INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

A WEB SERVER APPLICATION FOR INTRUSION DETECTION UTILIZING CRONJOB SCHEDULING ALGORITHM

UMEJURU DANIEL[1], EDAFEAJIROKE MICHAEL FAVOUR[2]
[1, 2,] Department of Computer Science, University of Port Harcourt Choba, Nigeria
E-mails: daniel_umejuru@uniport.edu.ng , michael.edafeajiroke@uniport.edu.ng

D.O.I: 10.5281/zenodo.18270092

ABSTRACT

Webserver application environment has become an attractive target for hackers due to high increase on deployment of web applications and adoption of cloud computing technologies. A webserver is a gateway through which the entire internet population connects to with the aim of sharing resources or providing online services. Webserver based applications are becoming the most common way to deliver and access online services, this trend also gained a higher increase especially during the covid-19 era. There is a high 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 even as technology evolves. To prevent common attacks of content corruption and 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 intrusion prevention and detection on webserver application environment using cronjob scheduling techniques has been developed. The new system adopted object oriented analysis and design methodology and was implemented using PHP7 server side scripting programming language, Laravel MVC framework and MYSQL relational database for the backend. The system has been developed, tested and was able detect and prevent intruders from gaining malicious access into the webserver application environment and also was able to send quick response message to the admin through sms messaging and emailing system. This quickly prompts the admin of the attempted intrusion and preventive measures are then taken to safeguard webserver. Hence this work will be beneficial to web developers and webserver administrators.

KEYWORDS: Web Server, Intrusion, Detection, Scheduling, Algorithm, Distributed Computing

1.0 Introduction

Since the arrival of cloud computing and other internet enabled technologies for the delivering of services globally, webserver applications environment is now used more than ever before. presently, we place more interest on web technology for everything we do from social contact to

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

the rendering of key services, this process now allows malevolent actors to invade into people's privacy, this now create risk in the internet space, a phenomenon known as cyber assaults. (Sreekanth et al 2023). Security talks about the confidentiality, integrity, and availability of systems and while data confidentiality talks about the ability to ensure that information is private to only authorized parties which must be guided from unauthorized parties to have access to, integrity reflects the accuracy of information which necessitates technology and processes that prevent unauthorized parties from inappropriately modifying information and availability refers to the ability to ensure that information is available to authorized parties and protected from unauthorized users and availability refers to the ability to ensure that information is available to authorized parties and protected from unauthorized users also (Samuel et al 2022).

Since the Internet became an open system, web server applications environments have been increasingly popular for delivering important services on a global scale, among other things. In a study conducted by (Sreekanth et al 2023), it was discovered that webserver attacks cost enterprises more than 100 times more than malware, and 50 times more than viruses, worms, and trojans each year. Several intrusion detection systems, among others, have recently been created and assessed. A webserver is a computer programme that fetches and serves web pages that are requested by a client. Web pages can be saved on the host computer's hard disc or on the hard drive of another computer. The main purpose of network security is to keep intruders at bay. However, the purpose of a Web site is to give the rest of the world regulated access to the network. The Apache web server is the most extensively used web server, with over 40 million web applications running on it, powering approximately 70% of all websites. The confidentiality, integrity, and availability of an organization's Web assets hosted on a distant server (e.g. Web pages and customer databases), as well as the organization's reputation, are all protected by webserver security. Webserver intrusion detection is the technique or act of monitoring events in the webserver environment and accurately reporting them to the right authorities when suspicious activity is detected via communication channels if IDS is present.(Victoria et al 2021)

Around the world, the utilization of Internet services and webserver-hosted application environments is skyrocketing. However, it has been shown that disrupting the operation of the Internet by targeting its infrastructure using internet services and protocols is rather simple. Following the widespread adoption of cloud computing and other internet technologies, malevolent hackers have turned their focus to the vulnerability of webserver application environments in order to exploit and obtain access to critical information. The number of intrusion attempts has steadily increased in recent years, with data indicating that up to 75% of cyber-attacks target webserver applications (Valeur et al 2021). In the field of webserver application security, intrusion detection methodology is still relatively young.

In the course of the last decade, the application and reception of webserver based applications like internet banking, online trading applications, online social contributing to a blog stage, long range informal communication locales, and other such administrations has soar. The webserver climate is logically turning into the essential hotspot for basically all application organization, and its

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

intricacy is developing, representing various security issues, including intrusions into organization protection. The climate where online applications are conveyed (webserver application climate) ought to be painstakingly planned and go through intensive security testing, and cognizant improvement procedures ought to be supplemented by an interruption recognition foundation that can recognize assaults and give early admonition about dubious action, as suggested by (Kumar et al. 2024). Therefore, webserver security stays a hotly debated issue among analysts, attributable to the quick development of web innovation.

