'National Conference on Advancements in Computer Science and Engineering'
International Journal of Scientific Research in Computer Science,
Engineering and Information Technology | ISSN : 2456-3307 (www.ijsrcseit.com)

Highly Secured and Reliable Communication in WSN Using Sandbox Security in Comparison with Network Security Platform

N. Aditya[1], L. C. Dhanush Raaghav[1], Hariprasad G[1], Dr. M. Ayyadurai[2], Dr.R.Pavithra Guru[2]
[1]Student, [2]Assistant Professor
Department of CSE, SRMIST Ramapuram Chennai, Tamil Nadu, India

ABSTRACT

As malware has become more sophisticated, monitoring suspicious malware detection behaviour has become difficult. Recent threats have incorporated advanced obfuscation techniques that can evade being detected by endpoints and network security products. Sandboxing protects the critical infrastructure of the organization from suspicious code as it operates in an isolated and separate environment. It also facilitates information technology organizations in testing malicious code in an isolated testing environment for understanding its working within the system and to detect similar malware attacks more quickly.

Basically, sandboxes are virtualized environments that simulate live systems to ensure that the tested executable runs in way that is almost the same, if not identical, to the real environment.

Keywords: System Sandbox, Operating System Security, Virtualization, Security Policy, Dynamic Analysis, Machine Learning.

I. INTRODUCTION

A sandbox is a security platform for running unknown executables in a dedicated environment without the risk of affecting the production systems. Basically, sandboxes are virtualized environments that simulate live systems to ensure that the tested executable runs in way that is almost the same, if not identical, to the real environment. Sandbox systems allow the monitoring in an isolated environment of suspicious executable files while minimizing the risk of compromising live systems[1]. Another important aspect of sandbox is that it minimizes human efforts in complex tasks like disassembling the executable to understand its purpose. This facilitates security administrator without extensive malware analysis training to perform a triage of suspicious files and only send confirmed malware for analysis.

Although malwares have been around since the early days of computers, the sophistication and innovation of malware has increased over the years. The latest ransomware has drawn attention to the dangers of malicious software, which can cause harm to private users as well as corporations, public services governments, and security institutions. To prevent this, malicious activity must be detected as early as possible, before it conducts its harmful acts which is a tedious task especially when dealing with new and unknown malware capable of virtually emulating entire end- user operating environments, a sandbox safely executes suspicious code so its

output activity can be observed. Early security sandboxes could only scan executable files but advanced platforms are now able to scan Adobe Flash, JavaScript, and Microsoft Office files, among others. Cutting-edge sandboxing solutions today now provide tight integration into the rest of the security infrastructure.

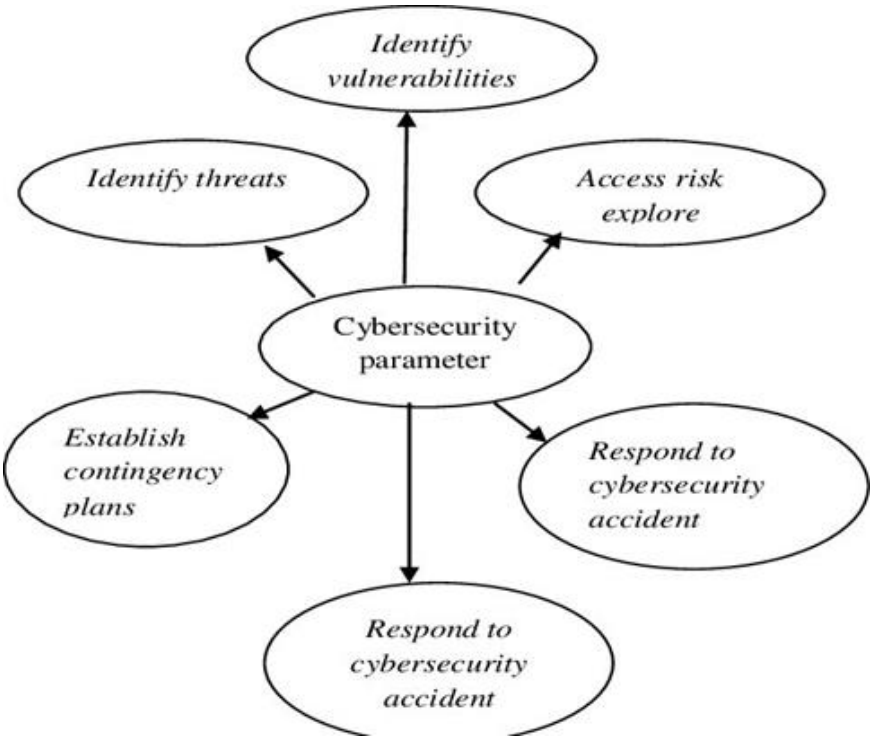

Figure 1: shows the parameters of Cyber Security.[4]

