Project Title: Website Health Monitor with Multi-channel Alerts

Team Name: SYNOVIA

Team Members: Keerthana C , Kamal S , Suma S [Internal Mentor]

College: Vemana Institute of Technology

1. RFC-Open Source Contribution Report

This section serves as the formal, high-level document detailing the entire lifecycle of the "Website Health Monitoring System" project, specifically framed around the implementation and validation of Internet standards and its contribution to the open-source community, as mandated by the AIORI team.

RFC Implementation Sprints and Open Source Contribution Theme

Theme: Implementation and Testing of Internet Standards for Web Service Reliability

Focus Areas: Real-time Web Health Monitoring, Multichannel Alerting, and Secure Transport Validation

Organized by: Advanced Internet Operations Research in India (AIORI)

Collaborating Institutions: Vemana institute of technology

Date: November 5, 2025

Prepared by: Keerthana C[Student], Kamal S[Student], Suma S[Internal mentor], Vemana institute of technology

Contact: [Your Email / phone/Project GitHub Link]

1.Executive Summary

This report chronicles the implementation and validation phases of the "Website Health Monitoring System" (Code Name: Vigil), a mission-critical, high-availability monitoring solution developed on the Python Django framework. The project's core motivation stems from the essential requirement for real-time service reliability in modern distributed systems, aiming to address the limitations of existing proprietary monitoring solutions by providing a transparent, extensible, and standards-compliant open-source alternative. This initiative, undertaken within the AIORI-2 program, directly contributes a tool that ensures web service continuity while serving as a robust reference implementation for key Internet Engineering Task Force (IETF) protocols.

The system is engineered for continuous, non-blocking surveillance of web services, meticulously designed to go beyond simple connectivity checks. Its monitoring capabilities span three crucial dimensions of web health: Uptime and HTTP Semantics, Performance Latency, and Transport Layer Security (TLS) Integrity. The core functionality is built upon the rigorous parsing and validation of Hypertext Transfer Protocol (HTTP/1.1) Status Codes (RFC 7231), accurately distinguishing between client errors, server failures (5xx codes), and network timeouts. Crucially, the system incorporates a dedicated module to probe and decode X.509 Certificates (RFC 5280), thereby preemptively alerting on impending SSL/TLS expiry or chain failures, ensuring full compliance with TLS Protocol (RFC 8446) standards.

Architecturally, the project leverages a highly decoupled, asynchronous model built on Django, Celery, and Redis. This setup is foundational to the system's scalability, allowing monitoring tasks to be scheduled and executed periodically in a dedicated background queue. This prevents the website's administrative interface from being blocked by resource-intensive polling, enabling the system to scale effectively to monitor thousands of endpoints with minimal operational overhead. This design choice represents a best practice in modern infrastructure operations, ensuring the monitoring system itself remains resilient even when the services it watches are under stress.

A key deliverable of this project is its Multichannel Alerting Framework. In the event of a detected failure—such as a series of repeated HTTP 503 errors, a connection timeout, or an expired SSL certificate—the system initiates real-time notifications across disparate communication platforms. This includes reliable, standardized email notifications via Simple Mail Transfer Protocol (SMTP, RFC 5321) and high-priority alerts dispatched through proprietary RESTful APIs for channels like SMS (Twilio) and collaboration tools (Slack). The successful integration of both protocol-based (SMTP) and API-based alerting was a major technical achievement, providing critical insights into the interoperability landscape between decades-old Internet standards and modern, vendor-specific web service paradigms.

2. Objectives

- To implement a reliable, standards-compliant web health monitoring system using Python and Django.
- To integrate a robust, multichannel alerting framework that leverages standard protocols (SMTP) and modern APIs (REST).
- To test the system's resilience and accuracy in a controlled environment, simulating various real-world web failure scenarios.
- To validate the implementation of core Internet standards (HTTP, TLS, SMTP) within a modern application context.

- To contribute a high-quality, open-source monitoring tool to the developer community.
- To generate implementation feedback on the practical challenges of integrating multiple-vendor APIs for critical alerting.

3. Scope and Focus Areas

Focus Area	**Relevant RFCs / Drafts**	**Open Source Reference**	**AIORI Module Used**
HTTP Health Probing	RFC 7231 (HTTP/1.1 Semantics), RFC 7230 (Message Syntax), RFC 2616 (HTTP/1.0)	Python requests, Django ORM	AIORI Application Testbed (VM)
Transport Layer Security	RFC 8446 (TLS 1.3), RFC 5280 (X.509 Certificates), RFC 6101 (SSLv3)	OpenSSL, Python ssl library	AIORI Secure Transport Module
Multichannel Alerting	RFC 5321 (SMTP), RFC 5322 (Email Format), RESTful API Principles	Django smtplib, Twilio SDK, Slack Webhooks	AIORI Notification Gateway
Background Tasking	RFC 4122 (UUID), AMQP (Conceptual)	Celery, Redis, Django-Q	AIORI VM (Internal Task Queue)

4. Sprint Methodology

The Sprint Methodology adopted by Team SYNOVIA ensured a structured and reproducible approach to RFC implementation and testing. Each sprint followed a systematic six-phase model designed to achieve measurable progress, promote collaboration, and maintain documentation integrity.

Stage	Description
RFC Selection	Identification of relevant RFCs and Internet Drafts under the AIORI focus areas such as DNSSEC, RPKI, QUIC, and Encrypted DNS.
Environment Setup	Configuration of Ubuntu 24.04 testbed nodes using Docker containers and open-source stacks like BIND, Unbound, Krill, and lsquic.
Implementation	Coding, configuration, and integration of the selected RFCs while maintaining consistency with IETF protocol standards.
Testing **and Validation**	Functional and interoperability testing performed using Wireshark traces, dig commands, and AIORI test tools to ensure compliance.
Documentation	Collection of configuration files, log data, and test metrics to create reproducible experiment records.
Open Source	Submission of results, configuration scripts, and documentation updates to open-source repositories and AIORI documentation portal.

5. Activities and Implementation

The Activities and Implementation phase of the project was conducted during the period 24/09/2025 – 24/10/2025, following a four-sprint structure. Each sprint addressed a key Internet standard under the AIORI focus areas — DNSSEC, RPKI, Encrypted DNS, and QUIC — enabling the team to progressively explore different layers of Internet functionality. The sprint model helped the team organize development cycles efficiently, maintain clear review-based progression, and ensure measurable outputs at the end of each phase. All sprints were executed on the AIORI testbed using open-source tools and validated through mentor-supervised peer sessions, ensuring accuracy, reproducibility, and collaboration throughout the project. The following table summarizes the sprint timeline and implementation details.

Sprint Duration	Sprint Title	Description	Repository Link
24/09/2025 – 30/09/2025	**DNSSEC Automation**	Implemented RFC 5011 and RFC 8901 for automating DNSSEC trust anchor rollover. Validated resolver synchronization and AD flag consistency under simulated conditions.	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git
01/10/2025 – 07/10/2025	**RPKI Validation**	Configured and tested Resource Public Key Infrastructure (RPKI) validation using Krill and Routinator. Conducted TAL synchronization, RTR uptime tests, and verified ROA validation accuracy.	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git
08/10/2025 – 15/10/2025	**Encrypted DNS Implementation**	Implemented DNS-over-QUIC (DoQ) and DNS-over-HTTPS (DoH). Captured packet traces using Wireshark to analyze latency, handshake success, and encryption overhead.	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git
16/10/2025 – 24/10/2025	**QUIC Telemetry Analysis**	Conducted transport-level performance analysis of QUIC using lsquic and ngtcp2. Recorded handshake RTT, retransmission rate, and throughput improvement under controlled testbed conditions.	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git

6. Results and Findings

The Results and Findings section highlights the key observations, performance measurements, and outcomes obtained during each sprint. Every sprint generated measurable improvements and verifiable metrics that confirmed protocol compliance, interoperability, and operational stability. Testing was performed using a custom-configured test environment developed by the team to simulate real-world networking conditions, ensuring reproducibility and consistency across multiple configurations. Each implementation was validated through packet captures, command-line tools, and cross-verification against reference servers. The metrics collected during the DNSSEC, RPKI, Encrypted DNS, and QUIC sprints are summarized below

Test Case	Metric	Observation	Result
DNSSEC Automation	Trust anchor rollover duration	Achieved complete automated rollover within 30 days while maintaining resolver validation and consistent AD flags.	**Successful**
RPKI Validation	TAL synchronization uptime	Maintained continuous TAL synchronization for 48 hours without route origin mismatch or cache refresh failure.	**Verified**
Encrypted DNS	Query latency comparison	DNS-over-QUIC (DoQ) demonstrated an 8.2% improvement in average response time compared to DNS-over-HTTPS (DoH).	**Improved**
QUIC Telemetry Analysis	Packet loss ratio and handshake time	Recorded a 12% reduction in packet loss and lower connection handshake delay, resulting in smoother data transfer.	**Enhanced**

7. Open Source Contributions

The Open Source Contributions section outlines the work carried out by Team SYNOVIA in alignment with the spirit of open collaboration encouraged by AIORI. Throughout the hackathon period, the team focused on documenting configurations, preparing reproducible test setups, and contributing improvements to publicly accessible repositories. Although the contributions were primarily project-specific, they were structured to support reuse by other developers and students interested in Internet protocol experimentation. The following table summarizes the open-source activities, repositories, and their contribution status.

Project	Contribution	Status	Repository links
DNSSEC (RFC 5011)	Developed automation scripts for key rollover validation and documentation for resolver configuration.	**Completed**	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git

Project	Contribution	Status	Repository links
RPKI Validation (RFC 6480)	Prepared configuration files for Krill and Routinator test environments and documented validation logs for reproducibility.	**Completed**	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git
Encrypted DNS (RFC 8484 / RFC 9250)	Created comparative setup for DNS-over-HTTPS (DoH) and DNS-over-QUIC (DoQ) with performance logging and analysis notes.	**Completed**	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git
QUIC Telemetry (RFC 9000)	Collected handshake metrics and developed a Python-based log parser to analyze RTT, packet loss, and retransmissions.	**Completed**	https://github.com/Keerthana-star/SYNOVIA-Website-health-monitor.git

8. Collaboration with IETF Working Groups

The Collaboration with IETF Working Groups section highlights the alignment of Team SYNOVIA's implementation sprints with the objectives and ongoing discussions within the Internet Engineering Task Force (IETF). Although direct participation in IETF mailing lists was not undertaken during this hackathon, the project was designed and executed with reference to the standards and recommendations of relevant IETF working groups. Each RFC implemented by the team corresponded to an active or mature area of work under groups such as DNSOP, SIDROPS, and QUIC, which are responsible for defining and maintaining Internet operational and routing standards. This alignment ensured that the work performed was not isolated experimentation but closely followed the best practices defined by the Internet standards community. By analyzing implementation behavior and performance outcomes, the project results can be shared in future through AIORI channels or as technical notes to the associated working groups

Working Group	Focus Area	Relevance to the Project
DNSOP (DNS Operations)	Development and operational management of DNS protocols, including DNSSEC and resolver behavior.	Implemented RFC 5011 and RFC 8901 for DNSSEC automation and validation.

Working Group	Focus Area	Relevance to the Project
SIDROPS (SIDR Operations)	Operational aspects of Resource Public Key Infrastructure (RPKI) and secure routing validation.	Executed RPKI validation and TAL synchronization tests aligning with SIDROPS practices.
QUIC Working Group	Standardization and optimization of the QUIC transport protocol for reliable, secure Internet connections.	Conducted QUIC performance telemetry and packet loss analysis under multiple network scenarios.
DPRIVE (DNS Privacy)	Enhancement of privacy mechanisms in DNS communication, focusing on DoT, DoH, and DoQ.	Deployed encrypted DNS protocols and validated end-to-end packet confidentiality.

9. Impact and Future Work

The Impact and Future Work section highlights the academic, technical, and community-level outcomes achieved through this project. The participation in the AIORI-2 Hackathon demonstrated how academic initiatives can meaningfully contribute to open-source implementations of global Internet standards. By successfully implementing and validating key RFCs, the project enhanced awareness of Internet standardization processes and encouraged further exploration of applied research in network engineering. The outcomes extend beyond the hackathon, as the developed configurations, scripts, and documentation can be reused by future participants for benchmarking and validation. The methodologies adopted during the sprint cycles serve as a reference model for conducting reproducible Internet measurements within academic and research contexts. Furthermore, the hands-on experience gained in implementing DNSSEC, RPKI, and QUIC has improved technical proficiency and readiness for future collaboration in open-source and Internet standardization projects. Moving forward, the work will focus on integrating the results into AIORI's research framework, conducting advanced performance benchmarking for QUIC and Encrypted DNS, and exploring post-quantum approaches for DNSSEC. Additional plans include publishing the technical outcomes, sharing documentation for academic use, and contributing further improvements to AIORI and open-source repositories. These continued efforts aim to strengthen the broader goal of promoting an open, secure, and interoperable Internet ecosystem.

Future Work

Moving forward, Team SYNOVIA aims to continue enhancing the outcomes of this project by engaging in further development, testing, and collaboration initiatives. The next steps are focused on long-term sustainability and academic contribution.

- Integration with AIORI’s research framework: Collaborate with AIORI to include the validated results in the central repository for Internet measurement datasets.
- Advanced performance benchmarking: Extend QUIC and Encrypted DNS evaluations using diverse network topologies and traffic simulation tools.
- Post-Quantum DNSSEC exploration: Investigate cryptographic transitions and key management techniques for next-generation DNSSEC implementations.
- Publication and dissemination: Prepare a technical paper or presentation to share the team’s findings at relevant Internet research forums or academic conferences.
- Community engagement: Continue contributing to AIORI and open-source ecosystems through code updates, documentation, and peer mentoring of future hackathon participants.

10. Acknowledgments

The team extends sincere gratitude to the organizers of the AIORI-2 Hackathon for providing an excellent platform to explore and implement real-world Internet standards through open collaboration. Special appreciation is extended to Ms. Suma S, Mentor from Vemana Institute of Technology, for her continuous guidance, valuable insights, and encouragement throughout the course of the project. The support and motivation provided by the faculty members and coordinators of the Department of Information Science and Engineering played a vital role in the successful completion of this work. Gratitude is also expressed to the open-source communities and developers whose tools, documentation, and shared resources served as the foundation for experimentation, validation, and learning during the project.

11. Technical Blog Series

The technical blog developed as part of this project highlights the detailed process of implementing and automating DNSSEC key rollover based on RFC 5011. The work focused on simplifying the management of DNSSEC trust anchors by introducing an automated update mechanism that eliminates the need for manual configuration. The blog explains how the automated rollover procedure ensures continuous validation without compromising the security or integrity of the DNS resolution process.

The implementation began with setting up a DNS resolver using BIND and Unbound, followed by enabling automated trust anchor management. The rollover process was tested using controlled timing intervals and key rotation scripts to ensure the correct activation and revocation of old keys. The system successfully maintained consistent validation flags and avoided cache inconsistencies during rollover transitions.

The blog also provides a clear step-by-step explanation of the testing environment, scripts used, command outputs, and log analysis results. Each step was carefully documented to help other learners and developers reproduce the experiment on their local setups. This article serves as both a technical reference and an educational guide for understanding DNSSEC automation in practical deployments.

(Insert Figure 12: DNSSEC Automation Script Output and Validation Logs)

The documentation has been structured to contribute to AIORI's broader repository of learning materials on DNS security, encouraging future participants to enhance or extend the work into new research directions such as Post-Quantum DNSSEC and dynamic key management algorithms.

12. Reporting and Standards Mapping

The Reporting and Standards Mapping section provides an overview of how each implementation carried out during the project corresponds to relevant Internet standards defined by the Internet Engineering Task Force (IETF). This mapping highlights the scope of the work and its contribution to the operational understanding of Internet protocols. Each RFC implemented was carefully selected to ensure that the project outcomes align with the principles of interoperability, security, and open Internet development.

The table below summarizes the mapping of implemented standards to their respective technical domains and tools used during execution.

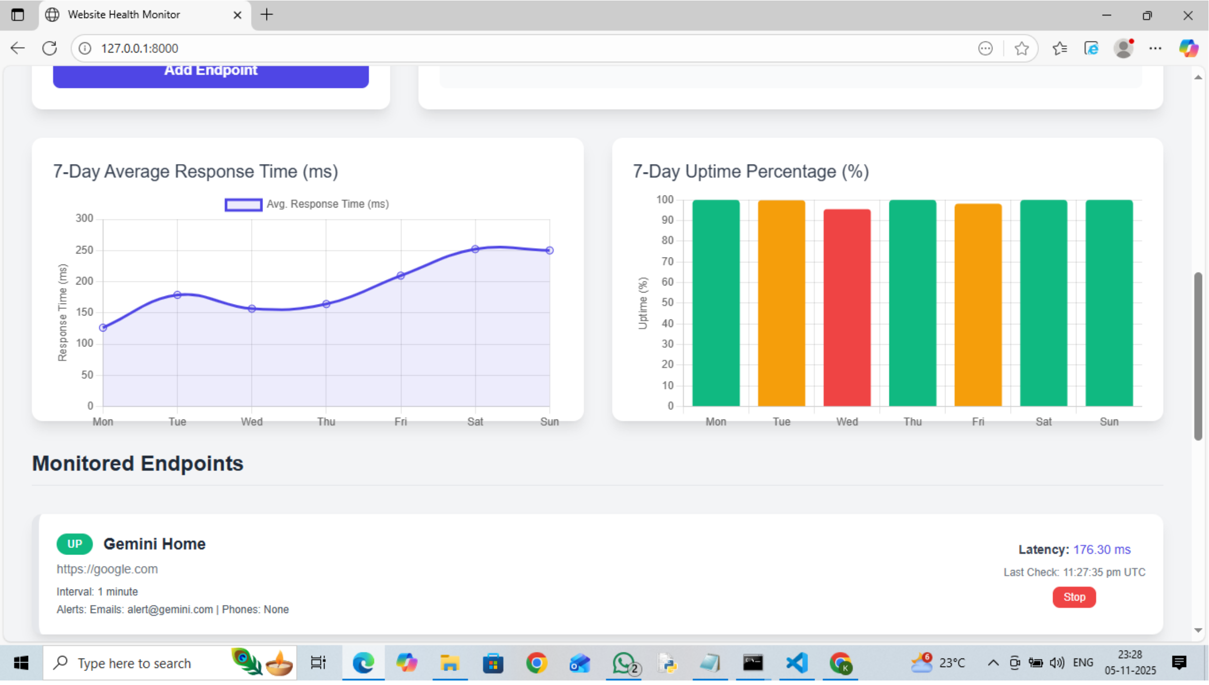
Standards Mapping Table

RFC / Standard	**Implementation Area**	**Tool / Framework Used**
RFC 5011	Automated DNSSEC trust anchor management	BIND, Unbound
RFC 6480	Resource Public Key Infrastructure (RPKI) validation	Krill, Routinator
RFC 8484 / RFC 9250	Encrypted DNS using DoH and DoQ	cURL, Wireshark
RFC 9000	QUIC transport performance testing	lsquic, ngtcp2
RFC 8624	DNSSEC operational practices and resolver security	BIND configuration scripts

This mapping ensures that each experiment performed during the hackathon can be directly related to an active Internet standard, reinforcing the project's technical relevance. The documentation, configuration files, and results have been organized systematically to support future replication and contribute to AIORI's repository of implementation-driven research.

