Cronjob Scheduling Algorithm: An Approach for Network Threat Detection and Prevention

Promise Enyindah
Department of Computer Science
University of Port Harcourt, Choba,
Rivers State, Nigeria

Umejuru Daniel
Department of Computer Science
University of Port Harcourt, Choba,
Rivers State, Nigeria

ABSTRACT
Network threat remains a leveraging parameter and serves as a tool for fraudulent individuals to exploit internet users due to voluminous usage of web connected devices and applications. A webserver is a gateway through which the entire internet population connects to with the aim of sharing resources or providing online services. Network and the web domain have been the pathway to deliver and have access to online services; this trend has also gained a higher increase as the need for online services to global users remain important and on the increase. There has always been an increase of intrusion on the cyber space since the web gained more concentration among others; the sophistication of attacks against these applications' environment has grown as even as the rising use for technology also increases. To prevent common attacks of content, corruption, data theft, integrity and privacy has become an increasing problem. While approaches to security have been improved upon in recent times, intrusion techniques have also become increasingly complex. In this research work an approach for network threat detection and prevention on webserver application environment using cronjob scheduling techniques has been developed. The new system adopted the Dynamic Systems Development Model (DSDM) Methodology and was implemented using PHP7 server-side scripting programming language, Laravel MVC framework and MYSQL relational database for the backend. The proposed system has been tested and was able detect and prevent intruders from gaining unauthorized access into the webserver application environment and also was able to send a rapid response message to the admin through SMS messaging and emailing system.

Keywords
Cronjob Algorithm, Digital Attack, Network, Threat, Detection, Prevention.

1. INTRODUCTION
Intrusion is the act of gaining unauthorized access to another person's personal information; intrusion can be prevented with the use of an intrusion detection system. A hardware or software program which monitors and traces behavior of a system for bad activity or policy breaches is known as an intrusion detection system (IDS). Typically, any intrusion activity or violation is reported to an administrator or gotten generally using a known security informed and events management (SIEM) systems [16] as technology has progressed, data security has become a more serious issue for global transactions. Most countries' economies are now accessible through the use of information transmission models, also known as the internet or World Wide Web. The virtual world known as cyber space was developed as a result of the integration of the Internet and information technology into practically every part of modern life. The internet's strength, however, is also its fragility [15].

The worldwide pandemic that hit the world in 2019 carried with it a large number of difficulties, provoking more organizations to go to web advances to convey their administrations all throughout the planet. This wonder has moved programmers' and gate crashers' consideration away from network-level assaults and toward webserver applications. There have been different episodes of spammers, crawlers, and programmers breaking into individuals' protection to get illegal admittance to their information, presenting huge obstacles to web clients, especially the people who go through with online exchanges utilizing web-facilitated data set driven web applications. Data is a valuable and exorbitant resource that, as other important resources inside an organization, should be shown, controlled, and arranged, particularly in cloud-facilitated applications [7].

Today digital assault is a broad and steadily expanding overall test that the globe is at present going up against. Since the web changed from restricted admittance and accessibility to boundless access from anyplace whenever, network protection weakness has expanded [2]. Information burglary has kept on heightening to where endeavors are searching for creative approaches to shield their information from programmers to empower secure information move, in addition to other things, for data security, especially web worker-based applications [4]. Interruption on the World Wide Web has kept on filling in fame among gate crashers, raising many worries among scientists and web software engineers about accepted procedures and interruption discovery framework arrangement that could assist with moderating the big number of interlopers on web worker applications in the internet. The issue originates from the way that the internet produces an awry awkwardness that vigorously favors vindictive entertainers that can go around digital protection methodology [11]. In view of the Internet's inclination and the refinement of data innovation, anybody can focus on a casualty from anyplace on the planet at somewhat cost and with minimal shot at being found by attacking their protection [3]. Interruption location is the unrelenting dynamic endeavors to find or distinguish the presence of intrusive or illicit activities in a specific framework, like a web worker, using a bunch of pre-modified measures to robotize the interaction. Cron work booking calculations are utilized inside the web worker to mechanize explicit activities consistently, and they have demonstrated to be very valuable in spaces of web worker the executives [9].

Intrusion detection has traditionally been done at the network perimeter, with an emphasis on detecting known attack signs and anomalous behavior. Intrusion detection systems have evolved into intrusion prevention systems, which stop harmful traffic before it reaches the network border. Since the inception of cloud computing, the web server has been a key player, as all internet-based applications are hosted on the web server, which also houses relational databases and any files stored on

it. As a result, both the research and commercial communities worked hard to provide secure communication services to online applications. Network-level security, such as port scanning, has received a lot of attention, and considerable progress has been made there as well [12].

2. THEORETICAL FRAMEWORK

Webserver application security is a continual risk management activity that includes implementing technology, policies, and processes, enforcing laws, and teaching and informing personnel involved in the creation and administration of web applications. The webserver application environment is depicted in the diagram below; Privacy, honesty, accessibility of reasonable data, and validation are generally factors that add to web worker security. A spilling worker can be terrible for an organization. Accordingly, security is the most confounded issue on which the advanced world is concerned. Indeed, even the most painstakingly arranged firewall framework can be penetrated by a gravely designed Web server application environment. A seriously planned firewall may deliver a site unusable [6].

In an intranet setting, where the Web server should regularly be arranged to perceive and verify various gatherings of clients, each with various access qualifications, things develop significantly more convoluted. The most utilized web server is Apache. The Apache worker presently runs practically 70% of every internet-based website, with over 1,000,000 destinations running on it. Understanding Apache's way to deal with security can help us in making different projects secure [1].