2.0 Overview of the Webserver

An apache webserver is an online Server based piece of software that fetches and serves web pages that have been requested by a client through a web browser. Web pages can be saved on the host computer's hard disc or on the hard drive of another computer (Abomhara, et al.2022). A Webserver is a giant computer that stores web content. Web servers are typically used to host web applications, although they can also be used for gaming, storage, FTP, and email. Web server software responds to requests for web resources, whereas a website is a collection of web pages. According to (Aulds, 2020) the Webserver application environment responds to client requests by either sending a file to the client associated with the requested URL or generating a response by calling a script and talking with the server's database.

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. (Zhang and Yuan 2022)

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 (Cova et al. 2021)

2.1 Types of Web Server

1. ApacheHTTP Server

The Apache Software Foundation has produced the world's most popular web server. The Apache web server is free software that may be installed on a wide range of operating systems, including

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

Linux, Unix, Windows, FreeBSD, Mac OS X, and others. The Apache Web Server is used by about 60% of web server machines.

2. Internet Information Services

Microsoft's Internet Information Server (IIS) is a high-performance Web server. This web server is compatible with Windows NT/2000/2003 (and may be on upcoming new Windows version also). Because IIS is intimately connected with the operating system, it is relatively easy to administer. It is packaged with Windows NT/2000 and 2003.

3. lighttpd

Lighttpd, pronounced lighty, is another free web server included with the FreeBSD operating system. This open source web server is quick, safe, and uses very little CPU power. Lighttpd is also compatible with Windows, Mac OS X, Linux, and Solaris.

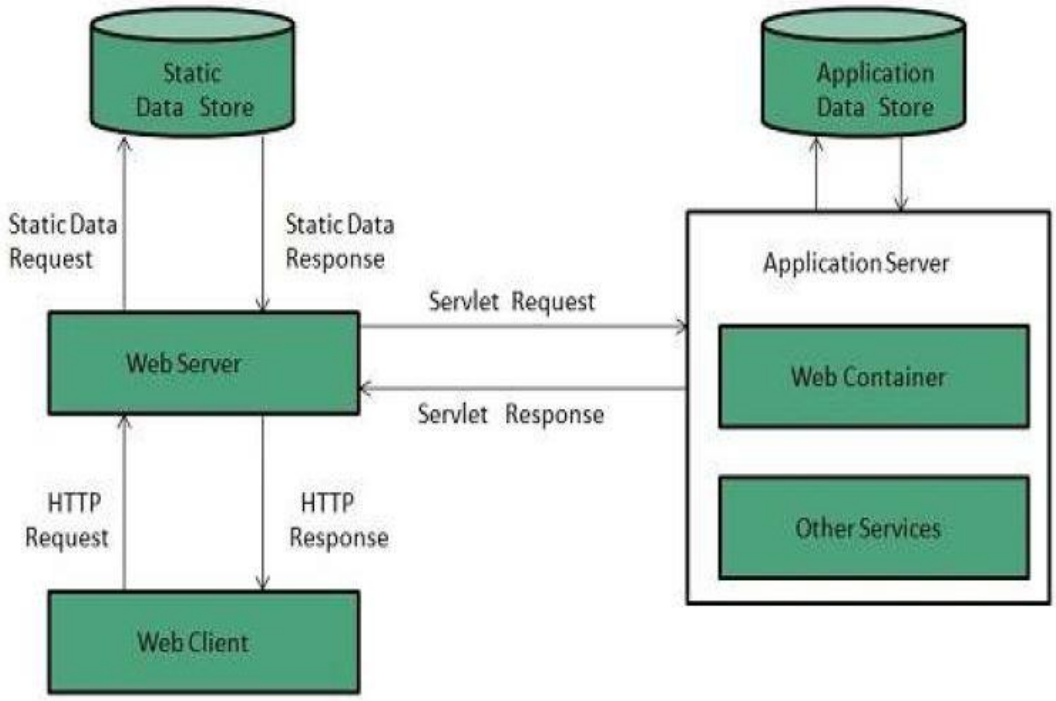

Figure 2.1: *Web Server Architecture*
(***Source***: *http*://www.tutorialspoint.com/internet_technologies/web_servers.htm accessed 12-04-2021)

2.1.2 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

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

widely utilized Web Server on the Internet. (Rajiv et al. 2012).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. Integrity and Privacy

A web server is our computer's mother board, upon which other components are built, and it serves as a portal through which the entire internet population can peer in. Integrity and privacy are the major concerns in preventing common assaults of content tampering and data theft.