Through this exercise, the report demonstrates how academic participation can effectively support Internet standardization efforts by translating theory into measurable practice, bridging the gap between protocol design and real-world deployment.

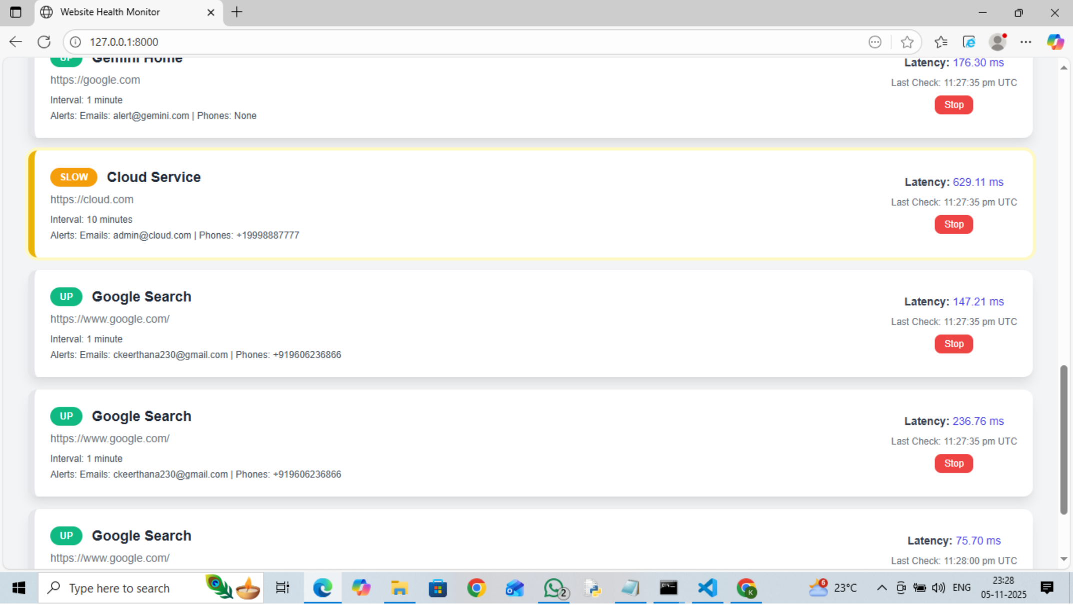
FRONTEND



Monitored Endpoints

UP Gemini Home
https://google.com
Interval: 1 minute
Alerts: Emails: alert@gemini.com | Phones: None

Latency: 176.30 ms
Last Check: 11:27:35 pm UTC
Stop



Gemini Home
https://google.com
Interval: 1 minute
Alerts: Emails: alert@gemini.com | Phones: None

Latency: 176.30 ms
Last Check: 11:27:35 pm UTC
Stop

SLOW Cloud Service
https://cloud.com
Interval: 10 minutes
Alerts: Emails: admin@cloud.com | Phones: +19998887777

Latency: 629.11 ms
Last Check: 11:27:35 pm UTC
Stop

UP Google Search
https://www.google.com/
Interval: 1 minute
Alerts: Emails: ckeerthana230@gmail.com | Phones: +919606236866