2.1 Web Servers Security Issues

For both Linux and FreeBSD, Apache is the most famous Web server. In view of its rules consistence, flexibility, dynamic shared articles, versatility, and programmability, it is the most widely utilized Web Server on the Internet [17]. Web servers are an enticing objective for programmers, which is the reason security, is a particularly significant theme for administrators of both web associated and intranet-associated workers. The overall security difficulties of a web server are examined in this segment.

1. Communication Channel Security: The Secure Sockets Layer (SSL) of TCP/IP is the most frequent method of communication channel security. For TCP/IP communications, the SSL protocol encrypt data, server authentication, and information integrity. As a result, it ensures the secrecy, authenticity, and integrity of data throughout the transaction.
2. Auditing and Logging: Across the layers of the application infrastructure, activities such as successful and failed logon attempts, data retrieval, modification, and deletion, network communication, and administrative operations, among others, should be audited and logged.
3. Denial-of-Service (DoS) Assaults: Denial-of-Service (DoS) attacks are those in which the attackers' purpose is to shut down the target rather than steal data. Authorized users are denied access to network services in these network-based assaults. DoS attacks can take many different forms and are aimed against a range of services, including the consumption of precious, restricted, or non-renewable resources, the destruction or manipulation of configuration information, and the physical destruction or alteration of network components [18].
4. File Permission: In a server, there are two file system roots: the document root, which contains all HTML pages, and the server root, which contains all logs and configuration files. It's critical to have the permissions for the server-side root correct because here is where all the sensitive data and CGI scripts are kept.

2.2 Cron Job Scheduling Techniques

A cronjob is a process that runs a script on your web server at regular intervals. Cronjobs are a component of the Unix operating system that interacts with the Apache web server environment [5]. In computers, scheduling is the process of allocating work to resources that will complete it. Threads, processes, and data flows are virtual processing pieces that are scheduled onto hardware resources like as processors, network lines, and expansion cards. The scheduling action is carried out by a scheduler. Schedulers are frequently used to keep all computer resources occupied (as in load balancing), to allow numerous users to properly share system resources, or to achieve a specific level of service quality [8]. Scheduling is essential to the calculation process. The following is the cronjob actions on a webserver:

1. Look for a file named.cronjob in all servers' home folders when they boot up.
2. Determine the next time each command must execute in the future for each cronjob file identified.
3. Add the commands to the event list, along with the appropriate time and time specifier.
4. Start the main loop:
   i. Look at the task entry at the top of the queue and figure out how far ahead it needs to run.
   ii. Rest for that amount of time.
   iii. Upon waking up and verifying the right time, run the job at the front of the queue (in the background) using the user's privileges.
   iv. Determine the next time this command will be run in the future and add it to the event list at that time value.

2.3 The Error Log Lists Server Errors

Keeping track of these records can aid in the detection of infiltration attempts. The logs can also be used to learn about penetration strategies. The refer log shows the URLs that the browser has visited previously and the URL that it is now viewing. Logging is supported by a variety of Apache modules. Here are a few examples: mod log forensic: This module allows you to log client requests for forensic purposes. Because logging is done both before and after processing a request, each request has two log lines in the forensic log. Module: This module keeps track of the number of bytes received and sent for each request. Module configuration: This module allows for configurable client request logging. Logs are written in a format that you may customize, and they can be saved to a file or sent to external software [10].

2.3.1 Access Control

Access control is provided by Apache's mod access module. Mod access, as the name says, allows you to regulate document access. It lets you control access to resources based on the client's host name, IP address, or network address. Mandatory Access Control (MAC) is an IP-based control, while Discretionary Access Control (DAC) is a password-based control (DAC). Mod access provides the following directives: Allow Controls which hosts have access to which parts of the server. Here are several examples:

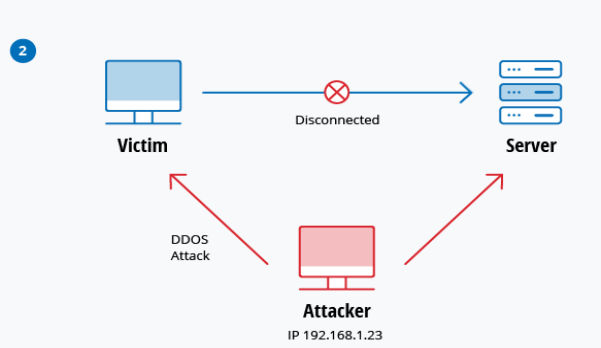

Fig 2.1: Dos Attack
(Source: A Complete Strategy for Web Application Security, (Hydara et al. 2023)

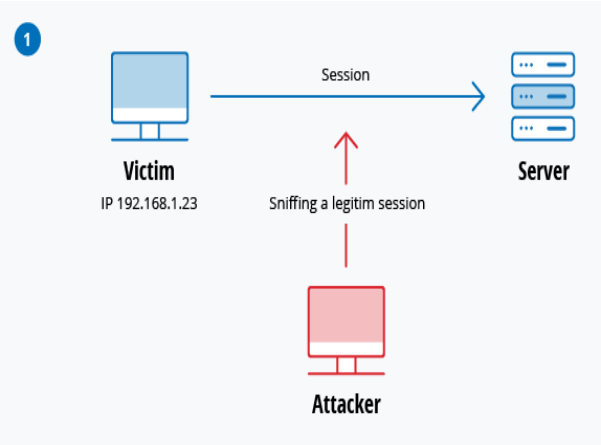

Fig 2.2: Session Hijacking
(Source: A Complete Strategy for Web Application Security, (Hydara et al. 2023)

1. Password Assault

Getting passwords is a far reaching and astonishing assault approach since passwords are the most commonly utilized structure for affirming clients to a data system. Looking at a singular's workspace, "sniffing" the association relationship for decoded passwords, using social planning, acquiring induction to a mysterious key informational collection, or straight guessing are in general ways to deal with acquire permission to a singular's mysterious key. This may incite the usage of force.

