iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 Issue: I Month of publication: January 2026

DOI: https://doi.org/10.22214/ijraset.2026.77039

ShieldX- Customized Firewall for Preventing Cyberattacks in Cloud

Thilakaveni P [1], Jasvin Sabari R S[2], Kabinesh S[3], Kiruthickkumar S[4], Nitheesh Kumar C[5], Sujith Harshal M[6]
[1]*Lecturer, Department of Computer Engineering, PSG Polytechnic College*
[2, 3, 4, 5, 6]*Student, Department of Computer Engineering, PSG Polytechnic College*

Abstract: Cloud computing is being widely adopted across many organizations due to its flexibility and ease of access. However, as more systems move to the cloud, protecting them from cyber threats has become a serious concern. Most traditional security tools, such as firewalls and antivirus software, respond only after an attack has already affected the system. This project, titled ShieldX, focuses on developing a firewall solution that works in a preventive manner by identifying threats at an early stage. The ShieldX system continuously observes network traffic, running processes, and file activities to identify suspicious behavior, including ransomware attacks, phishing attempts, logic bombs, and unauthorized access. Python is used to implement security rules and automate response actions, while cloud-based logging is used to store security events for later analysis. By stopping threats before they cause damage, ShieldX helps improve data safety, system availability, and overall cloud security in an effective and economical way.

Keywords: Cloud Computing, Cybersecurity, Preventive Firewall, Intrusion Detection, Ransomware Protection, Phishing Detection, Python-based Security, Network Monitoring, Cloud Security, Threat Prevention.

I. INTRODUCTION

Cloud computing has become an essential part of today’s digital environment, allowing organizations to manage the data, applications, and services more efficiently. While cloud platforms offer many advantages, they also attract a growing number of cyberattacks. Threats such as malware infections, data breaches and unauthorized access have increased as attackers to target cloud-based systems. In many cases, conventional security solutions are unable to prevent these attacks in advance and only detect them after system compromise.

To overcome these limitations, the ShieldX firewall has been designed as a preventive security mechanism which is suitable for cloud environments. Instead of depending only on post-attack analysis, ShieldX continuously monitors system behavior and network activity in real time. The firewall uses rule-based filtering to identify abnormal patterns and automatically applies security measures when suspicious activity is detected. In addition, the security logs are stored in the cloud, allowing administrators to monitor events and analyze potential risks. By combining real-time detection with automated response, ShieldX provides improved protection against modern cyber threats without significantly affecting system performance.

II. OBJECTIVE

The objectives are:

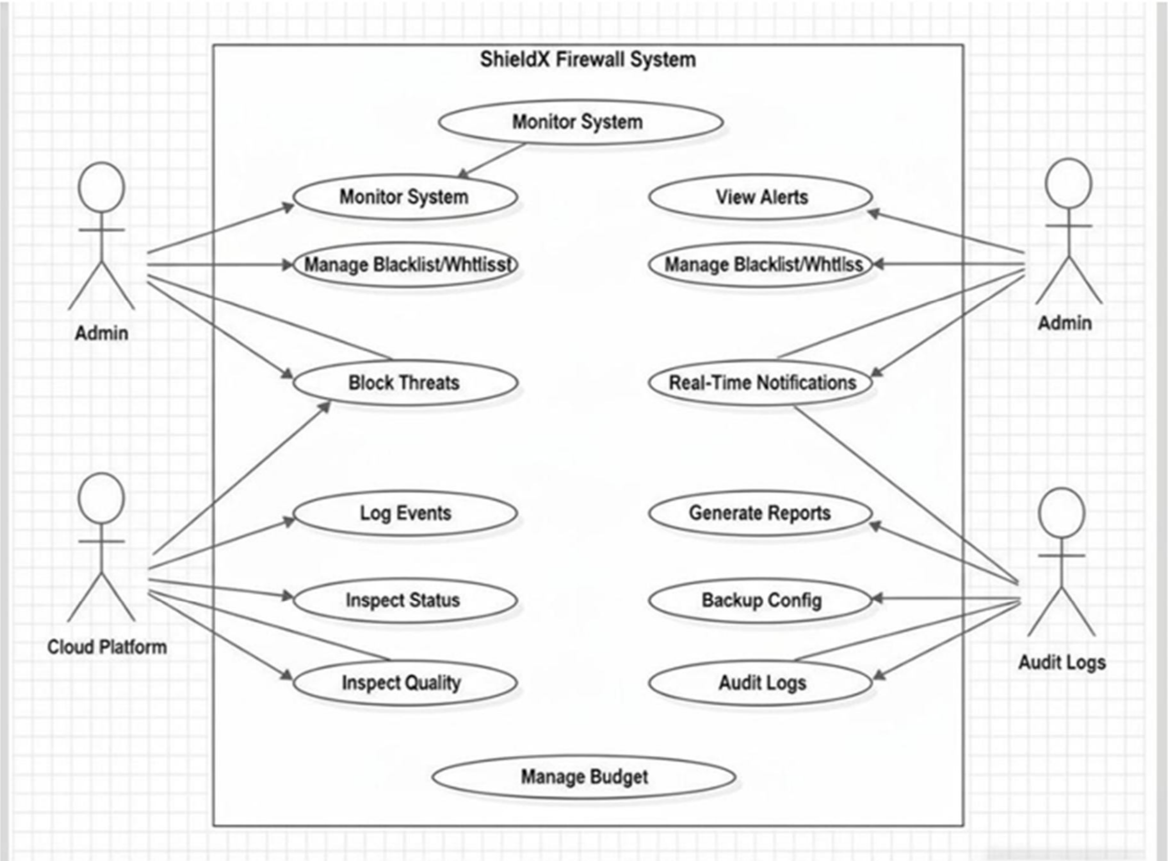
1) To design a proactive firewall system for cloud security
2) To monitor network traffic and system activities in real time
3) To detect and block malicious processes and unauthorized access
4) To integrate cloud storage for secure log management
5) To provide a user-friendly dashboard for security monitoring

