IIT MADRAS
Indian Institute of Technology Madras

Technology Transfer Office
TTO - IPM Cell

Industrial Consultancy & Sponsored Research (IC&SR)

SYSTEM AND METHOD FOR MALWARE DETECTION BY CROSS-DIMENSIONAL BEHAVIOURAL ANALYSIS

IITM Technology Available for Licensing

Problem Statement

- There is a need for **cross dimensional analysis** of malware behaviour since different types of malware have different effects on the **network, OS and hardware components** of a system.
- The present solution employs either software based or hardware based solutions for detection, thus not **utilizing the synergistic benefit** of combining both solutions.
- At present, the malware detection products apply a one-size-fits-all approach to identifying malware, whereas malware classes are different requiring **specialized handling of different classes.**

Technology Category/ Market

Computer Sciences & IT –
Machine Learning, Cyber Security

- **Applications** - BFSI, Aerospace, Defense, Healthcare
- **Market** - The global malware analysis market is growing at a **CAGR of 28.5%** from 2019-26 & projected to reach $24 million by 2026.

Technology

SYSTEM

The system comprises of

1. **Client device**, which may include smartphones, laptops and traditional workstations.
2. A **middle box server** (or the device may also function as a server).
3. **Gateway** (implemented through internet protocol) to connect to the Internet.

The data from the client devices is collected in the following ways:

- The network data is collected by the modules comprising the gateway. Modules which typically form part of the network such as **network protocol analyzer** collects this data from the network.
- The OS data is collected with the help of **data profilers** running in the background.
- The hardware data is collected with the help of **Performance Measurement Units** (PMU), which are already part of the drivers installed along with the system (Diagrammatic representation in **Fig. 4**).

METHOD

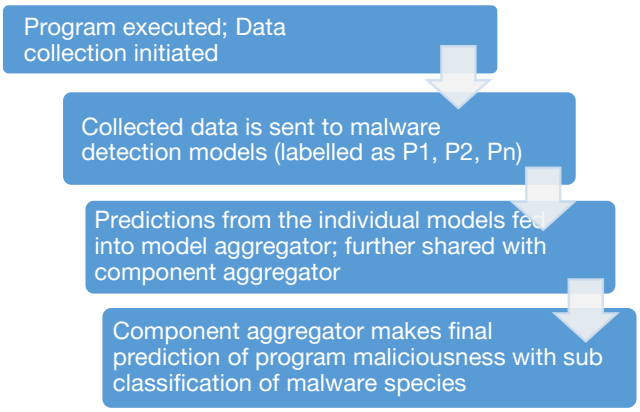


Fig. 1 & 2 further outlines the claimed method

Intellectual Property

- IN202241007976
- IITM IDF Ref. **2305**

Key Features / Value Proposition

- This technology is novel due to the **integrated analysis of network, hardware and OS components** (Fig. 3).
- The usage of model and component aggregators helps achieve an **F1-Score of 1** for most classes.
- Specialized predictors and aggregator functions helps in **better detection** and **user response**, (10% higher accuracy and 89% lower false positives than prior solutions).
- The holistic analysis increases resilience to system noise.

TRL (Technology Readiness Level)

TRL – 4, Technology is at a Proof of concept stage, and early stage validation has been done at laboratory scale.

Research Lab

Prof. Kamakoti Veezhinathan (Director-IITM)
Prof. Chester Rebeiro
Dept. of Computer Science & Engg. , IIT Madras

CONTACT US
Dr. Dara Ajay, Senior Manager
Technology Transfer Office,
IPM Cell- IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: smipm-icsr@icsrpis.iitm.ac.in
sm-marketing@imail.iitm.ac.in
Phone: +91-44-2257 9756/ 9719