2. Common Gateway Interface (CGI) Script

CGI scripts are constant projects that work on Web servers. They deal with an assortment of client inputs and, thus, get input from internet browsers, access data sets, and return data to the customer program. CGI scripts are like little workers. Accordingly, a defective content could be an objective for an assault. In two ways, CGI projects can uncover security defects: They could show data from the host that could help assailants in breaking into the worker. The client sources of info could be adequately troublesome to establish executable orders, causing the host machine to endure hurt. (Benson et al. 2022).

3. Access Control Access Control

Gaining access to see what's on a Web server, and more particularly, to execute what's on a Web server in the case of CGI scripts.

4. Transmission of data via TCP/IP Security was not a priority when the TCP/IP protocol was created. Therefore, right when characterized chronicles are moved from the Web laborer to the program, or when the end-customer conveys private information back to the specialist through a wrap up structure, it is weak against network snooping. (Mohammed et al 2021)

2.2 Types of IDS Attacks

1) Phishing

Phishing is the act of sending messages that tends to come from solid sources in deals to get individual information or persuade customers to take action. It is a blend of social orchestrating and movement confusion. It might be a hurtful relationship with an email that taints your machine. It may really be a relationship with a dangerous site needed to trick you into presenting malware or uncovering fragile data.it expected to deceive you into introducing malware or uncovering delicate data (Enoch 2020).

2) Drive-by attack

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

Drive-by download assaults are a typical way for malware to spread. Designers seek after frail objections and supplement a harmful substance into constrained by the designer so the HTTP or PHP code on one of the pages. This substance may obviously introduce malware on the PC of a guest to the site, or it might divert the difficulty to a site. (Gupta et al. 2022)

3) 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. (Christopher et al 2023)

4) 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. (Kieyzun 2022)

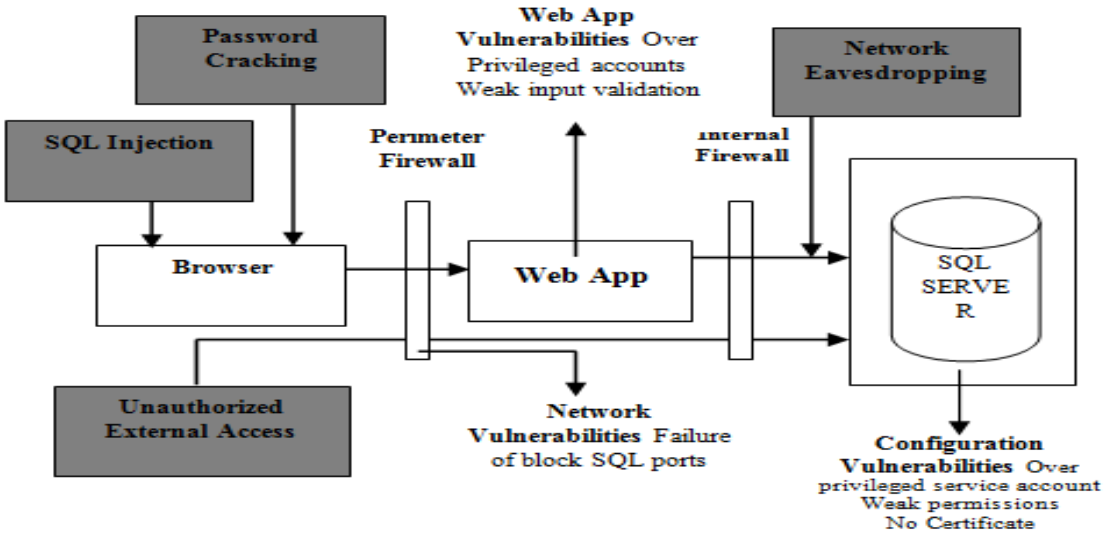

Figure 2.2: SQL Injection Attack

(Source: A Complete Strategy for Web Application Security, (Humayun et al. 2020**)**

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

2.2.1 Intrusion Detection System (IDS):

According to (Taha et al. 2021), an intrusion detection system (IDS) is a device or software programme that monitors network or system operations and detects any hostile activity. There are various parts to IDS:

1. Sensors that generate security events

2. A console to display events and alarms as well as control the sensors.

3. A central engine that stores the events logged by the sensors in a database and utilizes a set of rules to generate alarms based on the events.

IDS can be classed as Host-based Intrusion Detection System or Network-based Intrusion Detection System, depending on the stated objective or information source.

Host-based intrusion detection system

The earliest type of intrusion detection programming was built for the host-based intrusion detection system, with the original target system being the mainframe PC, where outside cooperation was uncommon.