III.WORKING PRINCIPLE

The ShieldX firewall works through continuous monitoring and automated threat prevention. The system watches incoming and outgoing network packets, system processes, and file activities to spot abnormal behavior. Using predefined rules and known attack signatures, the firewall analyzes the data to find potential threats. When it detects malicious activity, ShieldX quickly takes action by blocking IP addresses, terminating suspicious processes, or restricting unauthorized file access. All security events are logged and stored securely in the cloud, and real-time alerts are sent to administrators. This ongoing cycle of monitoring, detection, response, and logging ensures effective protection against cyberattacks.

1) The ShieldX system operates with continuous, real-time surveillance of all network activities, system logs, and running processes. It constantly monitors the data packets, user behavior and the system performance to detect any suspicious patterns. This stage ensures that every transaction, connection, and process is tracked to provide a comprehensive view of the system's security posture.
2) ShieldX utilizes both signature-based and rule-based detection techniques to identify anomalies or potential threats. Signature-based detection recognizes the known malware patterns or attack signatures, while rule-based detection applies predefined conditions and thresholds to identify unusual behavior. Together, these methods allow ShieldX to detect both known and emerging cyberattacks with high accuracy.
3) Response Once when a threat is detected, the system immediately initiates its automated response mechanism. ShieldX takes proactive measures such as blocking malicious network packets, terminating suspicious or harmful processes, isolating affected areas, and preventing any unauthorized data transfer. This rapid response minimizes potential damage and ensures that the critical resources remain secure and operational
4) All detected incidents and system actions are thoroughly logged and documented for future analysis. The ShieldX dashboard provides administrators with real-time alerts, visual reports, and the security summaries. Additionally, the system integrates with cloud based log management tools, enabling centralized access and efficient auditing of security events. This stage ensures full transparency and accountability across all security operations.
5) The final stage focuses on continuous improvement and optimization. Using feedback from past incidents, ShieldX refines its firewall rules, updates its detection algorithms, and enhances the overall system performance. Through machine learning and data analysis, the system becomes smarter and more adaptive over time, ensuring improved threat detection, faster response, and stronger protection against evolving cyber-attacks.