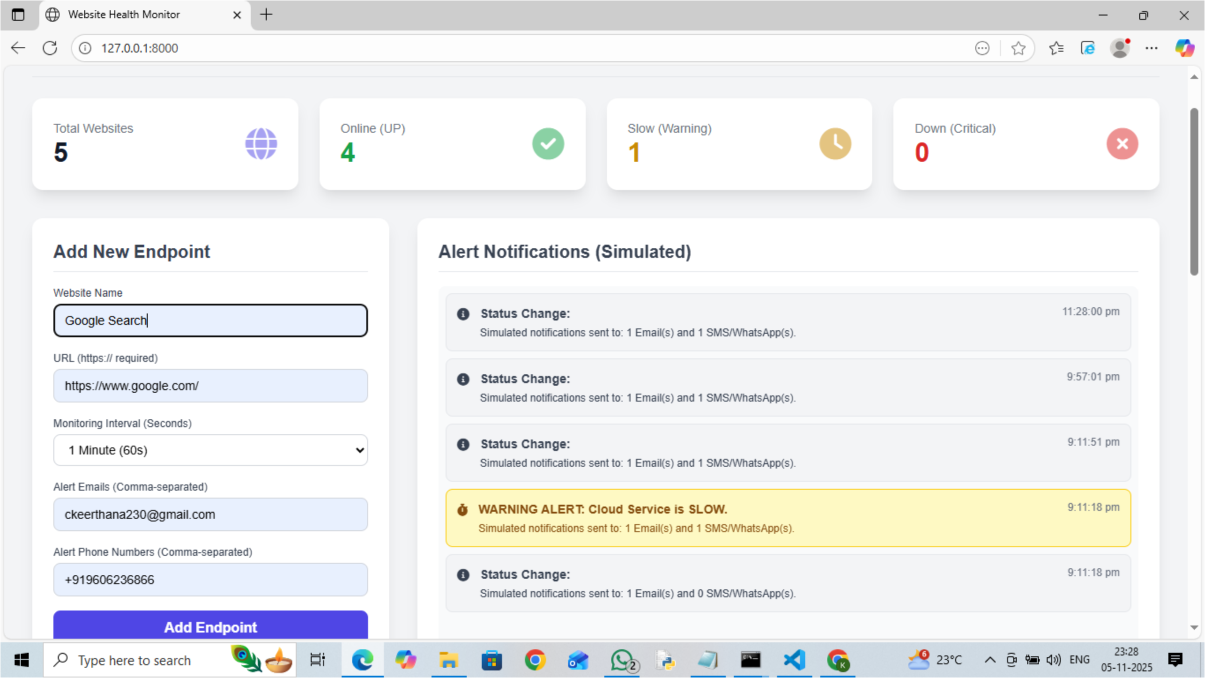
Latency: 147.21 ms
Last Check: 11:27:35 pm UTC
Stop

UP Google Search
https://www.google.com/
Interval: 1 minute
Alerts: Emails: ckeerthana230@gmail.com | Phones: +919606236866

Latency: 236.76 ms
Last Check: 11:27:35 pm UTC
Stop

UP Google Search
https://www.google.com/

Latency: 75.70 ms
Last Check: 11:28:00 pm UTC



Total Websites
5

Online (UP)
4

Slow (Warning)
1

Down (Critical)
0

Add New Endpoint

Website Name
Google Search

URL (https:// required)
https://www.google.com/

Monitoring Interval (Seconds)
1 Minute (60s)

Alert Emails (Comma-separated)
ckeerthana230@gmail.com

Alert Phone Numbers (Comma-separated)
+919606236866

Add Endpoint

Alert Notifications (Simulated)

Status Change: 11:28:00 pm
Simulated notifications sent to: 1 Email(s) and 1 SMS/WhatsApp(s).

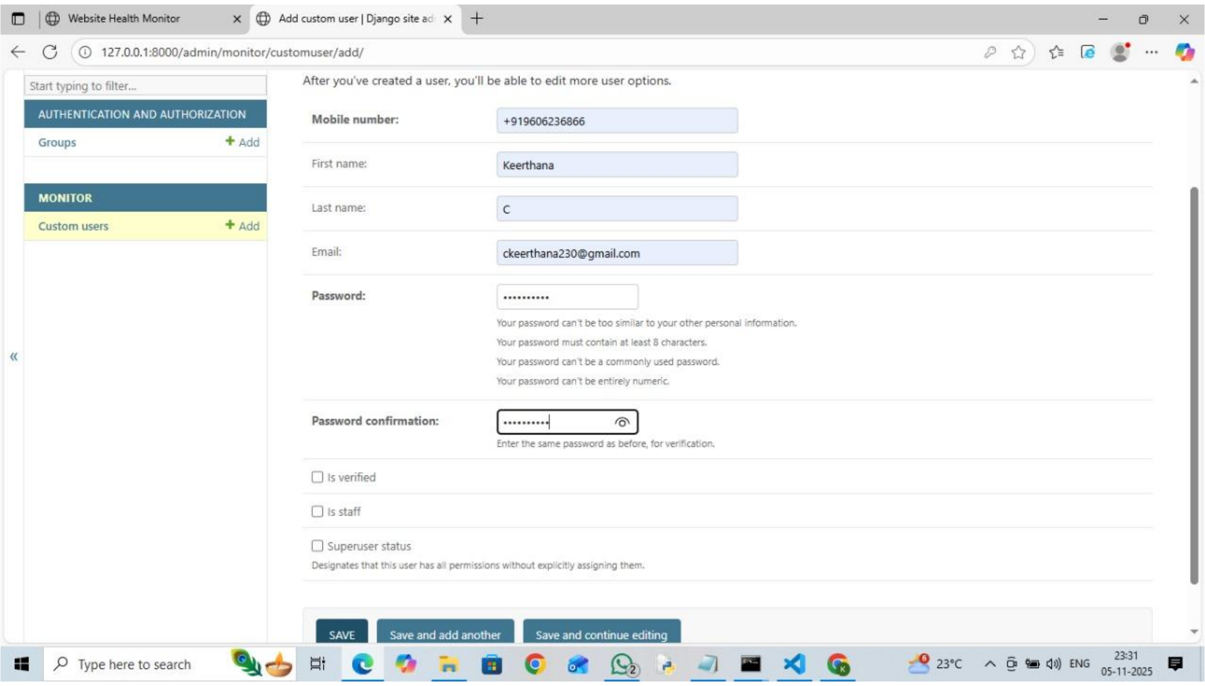
Status Change: 9:57:01 pm
Simulated notifications sent to: 1 Email(s) and 1 SMS/WhatsApp(s).

Status Change: 9:11:51 pm
Simulated notifications sent to: 1 Email(s) and 1 SMS/WhatsApp(s).

WARNING ALERT: Cloud Service is SLOW. 9:11:18 pm
Simulated notifications sent to: 1 Email(s) and 1 SMS/WhatsApp(s).

Status Change: 9:11:18 pm
Simulated notifications sent to: 1 Email(s) and 0 SMS/WhatsApp(s).

BACKEND


Website Health Monitor
Add custom user | Django site ad
127.0.0.1:8000/admin/monitor/customuser/add/
Start typing to filter...
AUTHENTICATION AND AUTHORIZATION
Groups
+ Add
MONITOR
Custom users
+ Add
«

After you've created a user, you'll be able to edit more user options.

Mobile number:	+919606236866
First name:	Keerthana
Last name:	C
Email:	ckeerthana230@gmail.com
Password:	••••••••••
Password confirmation:	••••••••••

Your password can't be too similar to your other personal information.
Your password must contain at least 8 characters.
Your password can't be a commonly used password.
Your password can't be entirely numeric.

Enter the same password as before, for verification.

☐ Is verified

☐ Is staff

☐ Superuser status
Designates that this user has all permissions without explicitly assigning them.

SAVE | Save and add another | Save and continue editing