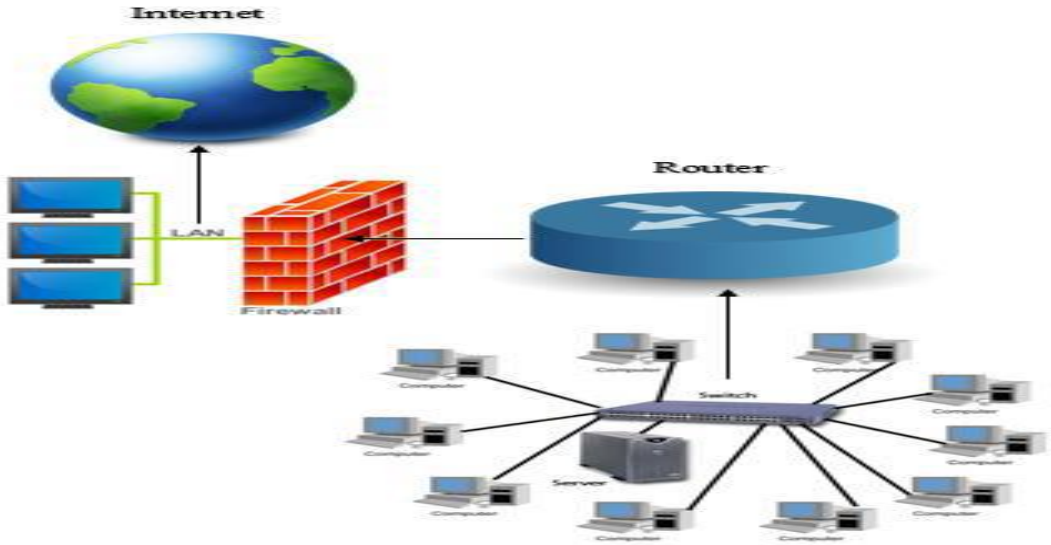

Figure 2.3: Host based intrusion detection system (**Source:** Ragupathi, 2023)

3.0 Methodology

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

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.