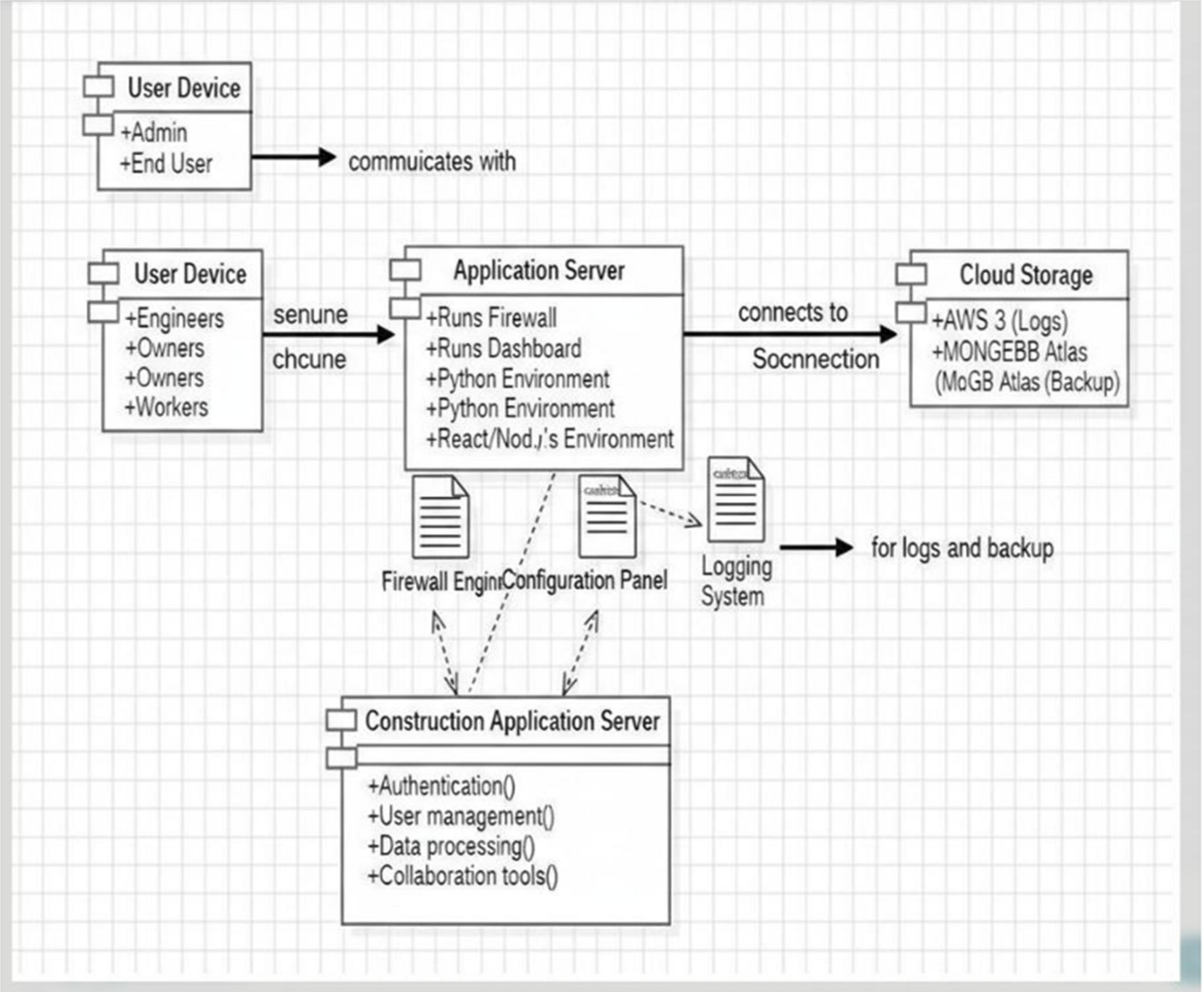
IV. USE CASE DIAGRAM



ShieldX Firewal System Use Case Diagram

The ShieldX use case diagram outlines the interactions between system actors and key functions. Users begin by signing in securely, then access a dashboard showing incident reports. They can submit new reports, upload evidence, and track report status. Administrators handle report verification, assign tasks, update progress, and generate system analytics. The integrated AI engine categorizes and prioritizes incidents automatically. Developers update the system based on user and stakeholder feedback, ensuring continuous improvement and adaptability to real-world needs.

V. DEPLOYMENT DIAGRAM



The deployment diagram illustrates the physical architecture of the ShieldX system, highlighting the distribution of software components across various hardware nodes. Users, including admins, engineers, owners, and workers, access the system through their respective devices, which communicate with the central Application Server. This server runs the dashboard, firewall, and both frontend (React/Node.js) and backend (Python) environments. The Construction Application Server handles domain-specific functions such as user authentication, data processing, and collaboration tools. It integrates with the firewall engine, configuration panel, and logging system to ensure secure and efficient operations.

All system logs and backups are directed to Cloud Storage services—AWS S3 for logs and MongoDB Atlas for database backups. This deployment structure ensures a secure, scalable, and modular environment, capable of handling real-time user interactions, secure data storage, and AI-driven processing.

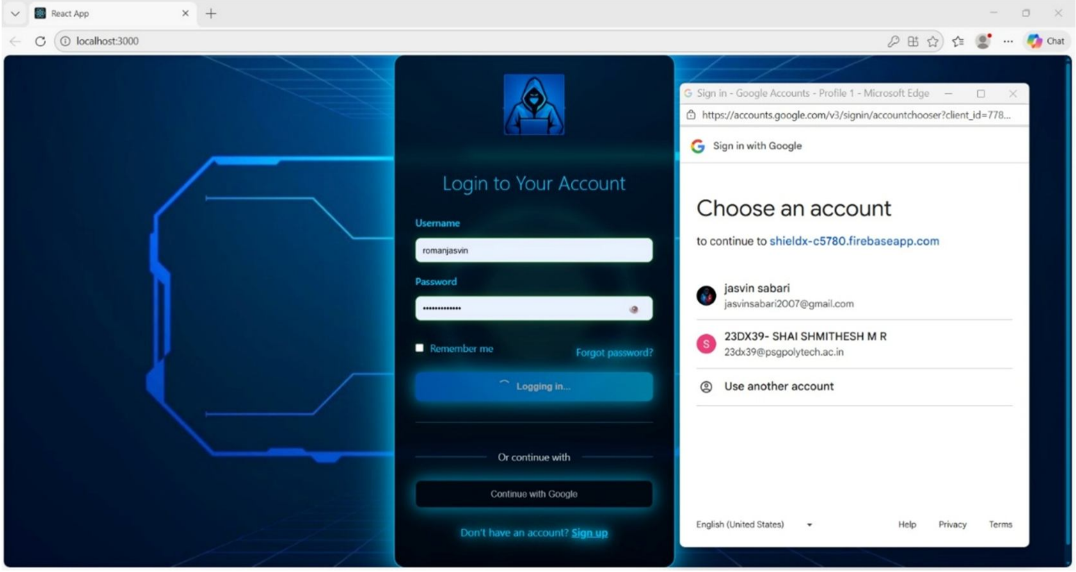
VI. MODULES

The modules are:

1) Authentication Module – User Login and Google Authentication

This module provides secure user access to the ShieldX system using login credentials or Google authentication.

The displayed output is the login page of the ShieldX system which is intended to grant secure user access. Users have the option to either input their username and password or use Google authentication for quicker and more secure access to log in. This authentication method guarantees that only legitimate users are able to access the system and it also assists in minimizing unauthorized access to cloud resources.



Login to Your Account

Username: romanjasvin

Password: ••••••••••••

□ Remember me

Sign in - Google Accounts - Profile 1 - Microsoft Edge

https://accounts.google.com/v3/signin/accountchooser?client_id=778...

Choose an account

to continue to shieldx-c5780.firebaseapp.com

jasvin sabari
jasvinsabari2007@gmail.com

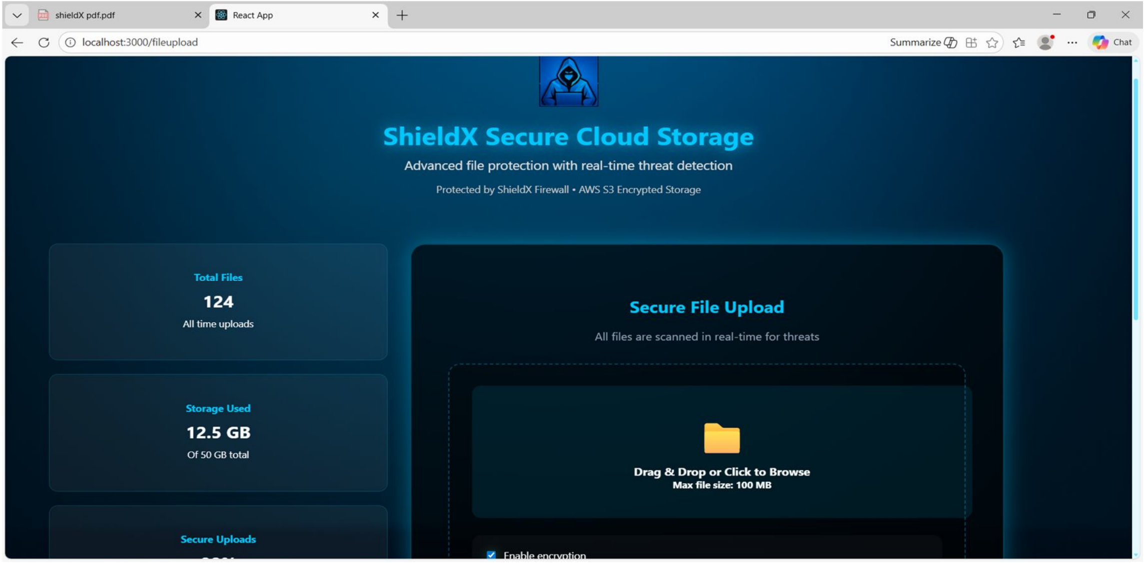
23DX39- SHAI SHMITHESH M R
23dx39@psgpolytech.ac.in

Use another account

Fig. 1 The output of the login page

2) Cloud Storage Module – Secure File Upload

This module allows users to upload files securely while performing real-time threat scanning before cloud storage.The main interface for the upload of files in the ShieldX application is what this output portrays. It is through this dashboard that users are allowed to upload files to the cloud and each file gets an automatic check for any suspicious or malicious activity before it is finally stored. This procedure aids in the prevention of the system being infected with malware from files and that only safe files are uploaded to the cloud storage.