2. SQL Injection Assault

With data set driven sites, SQL infusion has turned into an inescapable issue. It happens when an evildoer utilizes the info information from the customer to worker to run a SQL inquiry on the data set. The SQL Injection assault targets Web pages that permit clients to type text into structure handles that are then used to inquiry information bases then, at that point, used to question data sets. Programmers can enter a satire SQL inquiry, which modifies the question's inclination. Thus, the questions can be utilized to get to the connected data set and adjust or erase its substance [13].

3. XSS (Cross-Site Scripting) Attack

Outsider web assets are utilized in XSS assaults to run scripts in the casualty's internet browser or scriptable application. The attacker imbues a payload containing malignant JavaScript into the data base of a site. Exactly when the setback requests a page from the site, the site sends the page to the individual being referred to as program, alongside the aggressor's payload installed in the HTML body, where the pernicious content is executed. Cross-webpage prearranging assaults are constantly aimed at the facilitating web application's hidden working framework and, as a rule, the back-end information base. A web application that doesn't channel scripts from structure fields submitted to the web application is often designated by an aggressor. As a rule, assailants can embed code that is controlled by the client's program. This code will endeavor to take program treats containing banking meeting information, passwords, and other delicate data. The assailant then, at that point, utilizes meeting treats to emulate a real client meeting to a financial site, email account, etc [14].

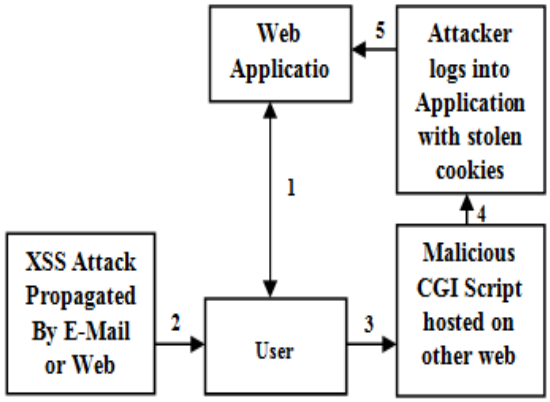

Fig 2. 3: XSS Attack Hijack Scenario
(Source:http://www.tutorialspoint.com/internet_technologies/web_servers)

3. METHODOLOGY

A software development methodology or system design methodology in software engineering is a framework that is used to structure, plan, and control the process of developing an information system. The methodology will be adopted in the analysis and design in this study is Dynamic Systems Development Model (DSDM) Methodology. The Dynamic Systems Development Model was developed in the U.K in the mid-1990. It is the evolution of rapid application development (RAD) practices. DSDM boasts the best-supported training and documentation of any of the agile software development techniques.

3.1 Cronjob Scheduling Algorithm

Cron is a period-based algorithm on webserver that sudden spikes in demand for a foundation on the webserver. Cron occupations are a standard strategy for planning assignments to run on a web server. Cron is a help running behind the scenes that will execute orders (occupations) at a predefined time, or at a standard span. The timetables are characterized in a setup document called a Crontab. A cron order has six fields: five date and time fields, and an order field. A task is run at whatever point the time, and date coordinates with the current time and date or at whatever point an activity coordinate with a timetable occasion.

Table 3.1 Cronjob Commands Expression

Cronjob Shorthand	command Values
@-reboot command	Run if there is an event or action
@-yearly command	(0 0 1 -1- *).
@-monthly command	(0 -0 -1- *- *)

@-weekly command	(0- 0 * -* 0).
@-daily command	(0 -0 *- * -*).
@-hourly command	(0- *- *- *- *).

Table 1 shows the cron commands expressions which can be used; one or more commands can also be combined to achieve a desired outcome. Cron expressions are used to configure instances of cronjob trigger. In the above table, the asterisks refer the specific blocks of time.