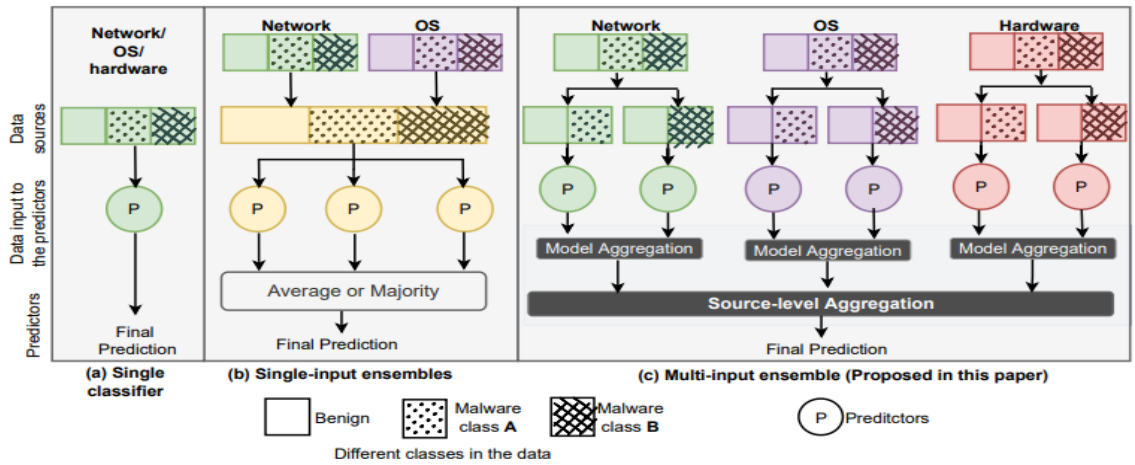


Fig. 1

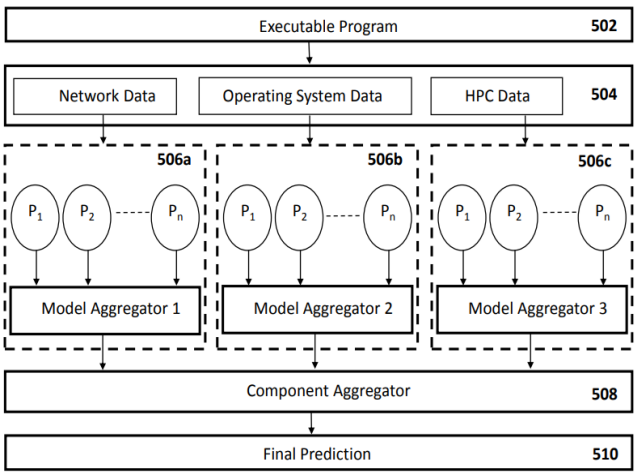
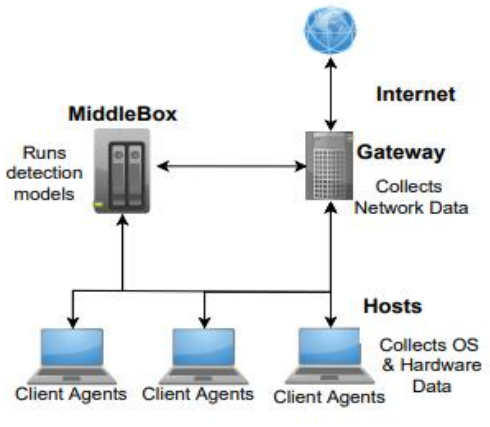


Fig. 2

Antivirus Software	N/OS/H	N+OS	N+OS+H
Huawei CN110874473A	✓		
Kaspersky US2021009406A1		✓	
Mandiant US10027689B1		✓	
Claimed Invention			✓ It performs further sub-classification from data obtained

OS - Operating System, N - Network, H - Hardware

Fig. 3



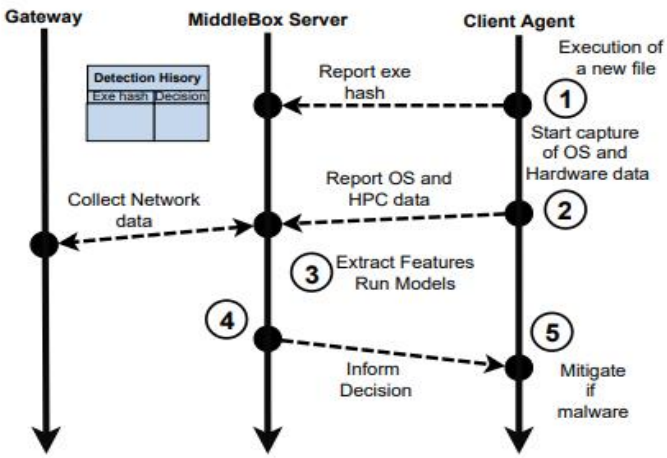


Fig. 4

CONTACT US
Dr. Dara Ajay, Senior Manager
Technology Transfer Office,
IPM Cell- IC&SR, IIT Madras

IITM TTO Website:
https://ipm.icsr.in/ipm/

Email: smipm-icsr@icsrpis.iitm.ac.in
sm-marketing@imail.iitm.ac.in
Phone: +91-44-2257 9756/ 9719