ShieldX Secure Cloud Storage

Advanced file protection with real-time threat detection

Protected by ShieldX Firewall • AWS S3 Encrypted Storage

Total Files: 124 — All time uploads

Storage Used: 12.5 GB — Of 50 GB total

Secure Uploads

Secure File Upload

All files are scanned in real-time for threats

Drag & Drop or Click to Browse
Max file size: 100 MB

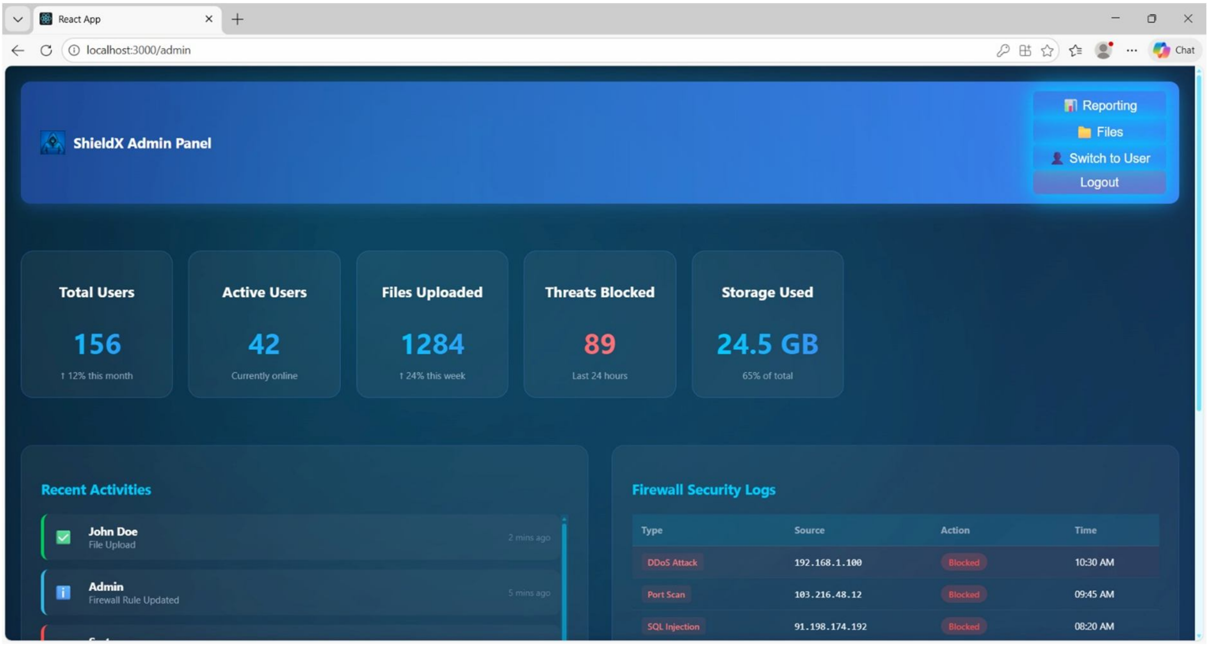
☑ Enable encryption

Fig.2 The Secure File Upload page

3) Admin Monitoring Module – Admin Dashboard

This module enables administrators to monitor users, file uploads, detected threats, and storage usage in real time.

This output depicts the control panel for the administrator of the ShieldX system. It shows among others, user activities, the number of uploaded files, and threats detected as well as storage used. The administrator can through this dashboard easily monitor the operations of the system, track security incidents, and implement actions to uphold the security of the entire system.



Total Users
156
↑ 12% this month

Active Users
42
Currently online

Files Uploaded
1284
↑ 24% this week

Threats Blocked
89
Last 24 hours

Storage Used
24.5 GB
65% of total

Recent Activities

✓ John Doe — File Upload — 2 mins ago

ℹ Admin — Firewall Rule Updated — 5 mins ago

Firewall Security Logs

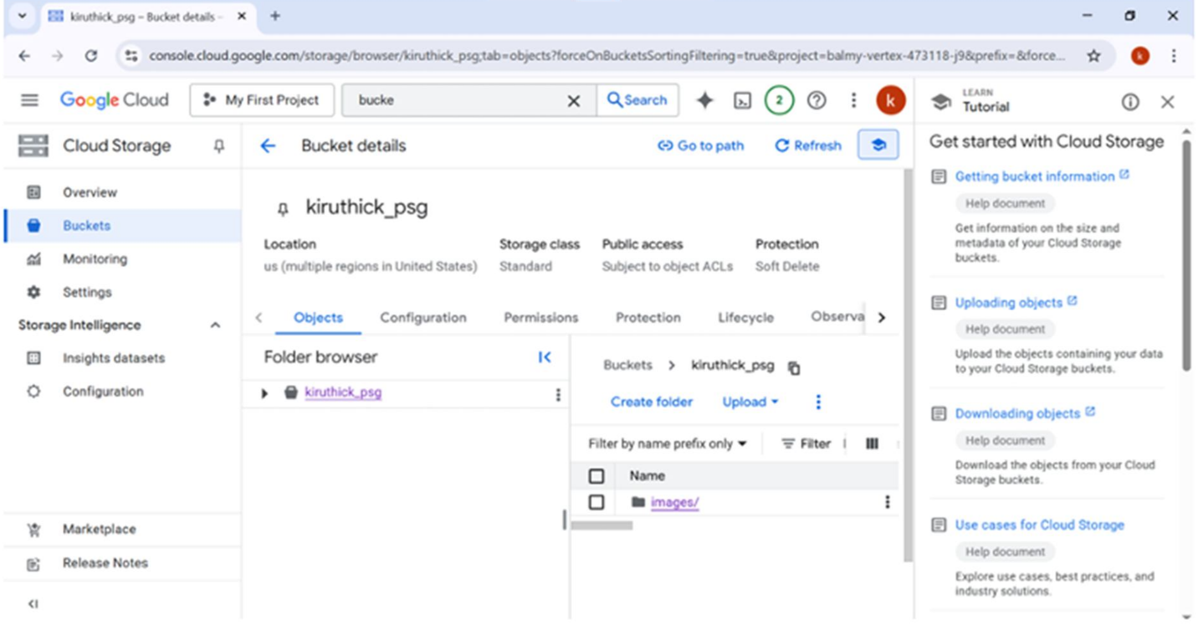
Type	Source	Action	Time
DDoS Attack	192.168.1.100	Blocked	10:30 AM
Port Scan	103.216.48.12	Blocked	09:45 AM
SQL Injection	91.198.174.192	Blocked	08:20 AM