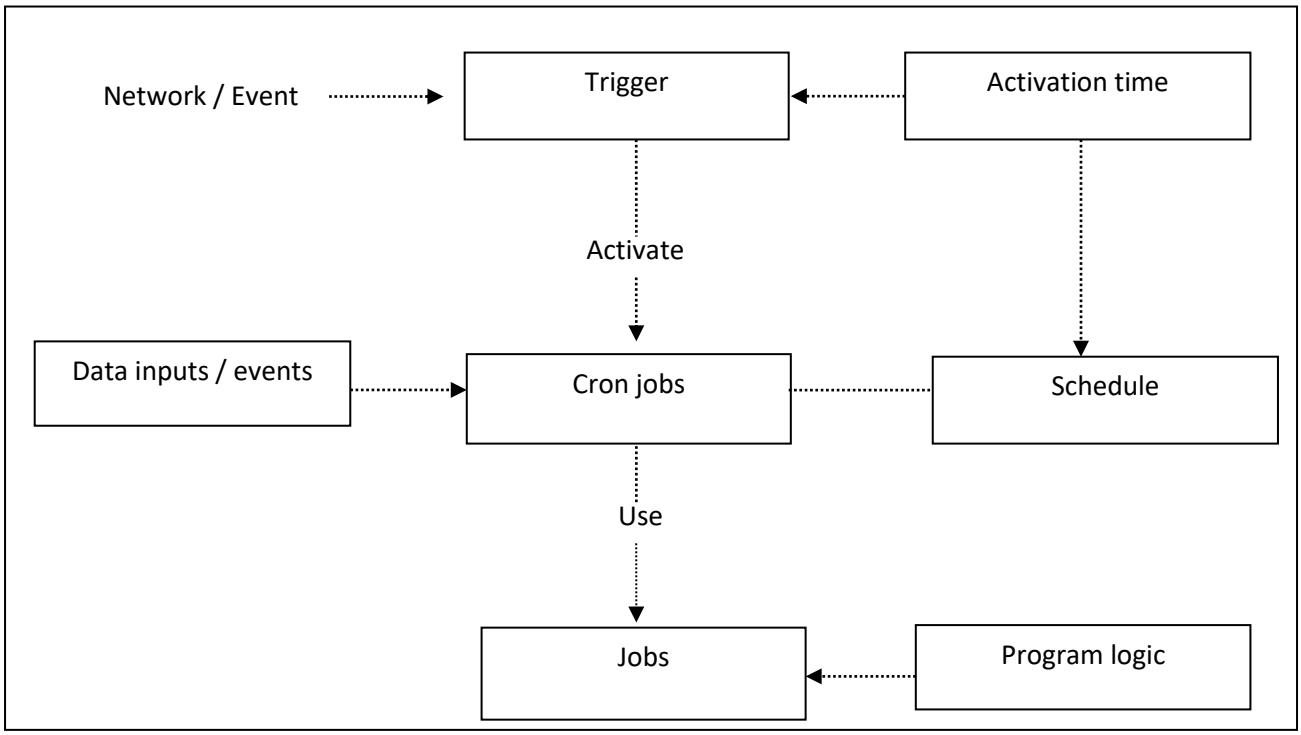

Fig 3.1: Overview of Cronjob Technique
(Fig 3.1 shows the general over-view of the cronjob techniques and how it works. Cron jobs are usually triggered by events for the activation of scheduled actions to be performed on the web server. Which help server administrators to automate certain task for webserver managerial purposes)

3.2 Proposed System Algorithm

START
Step 1: Connect to the network
Step 2: Load Apache webserver application Environment
Step 3: Load webserver Access GUI
Step 4: Set Cronjobs
Step 5: Get serverTimeStamp
Step 6: Get Events (set Action)
IF Events = True?Load CGI user Interface
Else Return to ***Step 3***
Step 7: N = 0 # number of current signatures
Step 8: Query MySQL database to retrieve the set of signatures detected, S.
Step 9: for every signature f in S do
Step 10: Get Pattern Matched
Step 11: Freq = number of occurrences of f
Step 12: LTime = last detection time of f
Step 13: if N <= MaxNum and Freq>= MinFreq and Ltime>= ValidTime then
Step 14: remove the signature from the secondary database
Step 15: add the signature in multiple IDS
Step 16: N = N+1
Step 17: Set Log File
Step 18: Set Ip / Proxy Ban mechanism
Step 19: Set Communication channel
Step 20: Analyze User Input(Compare request/pattern with known patterns in database)
Step 21: If User Input data = Valid, Grant Access
Step 22: Record Data to log File
else
Step 23: Send Alert / Notification
END

3.3 Output Design Specification

The yield of each framework is reliant upon the information or information got from the organization. The following is the determination of how the proposed framework will look like after the execution is finished.

