Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 1088-1091

NexusGuard: AI-Powered URL Phishing Guard and Real-Time Protection System

Suryan Jain, Mr. Pawan Kumar Jaiswal
Student, Assistant Professor
Amity University Raipur, Chhattisgarh, India
Suryan31jain@gmail.com, pkumar@rpr.amity.edu

Abstract
The proliferation of cyber threats has significantly increased the risk of phishing attacks, leading to a demand for security tools that are both intelligent and proactive. NexusGuard is a URL phishing guard system that utilizes artificial intelligence to help users identify malicious links before they interact with them. It is designed to be seamless and integrated directly into the browsing experience. NexusGuard features a minimalist and aesthetic look. It uses layouts that function across various digital interfaces. The platform includes tools like deep analysis, recent scan history, and interactive threat scores. It also integrates the Gemini AI Threat Intelligence API to provide real-time risk assessment. This makes it easier for users to identify suspicious activity and make safer decisions online. NexusGuard also lets you manage whitelists and view detailed threat reports. This project demonstrates how web engineering and artificial intelligence can be used to build security tools that are fast, efficient, and user-centric. The cybersecurity industry is changing because of the rise in sophisticated social engineering. NexusGuard is a phishing guard system that helps people protect their digital identities. It uses intelligence to make security easy and effective. NexusGuard has a lot of features that make it useful. It has a minimalist feel, is easy to navigate, and uses an AI guard that can protect you automatically. NexusGuard is a good example of how artificial intelligence can be used to make the internet safer

Keywords: Travel Booking System, AI-Powered Platform, Web Application, Digital Travel Platform, Smart Search System

I. INTRODUCTION

The digital landscape has changed a lot with the rise of sophisticated phishing platforms. This means attackers can now target people from anywhere in the world. People who browse the web now want more than just a simple way to check links. They want tools that look nice, provide instant feedback, and offer protection all the time while they are online

NexusGuard is a platform that tries to give people what they want. It puts all the tools people need for URL security into one place. This is better than tools that are hard to use and do not offer real-time protection. NexusGuard looks nice and is easy to use. People can use it to scan URLs, view threat scores, and receive automatic alerts in one place.

NexusGuard also has a background guard that can analyze sites and warn people of risks. This system works in real-time so people get protection right away. NexusGuard is a kind of security

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 1088-1091

tool that uses the latest technology to make safety easy for people. It is focused on making sure people can use it easily and that they are protected from malicious sites. NexusGuard is a solution for people who want to browse securely online

II. PROBLEM STATEMENT

Despite having manual URL scanners, users still have a hard time. They get frustrated with tools that are hard to navigate or require manual input for every link. Many security tools make users visit external sites to check one URL. This makes the experience feel disjointed and takes up much time. Users do not get help to understand why a specific link is dangerous.

Another big problem is that reactive security systems are not effective against Zero-Day attacks. Users often struggle to identify homograph attacks or masked subdomains. Traditional security interfaces often have outdated looks. The main problem is to create a security platform that does everything: it should integrate analysis, have an engaging interface, and use AI to assist users proactively. The system should handle threat data well and be fast and responsive

III. OBJECTIVES

- To make NexusGuard a security platform that's easy to use.
- The platform should have URL scanning, history, and real-time alerts in one place.
- We want to add features like a floating safety badge and color-coded risk scores.
- NexusGuard should have an AI guard that can automatically warn users of threats.
- We need to make it easy for people to manage their scan history so they can look at previous results.
- It would be great if people could whitelist safe sites, so we should add a whitelist function.
- The information about threats should be saved so we will use ways to store data.
- NexusGuard should work well on any device or browser to be used by many people

IV. SYSTEM ARCHITECTURE

The system follows a three-layer architecture:

4.1 Frontend (User Interface)

The frontend of NexusGuard is made to look minimalist and be easy to use. It has a dashboard that is similar to what you see on modern security tools. The main sections have reactive parts that catch your eye, like risk meters and scan animations. The developers used Tailwind CSS and Framer Motion to make all the animations smooth. This means when you scan a link or open a report, it looks neat. The typography uses clean fonts like Syne to ensure readability and a professional look.

4.2 Data Layer (Threat Intelligence Simulation)

The platform has a collection of information that includes known malicious patterns, TLD risks, and suspicious keywords. This information is set up to be realistic so users can see how a threat is identified. They also have real-time results from the Gemini API that make the detection feel instantaneous.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 1088-1091

4.3 State Management & Storage

NexusGuard uses Zustand for managing scan data. This helps handle recent results and whitelists. LocalStorage is used to keep user data even after they close the session. This way users can still access their scan history when they come back.

4.4 AI Integration Layer

The system uses a Gemini AI integration to help analyze URLs. It lets the system interpret the intent behind a link. If a URL is suspicious, the AI provides a risk score and a reason. This way users always get support in identifying threats.

V. METHODOLOGY

NexusGuard is made with the user in mind. The people who make NexusGuard want to make sure it is easy to use and works well. They start by making a dashboard that looks nice and is easy to navigate. This dashboard helps users find what they need when they are looking for security services. The extension part makes it easy to find things like current site scores and safety settings.

VI. WORKING OF THE SYSTEM

NexusGuard helps users find threats and block them. When you go to the dashboard or use the extension, you see an aesthetic interface with buttons to click and a search box for URLs. You can type in what you're looking for or let the guard monitor your tabs.

NexusGuard then shows you the risk level. You can look at the details and pick what you want to do, like block or ignore. You might see warnings if the site is dangerous. You can see all your recent scans in the history section where you can manage them. There is also a whitelist where you can save safe things.

VII. KEY FEATURES

- Advanced UI/UX design with minimalist layouts.
- Proactive background guard for real-time URL monitoring.
- Heuristic analysis and AI-powered risk scoring.
- Visual safety badges and full-screen warning overlays.
- Scan history management and whitelist functionality.
- Persistent data storage using Zustand and localStorage.

VIII. TECHNOLOGY USED

- **Frontend:** React (Vite), Tailwind CSS, Framer Motion, Lucide React.
- **Backend:** Node.js, Express.js, MongoDB (Mongoose).
- **AI & Security:** Google Gemini AI (1.5 Pro), Manifest V3 Extension.
- **DevOps:** Git, GitHub, Dotenv, Axios.

Innovation and Integrative Research Center Journal
ISSN: 2584-1491 | www.iircj.org
Volume-4 | Issue-5 | May-2026 | Page 1088-1091

IX. REAL WORLD APPLICATIONS

NexusGuard is a tool for cybersecurity. It works like big security platforms that people use to protect their data. Companies can use NexusGuard to help their employees avoid phishing. The platform has an AI guard that uses artificial intelligence to help identify malicious intent. This makes it a good choice for people who browse the web and want support.

X. ADVANTAGES

- The website and extension have a visually appealing design.
- It combines heuristic and AI analysis smoothly.
- It uses proactive monitoring to help the user.
- The system is fast and can handle many scans.

XI. LIMITATIONS

- The system needs internet access for the AI deep scan.
- It may have limited offline heuristic capabilities.
- The AI is dependent on an API for its deep intelligence responses.

XII. FUTURE SCOPE

NexusGuard will have features added like real-time screenshot analysis. We can also make a mobile app and send people alerts when they are targeted by phishing. NexusGuard will use programs that can predict new attack patterns just for the user.

XIII. CONCLUSION

NexusGuard shows us that we can use the internet and artificial intelligence to make a good security platform. The system is about making sure users have a great experience and that they can make safe choices. NexusGuard is a solution for people who want to browse securely. The project shows that new digital platforms can really change the security industry and make people safer.

References

[1] Google, "Gemini AI Documentation,"
[2] Meta Platforms Inc., "React Documentation,"
[3] Node.js Foundation, "Node.js Documentation,"
[4] MongoDB Inc., "MongoDB Documentation,"
[5] OWASP, "Phishing Prevention Cheat Sheet,"
[6] Chrome, "Manifest V3 Documentation,"
[7] I. Sommerville, Software Engineering, 10th ed. Boston, MA, USA: Pearson, 2015.