzer
  - Path matcher

# Proposed Solution.

- Data Leakage prevention in the Keyboard Level.
- Detect sensitive data with the help of Machine Learning.
- Alert the user for possible leakage of sensitive data.



# Rogue Access Point

- What is a Legitimate/Genuine Access Point?
- What is a Rogue Access Point ?
- Who Implements a RAP?
- What are the threats ?

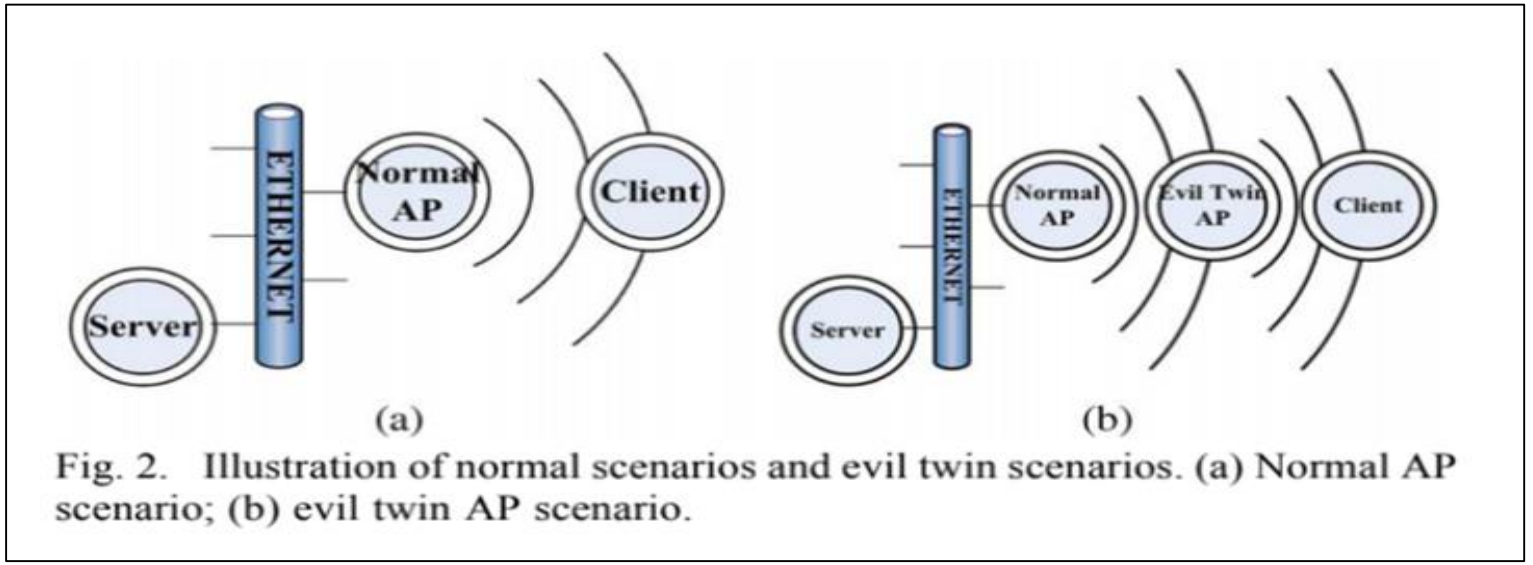



Fig. 2. Illustration of normal scenarios and evil twin scenarios. (a) Normal AP scenario; (b) evil twin AP scenario.

# Existing Security measures.

- **Hidden Markov Model.**
  - Detection in end hosts.
  - Training the model
  - Monitor for Sample packets.

- **Statistical Techniques.**
  - No authorized access list required.
  - Best for those who travel most.Uses Trained Mean Matching(TMM) and Hop Differentiating Technique(HDT).