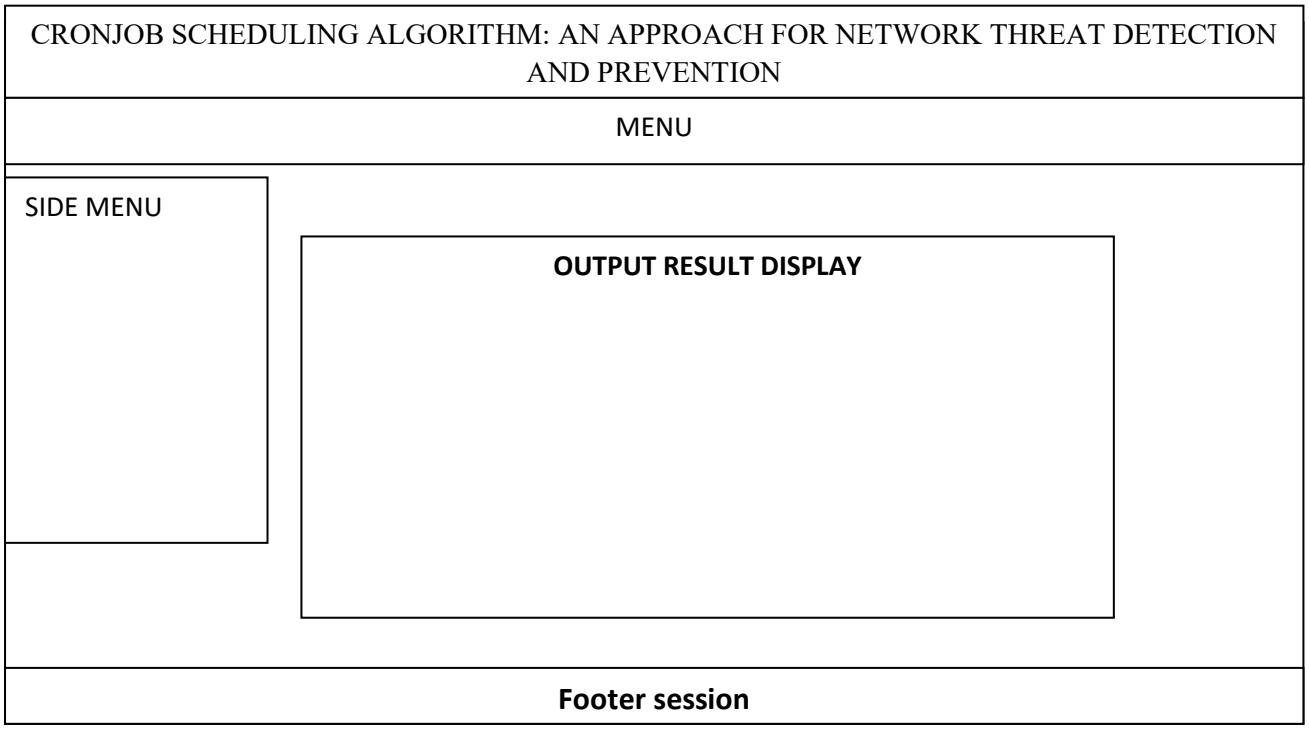

Fig 3.2: Output Design Specification
(**Fig 3.2 is the output design layout specification which represents typical layout of the GUI after implementation. This will further guide us on the implementation**)

4. RESULTS AND DISCUSSION

The developed system also detect and prevents intrusion in divers webserver intrusion tricks usually used to hijack the environment on most case such as SQL injections, proxy, Bots, spam, Brute force, ftpback logging, etc. A communication channel was also added into the new system to provide notification alerts to the admin on attacks for proactive actions were the need be, this uses SMS and emailing system mechanism. Our results show that Webserver applications are vulnerable against exploits on many different levels such as operating system, web server software, database, dynamic scripting language, interactions of the aforementioned).Web developers are not confident about the security of their applications and therefore very concerned about the webserver environment third party service providers. The developed system was deployed on namechip third party webserver application environment service provider were intrusions were performed using known techniques to test the developed system across different network and operating system to ascertain if the aims and objective were achieved in the study which are shown below.

4.1 Network Request Statistics across different Systems

Fig 4.1: Access Log Statistics

(**Fig 4.1** above shows the results obtained from the developed system been deployed it shows the Access log details analyzed using pie Chart for more visual illustration, it shows number of accesses across different browsers, operating systems and devices used to access the system, this can further provide more insight on how the developers can lay more phasis on. Below is a line chart that further gives us an over view and summary of the access detected from the previous chat.)

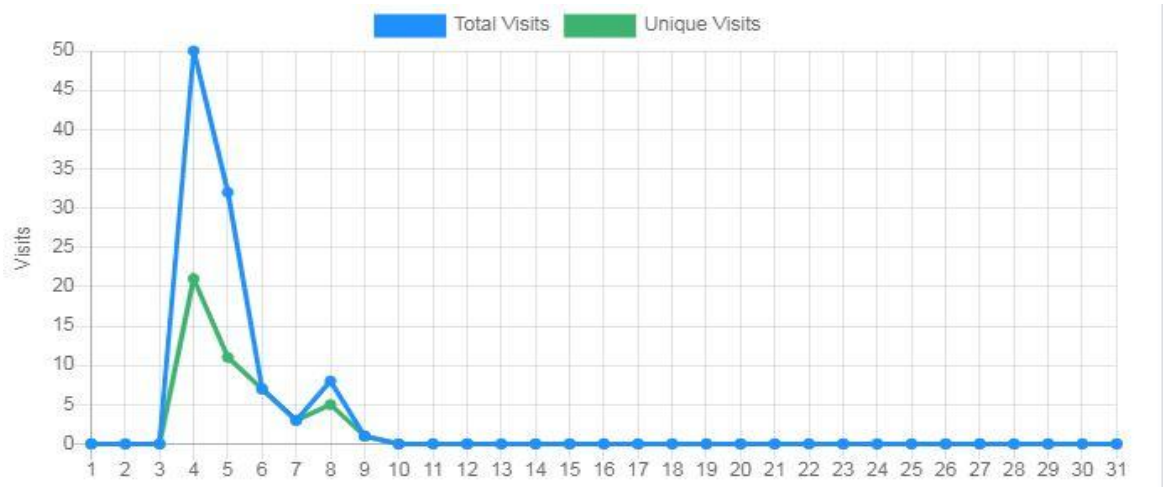

Fig 4.2: Visitors Chart

(**Fig 4.2** shows the number of visitors both unique and non-unique visitors. Unique visitors the visitors that visited real humans while non-unique visitors are bots. Bots are mini AI programs used in crawling URL mostly for search engine optimization and also used by hackers to launch dos attack over a webserver application environment in other to gain access using others means on the process. The proposed system prevents intruders from gaining access into the system using sql injection, brute force, bots, spam, proxy and also captures all their information records them to the database for administrative analysis and evaluation, below are intrusion data captured from users.)