Computer security, cybersecurity, or information technology security is the protection of computer systems and networks from information disclosure, theft of, or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. A sandbox is an isolated testing environment that enables users to run programs or open files without affecting the application, system or platform on which they run.

II. SCOPE OF THE PROJECT

Sandboxes are used to safely execute suspicious code without risking harm to the host device or network. Using a sandbox for advanced malware detection provides another layer of protection against new security threats—zero-day (previously unseen) malware and stealthy attacks.[6]

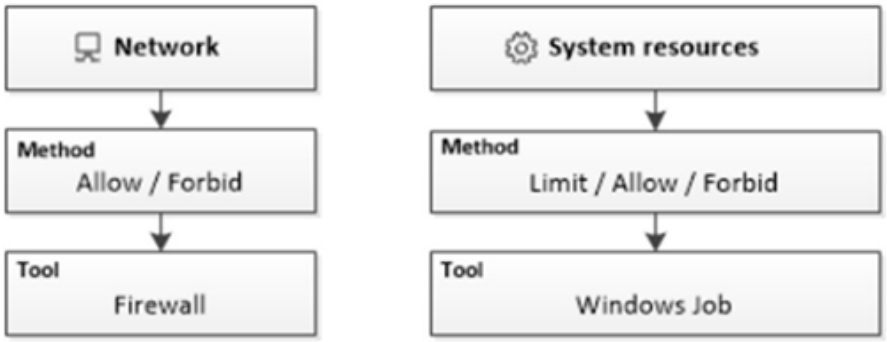

Figure 2: Network isolation, system resource and seEng control [3]

A sandbox is a system for malware detection that runs a suspicious object in a virtual machine (VM) with a fully-featured OS and detects the object's malicious activity by analysing its behaviour. If the object performs malicious actions in a VM, the sandbox detects it as malware.

A sandbox is an isolated testing environment that enables users to run programs or open files without affecting the application, system or platform on which they run. Software developers use sandboxes to test new programming code. Cybersecurity professionals use sandboxes to test potentially malicious software.

Sandboxing is a cybersecurity practice where you run code, observe and analyze and code in a safe, isolated environment on a network that mimics end-user operating environments. Sandboxing is designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code. Sandboxing keeps the code relegated to a test environment so it doesn't infect or cause damage to the host machine or operating system.

As the name suggests, this isolated test environment functions as a kind of "sandbox," where you can play with different variables and see how the program works. This is also a safe space, where if something goes wrong, it can't actively harm your host devices.

III. EXISTING SYSTEM

Computer security is the protection that is set up for computer systems and keeps critical information from unauthorized access, theft, or misuse. There are various practices in place that are widely in use, mainly for the protection of computer systems and networks and preventing potential malicious activities. Sandboxing is designed to prevent threats from getting on the network and is frequently used to inspect untested or untrusted code.

Antivirus software, firewalls as well as other technological solutions helps in the protection of computer networks and confidential information. Despite the fact that they help in the protection of online users and computer systems, it still poses serious threats to the users and organizations of such systems. Many organizations need to enhance their network infrastructure to ensure that they continue to protect computer systems and network to accomplish the main objective of enhancing network security

IV. PROPOSED SYSTEM

In computer security, a sandbox is a security mechanism for separating running programs, usually to mitigate system failures and/or software vulnerabilities from spreading. The isolation metaphor is taken from the idea of children who do not play well together, so each is given their own sandbox to play in alone. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users, or websites, without risking harm to the host machine or operating system [5]. A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as storage and memory scratch space. Network access, the ability to inspect the host system, or read from input devices are usually disallowed or heavily restricted.