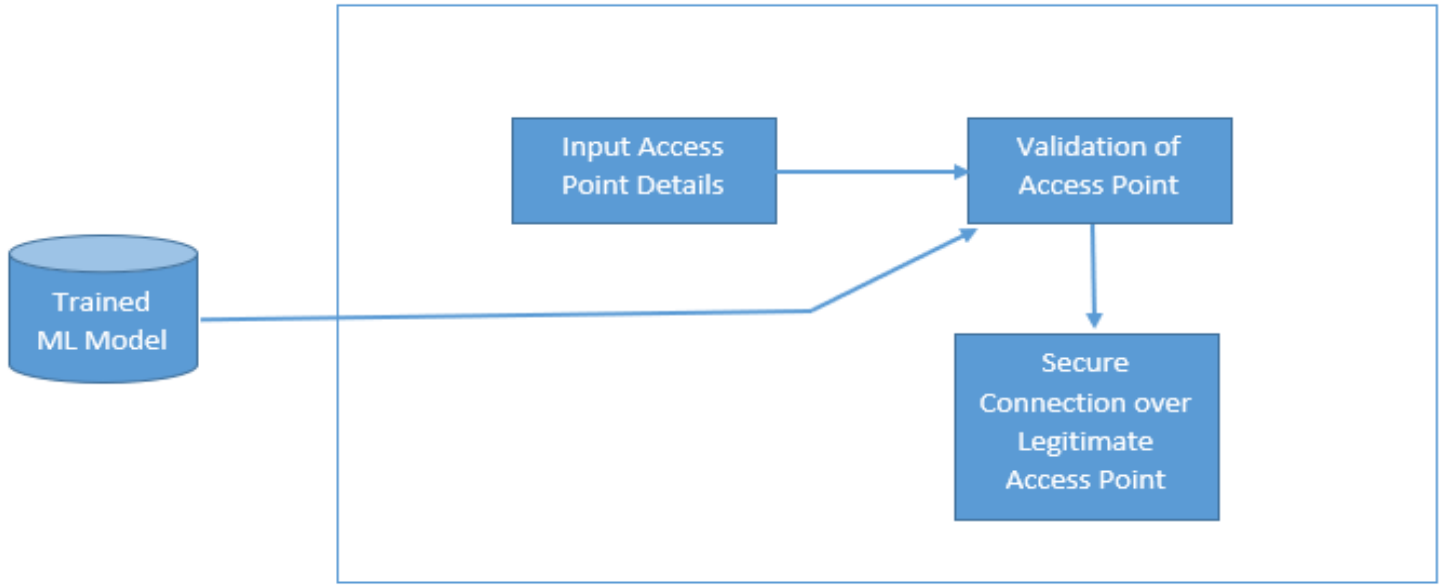
- **CETAD : Detecting Evil Twin Access Point Attacks in Wireless Hotspots**
  - Client end Evil Twin Access point Detector.
  - Compares the legitimate and Rogue AP’s
  - Focuses mainly on data parameters to detect Rogue AP’s

# Research Gap

- Methods implemented already.
- No efficiency.
- No Android mobile platform accompanied detection of RAP.

# Objectives

- Inbuilt RAP detector for mobile phones.
- At the point of connection.
- Validate details with help of machine learning.