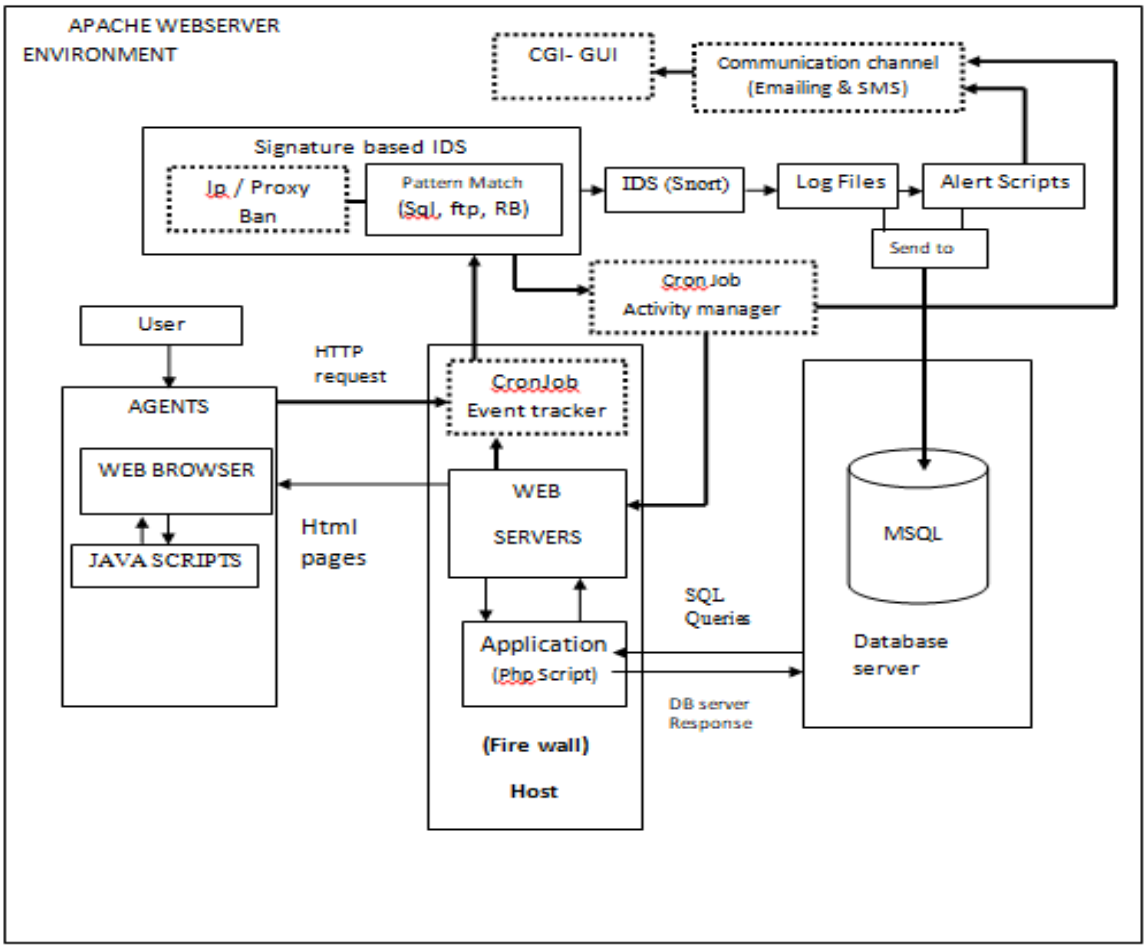

Figure 3.1: Architecture of the Proposed System

The proposed system architecture explanation is given below:

The Cronjob scheduling technique: is used to track every event that occurs on the server in order to trigger the IDS system to start working with the goal of keeping the webserver stable in order to improve resource availability and minimize quota utilization as seen in the previous system. The cronjob event tracker receives all the https requests, analyses them, and then passes them to the

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

IDS scripts for further analysis. All actions in the system are managed by the cronjob activity manager.

I. **Signature-based method**: compares given network traffic and log data to existing attack patterns in other to identify possible known attacks.
II. **The ip / proxy ban component:** was added to existing IDS scripts to provide an intrusion prevention mechanism on the server by capturing the user's IP and determining if the request is a proxy (bot request), etc. If a proxy is discovered at that stage, the request will be denied and the IP will be banned from further accessing the system.
III. **The CGI graphical user interface**: is a key component that bridges the gap between the log file and the web server administrator, given how time-consuming viewing and reading log files on the server may be. It presents the data entered into the database in a more comprehensive and visually appealing format for analysis and decision-making.
IV. **Communication channel components:** deliver instant alerts to the webserver administrator through email and SMS, calling for preemptive action to be taken if necessary.

4.0 Results and Discussion

Figure 4.1: Home page design layout

Figure 4.1 shows the proposed system landing page design interface which is usually lunched imediately the program runs or initiated.

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

Figure 4.2: Login page design interface

Figure 4.2 shows the user login design interface through which valid users can gain access to the system.

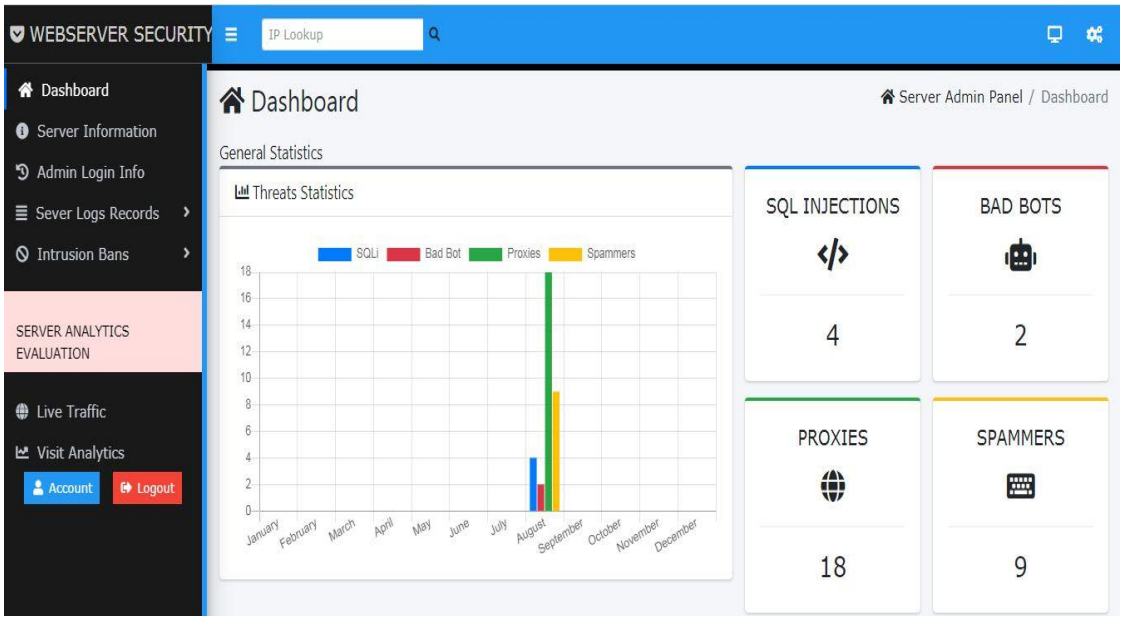

Figure 4.3: User Dashboard interface

Figure 4.3 shows the user dashboard interface through which user can navigate to other modules; it also shows some historical data on it for a quick preview.