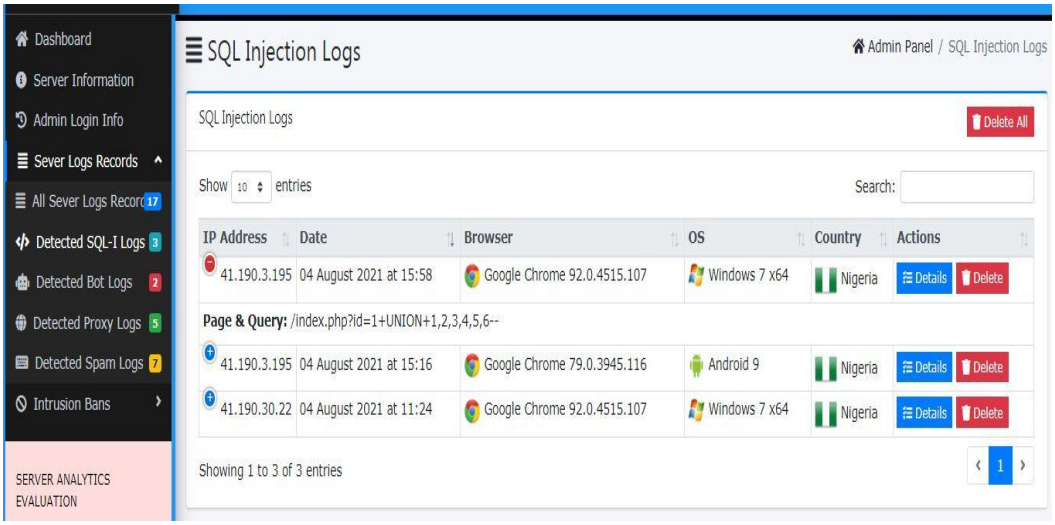

Fig 4.3: Detected SQL Injections Test Result

(**Fig 4.3** shows the log of detected SQL injection test result which gives a comprehensive record and knowledge of the occurrence.)

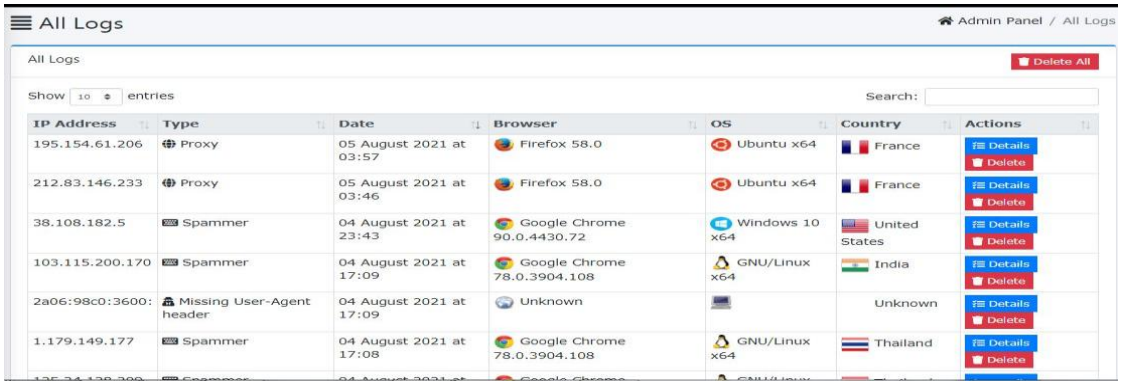

Fig 4.4: Intrusion Information

(**Fig 4.4** shows captured log details of users who attempted to gain access into the system their ip address, source, date, browser, operating system and country and current location of each visitor were also captured and further can be reviewed in a detailed view as shown below.)

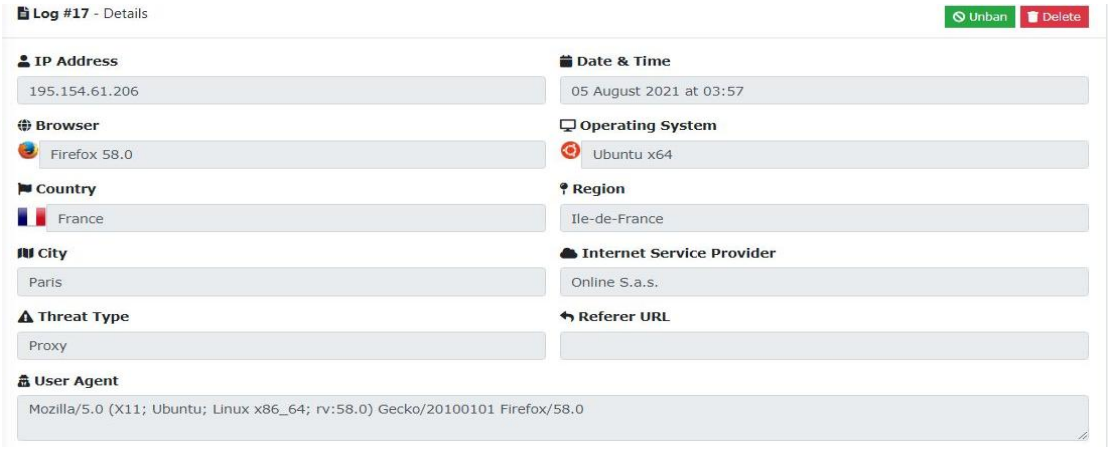

Fig 4.5: Single Log Preview

(**Fig 4.5** shows the data of each user captured by the system in better view including the current user location on the Google map and current address of the persons.)

Fig 4.6: Known Pattern Detected

(Fig 4.6 shows details of a single intrusion log in the system which high lights every information including tracking the location of the source of attack. the new system has been tested across different operate system and networks and it has shown to be effective in preventing and detecting webserver attacks from known and common methods. The developed system has provided a quick and responsive communication mechanism for the server administrator. The table below shows some of the parameters that were also captured in the system within the time frame of the deployment.)