Fig.3 The Admin Dashboard

4) Cloud Storage Module – Cloud Bucket Storage

This module ensures uploaded files are safely stored in the cloud bucket with proper organization and access control.

What the output illustrates is the cloud storage bucket that stores securely all the uploaded files. It also indicates that the files have not only been uploaded but also arranged orderly in the cloud. This storage view further allows the administrator to ascertain the presence of data, to better handle the files stored and to conduct auditing and backup operations.



console.cloud.google.com/storage/browser/kiruthick_psg;tab=objects?forceOnBucketsSortingFiltering=true&project=balmy-vertex-473118-j9&prefix=&force...

kiruthick_psg

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Subject to object ACLs	Soft Delete

□	Name
□	images/

Get started with Cloud Storage

Getting bucket information — Get information on the size and metadata of your Cloud Storage buckets.

Uploading objects — Upload the objects containing your data to your Cloud Storage buckets.

Downloading objects — Download the objects from your Cloud Storage buckets.

Use cases for Cloud Storage — Explore use cases, best practices, and industry solutions.

Fig.4 The Cloud Storage module

5) Searching for Buckets

The capability implies showing the available cloud storage buckets or folders in a list. The backend communicates with a storage API (ex. AWS S3 ListBuckets, Google Cloud Storage ListBuckets) to get and show the existing containers. Proper IAM roles and access keys are a must to make sure the access is secure. The frontend shows the user the list for more actions.

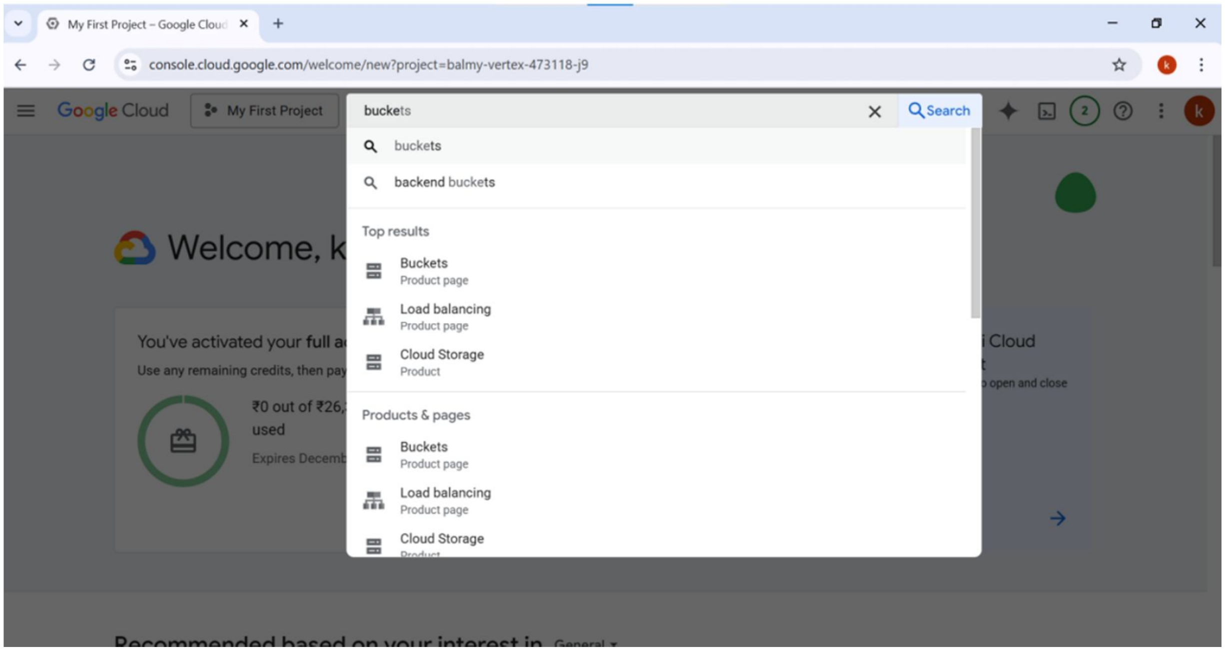
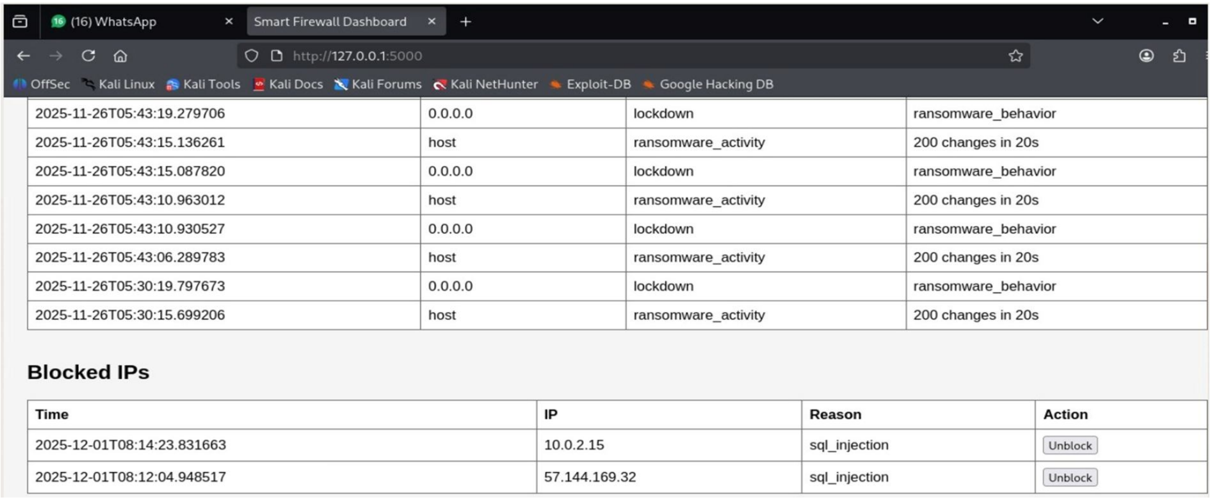