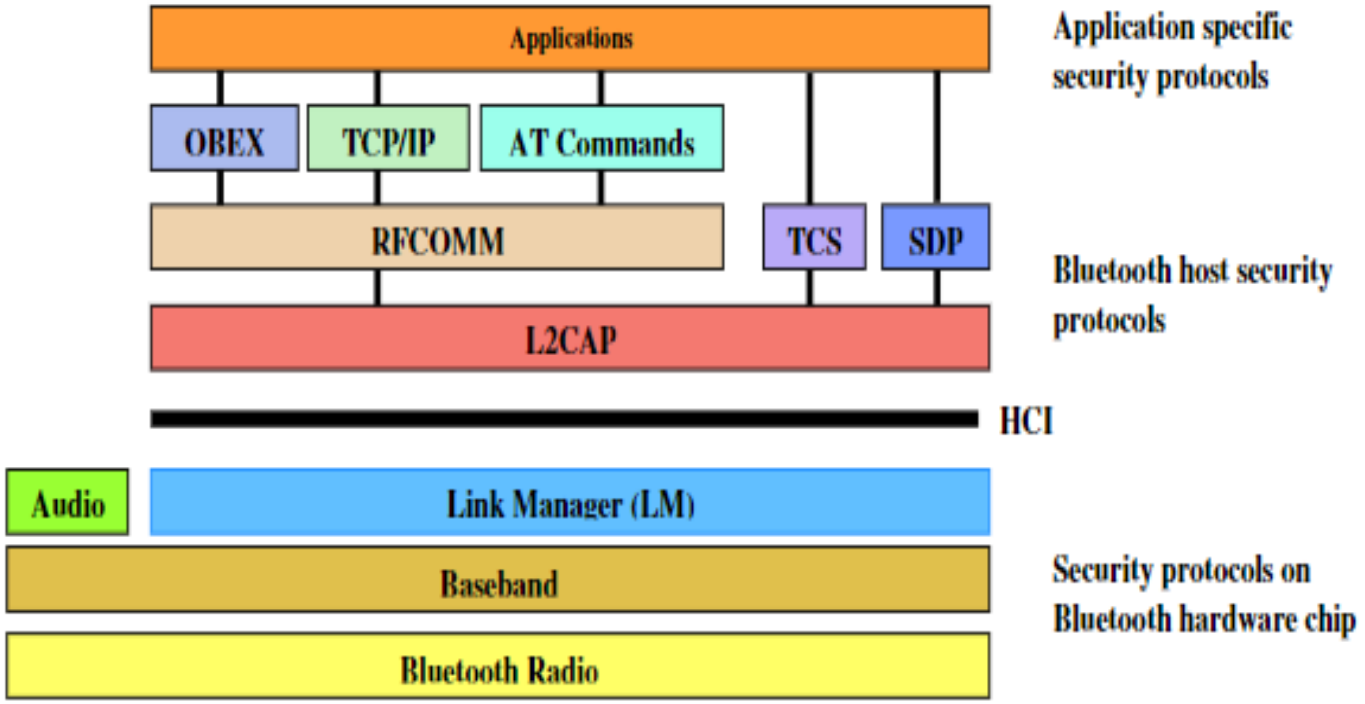


# Secure Bluetooth

- What is Bluetooth?
  - Exchange data between fixed and mobile devices over short distances using radio waves.
  - Bluetooth is a strong, simple and cost-efficient technology
  - Developed by Bluetooth Special Interest Group (SIG).
  - Available in mobile phones, laptops, Speakers/Earphones, Personal Digital Assistant.
  - Bluetooth versions – 1, 1.1, 1.2, 2.0, 2.1, 3.0, 4.0, 4.1, 4.2, and 5

- How Bluetooth works?
  - Using short-range wireless exchange of communication between attached two gadgets together.
  - Uses Frequency Hopping Spread Spectrum (FHSS)

# Currently Available Security Measures




OBEX - Object Exchange Protocol
SDP - Service Discovery Protocol
HCI - Host Controller Interface

Protocol stacks defines the connectivity between devices according to the standards.

# What are the vulnerabilities common to all Bluetooth versions?

| | |
|---|---|
| **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. |
| **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. |
| **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). |
| **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. |
| **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. |
| **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. |
| **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. |

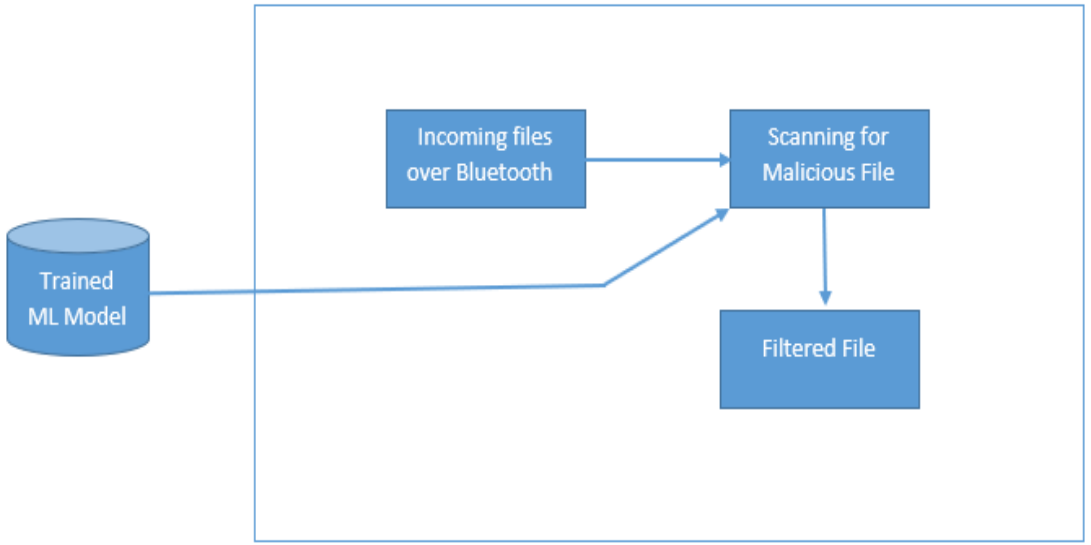
# What are the Threats related to Bluetooth?

- Threats common to wireless connectivity
  - Eavesdropping
  - Denial of service
  - Impersonation
  - Man-in-the-middle

- Specific threats for Bluetooth connectivity
  - Bluesnarfing - Any unauthorized access
  - Bluebugging - Let them listen
  - Bluejacking - Sends fake messages
  - Location tracking - Discover the location
  - Key management - Discovering the unit key

# Proposed Mitigation Techniques

- Implanting a firewall in Bluetooth
  - Collect data set about malware files.
  - Defining machine learning algorithms.



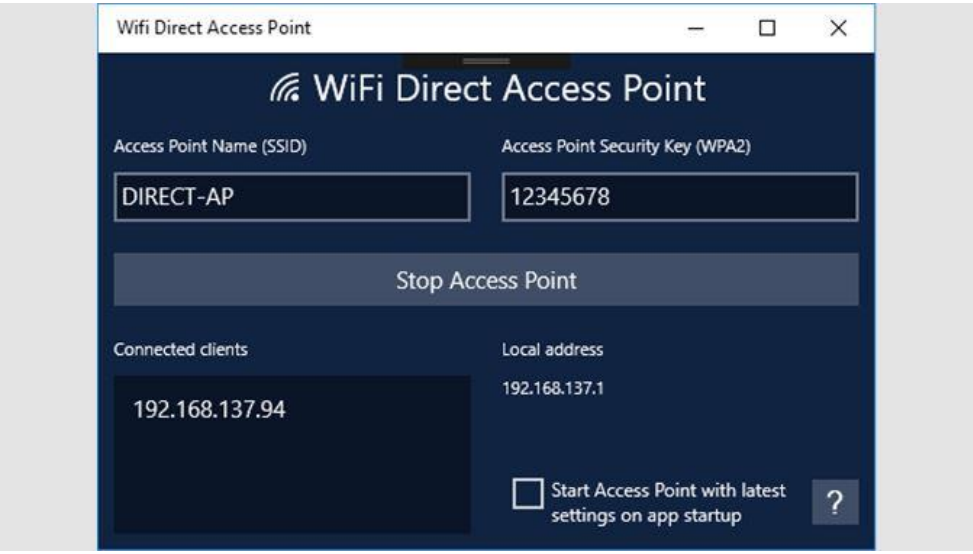
- Monitor the incoming traffic for malicious files
- Alerting the user for Malicious connections and files.
- Securing outgoing files.
- Validating Bluetooth Devices.
  - Defining the Bluetooth Addresses.
- Maintaining the logs for all the activities done through Bluetooth channels.

# Secure Wi-Fi Direct

- What is Wi-Fi Direct?
  - Communication between two devices to transfer file.
  - Works with Peer to Peer technology.

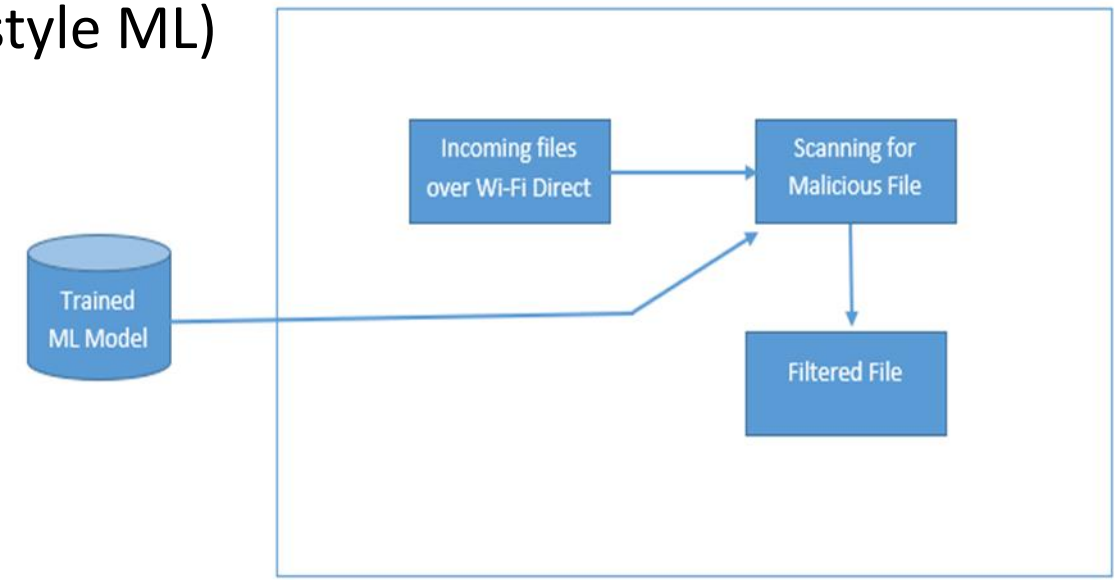
- How Wi-Fi direct establish connection with devices?

