Patent Search

Invention Title	A NOVEL SYSTEM FOR IDENTIFYING CYBER SECURITY ATTACKS USING ARTIFICIAL INTELLIGENCE
Publication Number	47/2023
Publication Date	24/11/2023
Publication Type	INA
Application Number	202341069360
Application Filing Date	14/10/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06F0021550000, G06N0003000000, G06N0005040000, G06N0020000000, G06N0007000000

Inventor

Name	Address	Country
Mr.Kuchinad Vaishak	Assistant Professor, Department of Cyber Security, CMR College of Engineering & Technology (CMRCET), Hyderabad, Telangana, India. Pin Code:501401	India
Mrs.P R Rajakumari	Assistant Professor, Department of ECE, RK College of Engineering-Vijayawada, NTR District, Andhra Pradesh, India. Pin Code:521456	India
Mr.Jaswant Narendra Saxena	Post Graduate Student, Advanced Management- Management Information System, Yale University, New Haven, United States. Po.Box: 06520	U.S.A.
Mr.Ananya Nagraj	Post Graduate Student, Master of Science (MS) in Management Information Systems, Stevens Institute of Technology, New Jersey, United States. Po.Box: 07030	U.S.A.
Mr.Sagar Choudhary	Assistant Professor, Department of Computer Science and Engineering, Quantum University, Roorkee-Dehradun Highway, Mandawar, Roorkee, Uttarakhand, India. Pin Code:247167	India
Mrs.Pavani Kollamudi	Senior Assistant Professor, Department of ECE, Lakireddy Bali Reddy College of Engineering, L.B Reddy Nagar, Mylavaram, Krishna District, Andhra Pradesh, India. Pin Code:521230	India
Mrs.C.Radhika	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering (IARE), Dundigal, Hyderabad, Telangana, India. Pin Code:500049	India
Dr.K.G.S.Venkatesan	Professor, Department of CSE, MEGHA Institute of Engineering & Technology for Women, Edulabad, Hyderabad, Telangana, India. Pin Code:501301	India
Mr.D.Anandan	Assistant Professor, Department of Computer Science and Engineering, V.S.B Engineering College, Karudayampalyam post, Karur, Tamil Nadu, India. Pin Code:639111	India
Dr.S.Vinod Kumar	Associate Professor, Department of Chemical Engineering, St.Joseph's College of Engineering, Padur, Chennai, Tamil Nadu, India. Pin Code:603103	India

Applicant

Name	Address	Country
Mr.Kuchinad Vaishak	Assistant Professor, Department of Cyber Security, CMR College of Engineering & Technology (CMRCET), Hyderabad, Telangana, India. Pin Code:501401	India
Mrs.P R Rajakumari	Assistant Professor, Department of ECE, RK College of Engineering-Vijayawada, NTR District, Andhra Pradesh, India. Pin Code:521456	India
Mr.Jaswant Narendra Saxena	Post Graduate Student, Advanced Management- Management Information System, Yale University, New Haven, United States. Po.Box: 06520	U.S.A.
Mr.Ananya Nagraj	Post Graduate Student, Master of Science (MS) in Management Information Systems, Stevens Institute of Technology, New Jersey, United States. Po.Box: 07030	U.S.A.
Mr.Sagar Choudhary	Assistant Professor, Department of Computer Science and Engineering, Quantum University, Roorkee-Dehradun Highway, Mandawar, Roorkee, Uttarakhand, India. Pin Code:247167	India
Mrs.Pavani Kollamudi	Senior Assistant Professor, Department of ECE, Lakireddy Bali Reddy College of Engineering, L.B Reddy Nagar, Mylavaram, Krishna District, Andhra Pradesh, India. Pin Code:521230	India
Mrs.C.Radhika	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering (IARE), Dundigal, Hyderabad, Telangana, India. Pin Code:500049	India
Dr.K.G.S.Venkatesan	Professor, Department of CSE, MEGHA Institute of Engineering & Technology for Women, Edulabad, Hyderabad, Telangana, India. Pin Code:501301	India
Mr.D.Anandan	Assistant Professor, Department of Computer Science and Engineering, V.S.B Engineering College, Karudayampalyam post, Karur, Tamil Nadu, India. Pin Code:639111	India
Dr.S.Vinod Kumar	Associate Professor, Department of Chemical Engineering, St.Joseph's College of Engineering, Padur, Chennai, Tamil Nadu, India. Pin Code:603103	India

Abstract:

This invention presents a Novel System for Identifying Cyber Security Attacks using Artificial Intelligence. The present invention comprising of employing an AI-driven instantaneous examination of network traffic, system logs, and user behavior, identifying irregularities within the data as signals pointing to potential cyberattacks, in immediate incident response measures in real-time to alleviate the impact of the cyber security incident and conveying information about detected threats and provi response alternatives to users via a user-friendly interface. Accompanied Drawing [FIG. 1-2]

Complete Specification

Description:[001] The invention, in general, relates to the field of artificial intelligence systems and methods. More specifically, the present invention relates to a Nov System for Identifying Cyber Security Attacks using Artificial Intelligence.

BACKGROUND OF THE INVENTION

[002] The following description provides the information that may be useful in understanding the present invention. It is not an admission that any of the informati provided herein is prior art or relevant to the presently claimed invention, or that any publication specifically or implicitly referenced is prior art.

[003] In an era where the digital landscape has become the backbone of global economies, infrastructure, and communication, the battle for safeguarding this realr relentless cyber threats is more critical than ever. Cybersecurity breaches have escalated in frequency and sophistication, posing substantial risks to the privacy, int and stability of our digital world. Traditional cybersecurity systems are hindered by their inability to adapt to emerging threats.

[004] The rapid evolution of technology has ushered in a complex and interdependent ecosystem, offering immense opportunities for innovation, but also creating ground for malicious actors seeking to exploit vulnerabilities. Conventional cybersecurity measures, often reliant on predefined rules and signature-based detectior struggling to keep pace with the ever-evolving tactics employed by cybercriminals. This is where the present invention steps in, bridging the gap with the power of a intelligence.

[005] Accordingly, on the basis of aforesaid facts, there remains a need in the prior art to provide a Novel System for Identifying Cyber Security Attacks using Artificia Intelligence. Therefore, it would be useful and desirable to have a system, method, apparatus and interface to meet the above-mentioned needs.

SUMMARY OF THE PRESENT INVENTION

View Application Status