Home (http://ipindia.nic.in/index.htm) About Us (http://ipindia.nic.in/about-us.htm) Who's Who (http://ipindia.nic.in/whos-who-page.htm)
Policy & Programs (http://ipindia.nic.in/policy-pages.htm) Achievements (http://ipindia.nic.in/achievements-page.htm)
RTI (http://ipindia.nic.in/right-to-information.htm) Feedback (https://ipindiaonline.gov.in/feedback) Sitemap (shttp://ipindia.nic.in/itemap.htm)
Contact Us (http://ipindia.nic.in/contact-us.htm) Help Line (http://ipindia.nic.in/helpline-page.htm)

Skip to Main Content

inPASS Indian Patent Advanced Search System (http://ipindia.nic.in/index.htm) INTELLECTUAL PROPERTY INDIA PATENTS | DESIGNS | TRADE MARKS GEOGRAPHICAL INDICATIONS (http://ipindia.nic

Patent Search

Invention Title	Real-Time Cyber Incident Discovery and Visualization Using Adaptive Machine Learning
Publication Number	19/2025
Publication Date	09/05/2025
Publication Type	INA
Application Number	202541034291
Application Filing Date	08/04/2025
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06N20/00, G06F21/55, G06N3/08, G06Q10/06

Inventor

Name	Address	Country
Mamatha Deenakonda	Assistant Professor Department of EEE Vishnu Institute of Technology, Bhimavaram KOVVADA BHIMAVARAM Andhra Pradesh India 534202	India
K J Sai Sashank Varma	UG Student Department of CSE Sagi Ramakrishnam Raju Engineering College Chinnamiram BHIMAVARAM Andhra Pradesh India 534204	India
U Padma Jyothi	Assistant Professor Department of CSE Vishnu Institute of Technology, Bhimavaram KOVVADA BHIMAVARAM Andhra Pradesh India 534202	India
Indukuri Yaswanth Varma	UG Student Department of CSE Sagi Ramakrishnam Raju Engineering College Chinnamiram BHIMAVARAM Andhra Pradesh India 534204	India

Applicant

Name	Address	Country
Vishnu Institute of Technology, Bhimavaram	Vishnu Institute of Technology, Bhimavaram KOVVADA BHIMAVARAM Andhra Pradesh India 534202	India

Abstract:

This project, Real-Time Cyber Incident Discovery and Visualization Using Adaptive Machine Learning, aims to create a tool that collects, analyzes, and categorizes real-incident data from sources like forums, social media, and paste sites. Leveraging machine learning, the tool identifies and monitors platforms that share cyber incide information, building a structured database for timely and comprehensive threat detection. This data is organized by industry sectors, Advanced Persistent Threats (A relevant strategic issues, providing critical insights and visualizations. Designed to scale with evolving cyber threats, the system continuously integrates new data sour adapts to the shifting threat landscape. A user-friendly interface enables cyber security professionals and authorities to receive timely alerts, make informed decision respond proactively to cyber incidents. The project specifically addresses the National Technical Research Organization's (NTRO) need for a tool that enhances cyber r India by empowering stakeholders in Critical Information Infrastructure (CII) to detect, assess, and mitigate cyber risks in real-time.

<u>Complete Specification</u>

Description:The system is designed as a comprehensive cyber incident feed generator that utilizes advanced machine learning algorithms to dynamically identify ar monitor various platforms that share cyber incident data, such as forums, social media, and paste sites. It begins by aggregating real-time data from these non-trad sources, employing data mining techniques to extract relevant information related to cyber threats. The collected data is then structured into a well-organized datal facilitating easy access and analysis. The system analyses this information to identify patterns, categorize incidents based on industry sectors and Advanced Persist Threats (APTs), and generate actionable insights. It features a user-friendly interface that provides cybersecurity experts and authorities with intuitive visualizations timely alerts, enhancing situational awareness and enabling proactive response to emerging threats. The architecture is designed to be scalable and adaptable, ens can accommodate evolving threat landscapes and incorporate new data sources as they arise. Overall, this innovative system aims to empower organizations with t intelligence needed to fortify their defences and improve their overall cybersecurity posture in a rapidly changing digital environment. , Claims:We Claim

Dynamic Identification and Monitoring: The system uniquely utilizes advanced machine learning algorithms to dynamically identify and monitor a wide range of nor traditional platforms that disseminate cyber incident data, thereby capturing emerging threats in real-time.
Comprehensive Data Collection: Our invention incorporates a robust data collection module that aggregates and structures data from diverse sources, including for social media, paste sites, and other relevant online platforms, ensuring comprehensive coverage of potential cyber threats.
Real-Time Analytics and Insights: The system offers real-time analytics capabilities that categorize and analyse collected data based on industry sectors, Advanced Persistent Threats (APTs), and strategic issues, providing actionable insights that enhance situational awareness

View Application Status

राष्ट्रीय मतदाता सेवा पोर्टल
NATIONAL VOTERS' SERVICES PORTAL

Terms & conditions (http://ipindia.gov.in/terms-conditions.htm) Privacy Policy (http://ipindia.gov.in/privacy-policy.htm)
Copyright (http://ipindia.gov.in/copyright.htm) Hyperlinking Policy (http://ipindia.gov.in/hyperlinking-policy.htm)
Accessibility (http://ipindia.gov.in/accessibility.htm) Archive (http://ipindia.gov.in/archive.htm) Contact Us (http://ipindia.gov.in/contact-us.htm)
Help (http://ipindia.gov.in/help.htm)

Content Owned, updated and maintained by Intellectual Property India, All Rights Reserved.

Page last updated on: 26/06/2019