Harhit Suthar, 2025, 13:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Cybersecurity Solutions for Modern Threats

Harhit Suthar, Prathinav Kothia, Vishal Bharvadiya, Smit Bharatbhai Kanani, Ami Shah
Department of Computer Science & Engineering, Parul University, Vadodara, India

Abstract- This project focuses on enhancing cybersecurity for websites and applications, protecting users from modern threats like phishing and data breaches. It aims to create a secure digital environment by implementing strong security measures. One of the key features of the project is a user-friendly complaint registration system, allowing individuals to report cyber fraud directly without having to visit a cybercrime office. Additionally, it provides users with real-time updates on the latest cybercrime incidents and ensures that their email and phone number are not exposed on external websites. To further assist users, an AI- powered chatbot is integrated into the system, offering real-time guidance on cybersecurity-related queries. The project tests the effectiveness of its security measures to ensure they can withstand real-world threats. Beyond protection, the project aims to educate users and businesses on best practices for staying safe online. The ultimate goal is to deliver a secure, easy-to-use platform that helps individuals and businesses stay protected from evolving cyber risks.

Index Terms - Cybersecurity, Phishing Prevention, Data Pro- tection, AI Chatbot, Cybercrime Reporting, Security Awareness, Vulnerability Analysis.

I. INTRODUCTION

Background

Cybersecurity has become a fundamental pillar in the digital era, offering protection against the increasing prevalence of cy- ber threats such as phishing, data breaches, and financial fraud. As cyber criminals continuously develop more advanced attack techniques, critical sectors such as banking, e-commerce, and corporate enterprises face escalating risks leading to financial losses and privacy compromises. Traditional security approaches often rely on static and signature-based methods, which are insufficient to counter modern, dynamic cyber threats. There is a growing demand for proactive, intelligent cybersecurity solutions that can protect users and enterprises in real time.

Problem Statement

While various cybersecurity tools currently exist, there remain significant challenges that hinder effective protection and user engagement, including:

- Reactive Security Measures: Most traditional systems respond post-incident and lack proactive threat detection.
- User Engagement and Awareness: Many users are un- aware of how to report cyber fraud efficiently, resulting in delayed responses.
- Fragmented Support Systems: Cybersecurity assis- tance and complaint filing processes are fragmented, requiring users to interact with multiple platforms or agencies.
- Lack of Real-Time Guidance: Users rely on static information rather than interactive and instant support for their cybersecurity concerns.

Objectives

This project, Cybersecurity Solutions for Modern Threats, aims to develop a unified platform that addresses these gaps by:

- Integrating AI-driven real-time threat detection to proac- tively monitor risks.
- Providing a streamlined, user-friendly complaint regis- tration system to report cybercrime directly from the platform.
- Embedding an AI-powered chatbot to offer instant cyber- security assistance and guidance.
- Conducting security audits that identify vulnerabilities such as weak encryption and authentication flaws.

Scope and Contribution

Unlike conventional cybersecurity systems, this platform offers an integrated, user-centric approach combining proactive AI threat monitoring, direct fraud complaint registration, and conversational AI assistance. It aims to empower users and or-ganizations by simplifying cyber incident reporting,

enhancing threat detection accuracy, and providing continuous education on best security practices, thereby creating a safer digital environment for all.

II. LITERATURE SURVEY

Cybersecurity platforms are vital for protecting digital sys- tems and users from threats like phishing, data breaches, and fraud. Existing research and implementations have contributed significantly across detection, prevention, and user support functionalities, yet gaps remain that this work seeks to over- come.

Existing Cybersecurity Systems and Research

Several notable works highlight different focuses and limi- tations:

- Scam Website Detection: Baby [1] proposed a web- based system integrating protocols and APIs like Virus- Tool to detect fraudulent websites. While effective for detection, the solution lacked integrated user complaint reporting and interactive support features now included in our platform.
- Comprehensive Cyber Attack Studies: Nirwan and Dhaliwal [2] examined various cyber threats and counter- measures, emphasizing detection but omitting streamlined reporting or real-time user assistance, which are imple- mented in our project.
- Vulnerability Testing on Indian Websites: Shivam et al.

assessed Indian government and private websites with tools such as sitecheck.sucuri.net, revealing vulnerabili- ties like poor authentication and encryption. Our platform builds on such findings by simulating cyber-attacks and providing active remediation recommendations.

- Systematic Study of Web Security: Kong [4] catego- rized web security into client, server, and transmission mechanisms, focusing on authentication and encryption. Our system extends these principles with AI-driven mon- itoring for adaptive threat detection.
- AI in Cybersecurity: Ferrag et al. [5] reviewed genera- tive AI's role in cybersecurity, highlighting both potential and risks. Our solution harnesses AI for enhanced threat detection coupled with a safe, user-centric chatbot for cybersecurity guidance.

