Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

# Making Layered Security through a Sand box Model

**Priti Saxena[1], Dr. R. B. Patel[2]**

[1]PhD Research Scholar Veer Madho Singh Bhandari Uttarakhand Technical University Dehradun, India, pritisaxena82@gmail.com

[2]PhD Supervisor - Professor and HOD Computer Science and Engineering, Chandigarh College of Engineering and Technology, Sector 26, Chandigarh, India, drpatelrb@gmail.com

***Article Info***
***Page Number: 9166 – 9172***
***Publication Issue:***
***Vol 71 No. 4 (2022)***

***Article History***
***Article Received****: 15 September 2022*
***Revised****: 25 October 2022*
***Accepted****: 14 November 2022*
***Publication****: 21 December 2022*

***Abstract***

Sandboxing keeps the script isolated inside a test environment and prevents it from contaminating or negatively impacting the operating system or host device. As the name indicates, this limited testing environment functions as a kind of "sandbox," enabling you to experiment with different elements to understand how the system functions. Additionally, it is a secure setting in which everything that goes wrong could not have an adverse effect on your host devices. Internet usage has completely changed the banking industry in the modern era. At all three levels, financial industries are currently subject to a variety of threats. It is the authentication and access control problems on the client and server sides. Additionally, one of the main issues of flooding attacks is DDOS. The issue is network congestion in the communication channel. A cybersecurity approach called sandboxing involves running code on a system that simulates end-user working settings, analyzing it, and coding in a secure, enclosed environment. It is frequently used to examine unidentified or insecure code with the purpose of preventing the potential threat from accessing the network. This article's goal is to propose an idea for creating a sandbox security policy for banking servers utilizing IP addresses. It offers a defense against DDOS and ARF spoofing.

## INTRODUCTION

Sandboxing is a cybersecurity strategy in order to execute, monitor, and evaluate code in a safe, isolated environment on a network that simulates end-user operating systems. Sandboxing is often utilized to examine untrusted or untested programs and avoid threats from accessing the network. Sandboxing keeps the code limited to a test environment to avoid infection or harm to the host machine or operating system. As the name indicates, this closed-off testing environment acts as a

kind of "sandbox," allowing you to experiment with different settings and see how the software responds. Furthermore, any errors won't actively harm your host devices in this secure environment. All transactions take place through the sandbox, whether they are bank-to-client or client-to-bank. The sandbox functions similarly to an onion browser, changing its IP after a few minutes or at the user's request. The IP changes in the planned work after each transaction. After every 10 minutes, the MAC changes. The data packet received by the sandbox is transmitted with a new IP address, the sandbox's Mac address, and the transaction ID after the network information has been removed. Data is sent to the correct bank account with the aid of Transmission ID. The issue of resource management and allocation is resolved in this way.

## LITERATURE REVIEW

One of the works done in 1989 focused on the technical details of the connection control ISDN access protocols. The future work required the protocol for direct extension and packet bearer services [6]. A protocol that enables a wireless access system to multiplex the system information, alerting, and priority access protocol is defined in 1996 [7]. In 2012, the authors have suggested the need for energy-efficient protocols. According to them, idle listening is the main energy loss in the majority of the MAC protocols. They have proposed a TAD-MAC protocol. It is dependent on the traffic status register bank's wake-up interval. The performance of non-dynamic protocols degraded significantly in terms of energy consumption, quality of service, and latency; thus, change is essential [8]. Presenting a unifying paradigm for the synthesis of continuous time-based linear and non-linear state-dependent consensus network protocols [9]. As preliminary research, the authors in [10] have focused on the conditions of the dynamics of agents and network topology to guarantee the presence of limited data rate inter-agent control and communication protocol. They faced the problem of packet droplets and communication delays. The present paperwork finds out the solution to the problem. To differentiate between execution nodes and consensus nodes, Jian and his fellow members have designed a novel model for smart contract execution. But they faced the limitations of alleviation of denial-of-service assaults, rather than completely eliminating them and the second is the change in the coding paradigm [11]. Some of the papers worked on finding the traces in the executed code when the scanner carries out the attacks. The main challenge was the identification of the traces of the exploited vulnerabilities [12]. One more study done in 2010 was based on the public key and certificate concept to provide a solution for user-centric security identity management which accommodates resources and users' security requirements such as authentication and authorization, but it failed due to a lack of prior experience in computational grid