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

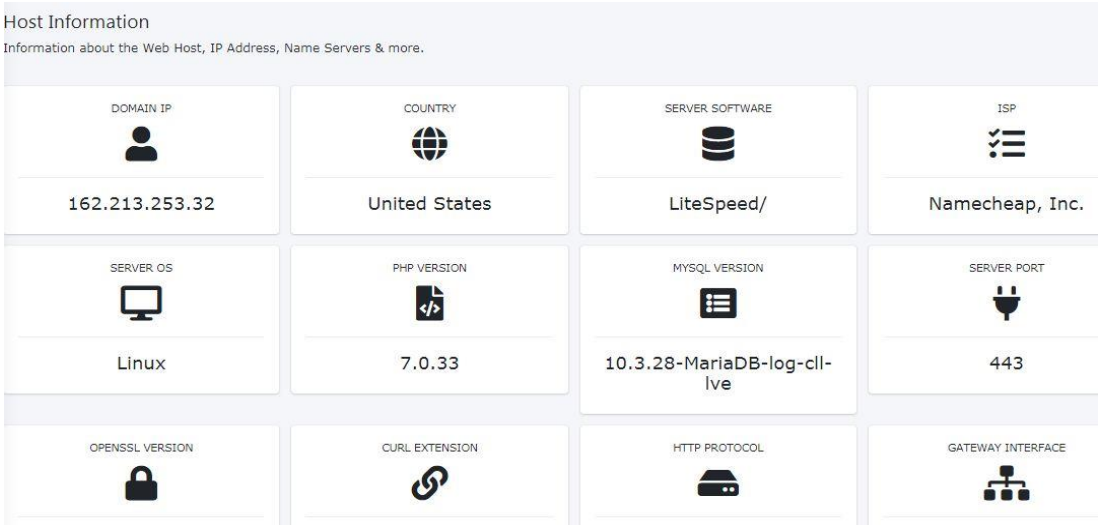

Figure 4.4: Host information GUI

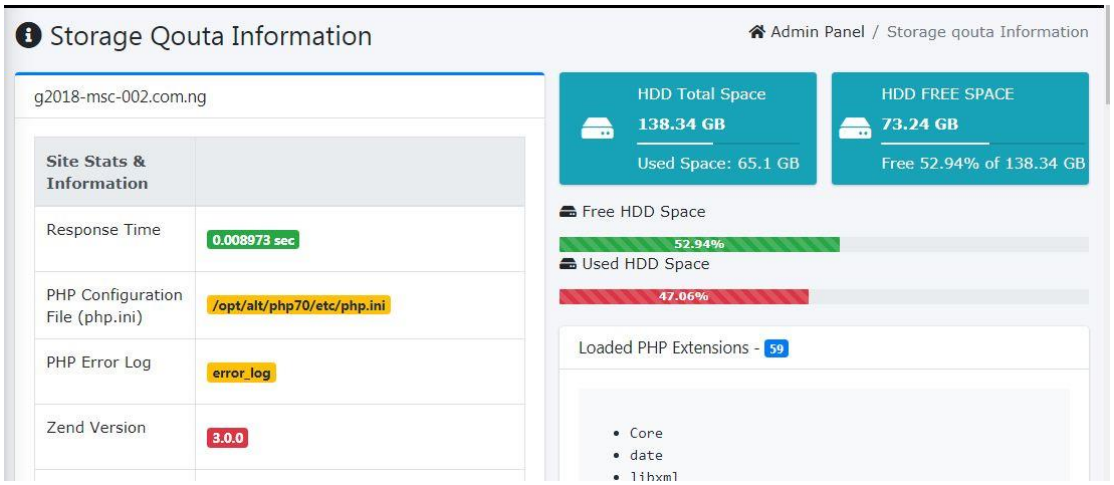

Figure 4.5: Server Storage Quota GUI

Figure 4.5 shows the server storage quota, hence it contained the server storage space and usage statistics such as available storage space and used storage space.

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

Figure 4.6: File statistics and count interface

Figure 4.6 shows the total number of files on the server which will assist the server administrator to know when their additional fill added and who adds the file.

