Patent Search

Invention Title	SYSTEM AND METHOD FOR AUTOMATED CYBERSECURITY THREAT DETECTION AND MITIGATION USING ARTIFICIAL INTELLIGENCE
Publication Number	38/2025
Publication Date	19/09/2025
Publication Type	INA
Application Number	202541083617
Application Filing Date	03/09/2025
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0009400000, G06N0020000000, G06N0003088000, G06F0021550000, G06N0003045000

Inventor

Name	Address	Country
Dr. G. Syam Prasad	Professor & HoD, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Siva Naga Prasad Mannem	Assistant Professor, Department of Information Technology, Vishnu Institute of Technology (Autonomous), Kovvada, West Godavari District, Pin: 534202, Andhra Pradesh, India	India
Gudise Suresh Kumar	Assistant Professor, Department of Computer Science and Engineering, Dhanekula Institute of Engineering and Technology (Autonomous), Ganguru, Vijayawada, Pin: 521139, Andhra Pradesh, India	India
Sk. Ahmad Mohiddin	Associate Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Md. Ahmed	Assistant Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
A. Koteswara Rao	Assistant Professor, Department of Computer Science and Engineering, Lakireddy Balireddy Colleg of Engineering (Autonomous), Mylavaram, NTR District, Pin: 521230, Andhra Pradesh, India	India
K. Venkateswara Rao	Assistant Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Dr. K. Narasimha Raju	Associate Professor, Department of Computer Science and Engineering, Gayatri Vidya Parishad College of Engineering (Autonomous) Madhurawada, Visakhapatnam, Pin: 530048, Andhra Pradesh, India	India
Peddini Suresh Kumar	Research Scholar, Department of Electronics and Communication Technology, National Institute of Technology, Cachar Silchar, Pin: 788010, Assam, India	India
P. Ashok Kumar	Assistant Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Jonnalagadda V N Raju	Assistant Professor, Department of Information Technology, Dhanekula Institute of Engineering and Technology (Autonomous), Ganguru, Vijayawada, Pin: 521139, Andhra Pradesh, India	India
A. Karna Rao	Assistant Professor, Department of Electronics and Communication Engineering, DVR &HS MIC College of Technology, Kanchikacherla, Vijayawada, NTR District, Pin: 521180, Andhra Pradesh, India	India

Applicant

Name	Address	Country
Dr. G. Syam Prasad	Professor & HoD, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Siva Naga Prasad Mannem	Assistant Professor, Department of Information Technology, Vishnu Institute of Technology (Autonomous), Kovvada, West Godavari District, Pin: 534202, Andhra Pradesh, India	India
Gudise Suresh Kumar	Assistant Professor, Department of Computer Science and Engineering, Dhanekula Institute of Engineering and Technology (Autonomous), Ganguru, Vijayawada, Pin: 521139, Andhra Pradesh, India	India
Sk. Ahmad Mohiddin	Associate Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Md. Ahmed	Assistant Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
A. Koteswara Rao	Assistant Professor, Department of Computer Science and Engineering, Lakireddy Balireddy Colleg of Engineering (Autonomous), Mylavaram, NTR District, Pin: 521230, Andhra Pradesh, India	India
K. Venkateswara Rao	Assistant Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Dr. K. Narasimha Raju	Associate Professor, Department of Computer Science and Engineering, Gayatri Vidya Parishad College of Engineering (Autonomous) Madhurawada, Visakhapatnam, Pin: 530048, Andhra Pradesh, India	India
Peddini Suresh Kumar	Research Scholar, Department of Electronics and Communication Technology, National Institute of Technology, Cachar Silchar, Pin: 788010, Assam, India	India
P. Ashok Kumar	Assistant Professor, Department of Computer Science and Engineering, Sri Vasavi Institute of Engineering and Technology (Autonomous), Nandamuru, Pedana, Krishna District, Pin: 521369, Andhra Pradesh, India	India
Jonnalagadda V N Raju	Assistant Professor, Department of Information Technology, Dhanekula Institute of Engineering and Technology (Autonomous), Ganguru, Vijayawada, Pin: 521139, Andhra Pradesh, India	India
A. Karna Rao	Assistant Professor, Department of Electronics and Communication Engineering, DVR &HS MIC College of Technology, Kanchikacherla, Vijayawada, NTR District, Pin: 521180, Andhra Pradesh, India	India

Abstract:

The present invention relates to a system and method for automated cybersecurity threat detection and mitigation using artificial intelligence. The system comprises collection module for aggregating network traffic, endpoint activity, and user behavior; an AI-based detection engine employing supervised, unsupervised, and deep l models to identify both known and unknown threats; a threat intelligence integrator for enhancing detection accuracy through external feeds; and an automated mit module for executing countermeasures such as IP blocking, process termination, and device isolation. A feedback and reinforcement learning loop continuously refin models, thereby reducing false positives and adapting to evolving attack patterns. The invention provides real-time, self-adaptive cybersecurity defense applicable to networks, cloud infrastructures, and IoT ecosystems.

Complete Specification

Description:The present invention relates to the field of cybersecurity and information technology, and more particularly to an artificial intelligence (AI)-based syste method for automated threat detection and mitigation in computer networks, enterprise infrastructures, cloud environments, and Internet of Things (IoT) ecosyste invention employs adaptive machine learning models, intelligent threat analytics, and real-time automated response mechanisms to identify, classify, and neutralize evolving cyber threats with minimal human intervention.

BACKGROUND OF THE INVENTION

The following description of related art is intended to provide background information pertaining to the field of the disclosure. This section may include certain asp the art that may be related to various features of the present disclosure. However, it should be appreciated that this section be used only to enhance the understan the reader with respect to the present disclosure, and not as admissions of prior art.

Cybersecurity has become a critical domain as enterprises, governments, and individuals increasingly rely on digital infrastructures for communication, commerce, data storage. With the proliferation of cloud computing, mobile devices, and IoT systems, attack surfaces have expanded significantly, providing malicious actors wi opportunities to exploit vulnerabilities. Traditional defense mechanisms, while useful, often fail to keep pace with the dynamic nature of modern cyber threats.

Conventional security solutions such as firewalls, intrusion detection systems, and antivirus software primarily depend on predefined signatures and static rules. W effective against known attacks, these tools are unable to detect novel or zero-day exploits, as they lack the adaptive intelligence required to respond to new attack

View Application Status