experience [13]. A sandbox panda model was created to provide scalability to commercial banks [14]. After a study, it is seen that HTTP provides an "end-to-end security" solution that protects from a MitM attack but doesn't provide protection against it. It was observed that current sandbox technologies fail to identify bots [15]. A new authentication scheme was introduced in 2017, wherein, the authors have analyzed the security of a smart grid that influences infrastructural help to attain fine-grained power consumption monitoring in an effort to provide improved efficacy and security, but it needs the use of the anonymizing network to avoid the message source identification [16].

## METHODOLOGY

All of these gadgets, including smartphones, are hampered by issues with processing speed and storage capacity. The amount of computing and storage space required to implement a payment protocol is thought to be minimal for devices with limited resources. When certificates are revoked, stored, and distributed, PKI incurs significant communication and storage costs. Therefore, there is a contradiction between PKI and mobile smart devices. To counteract the server-side assaults that are carried out during online transactions, numerous alternative methods and protocols have been created. Reserve Bank of India (RBI) has continually worked to increase the security of internet banking transactions. It is usually preferable to take preventative steps or incorporate security features during the analysis phase to lower post-attack costs. A security policy is therefore introduced as a result.

## OVERALL WORKING MODEL

A sandbox security policy is suggested to address these impacts and provide the aforementioned benefits at the server level while preventing server-side attacks. All transactions take place through the sandbox, whether they are bank-to-client or client-to-bank. The sandbox functions similarly to an onion browser, changing its IP after a few minutes or at the user's request. The IP changes in the planned work after each transaction. After every 10 minutes, the MAC changes. The data packet received by the sandbox is transmitted with a new IP address, the sandbox's Mac address, and the transaction ID after the network information has been removed. Data is sent to the correct bank account with the aid of Transmission ID. The issue of resource management and allocation is resolved in this way. Additionally, it maintains a barrier between the host and the transactions.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows the Classification Model for execution process of the sandboxed application. In Figure 2, we explain the problem statement of the model. Figure 3 covered the predictive model in the case of the separation of voices from the cocktail party problem. Figure 4 is described the enhancement model. While Figure 5 shows the results and outcomes.