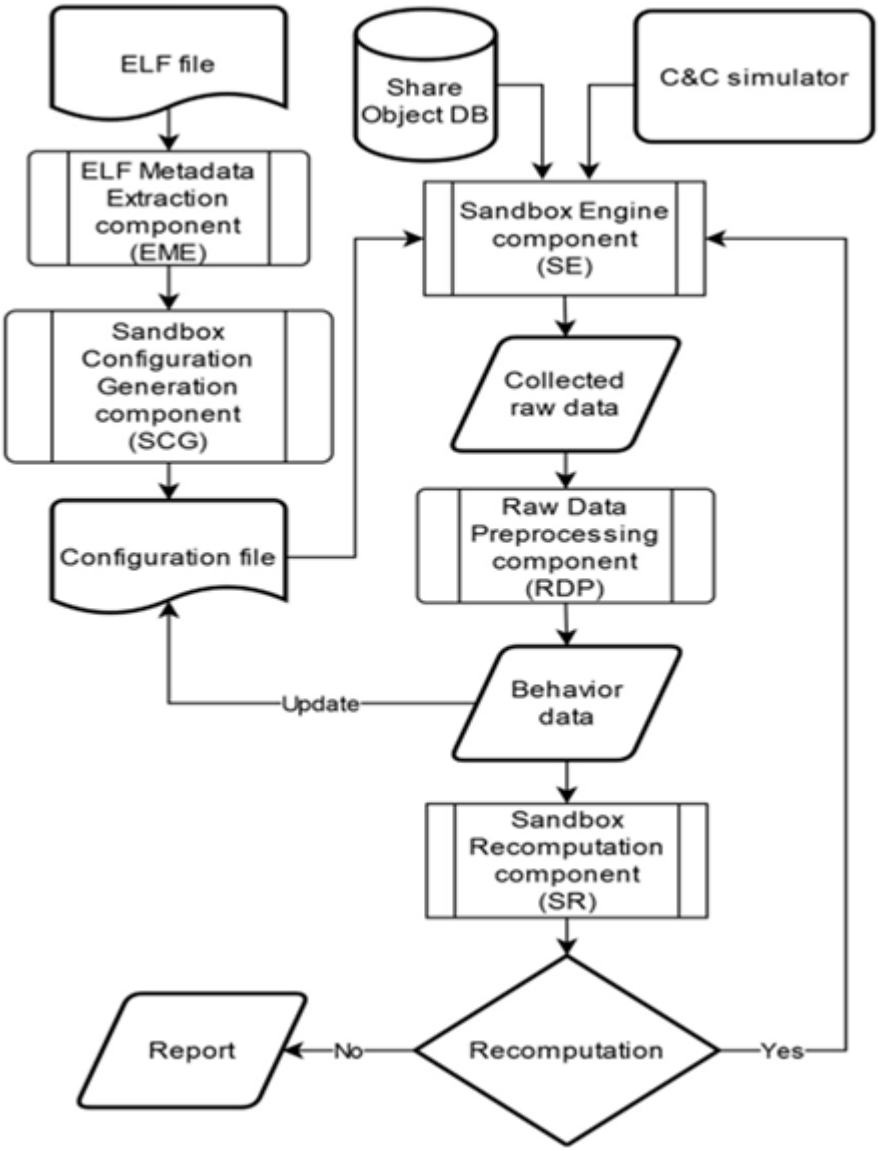

Figure 3: The general architecture of V-Sandbox[2]

The proposed system is completely a Machine learning model. The main tools used in this project are Anaconda prompt, Visual studio, Kaggle data sets, Jupyter Notebook and the language used to execute the process in Python. The above- mentioned tools are available for free and technical skills required to use this tools are practicable. From this we can conclude that the project is technically feasible.

V. ADVANTAGES

- Does not risk your host devices or operating systems.
- Evaluate potentially malicious software for threats.
- Test software changes before they go live.
- Quarantine zero-day threats.
- Complement other security strategies.