Fig.2 The Searching for Buckets page

A. Smart Firewall Monitoring and Threat Response Dashboard

The current output presents the Smart Firewall Dashboard of the ShieldX system, which is continuously showing the security events that the firewall has detected in real-time. The table records different activities such as the behavior of ransomware and changes of the files connected with ransomware, together with the time of detection and the action taken by the system. The firewall's lockdown action is automatically triggered to prevent further damage when suspicious behavior, for example, rapid file modifications within a short period, is detected. The dashboard contains a distinct section for the IP addresses that have been blocked. This section indicates the IP addresses that have been recognized as harmful, together with the cause of blocking, for example, SQL injection attempts. The unblock option enables the administrator to manually assess and lift the block on an IP address if necessary. To sum up, this output illustrates the continuous monitoring of system activity by the ShieldX firewall, threat detection in real-time, and the taking of immediate preventive measures to safeguard the system against cyberattacks.



2025-11-26T05:43:19.279706	0.0.0.0	lockdown	ransomware_behavior
2025-11-26T05:43:15.136261	host	ransomware_activity	200 changes in 20s
2025-11-26T05:43:15.087820	0.0.0.0	lockdown	ransomware_behavior
2025-11-26T05:43:10.963012	host	ransomware_activity	200 changes in 20s
2025-11-26T05:43:10.930527	0.0.0.0	lockdown	ransomware_behavior
2025-11-26T05:43:06.289783	host	ransomware_activity	200 changes in 20s
2025-11-26T05:30:19.797673	0.0.0.0	lockdown	ransomware_behavior
2025-11-26T05:30:15.699206	host	ransomware_activity	200 changes in 20s

Blocked IPs

Time	IP	Reason	Action
2025-12-01T08:14:23.831663	10.0.2.15	sql_injection	Unblock
2025-12-01T08:12:04.948517	57.144.169.32	sql_injection	Unblock

Fig.2 The blocked IP’s

VII. IMPLEMENTATION

The ShieldX firewall uses Python for backend security tasks and web technologies for user interaction. The system operates within a cloud environment, acting as a protective gateway between users and cloud resources. Network traffic and system activities are monitored in real time with Python libraries, and firewall rules are enforced dynamically. A web-based dashboard allows administrators to manage security rules, view logs, and monitor system performance. Cloud platforms like AWS and MongoDB Atlas are used for scalable log storage, ensuring secure data retention and easy access for audits.

VIII. CONCLUSION

The ShieldX firewall illustrates the benefits of a proactive approach to cloud security by preventing cyber threats before they cause harm. Through continuous monitoring, intelligent rule-based enforcement, and automated responses, the system greatly enhances data protection and system reliability. The integration of cloud-based logging and real-time alerts further boosts administrative control and transparency. This project shows that preventive firewall solutions like ShieldX are essential for securing modern cloud environments against evolving cyber threats.

REFERENCES

[1] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed. Boston, MA, USA: Pearson Education, 2017.