## PRACTICAL IMPLEMENTATION OF THE MODEL

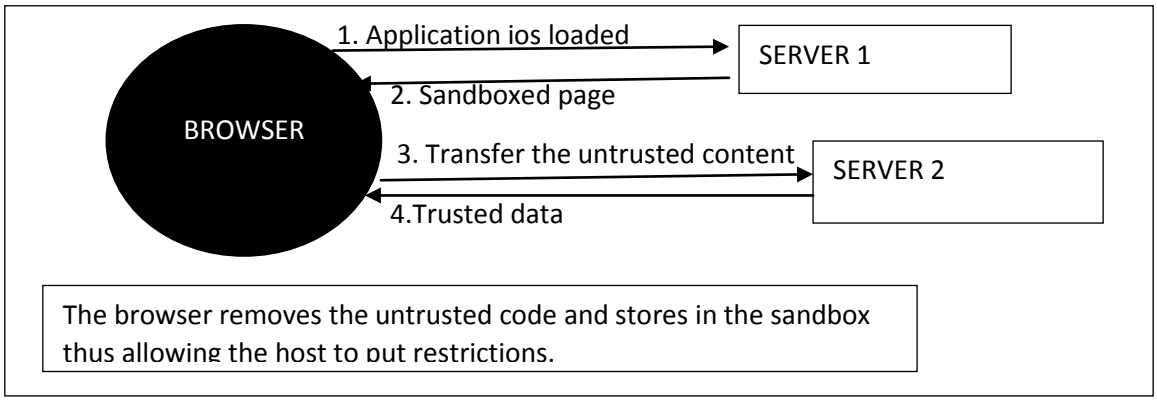


Figure 1: Overall Process of Banking Server with Sandboxing

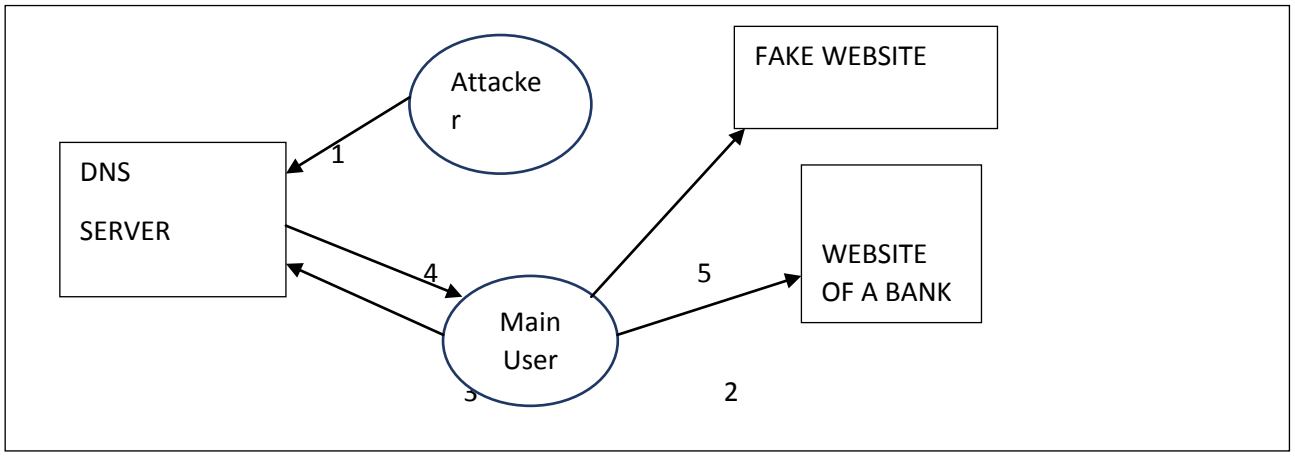


Figure 2: Problem Statement

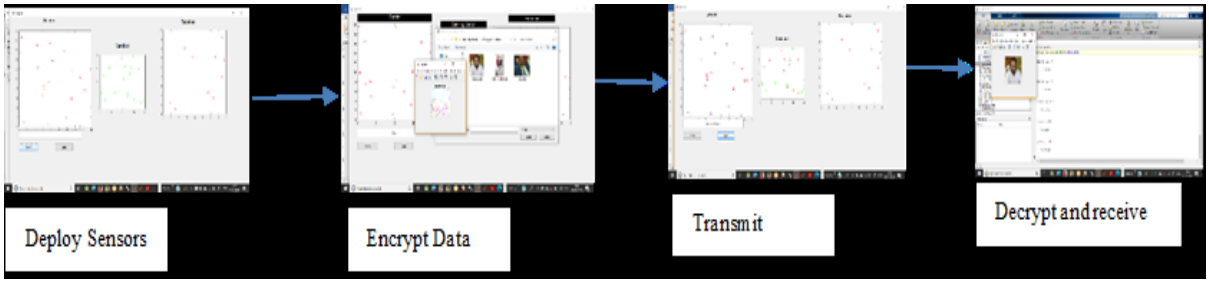


Figure 3: Proposed Model

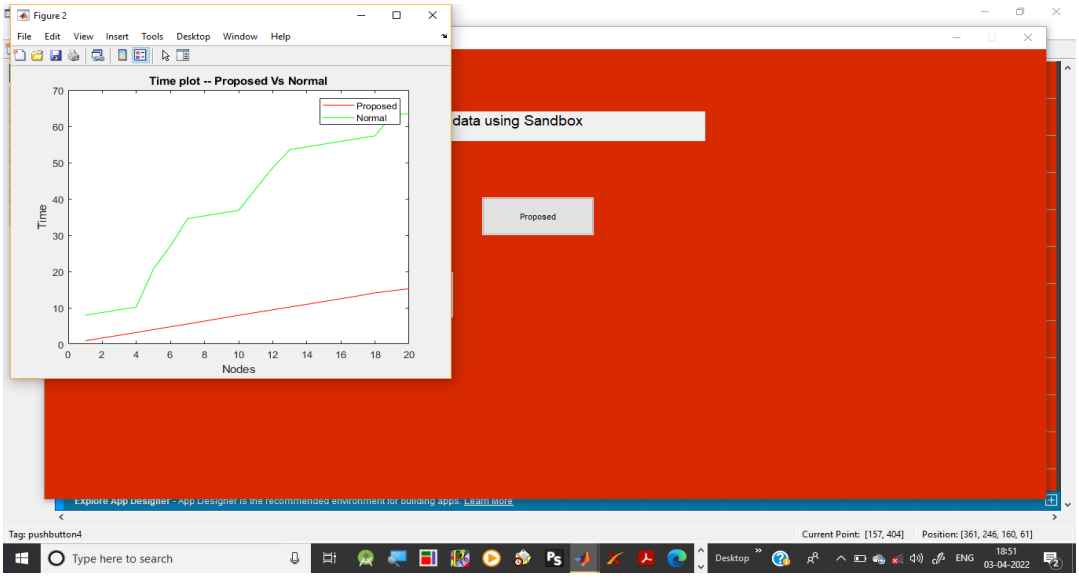


Figure 4: Predictive Model for Proposed Approach with Outcomes

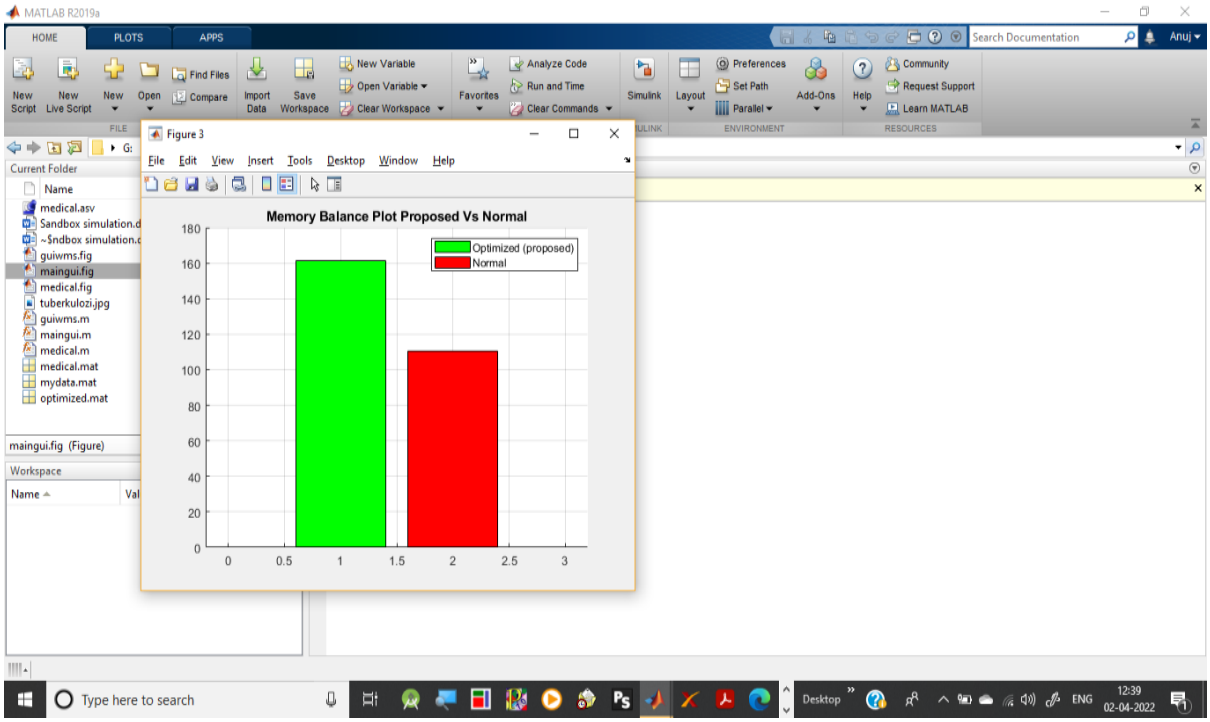


Figure 5: Outcome or Result

## CONCLUSION

The proposed SBSSB model secures the banking servers without compromising on speed and bandwidth. The Proposed model SBSSB reduces the transaction time by 70% over the traditional systems. The unique sandbox model which changes its IP address and MAC address frequently enables it to avoid DBS server spoofing, ARP spoofing, and IP address spoofing. The proposed

model SBSSB is not vulnerable to known attacks. A cybersecurity approach called sandboxing involves running code on a system that simulates end-user working settings, analyzing it, and coding in a secure, enclosed environment. It is frequently used to examine unidentified or insecure code with the purpose of preventing the potential threat from accessing the network. This article's goal is to propose an idea for creating a sandbox security policy for banking servers utilizing IP addresses. It offers a defense against DDOS and ARF spoofing.

**REFERENCES**

[1] T. de Coatpont, Cybercriminals are increasing their attacks on smartphones, easy data-rich targets, http://www.firstpost.com/ tech/news analysis/cybercriminals-are-increasing-their-attacks-on-smartphones-easy data- rich-targets-3698697. html, 2017.

[2] Mobile Top 10 Security Threat Risk, www.owasp.org/index.php/ Mobile_Top_10_2016-Top_10, 2021.

[3] Kai Qian, Reza M. Parizi, Dan Lo, OWASP Risk Analysis Driven Security Requirements Specification for Secure Android Mobile Software Development, College of Computing and Software Engineering, Kennesaw State University, Marietta, GA, USA, IEEE, 2018.

[4]Internet live stats, Total number of websites, https://www.internetlivestats.com/total-number-of-websites/.March 2012.

[5]K.Ryan,Patched zoom exploit:Altering camera settings via remote SQL injection, https://medium.com/@keegan.ryan/patched-zoom_exploit-altering-camera-settings-via-remote-sql-injection-4fdf3de8a0d, June 2020.

[6]Wendy M. Harman and Cheryl F. Newman, ISDN Protocols for Connection Control, IEEE Journal on Selected Areas in communications, vol. 7, no. 7. September 1989.

[7] Vijay K. Varma, Anthony R.Noerpel, Integrated Alerting and System Broadcast Channel for a Wireless Access System, IEEE TRANSACTIONS on vehicular technology, vol. 45, no. 1, February 1996.

[8] Muhammad MahtabAlam, Olivier Berder, Daniel Menard, and Olivier Sentieys,TAD-MAC: Traffic-Aware Dynamic MAC Protocol for Wireless Body Area Sensor Networks. IEEE Journal on emerging and selected topics in circuits and systems, vol. 2, no. 1, March 2012.

[9] Sami El-Ferik, Yazan M. Al-Rawashdeh, and Frank L. Lewis, A Framework of Multi-agent Systems Behavioral Control under State-Dependent Network Protocols. IEEE Transactionson control of network systems, vol. 7, no. 2, June 2020.

[10] Yang Meng, Tao Li, and Ji-Feng Zhang,Coordination over Multi-Agent Networks with Unmeasurable States and Finite-Level Quantization, IEEE Transactions on automatic control, vol. 62, no. 9, September 2017.

[11] Jian Liu, Peilun Li, Raymond Cheng, N. Asokan, Parallel and Asynchronous Smart Contract Execution, IEEE Transactions on parallel and distributed systems, vol. 33, no. 5, May 2022.

[12] Joao Caseirito, Iberia Medeiros, Finding Web Application Vulnerabilities with an Ensemble Fuzzing, 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental vol. (DSN-S), 2021.

[13] A. N. Haidar, S. J. Zasada, P. V. Coveney, Audited Credential Delegation - A User-Centric Identity Management Solution for Computational Grid Environments, Sixth International Conference on Information Assurance and Security, 2010.

[14] Wei-Tek Tsai, Zihao Zhao, Chi Zhang, Lian Yu, Enyan Deng, A Multi-Chain Model for CBDC, Digital Society & Blockchain Laboratory, Beihang University, Beijing, P. R. China, 5th International Conference on Dependable Systems and Their Applications (DSA), 2018.

[15] Aditya K. Sood, SheraliZeadally, Senior Member, IEEE, and Richard J. Enbody, An Empirical Study of HTTP-based Financial Botnets, IEEE Transactions on dependable and secure computing, vol. 13, no.2, March/April 2016.

[16] TassosDimitriou, Senior Member, Ghassan O. Karame, Member, Enabling Anonymous Authorization and Rewarding in the Smart Grid, IEEE Transactions on dependable and secure computing, vol. 14, no.5, September/October 2017.