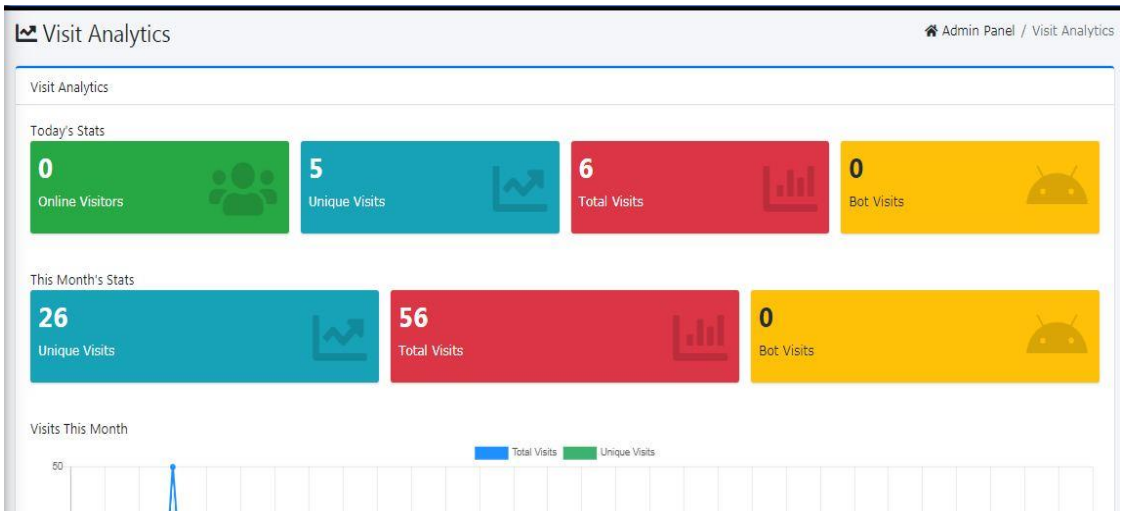

Figure 4.7: Server visit analytics

Figure 4.7 shows the numbers of visitors on the server

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

INTERNATIONAL JOURNAL OF MODERN TECHNOLOGY AND ENGINEERING RESEARCH
VOLUME-4, ISSUE-1, JANUARY, 2026 ISSN (Online): 2158-2268
https://caarnjournals.com/index.php/ijmter/index
A Peer Reviewed (Refereed) International Journal
Open Access

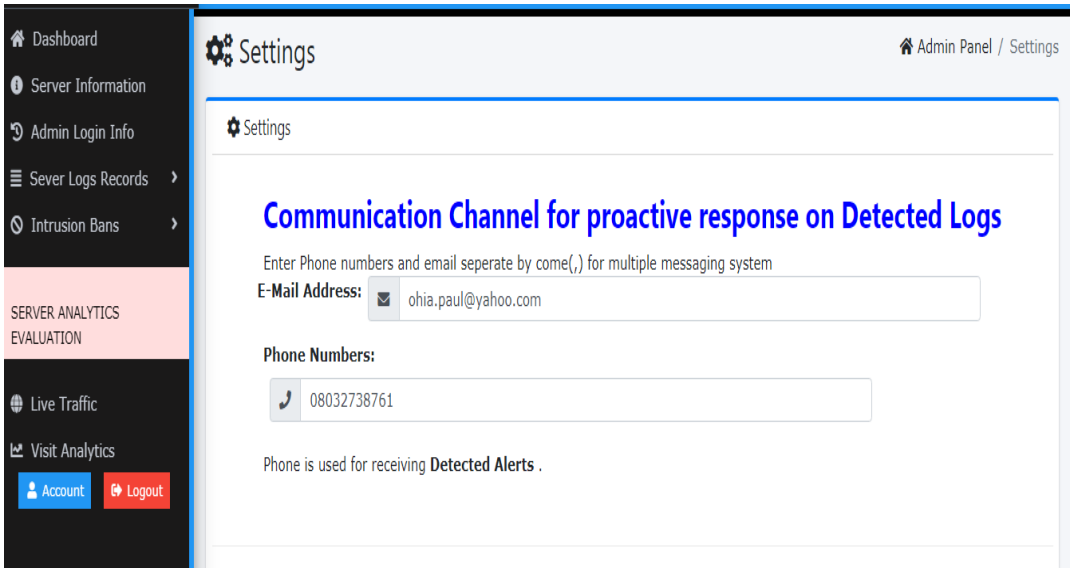

Figure 4.8: communication channel

Figure 4.8 shows the communication channel interface through which user's email and phone number is added into the system for log alerts and updates.

4.5 Results Discussion

Webserver intrusion and prevention system remain a new area of interest among programmers and researchers following the emergency and high adoption of cloud computing technologies and emergence of new web technologies. This has been the driven factor on the increase of intruders among others on the webserver application environment using different tools and means to gain unauthorized access into the webserver. No matter how a web application is secured if the webserver application environment is not secured the entire system can be hijacked by an intruder. The result obtained from this study is an improved webserver application intrusion detection and prevention system using cronjob scheduling algorithm. The webserver is usually measured by storage quota which is affected critically based on the usage of resources on webserver especially were shared hosting is been deployed within the environment, Recent intrusion detection system were IDS programs runs on a continues background check this slowdowns environment it slows down the server performance which increases the resource limit usage of the entire system. Such tends to promotes DOS attack. The application of cronjob in this new system helps reduces the resource limit usage by initiating the intrusion detection modules only when there is an event or action on the server not on a continuous process, Hence every action or events that occur on the server is been captured and controlled by the cronjob manager. The developed system also detect and prevents intrusion in diverse webserver as intrusion tricks are usually used to hijack the environment on most cases 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

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

alerts to the admin on attacks for proactive actions were the need arises made possible by the SMS and emailing feedback system mechanism.