[2] T. Erl and E. Monroy, Cloud Computing: Concepts, Technology, Security, and Architecture, 2nd ed. Pearson, 2024..

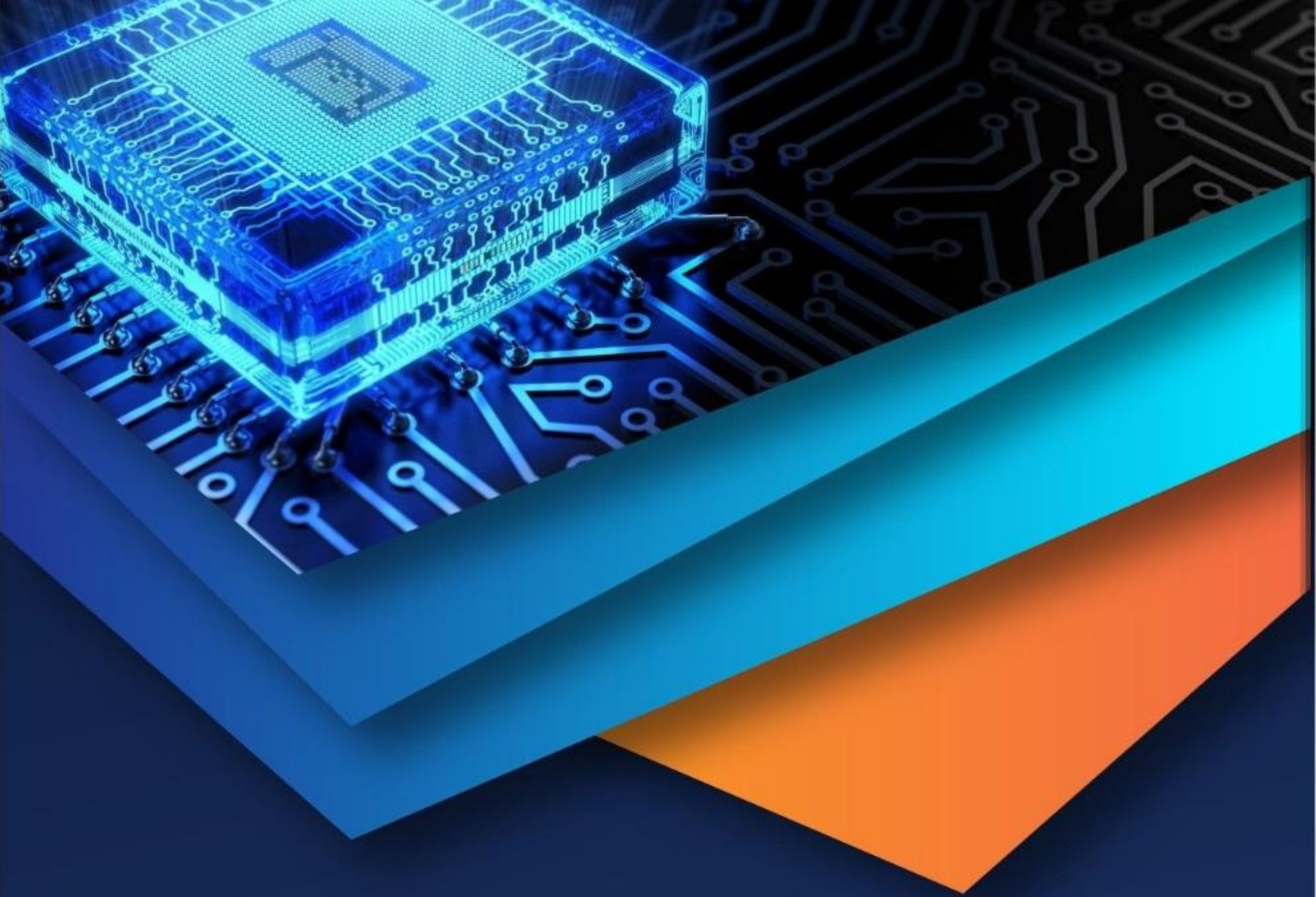
[3] D. Kim and M. G. Solomon, Fundamentals of Information Systems Security, 3rd ed. Burlington, MA, USA: Jones & Bartlett Learning, 2018.

[4] G. Rodola, D. Watts, and E. Larson, “Psutil: Cross-platform library for process and system monitoring in Python,” Psutil Documentation, 2023.

[5] P. Biondi and A. Ebalard, “Scapy: Interactive packet manipulation tool,” Scapy Documentation, 2023.

[6] M. N. Rajkumar, M. Nithya, and M. Krithika, “Security requirements and mechanisms in vehicular ad-hoc networks (VANET),” *World Scientific News*, vol. 41, pp. 200–207, 2016.

[7] J. S. Murthy, S. G. M. and S. K. G., eds., Cloud Security: Concepts, Applications and Practices. CRC Press, 2024.



10.22214/IJRASET

INDEX COPERNICUS
45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY