Intrusion Detection System in Mobile and Online Banking Network

Ibebuogu C.C[1], Amaefule I. A[2], Mirian Raymond[3]

[1&2]*Department of Computer Science, Imo State university, Owerri, Imo State Nigeria.*
[3]*Department of Statistics, Imo State university, Owerri, Imo State Nigeria.*

ABSTRACT

The denial-of-service attacks on well-known websites demonstrate that no open computer network is safe from incursions. Software upgrades frequently present new issues, and system software frequently has bugs that could lead to security issues. The work aims to develop an intrusion detection system that can monitor, examine, and identify actions of unauthorized users (Access Attempts), notify the relevant authority (the administrator) of the incursion, and create an environment that is largely free from intrusions. This study was driven by the growing need for network connectivity, which makes it harder, if not impossible, to isolate a system from outside intrusion. Furthermore, using wireless connectivity exposes the network to threats like latent eavesdropping and aggressive interference. Finally, the absence of a centralized point for monitoring and management makes it difficult to establish a clear line of defense. The system that is being developed will take a picture of the intruder, stop them from transferring money by encrypting the International Transfer Code (ITC), Money Laundering Code (MLC), and Transaction Access Code (TAC), and notify the admin and account owner automatically when there is an intrusion and further development.

Keywords: *Authentication, Authorization, Backdoor, Intruder, Encryption, Denial of Service Attack*

I. INTRODUCTION

It is reasonable to carefully examine the kinds of data that go into and come out of computers in an era where number of transactions on networked computers (the internet) is growing daily to ensure that the information is secure. Firewalls are system protection mechanisms that ward off hackers, intruders, and malicious software from your home computer, workplace computer, and networked computers [1]. It guards against malicious software that might end up on your computer from nosy hackers and attackers. Utilizing your computer system without any security precautions, such as a firewall, will put you at significant risk, especially if you're connected to the internet, the information superhighway. An efficient firewall uses code to create a blockage and determine whether each data packet that flows through your device has to be blocked or allowed to flow. This separates your system from the internet.

A firewall is generally understood to be a type of network security system that monitors and controls every network connection that comes and goes in compliance with security policies that have been previously determined [2]. In general, a firewall builds a wall between a reliable, secured internal network and an external network—like the internet—that is assumed not to be protected or trusted. Even a stand-alone PC or a network of linked PCs can be easily used to identify dangerous software and dishonest hackers while they are online. Every internet connection has a firewall installed, which means that all data transit is closely watched. You can also tweak it to obey regulations. Simply said, these regulations are security regulations that the network manager may establish up to permit access to their Telnet servers, internet servers, FTP servers. This gives the network manager or system owner complete control of the traffic that enters and exits their computer networks [3].

Firewalls are often not able to defend against malicious mobile code, insider assaults, or insecure moderns, despite the fact that they are susceptible to configuration problems and vague or undefined security regulations. Due to the

following firewall flaws, intrusion detection systems (IDS) were developed in tandem with firewalls to capture intruders who wreak havoc on networks but are not detected by firewalls.

Network security has evolved due to the swift expansion of internet connections and mobile computing applications. We now know that no open computer network is safe from assaults thanks to the recent denial of service attacks on well-known websites. Wireless ad-hoc networks are predominantly vulnerable because of its open medium, dynamically changing topological structure, cooperative algorithms, nonexistence of a central monitoring and administration point, and hazy line of defense. Firewalls and encryption software alone are no longer adequate or efficient means of network security [4].

[5] stated that a lot of intrusion detection methods that were created for fixed wired networks are no longer relevant in this new setting. In order to safeguard mobile computing applications and wireless networks, we must look for innovative architecture and defenses. In this study, we'll look at wireless network vulnerabilities and integrate intrusion detection into the mobile computing environment's security architecture. Additionally, we will demonstrate this architecture and assess its essential mechanisms, which include using mobile agents for mobile ad hoc network misuse, anomaly, and intrusion detection.

A. Different categories of Intrusion Detection Systems

Although they do the same task, detection systems for intrusions differ slightly in how they go about things. In total, there are five distinct types of IDS. Let's examine each one's specifics, benefits, and downsides [6].

1. Network Intrusion Detection System: An approach that monitors the whole network through single or more checkpoints. In general, for it to be utilized, a Network intrusion detection system needs to be placed on hardware that is a part of your network's architecture. All packet—a collection of data—that traverses your Network Intrusion Detection System after deployment will be analyzed.

All of the activity that traverses it can be analyzed by a typical NIDS. That being said, because overload of data may lead you to overlook an attempted attack, you may choose not to review each bit of information that comes through your NIDS. To solve this issue, the majority of NIDSs permit you to put up a set of "rules" that describe the form of transmissions your NIDS will recognize and record. Guidelines allows you concentrate on particular kind of traffic, yet they as well need some knowledge of the NIDS structure.

Systems for detecting network intrusions have several advantages.

a. The capacity to analyze all incoming and outgoing traffic.
b. the ability to identify events in real-time, enabling prompt response times; and
c. the fact that they are more difficult for attackers to detect.
d. They can be positioned tactically in important locations.

Nevertheless, potential drawbacks of the network intrusion detection system include:

a. **Manual maintenance:** Since NIDS are usually put on specialized hardware, you might have to invest more time in manually managing them.
b. **Low specificity** - An intrusion detection system's likelihood of missing indicators of a breach increases with the volume of traffic it monitors.

2. Network Node Intrusion Detection System: Although it functions differently from a (NIDS), it is nonetheless regarded as a distinct kind of IDS. A Network Node Intrusion Detection Systems also looks at the packets that pass across it. But, instead of depend on on one gadget to track entire network activities, the system monitors individual device linked to the network.

This distinction has a number of benefits, such as:

a. **Faster speeds:** The system can operate faster since each NNIDS agent analyzes less traffic.

b. **Using less space and resources:** Similarly, NNIDS consumes less system resources. It is very simple to install on your existing servers.

The requirement for several installations is the primary disadvantage of choosing a Network Node Intrusion Detection System. Whereas a NIDS only requires a single gadget, a NNIDS requires numerous gadgets, one for each server you want to observe. All of these NNIDS agent must also submit their reports to a single console.

3. Host Intrusion Detection System: offers an improved form of Network node Intrusion Detection system machine independence. Using a HIDS, can deploy IDS program on all devices linked to the network. Host Intrusion Detection System execute its task by taking "snapshots" of the allocated device. Matching the most recent snapshot with previous records, the Host Intrusion Detection System can recognize any variations that may show an intrusion.

Host Intrusion Detection System have the following benefits:

a. They can be placed on servers or PCs.
b. They can identify the impacted device.
c. They inform administrators when changes are made to or deletions of analytical system files.
d. They perform exceptionally effectively in the face of insider threats.

However, "after-the-fact" monitoring might cause problems for Host Intrusion Detection System solutions. Since several HIDS solutions depend on records that document intrusions, the general mean duration for response (MTTR) may be longer with these solutions. Continuous surveillance is therefore required for a HIDS to be used as effectively as possible.

4. Intrusion Detection System Based on Protocol: are one kind of intrusion detection system that monitors the protocol that is being used. This technology essentially analyzes the Hypertext Transfer Protocol or Hypertext Transfer Protocol (Secure) protocol traffic that is passing across your gadgets and the server. A PIDS is often located at a server's front end. The system can keep an eye on both incoming and outgoing traffic to safeguard your web server. Because PIDSs concentrate on the protocol—that is, the way devices transfer data inside a particular network—they rarely make up a wide-ranging IDS solution. Nonetheless, they can fortify an existing strong cybersecurity solution.

5. Intrusion Detection System Based on Application Protocol: focuses on software application security. APIDSs are employed for tracking the communications among applications and servers and are commonly connected to host-based intrusion detection systems. An APIDS is typically installed across a number of servers. Like a PIDS, an APIDS is not going to satisfy all of your network surveillance needs. However, it can function effectively with many IDS models.

Cybercriminals, however, are constantly looking for novel ways to breach this environment's security and steal people's belongings. The collaboration of the various parties involved in the online exchange process—such as users and technologies—is what determines the safety of online banking.

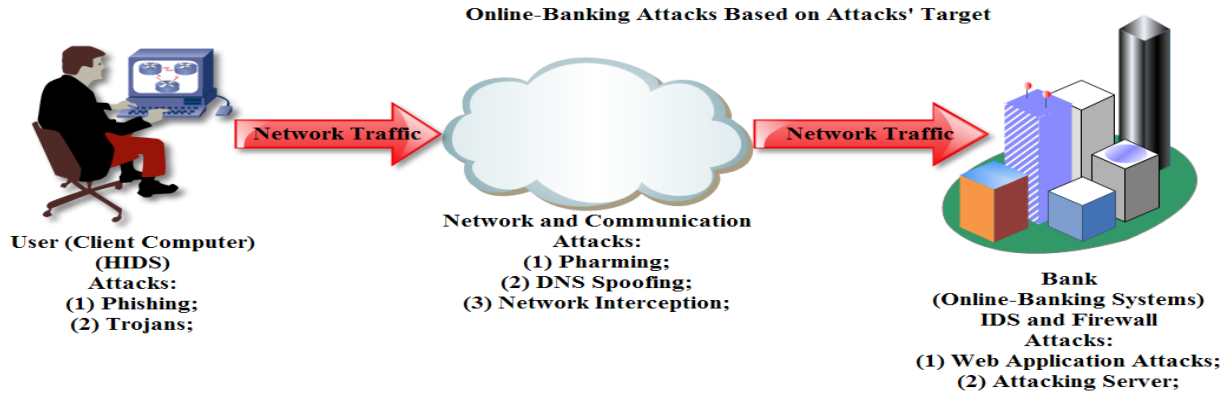

Figure 1: Online-Banking Attack

A. Intrusion Detection System Methods

Your security strategy depends on several distinct detection techniques to keep you secure, based on the sort of intrusion detection system you select. A quick summary of each is provided here [7].

1. Signature-Based Intrusion Detection: (SIDS) seek to correlate behaviors with indications of known intrusions. A database of earlier intrusions is essential to a SIDS. In the event that activity on your network corresponds with the "signature" of a database breach or assault, the detection system alerts the administrator. Since the database is the cornerstone of a SIDS solution and SIDS can only detect attacks that it detects, regular database upgrades are required. Therefore, if your company is victim of a never-before-seen intrusion strategy, no amount of database upgrades will protect you.

2. Anomaly-Based Intrusion Detection: Conversely, these novel zero-day attacks can be noticed by an anomaly-based intrusion detection system (AIDS). A SIDS builds a model of "normal" behavior using statistical data and machine learning (ML). The system flags traffic as suspicious whenever it deviates from this usual pattern. The main problem distinguishing AIDS from SIDS is the possibility of false positives. After all, some alterations are just signs of shifting organizational behavior and not all of them are the consequence of malevolent conduct. However, a SIDS may flag any and all anomalies as intrusions because it lacks a database of known attacks to consult.

3. Hybrid Intrusion Detection: The benefits of both strategies are combined in this kind of system. By looking for trends and isolated incidents, a hybrid intrusion detection system may recognize both novel and tried-and-true infiltration techniques. The one disadvantage of a hybrid system is the even larger rise in problems that are reported. Looking at the primary drive of an intrusion detection system is to notify users of possible intrusion; it's challenging to perceive this spike in alerts as an undesirable thing.

II. LITERATURE REVIEW

Ad hoc networks, according to [8], are made up of a group of wireless mobile nodes that come together to create a network on the fly without the need for centralized management. Since wireless network interfaces have a limited transmission range, it might be required for one mobile node to ask other hosts to help forward a packet to its intended location in such an environment. Every mobile device in the network performs the dual roles of host and router, forwarding packets for other devices that may not be in immediate transmission distance from each other. Ad hoc routing allows any node to locate multi-hop paths towards any other device on the network because each device participates in this protocol. Although the mobile devices in the network constantly build connectivity between themselves in order to create their own network on the fly, the concept of a mobile ad hoc network is also known as infrastructure less networking.

[9] proposed that while mobile ad hoc networks offer several benefits over conventional wired networks, they also present a distinct set of difficulties. First, secure communication presents difficulties for MANETs. For instance, the cryptographic techniques used for encrypted messages are limited by the resource limitations on nodes in ad hoc networks. As such, it is vulnerable to a variety of link attacks, such as active imitation, message replay, and message distortion, as well as passive eavesdropping. Second, mobile nodes are easily compromised if they are not properly protected. An attacker has the ability to listen in on all wireless communication channel traffic, alter it, and try to pass off any traffic as coming from a valid network node. Lastly, with regard to of a security solution, static setup could not be sufficient for the constantly evolving topology. A malicious node can easily launch various attacks, such as Denial of Service (DoS) attacks, and overwhelm the network with bogus routing requests by posing as a valid modification to routing information and providing inaccurate updating information. Ultimately, in wireless MANETs, an absence of collaboration and limited capabilities is typical, making it difficult to discern abnormalities from normalcy. Due to its inherent open medium, unpredictable topology, lack of central authority, distribution cooperation, and limited capability, wireless MANETs are generally especially vulnerable.

The purpose of an intrusion detection system (IDS) is to secure data, systems, and networks using a combination of hardware, software, and defensive and proactive techniques [10]. At the host, network, and application levels, it is functional. After analyzing system or network traffic or managing inbound connections to various ports, it looks for and identifies attacks as they happen. It is capable of identifying known attacks, anomalous network traffic, malicious data, abuse, and illegal access to networks and systems by outside or internal users. It provides the security manager with information and alerts through various warnings and notifications. Occasionally, it disconnects dubious connections or restricts dangerous traffic. Generally speaking, intrusion detection systems (IDSs) have three primary functions: evaluation, response, and reporting in relation to attacks on computer systems and networks. IDSs employ a variety of techniques to find attacks.

As per reference [11], the field encompasses all the techniques and methods employed to protect computer-based devices, data, and services against illicit or unintentional access, alteration, or destruction. Its significance is growing due to the growing dependence of nearly all societies across the globe on computer systems. In order to comprehend how to secure a computer system, one must first comprehend the different kinds of "attacks" that might be launched against it.

[12] contrasts specification-based detection, misuse detection systems, and anomaly detection systems. Emergency services, such as disaster recovery and relief efforts, are among the most crucial areas where MANETs are used because regular wired networks have already been destroyed. MANETs are being used in a wide range of various application sectors, including commercial, educational, and entertainment, to connect people.

[13] made use of soft computing (fuzzy logics), secure routing, key exchange, and authentication; generic programming (linear genetic programming, gene-expression programming, and multi expression programming; LGP, MEP, and GEP); and different methods to solve multivariate problems.

deploy Markov chain (MC) and ad hoc On Demand Distance Vector (AODV) routing algorithms to address the issue of AODV routing protocols, capture RREQ and RREP messages, and identify run-time infractions of the requirements [14]. Effective temporal aspects of MANET routing patterns can be captured by a local detection engine that is MC-based.

III. METHODOLOGY

In order to protect against malicious inbound connections, a second line of protection is provided by the Intrusion Detection System (IDS). The option to use Windows Firewall in conjunction with an intrusion detection system may offer extra security, even if it is typically not advised to enable two firewalls due to the possibility of conflicting rules and decreased system performance.

The intrusion detection system's second layer can trap malware that have evaded firewalls. When such malevolent intruders are caught by IDS, it instantly alerts an admin or non-security agent. The administrator or non-security agent then distributes the details to all endpoints for scanning (for known and new viruses) and filtering of both inbound and outbound network traffic. The program will automatically collect data regarding the attempted break-in's origin and generate reports to assist law enforcement in apprehending the offenders.

These latest advancements enable intrusion detection systems (IDS) in mobile ad hoc networks to safeguard network nodes and largely thwart malicious attacker activity.

The purpose of this inference engine architecture is to: Track and examine user actions and system events; Identify trends in system events that link to known threats; When assaults are detected, notify the relevant user. Assign critical security monitoring tasks to non-security specialists, maintain a largely intrusion-free environment, and minimize security flaws to give mobile ad hoc networks (MANETs) the comfort and scalability they need to endure over time.

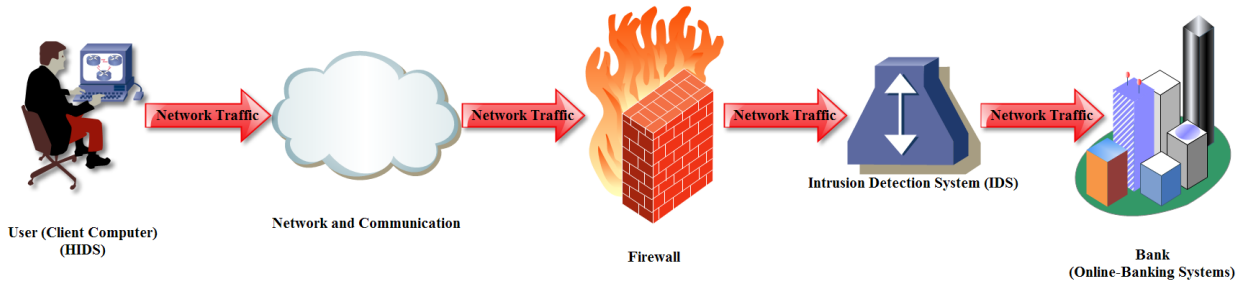

Figure 1: Intrusion Detection Architecture for Online-Banking

IV. CONCLUSION

IDS functions as a kind of automatic defense system, spotting harmful activity on the server or network. Ad hoc networks are a field of study that is becoming more and more viable and has many real-world applications. However, because of their constantly shifting topology, lack of traditional security infrastructures, and open communication channels—which, compared to their wired parallels, cannot be secured—mobile ad hoc networks, or MANETs, remain incredibly susceptible to assaults. To strengthen network security, intrusion detection can be used in conjunction with intrusion prevention strategies (which include authentication, encryption, secure MAC, secured routing, etc.). To improve intrusion detection for the Wi-Fi ad hoc setting, new methods must be created. The purpose of an intrusion detection system is to recognize network intrusions or assaults on mobile devices. When properly built, intrusion detection systems can detect inappropriate behavior and assist in providing sufficient security. As a result, an IDS is now a crucial part of the defense-in-depth security procedures that MANETs require. Customers of financial organizations are increasingly able to access internet banking; in fact, several banks operate exclusively via the internet. The majority of banking can be done virtually by anyone thanks to the abundance of possibilities. Switching to an online banking system can be advantageous for individuals as well as businesses.

V. ACKNOWLEDGMENT

We would like to thank the Vice Chancellor of Imo State University in Owerri for encouraging collaboration in research inside the institution, as well as the TETFund for funding this study.

REFERENCES

[1] Funnel, S.M. (2005). Computer insecurity: Risking the system. Springer-Verlag, London.

[2] Palo, Alto (2013). Next generation firewalls: Restoring effectiveness through application visibility and control

[3] Zwicky, R. and Giberson, F. (2000). Parallel computing security. Retrieved From http://www.worktanksolutions.com

[4] Souley A.-K.H. and Cherkaoui S., (2005), Advanced mobility models for adHoc network Simulations, Systems Communications, 2005. Proceedings 14- 17 Page(s):50 – 55.

[5] Yi, S. Naldurg P. and Kravets R. (2001) Security-aware routing protocol for wireless ad hoc networks. In Proceedings of ACM MobiHoc

[6] Ansam Khraisat and Ammar Alazab (2021). A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00077-7*

[7] Helixistorm (2023). Understanding the 5 Types of Intrusion Detection Systems https://www.helixstorm.com/blog/types-of-intrusion-detection-systems/

[8] Arcodia,C., & Barker,T . (2007) Computer programming essential (second Edition)

[9] Paxson, Vrn, (1998) ‘’Bro: A System for Detecting Network Intruders in Real-Time ,’’ proceedings of the 7th USENIX Security Symposium, San Antonio, TX.

[10] Denning D.E., (1986) An Intrusion Detection Model’’, proceedings of the seventh IEEE Symposium on security and privacy, pages 199-131.

[11] Kumar A et.al (2013). A Review on Intrusion Detection Systems in MANET, International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, ISSN: 2319-5967.

[12] Kathole A.B. et al. (2012). A Review Paper on Comparison and Analysis of Different Attack and Intrusion Detection System. Inter-national Journal of Cryptography and Security, ISSN: 2249-7013 & E-ISSN: 2249-7021, Volume 2, Issue 1, pp.-18-21.

[13] Nabil Ali Alrajeh, S. Khan, and Bilal Shams., (2013). Intrusion Detection Systems in Wireless Sensor Networks: A Review, International Journal of Distributed Sensor Networks Volume 2013, Article ID 167575.

[14] Anand Babu G. L, G. Sekhar R. and Swathi A. (2012). Intrusion Detection Techniques in Mobile Ad hoc