VI. CONCLUSION

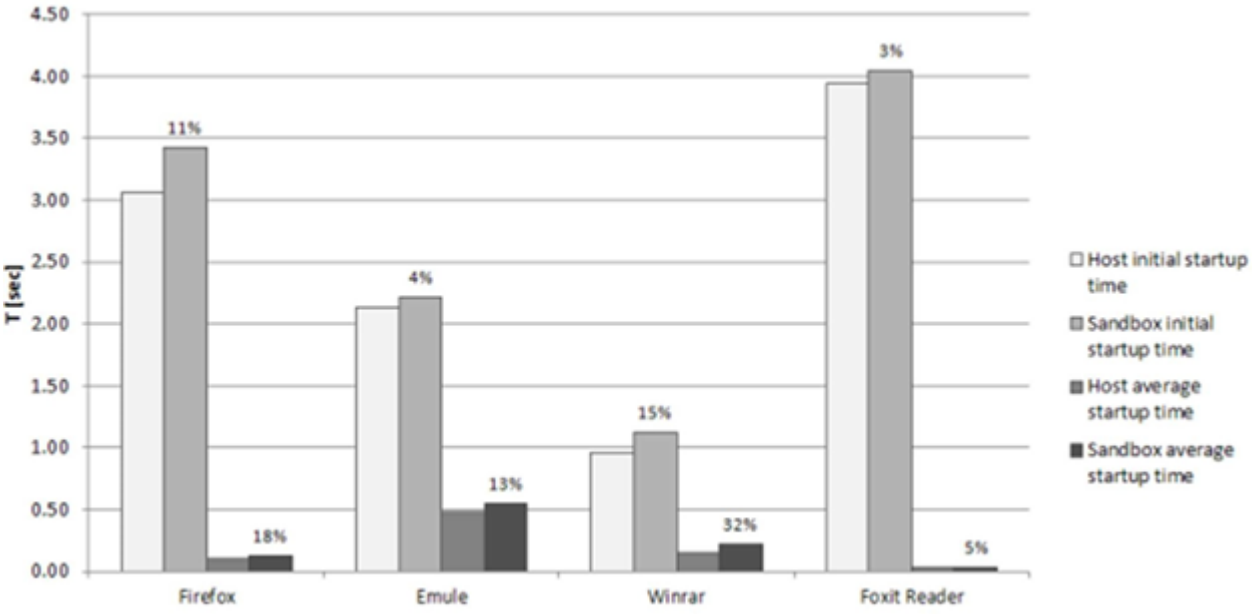

Figure 4: Initial and subsequent startup times of the programs in the sandbox[3]

Like a development testing environment, a sandbox can be used to run any application on a safe resource before deploying it to production or giving it access to production resources. A sandbox lets organizations run programs that could potentially cause issues, whether from malware or unintended software flaws, without bogging down or damaging business- critical resources. A sandbox is often used as quarantine for unknown email and attachments. Email filters will detect potential malicious email messages and attachments, but an administrator needs a safe place to view them to detect false positives. Malicious documents may contain macros that exploit flaws in popular productivity apps such as Microsoft Office. An administrator can use a sandbox virtual machine to open attachments and view the macros to see whether they're safe.

For organizations that do not have specialized cybersecurity staff, a sandbox can be used by any employee to isolate suspicious programs. A sandbox can let workers run unknown code without exposing their systems to new threats.

VII. FUTURE ENHANCEMENTS

A custom OS or custom Rom can be used to enhance the user interface.

As for the future, much more advanced security updates will be provided monthly which will be released under maintenance.

In the proposed idea, the system won't be affected in any sorts of way as the testing occurs completely in an isolated environment.

VIII. REFERENCES

[1]. Jonathan Aldrich , William L. Scherlis , Lujo Bauer Bruno Amizic , A Theory and Tools for Applying Sandboxes Effectively 2016.

[2]. HAI-VIET LE 1,2 AND QUOC-DUNG NGO 3 1 Institute of Information Technology, Vietnam Academy of Science and Technology, Hanoi

[3]. Liberios Vokorokos, Anton Baláž, Branislav Madoš Department of Computers and Informatics, Faculty of Electrical Engineering and Informatics, Technical University of Košice

[4]. Michael Maass, Adam Sales, Benjamin Chung, A systematic analysis of the science of sandboxing 2016.

[5]. F-Secure,Practical malware analysis based on sandboxing 2014.

[6]. Dr.Stevens, A Survey on Application Sandboxing Techniques 2017.