Intrusion Detection, Investigation on Internet of Everything (IOE) Environment Research Project (IDIE)

Dr. Mie Mie Su Thwin
Professor
Head of Cyber Security Research Lab
University of Computer Studies, Yangon
Myanmar

Project Members

Project Leader

- **Dr. Mie Mie Su Thwin**

Project Members

- **Naing Linnn Htun**
- **Cho Cho San**
- **Su Su Win**
- **Ye Myint Thu**
- **Htet Naing Shein**
- **Chan Thar**
- **Phwe Phwe**
- **Nyein Chan Su Lwin**

Background and Target

Our project involves the following:

Network-based Intrusion Detection, Prevention and Monitoring

Vulnerability Assessment

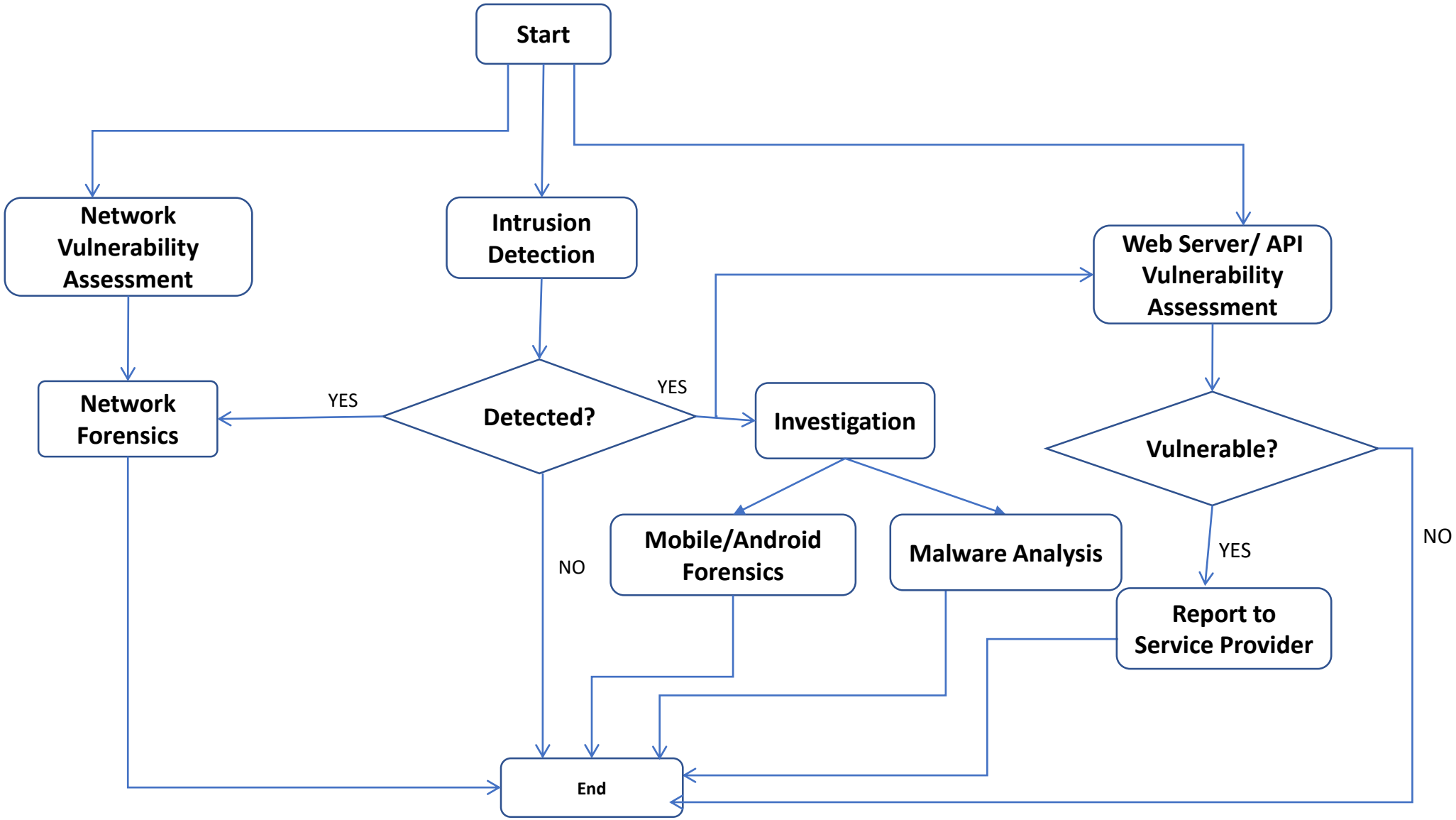
Forensics Investigation

Malicious Software Identification, Warning and Alerting

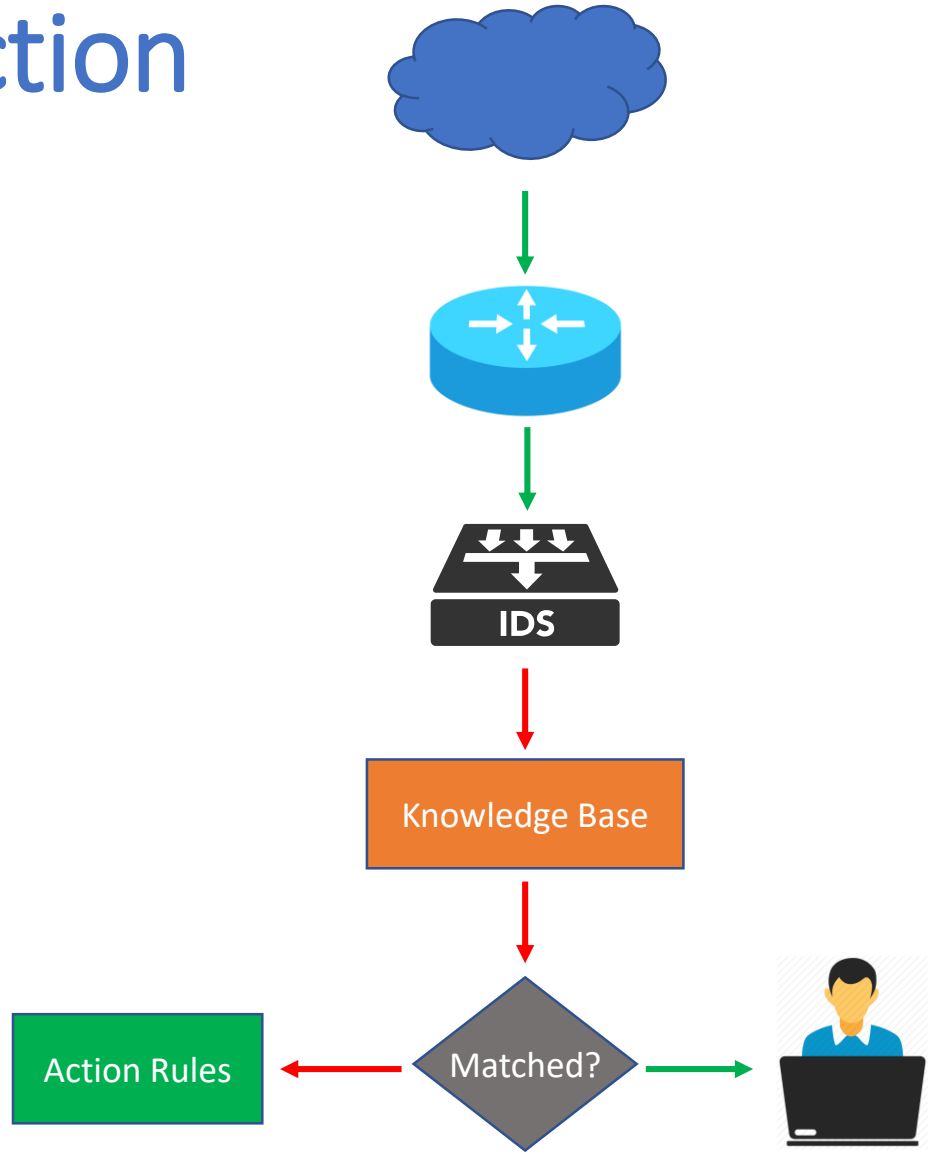
Background and Target (Cont'd)

- A **network intrusion detection system** (NIDS) is crucial for network security because it enables you to detect and respond to malicious traffic.
- The proposed system can evaluate the **risk assessments of the vulnerabilities** which are identified and detected in web server.
- **Forensic investigation** is any kind of science used in the legal or justice system to support and uphold the law. When a crime has been committed and evidence is collected at the scene, investigators analyze and report it to the expert court testimony about their findings and investigated results.
- **Malware analysis and classification** play essential role in cyber crime incident handling systems to identify malicious activities.