Risk Analysis for Web Applications: Bhatt [6] empha- sized continuous security testing and user awareness to mitigate cyber risks. Our platform addresses user engage- ment through accessible complaint filing and proactive education features.

Key Theories and Findings

Prior research collectively underscores:

- Digitization advances accessibility and engagement in cybersecurity efforts.
- User mentorship and support improve security awareness and incident response.
- Verification and trust mechanisms are critical to prevent fraudulent activities.
- Integration of AI enables dynamic and proactive threat mitigation.

Research Gap

While useful individually, current systems suffer from:

- Fragmented tools lacking integrated user support and real-time assistance.
- Limited real-time AI-driven threat detection responsive- ness.
- Insufficient coverage in automated vulnerability testing.
- Low user awareness and cumbersome complaint proce- dures.
- The proposed platform fills these gaps by combining AI- powered monitoring, streamlined complaint registration, and an intelligent chatbot, all within a unified user-friendly inter- face.

III. METHODOLOGY

Development Approach – Agile Scrum Model

The development of the Cybersecurity Solutions for Modern Threats platform follows the Agile Scrum methodology. This iterative framework supports continuous progress, adaptability to evolving user requirements, and frequent stakeholder input. Such an approach ensures that each development sprint de- livers a fully functional module, facilitating incremental and manageable system growth while maintaining development efficiency.

Key benefits of adopting Scrum include:

- Iterative Development: Progressive delivery of func- tional components in each sprint.
- Continuous Feedback: Stakeholder reviews help refine features and improve overall quality.
- Flexibility: Ability to accommodate changes in require- ments during the development lifecycle.
- Enhanced Collaboration: Regular team communication ensures alignment and efficient coordination.

Tools and Technologies Used

Table I
Tools and Technologies Used in The Project

Category	Technology Used
Frontend	Flutter
Backend	Node.js, Express.js, Prisma ORM, Supabase, Firebase
Database	Supabase Storage
Authentication	Firebase Auth, Supabase Auth
Project Management	Agile Scrum Workflow
Version Control	GitHub
Testing	Postman (API Testing)
Deployment	PlayStore

System Architecture

The platform is structured in a three-tier architecture for modularity and scalability:

- Frontend (Client Layer): Utilizes Flutter for a re- sponsive user interface communicating securely with the backend through REST APIs.
- Backend (Application Layer): Developed with Node.js and Express.js, incorporating Prisma ORM and Mon- goose to manage database interactions. Implements Fire- base/ Supabase-based authentication to secure sessions.
- Database (Data Layer): Firebase/Supabase stores user credentials, complaint data, chat logs, security reports, and other application data.

Authentication Flow

User authentication is handled securely via the following process:

- User credentials are validated by the backend through a protected login API.
- Upon successful validation, a Firebase is generated and stored in an uid.
- Middleware on the backend verifies the secure on every protected resource request to authorize access.
- This process ensures secure, seamless user sessions while safeguarding sensitive user data against unautho- rized access.

IV. SYSTEM DESIGN AND ARCHITECTURE

Architectural Overview

The platform adopts a three-tier architecture focusing on scalability and maintainability:

- Frontend: Responsive user interface developed with Flutter , enabling users to interact seamlessly with plat- form features.
- Backend: Node.js and Express.js server handles applica- tion logic, APIs, and secure session management using Firebase uid.
- Database: MongoDB serves as the primary data store for user accounts, complaints, security events, chatbot data, and logs.

Key Modules

- User Authentication Verification: Implements cookie- based JWT authentication to securely restrict access and prevent unauthorized or fraudulent user profiles.
- Fraud Complaint Registration: Allows users to file cyber fraud complaints easily, with backend integration to government cybercrime portals.
- AI Chatbot Assistance: Provides real-time security guid- ance and answers user queries related to cybersecurity.
- Vulnerability Analysis: Performs automated auditing of websites and applications for weak encryption, authenti- cation issues, and common vulnerabilities.
- Tips and Advisory: Delivers cybersecurity tips, news, and educational posts to keep users informed and proac- tive.

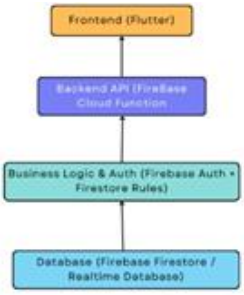

Fig. 1. System Architecture of the Cybersecurity Platform

Data Flow

- User registration and login requests are received and processed by the backend API.
- The backend handles business logic, interacts with the database for data persistence and retrieval.
- Responses are returned in JSON format to the frontend, enabling dynamic UI updates.
- Real-time notifications and updates are facilitated through WebSockets or periodic polling mechanisms to keep users informed of relevant events.

V. IMPLEMENTATION

The development followed the Agile Scrum methodology, ensuring iterative progress and integration of feedback across core system modules. The implemented modules are as fol- lows:

- User Authentication: Secure login using Firebase uid tokens and password hashing with bcrypt to protect user credentials.
- Profile Management: Users can update personal details, security settings, and preferences to maintain accurate accounts.
- Complaint Registration: Users can easily file cyber fraud complaints through a streamlined interface con- nected to government cybercrime portals.
- AI Chatbot: An AI-powered chatbot assists users by answering cybersecurity-related queries in real-time, supporting users to take preventive or corrective actions.
- Tips and Advisory: Regularly updated cybersecurity tips and news help educate users and keep them in- formed about emerging threats.
- Cyber News Feed: Displays up-to-date information on recent cybercrime incidents to raise situational aware- ness.
- Admin Dashboard: Facilitates management of user activities, complaints, chatbot logs, and overall platform maintenance.

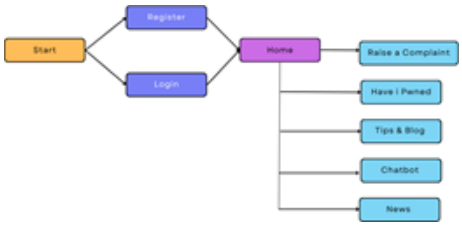

Fig. 2. System Architecture of the Cybersecurity Platform

VI. SYSTEM WORKFLOW AND AI CHATBOT IMPLEMENTATION

This system integrates FirebaseDb, Supabase, Supabase Vector Database, and Google's Generative AI (Language Model) into a unified pipeline. The aim is to synchronize unstructured data from database collections and JSON sources into the vector database, enable semantic search through

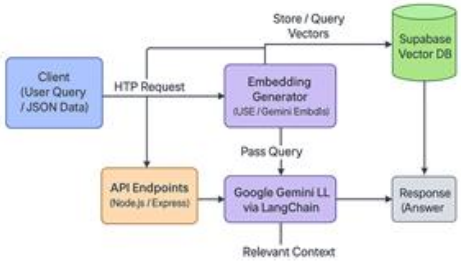

Fig. 3. System Architecture of the Cybersecurity Platform

embeddings, and leverage large language models (LLMs) for context-aware natural language interaction.

The resulting architecture enables an intelligent assistant that can retrieve knowledge grounded in organizational data such as user profiles, discussions,

events, and opportunities, making it particularly suited for cybersecurity and financial platforms providing real-time guidance.

Chatbot Setup

- Supabase Vector Database Client – Provides high- performance semantic search and persistent storage of vectorized knowledge.
- LangChain with Google Generative AI – Interfaces with Google's Gemini LLM through LangChain abstrac- tions to generate contextually relevant responses.
- Universal Sentence Encoder (USE) – Employed for transforming textual data into 512-dimensional embed- dings that capture semantic similarity.

Supabase Vector DB Initialization

Supabase Vector Database serves as the semantic memory layer. The system initializes a project-specific vector store (e.g., chatbot knowledge index). Data is embedded with USE and upserted into the index along with metadata. The Supabase infrastructure manages similarity search using cosine distance, enabling fast retrieval even at scale.

Universal Sentence Encoder (USE)

The embedding model converts text into dense numerical representations. Semantic similarity ensures queries such as "upcoming hackathon" and "new coding event" map to nearby regions in the embedding space. Batched embedding genera- tion (e.g., 32 documents per batch) improves efficiency and reduces memory overhead.

Google Generative AI Configuration

The LLM (Gemini) is integrated through LangChain with a temperature setting of 0.3, prioritizing factual, grounded, and low-variance responses. Combined with vector search results from Supabase, this forms a Retrieval-Augmented Generation (RAG) pipeline that anchors model outputs in reliable data.

System Components and Workflow

- Environment Initialization: Load API keys and config- urations; import Supabase client, USE, and LangChain LLM components.
- Index Management: Connect to Supabase vector table; create and configure if absent.
- Embedding Model Setup: Load USE and compute embeddings for incoming text data.
- Metadata Processing: Normalize and sanitize metadata fields to exclude irrelevant or sensitive information.
- Data Synchronization: Extract textual data from Su- pabase or Firebase, generate embeddings, and batch- insert into Supabase Vector DB.
- API Endpoints:
- Synchronize new or updated documents (profiles, discussions, events) with Supabase Vector DB.
- Accept user queries, generate embeddings, and re- trieve relevant vectors from Supabase.
- Use LangChain with Gemini to compose final re-sponses grounded in retrieved context.

VII. RESULTS AND DISCUSSION

The Cybersecurity Solutions for Modern Threats platform was successfully developed and tested across all core modules. The system provides a secure and interactive environment where users can effectively manage cybersecurity risks.

System Outputs

- User Authentication Verification: Login and registra- tion are secured with cookie-based JWT authentication, ensuring only authorized users access the system. Users cannot proceed without completing their profile.
- Complaint Registration: Enables users to report cyber fraud seamlessly through a streamlined interface con- nected to government cybercrime portals.
- AI Chatbot Assistance: Offers real-time, AI-driven an- swers to cybersecurity-related queries, guiding users on prevention and response actions.
- Vulnerability Analysis: Automated audits identify secu- rity weaknesses such as improper encryption and poor authentication.

- Tips and News Feed: Provides users with up-to-date security tips and news on recent cybercrime incidents.
- Admin Dashboard: Administrators can manage user activities, complaints, chatbot logs, and system metrics efficiently.

Comparative Advantages

Compared to existing cybersecurity platforms, this solution delivers:

- Comprehensive integration of AI-based threat detection, complaint handling, and user support.
- Robust authentication mechanisms ensuring data integrity and privacy.
- An intuitive and accessible user interface leveraging modern web technologies (React.js, MongoDB).
- Automated detection and reporting of vulnerabilities and suspicious activities.

Evaluation and Feedback

Initial testing with a small group of users revealed:

- The interface is user-friendly and straightforward.
- Users found the chatbot responses timely and helpful.
- The complaint registration process is significantly simpler than traditional methods.
- The platform's security auditing instills increased confi- dence among users.

System Testing and Evaluation

Module	Test Performed	Expected Result	Actual Re- sult
Login Authenti- cation	Correct credentials entered	Redirect to dash- board	Passed
Profile Comple- tion	User updates pro- file	Profile updated successfully	Passed
Complaint Reg- istration	File cyber fraud complaint	Complaint stored	Passed
AI Chatbot	Query cybersecu- rity topic	Relevant answer provided	Passed
Security Audit	Active vulnerabil- ity scans	Vulnerabilities identified	Passed
Tips and News Feed	Access tips and news	Updated informa- tion displayed	Passed

Table II
Functional Testing Results

VIII. CONCLUSION AND FUTURE SCOPE

Conclusion

The Cybersecurity Solutions for Modern Threats project successfully demonstrates an integrated platform that empow- ers users with tools for proactive cybersecurity management. By combining AI-driven threat detection, a direct complaint registration system, and an interactive AI chatbot, the plat- form addresses common challenges faced by individuals and organizations alike. Its modular architecture ensures security, scalability, and ease of use, making it a viable tool for enhancing digital safety.

Future Scope

To further enhance the platform, future work will focus on:

  - Mobile Applications and Browser Extensions: Devel- oping dedicated apps and extensions to increase accessi- bility.
- Advanced AI Recommendations: Leveraging machine learning to provide personalized security advice and threat predictions.
- Social Media Integration: Connecting with platforms like LinkedIn for threat intelligence sharing and user engagement.
- Blockchain for Secure Reporting: Implementing blockchain technology to ensure transparency and secu- rity in complaint and donation processes.

Acknowledgment

We sincerely thank Prof. Ami Shah for her exceptional guidance and Dr. Amit Barve for his leadership and support throughout this project.

REFERENCES

1. A. Baby, "An Integrated Web-based Approach for Security Enhancement by Identification and Prevention of Scam Websites," 2nd Int. Conf. Ad- vances in Computing, Communication, Embedded and Secure Systems, 2021.
2. S. Nirwan and B. K. Dhaliwal, "A Comprehensive Study of Cyber Attacks and Countermeasures," Int. Conf. Inventive Computation Tech- nologies, 2023.
3. K. Shivam et al., "A Research Study on Web Application Security," Int. Journal of Multidisciplinary Research Transactions, 2022.
4. F. Kong, "Research on Security Technology Based on Web Application," Information Science and Management Engineering, 2016.
5. M. A. Ferrag et al., "Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities," Internet of Things and Cyber–Physical Systems, 2025.
6. D. Bhatt, "Cyber Security Risks for Modern Web Applications: Case Study Paper for Developers and Security Testers," Int. Journal of Scientific & Technology Research, 2018.