- Currently available security measures?
  - SAS(Short Authentication String)
  - WPA 2 (Wi-Fi Protected Access)



- How Wi-Fi direct affects in security of a mobile phone?
  - Accepts any kinds of files without any verification.
  - Two way transaction is possible without any restrictions.

- What we propose to implement in order to secure wi-fi direct
  - Implementing firewall. (behavior style ML)
  - Implement write block.
  - User accessible logs.



# Pre-requirements

- 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.

# Common objectives

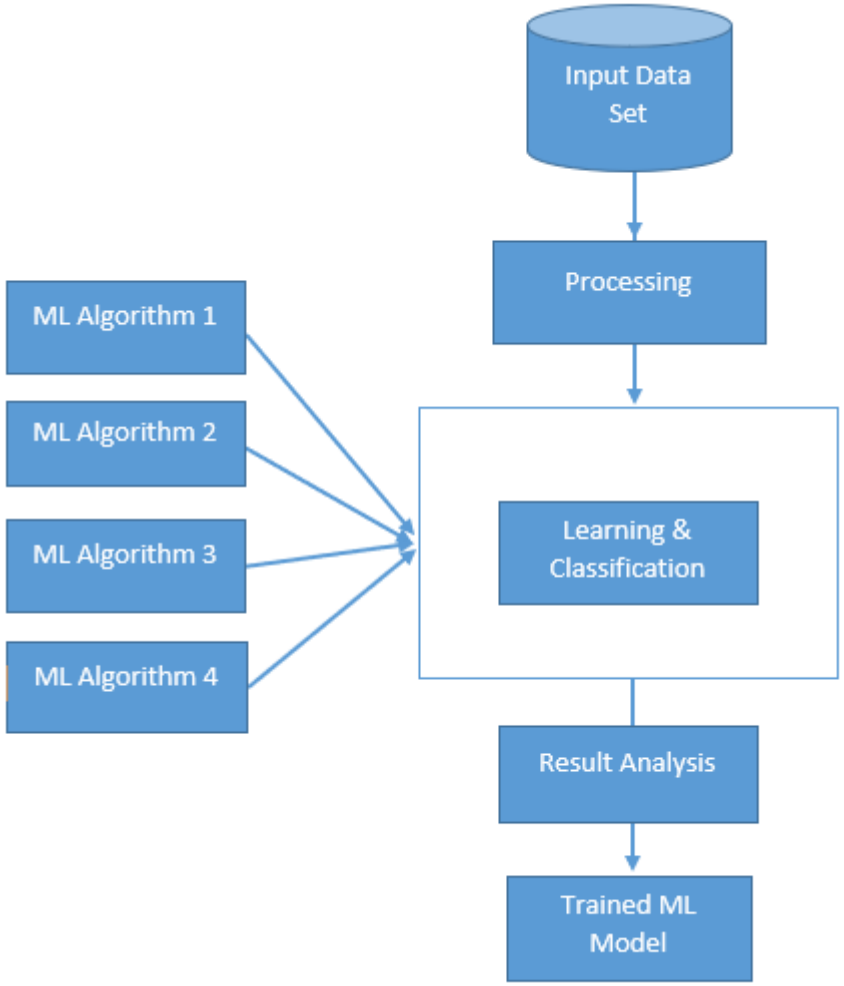
- Ease of use
  - System level architecture to improvise user experiance.
- Minimal use of available resources.
  - New implementations must use minimal amount of resources.
- Analyzation of data
  - Use of available malware signature and behaviour for optimal data set.
- Knowledge acquisition
  - Giving the user full knowledge on the end product.

- Out of the box experience.

- Decrease the requirement of 3rd party apps.

# Machine Learning Architecture.

- Collect Finalized Data Set.
- Preprocess.
- Use of multiple ML algorithms.
    - K-Nearest Neighbors
    - SVM
    - Naïve Bayes
    - Learning vector Quantization
- Result analysis.



| | 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 | | ✔ |

# Q & A

# Thank You