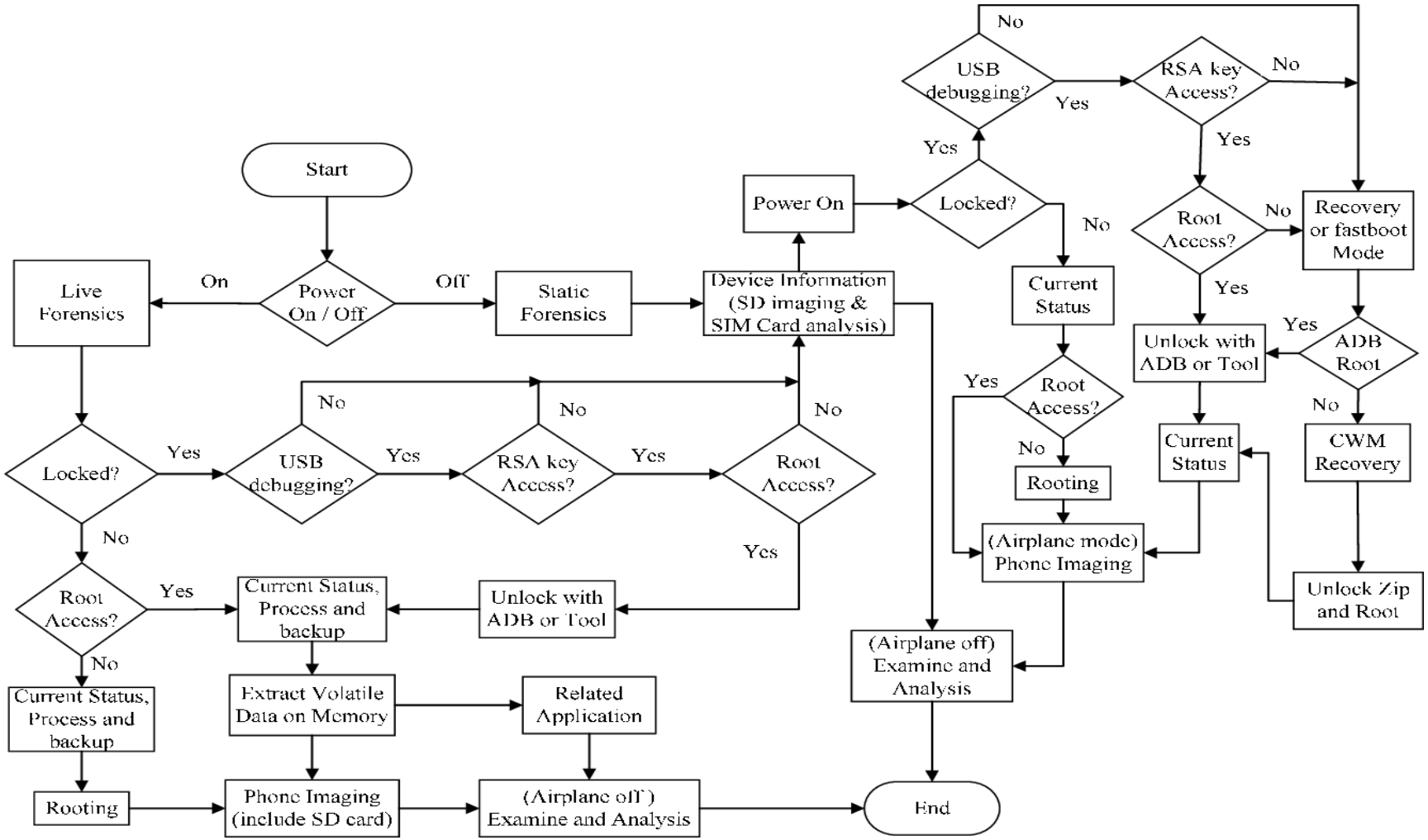
Proposed System Overview



Intrusion Detection



Investigation Smart Phone Forensics (Android)



Modules Explained

Sr. No	Module	Background Method	Reason
1	Network-based Intrusion Detection, Prevention and Monitoring	Artificial Neural Network (ANN)	Flexibility
2	Vulnerability Assessment	Artificial Neural Network (ANN)	
3	Forensics Investigation	Pattern Matching Techniques	
4	Malicious Software Identification, Warning and Alerting	Convolutional Neural Network (CNN)	Great at feature extraction and classification

Impacts of Proposed Method (Cont'd)

Proposed IDIE Framework is

- **Applicable**
- **Simple**
- **Extendable**
- **Generic**
- **Portable**

Solution to all our ASEAN Countries.

Impacts of Proposed Method (Cont'd)

It involves

- **Detecting Intrusions** from **IOE** (Internet of Everything) for more secure smart devices
- **Forensics Analysis** for Investigation Intrusion to support Crime Investigation
- **Identify** the Malware-based Cyber Crime Incidents
- **Creating Safety Environment** for people to use smart devices in the future
- **Minimize the risk** of using smart devices
- **Harden the security** of smart devices of future generations

Impacts of Proposed Method (Cont'd)

- The proposed project is an **important step towards a smart partnership of regional research communities by leveraging on the existing research facilities and laboratories of each participating institution.**
- Our **proposed Project is in need of support from the ASEAN-IVO funding, bringing together researchers in the field of Intrusion Detection and Investigation on IOE system to develop and encourage more research works** with developed and advanced country, **Japan** and other **developed and developing countries of ASEAN.**

Output or Outcome of Proposed method

- **Malware identification, warning, alerting and reporting** about malicious software
- Warning, alerting and reporting the **status of network traffic and application** (Normal or Abnormal)
- **Intrusion, Detection, Prevention, Monitoring And Forensics Investigation** System
- After this process, the final outputs are the **risks assessment**, some examples of infected payloads and vulnerabilities management.

Conclusion

- As technology advances, **everything becomes connected to the Internet**
- As more and more devices are **connected to the Internet, the probability of cyberattacks increases**
- We would like to **present and implement a framework that could detect the cyberattacks, track the attackers and identify the malware that attackers used.**
- Our framework will not only be **useful, it will also be lightweight and portable that general public can use it easily.**