PRESIDENCY UNIVERSITY
Private University Estd. in Karnataka State by Act No. 41 of 2013
Itgalpura, Rajankunte, Yelahanka, Bengaluru – 560064

CENTRALIZED APPLICATION CONTEXT – AWARE FIREWALL

A PROJECT REPORT

Submitted by

SANJANA K- 20221IST0109

HARINI K HEGDE- 20221IST0100

SNEHA S- 20221IST0114

Under the guidance of,

Dr. POORNIMA S

BACHELOR OF TECHNOLOGY

IN

INFORMATION SCIENCE AND TECHNOLOGY

PRESIDENCY UNIVERSITY

BENGALURU

DECEMBER 2025

PRESIDENCY UNIVERSITY

Private University Estd. in Karnataka State by Act No. 41 of 2013

Itgalpura, Rajankunte, Yelahanka, Bengaluru – 560064

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that this report "CENTRALIZED APPLICATION CONTEXT AWARE FIREWALL" is a Bonafide work of "SANJANA K (20221IST0109), HARINI K HEGDE (20221IST0100), SNEHA S (20221IST0114)", who have successfully carried out the project work and submitted the report for partial fulfilment of the requirements for the award of the degree of BACHELOR OF TECHNOLOGY in INFORMATION SCIENCE AND TECHNOLOGY during 2025-26.

Dr. Poornima S
Project Guide
PSCS
Presidency University

Ms. Benitha Christinal J
Program Project Coordinator
PSCS
Presidency University

Dr. Sampath A K
Dr. Geetha A
School Project Coordinators
PSCS
Presidency University

Dr. Pallavi R
Head of the Department
PSCS
Presidency University

Dr. Shakkeera L
Associate Dean
PSCS
Presidency University

Dr. Duraipandian N
Dean
PSCS & PSIS
Presidency University

Examiners

Sl. no.	Name	Signature	Date
1			
2			

PRESIDENCY UNIVERSITY

PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

DECLARATION

We the students of final year B. Tech in INFORMATION SCIENCE AND TECHNOLOGY at Presidency University, Bengaluru, named SANJANA K, HARINI K HEGDE, SNEHA S, hereby declare that the project work titled **"CENTRALIZED APPLICATION CONTEXT AWARE FIREWALL"** has been independently carried out by us and submitted in partial fulfilment for the award of the degree of B. Tech in INFORMATION SCIENCE AND TECHNOLOGY during the academic year of 2025-26. Further, the matter embodied in the project has not been submitted previously by anybody for the award of any Degree or Diploma to any other institution.

SANJANA K	USN: 20221IST0109	Signature 1
HARINI K HEGDE	USN: 20221IST0100	Signature 2
SNEHA S	USN: 20221IST0114	Signature 3

PLACE: BENGALURU

DATE:

ACKNOWLEDGEMENT

For completing this project work, We/I have received the support and guidance from many people whom I would like to mention with a deep sense of gratitude and indebtedness. We extend our gratitude to our beloved **Chancellor, Pro-Vice Chancellor, and Registrar** for their support and encouragement in the completion of the project.

I would like to sincerely thank my internal guide, **Dr. Poornima S, Assistant Professor**, **Senior Scale** Presidency School of Computer Science and Engineering, Presidency University, for her moral support, motivation, timely guidance, and encouragement provided to us during the period of our project work.

I am also thankful to **Dr. Pallavi R, Professor, Head of the Department, Presidency School of Computer Science and Engineering** Presidency University, for her mentorship and encouragement.

We express our cordial thanks to **Dr Duraipandian N, Dean PSCS & PSIS, Dr Shakkeera L**, Associate Dean, Presidency School of Computer Science and Engineering, and the Management of Presidency University for providing the required facilities and intellectually stimulating environment that aided in the completion of my project work.

We are grateful to **Dr Sampath A K, and Dr Geetha A, PSCS** Project Coordinators**, Ms. Benitha Christinal J, Program Project Coordinator**, Presidency School of Computer Science and Engineering, or facilitating problem statements, coordinating reviews, monitoring progress, and providing their valuable support and guidance.

We are also grateful to the Teaching and Non-Teaching staff of Presidency School of Computer Science and Engineering, and also staff from other departments who have extended their valuable help and cooperation.

SANJANA K

HARINI K HEGDE

SNEHA S

Abstract

The rapid expansion of distributed applications, Internet of Things (IoT) ecosystems, and multi-platform enterprise networks has created an imperative for intelligent, adaptable, and centrally managed security solutions. Traditional firewalls rely on rigid rule sets and manual access control configuration which often cannot handle dynamic application behaviours, changing user context and immediate network threats. They are inefficient: they lead to false positives, misconfigured policies, and weaknesses that attackers can exploit. In the effort to address this problem, this work proposes CACAF – Centralized Application Context-Aware Firewall which is a state-of-the-art security framework designed to consolidate policy enforcement, improve anomaly detection features and adapt to real-time operational situations intelligently.

CACAF runs on a centralized server where all firewall rules are stored on a policy server and then are analysed and distributed in one single central location. Unlike legacy firewalls, CACAF does not only evaluate packet behaviour in a traditional manner but also focuses on application context, user identity, device status, and conduct behaviour. The architecture includes machine learning-supported anomaly detection to identify irregular or questionable activities which could circumvent rule-based filtering. The lightweight agents deployed across end-system devices communicate with the central controller to update on policies, transmits real-time telemetry data, and carry out contextual filtering, without compromising performance. This combination of architecture of modular features guarantees a consistent enforcement through the network and streamlines configuration. The platform is built upon a multi-layered pipeline: device registration and authentication, context extraction, intelligent policy matching, adaptive rule enforcement, and machine learning to perform an anomaly analysis.

Secure REST API (or socket) communication layer ensures access is encrypted, authentic and between agents and server. The organized policy engine enables admins to build application-aware rules based on user role, device posture, geolocation, time-of-access, traffic classification, among other parameters, for each application and environment. The anomaly detection module uses supervised and unsupervised learning to detect anomalies, such as unusual use of bandwidth or attempts to gain unauthorized access to a port. This framework improves enterprise and institutional security with centralized governance and reduces bureaucratic processes thanks to context-specific decision-making. We show that CACAF significantly reduces the rate of misclassification, and significantly decreases latency in updating policy. The accuracy of the detection of attack is significantly increased. Centralized monitoring also makes advanced features—like threat correlation analysis, unified audit logs, and automatic rule optimization—easier to do. CACAF: A scalable adaptive intelligent firewall solution designed for modern cybersecurity requirements that provides strong protection across varied environments while still maintaining operational efficiency.

Table of Content

List of Figures

List of Tables

Abbreviations

AI	Artificial Intelligence
ML	Machine Learning
IoT	Internet of Things
WFP	Windows Filtering Platform
TLS	Transport Layer Security
DPI	Deep Packet Inspection
SDGs	Sustainable Development Goals
CERT-In	Computer Emergency Response Team – India
NCRB	National Crime Records Bureau
NGFW	Next-Generation Firewall
SIEM	Security Information and Event Management
TCP	Transmission Control Protocol
SRS	Software Requirement Specification
HTTPS	Hyper Text Transfer Protocol Secure
CACAF	Centralized Application Context-Aware Firewall
DPDPA	Digital Personal Data Protection Act
ISO	International Organization for Standardization
CI/CD	Continuous Integration / Continuous Deployment
VCS	Version Control System