Table 4.1 shows the number of treats recorded within few periods of time the program was deployed

Type Of Treats	Total Attempts
Sql Injection	4
Brute Force	1
Spam	10
Proxy	18
Bots	2

Table 4.2 Visitors by Location

Location	Number
United states	**10**
Russia	**3**
Nigeria	**6**
Netherland	**2**
Ireland	**2**
India	**1**
Thailand	**2**
Germany	**1**
France	**4**
United Kingdom	**1**

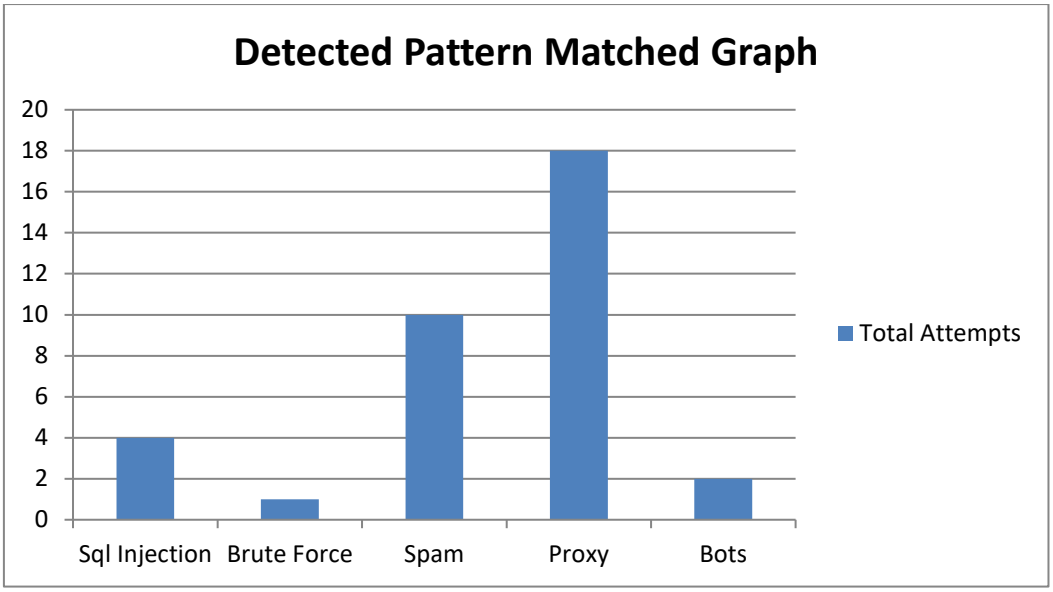

Fig 4.7: Comparison Graph of Total Threats Attempt Detected

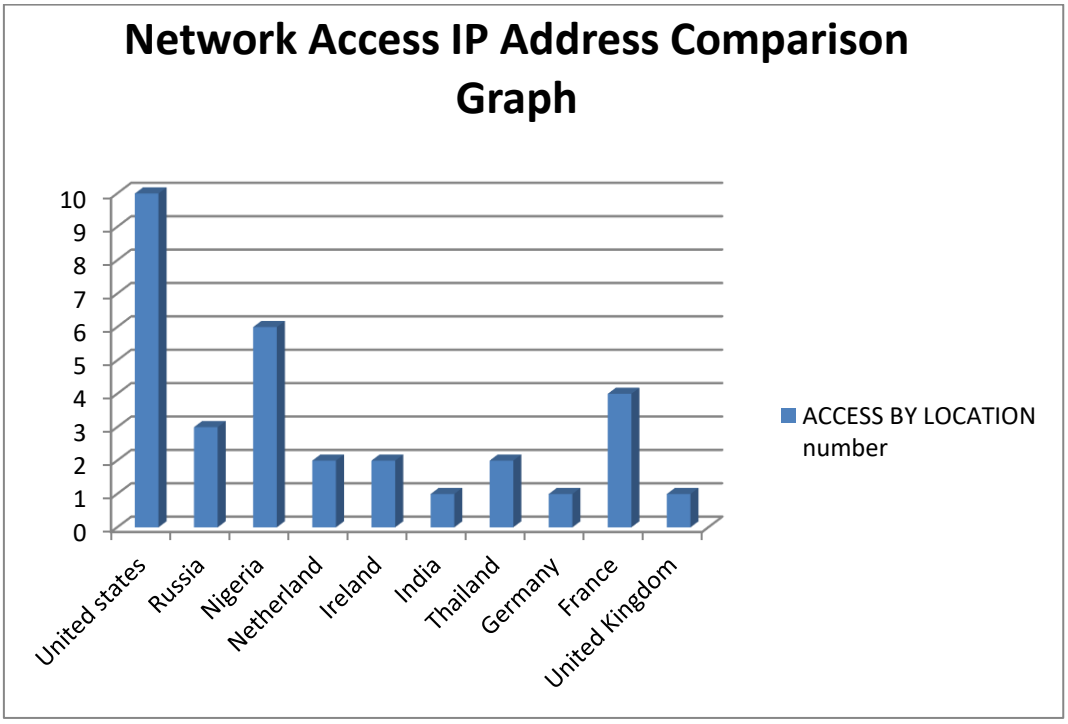

Fig 4.8: Network Access IP Address Comparison Graph

Table 4.3 Explanations of Results

S/N	TITLE	SUMMARY
01	Deployment / Testing	A new system has been developed and deployed on Namecheap shared Hosting server and can be accessed through https://g2018-msc-002.com.ng/secured-server_temporally for cross examination purpose. The system has been tested using known pattern matching techniques namely; SQL Injection, Proxy, Rule based across different operating system and network. The new system detection intrusion and prevents agent access and records the log to the database for administrative analysis and evaluation.