5.0 Conclusion

Webserver security comes to being from confidentiality, integrity, availability of appropriate information and authentication. A poorly secured webserver application environment can cause a serious harm to an organizational data no matter how secured the application is assumed to be. The use of internet/web based applications is increasing to a great extent with the abnormal and malicious activities also been recorded on daily bases. So Intrusion Detection Systems have become a needful component on the webserver application environment. In this Research, we present and implemented an Intrusion Detection System on webserver application environment by applying Cronjob scheduling technique to enhance inefficient detection of various categories of webserver intrusions and also prevent attacks using known pattern matching methods. The performance of our new system has also been evaluated by deploying it into a namechip live share hosting webserver to obtain our log dataset which showed reasonable detection rates. The developed system can be deployed into any webserver application development environment.

REFERENCES

Abomhara, M.& Køien, G.M. (2022). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. *Internet of things and cyber security 4*(1), 65–88.

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

Benson, V. &McAlaney, J. (2022).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.

Christopher, K. Giovanni, V. & William Robertson, (2023). A multi model approach to the detection of web based attacks", *Journal of Computer Networks* 1 (8) 41-55.

Cova, M. Balzarotti. D., Felmetsger, V &Vigna.G. (2021).Swaddler: An Approach for the Anomaly-Based Detection of State Violations in Web Applications. *Proc. Int'l Symp. Recent Advances in Intrusion Detection* 1(7) 2-15.

Edafeajiroke, M. F., Abdulsalam, S. O., Shuaib, M. U., & Babatunde, R. S. (2024). Development of an Intrusion Detection System using ANOVA Feature Selection and Support Vector Machine Algorithms. Journal of Applied Computer Science and Intelligent Technologie, 4(1), 8908. https://doi.org/10.17492/ Computology.v4i1.2406

Enoch, S.Y (2020).A systematic evaluation of cyber security metrics for dynamic networks. *Computer Networking* 144, 216–229.https://doi.org/10.1749 2/computology.v4i1.2406

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications

Gupta, Shashank, & Gupta, (2022). XSS-SAFE: A server-side approach to detect and mitigate crosssite scripting (XSS) attacks in JavaScript code. *Arabian Journal for Science and Engineering* 41(3) 897–920.

Kieyzun, A. (2022).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.

Kumar.S., & Somani, V. (2024). Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques. *International Journal of Advance Research in Computer Science and Management,* 4(4),125-129.

Mohammed A., Ambusaidi, Xiangjian He, Priyadarsi Nanda &Zhiyuan Tan, (2021). Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm. *IEEE transactions on Computers,*2(1) 2986 - 2998.

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.

Samuel, K. O., & Osman, W. R.(2022) Cyber Terrorism Attack of the Contemporary Information Technology Age: Issues, Consequences and Panacea. *International Journal of Computer Science and Mobile Computing,* 3(5),1082-1090.

Sreekanth, G. Shakeeba S. Khan, R. &Tuteja R. (2023). Security in Cloud Computing using Cryptographic Algorithms, *International Journal of Innovative Research in Computer and Communication Engineering* 3(1), 66-78.

Taha, A.F.; et al. (2021) Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs. *IEEE Trans. Smart Grid* 9(2), 886–899

Valeur. D, Vigna. G, Balzarotti, F, Robertson, C. Kruegel, &Kirda E, (2021). Reducing Errors in the Anomaly-Based Detection of Web-Based Attacks through the Combined Analysis of Web Requests and SQL Que-ries. *Journal of Computer Security,* 17, (3)305-329.

Victoria Felmetsger, Ludovico Cavedon, Christopher Kruegel,& Gio-vanni Vigna,(2021). Towards Automated detection of logic vulnerabilities in web applications, *International Journal of Advanced Research in Computer Science and Software Engineering* 1(4)55-63.

Zhang &Yuan, (2022).Proposed a Study of database intrusion detection based on improved association rule algorithm, *International Journal of Advanced Research in Computer Science and Software Engineering* 1(2)23-25

Received: 25th Nov., 2025 | Accepted: 22th Dec., 2025 | Published: 15th Jan., 2026
Publisher: Valenciao-Giant Excellence Publications