02	Cronjob Technique	In Our New System the Cronjob Was Used to Trigger the Ids Mechanism Based on Event or Action Using Time Stamp. With The Aim of Stabilizing the Server and Maintaining the Resource Usage Limit and Quota. this will help mitigate DDoS attack by prevent further access or resource usage when there is regular resource request be seconds or otherwise the system can be terminated and IP address will ban.
03	Data Log Visualization through an improved CGI graphical user interface	One of the most contributions to the existing body of knowledge is the visualization of log data from a GUI which has never been an easy task in webserver administration. the new GUI was able to capture total number Files in a detailed and sorted manner for quick decision in the application environment. as shown is one of the means used in exploiting the server is by uploading malicious files into it. With this GUI one can easily know when such occur by any means since the server are provided by their party service providers.
04	Communication Channel using Mobile text messaging and emailing system.	In our new system log notification and communication mechanism was added to provide quick and proactive detected alerts to the server admin directly on mobile phones and email. this mechanism has also been tested, ones there is an attempt of intrusion or detected abnormally, the new system trigger a notification to the admin
05	Location of Network treats Using Google map latitude and longitude embedment	In our new system, location of treats is also captured by country, operating system, agent, time, source, means of attack and current location using the google latitude and longitude. This will help for administrative purposes in the cases were the attacker need to be captured.
06	Visitors Analytics and visualization	Our new system provides visitors analytics and visualization in a detailed manner for a better decision making towards managing such system

5. CONCLUSION

The use of web-based applications is increasing to a great extent as well as the malicious activities also being recorded on daily bases. Hence, intrusion detection systems have become a needful component on the webserver application environment. In this paper work, we developed and implemented an intrusion detection system on webserver application environment by utilizing Cronjob scheduling technique which efficiently detected various types of webserver intrusions and also prevented attacks using known pattern matching methods. The developed system can be deployed into any webserver application development environment and used to properly safeguard the webserver, especially in organizations where sensitive and confidential data are always high targets. Further work need to be carried out in future on the security pattern of applications that are deployed on the webserver application environment in other to enhance and bridge the gap between them for better collaboration and technological adaptation. There is need to expand the work to cover other wider security challenges focusing on the application area and third party.

6. REFERENCES

[1] Alguliyev, Imamverdiyev.V., &S. Ukhostat, Y. (2020). Cyber-physical systems and their security issues. Computer Security. 1(2), 212–223.

[2] Aulds, C (2020). Linux Apache Web Server Administration, lates Edition. SybexInc. 1(1)2

[3] Auxilia, D. & Tamilselvan, (2022). Anomaly Detection Using Negative Security Model in Web Application. Security models in web applications, 2 (1)34-38

[4] Bendovschi, A. (2024). Cyber-Attacks - Trends, Patterns and Security Counter measures. Proceedings on Economics and Finance, (15) 24-3.

[5] Benson, V. &McAlaney, J. (2021). Frumkin, L.A.: Emerging threats for the human element and Counter measures in current cyber security landscape. Psychological and Behavioral Examinations in Cyber Security, 1(2) 266–271.

[6] Bharadwaja, Sun.W., Niamat, M.&Shen, F (2021). Collabra Xen Hypervisor based Collaborative Intrusion Detection System, Eighth International Conference on Information technology: New Generations, 1(2) 695-700.

[7] Cabaj, K., Kotulski, Z., Księżopolski, B., &Mazurczyk, W. (2022) Cyber security: trends, issues, and challenges. EURASIP Journal on Information Security. 2(1)34-41

[8] Cenzic (2024). Cenzic, Application Vulnerability Trends Report: 2014, description available at: www.cenzic.com (website visited on April 12, 2021).

[9] Fan, Lejun, Yuanzhuo Wang, Xueqi Cheng, Jinming Li, & ShuyuanJin (2020). Privacy theft malware multi process collaboration analysis. Security and Communication Networks 8 Arabian Journal for Science and Engineering (1) 3171–3189.

[10] Gross, M. L., Canetti, D., &Vashdi, D. R. (2020). Cyber terrorism: its effects on psychological well-being, public confidence and political attitudes. Journal of Cyber Security, 3(1), 49–58.

[11] Hydara, I (2023). Current state of research on crosssite scripting (XSS) a Systematic Literature Review. Technol. 5(8), 170–186

[12] Juan A, Juan Manuel PikatzaAtxa, (2015). Intrusion Detection in web applications using text Mining. Journal of Artificial Intelligence, 4 (2) 56-59

[13] Kieyzun, A. (2023). Automatic creation of SQL injection and crosssite scripting attacks. In: Proceedings of the 31st International Conference on Software Engineering. IEEE Computer Society.IOSR Journal of Computer Engineering (IOSR-JCE), 19(5), 01-04.

[14] Kruegel. C &Vigna, G (2021). Anomaly Detection of Web-Based Attacks, Proc. 10th ACM Conf. Computer

and Comm. Security (CCs'03), Oct. 2013

[15] Mazari, A.I. (2021). Cyber terrorism taxonomies: definition, targets, patterns, risk factors, and mitigation strategies. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, IGI Global, Hershey 1(2) 608–621.

[16] Mohammed A., Ambusaidi, Xiangjian He, Priyadarsi Nanda &Zhiyuan Tan, (2020). Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm. IEEE transactions on Computers,2(1) 2986 - 2998.

[17] Rajiv. A, A.Prashanthi, Ch. Bharadwaja (2022). Web Server Security evaluation and analysis. International Journal of Computer Science and Mobile Computing, 1(2)23-32.

[18] Sekar, R. (2023). An Efficient Black Box Technique for Defeating Web Application Attacks", Proc. Network and Distributed system security sump. (NDSS) 3(1)12-19.