Patent Search

Invention Title	DESIGN AND ANALYSIS OF MACHINE LEARNING SECURITY FRAMEWORK FOR IOT SYSTEMS
Publication Number	35/2023
Publication Date	01/09/2023
Publication Type	INA
Application Number	202341055623
Application Filing Date	19/08/2023
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMPUTER SCIENCE
Classification (IPC)	G06N0003080000, G06F0021550000, G06N0003040000, G06N0020000000, G06N0003000000

Inventor

Name	Address	Country
Ms. V. S. Saranya	Assistant Professor, Department of Computing Technologies, School of Computing SRM Institute of Science and Technology, Kattankulathur Campus, Kattankulathur- 603203	India
Ms. Indira Kambala	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana - 500043, India	India
Dr. P. V. Sarath Chand	Associate Professor, Department of Computer Science and Engineering, Pallavi Engineering College, Kuntloor, Hyderabad – 501505, Telangana, India	India
Mr. Avula Lakshmaiah	Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering & Technology, Facing Main Road, Sheriguda, Ibrahimpatam, Hyderabad, Telangana - 501510	India
Mr. Addagatla Prashanth	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana - 500043, India	India
Dr. A Ugendhar	Associate Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Hyderabad - 501506, Telangana, India	India
Mr. Syed Muqthadar Ali	Senior Assistant Professor, Department of Computer Science and Engineering CVR College of Engineering, Vastunagar, Mangalpalli (V), Ibrahimpatnam (M), Rangareddy (D), Telangana 501 510, India	India
Mr. Ganesh Naidu Ummadisetti	Assistant Professor, Department of Computer Science and Business system, B V Raju Institute of Technology, Narsapur, Medak – 502313, Hyderabad, Telangana, India	India

Applicant

Name	Address	Country
Ms. V. S. Saranya	Assistant Professor, Department of Computing Technologies, School of Computing SRM Institute of Science and Technology, Kattankulathur Campus, Kattankulathur- 603203	India
Ms. Indira Kambala	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana - 500043, India	India
Dr. P. V. Sarath Chand	Associate Professor, Department of Computer Science and Engineering, Pallavi Engineering College, Kuntloor, Hyderabad – 501505, Telangana, India	India
Mr. Avula Lakshmaiah	Assistant Professor, Department of Computer Science and Engineering, Sri Indu College of Engineering & Technology, Facing Main Road, Sheriguda, Ibrahimpatam, Hyderabad, Telangana - 501510	India
Mr. Addagatla Prashanth	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Dundigal, Hyderabad, Telangana - 500043, India	India
Dr. A Ugendhar	Associate Professor, Department of Computer Science and Engineering, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Hyderabad - 501506, Telangana, India	India
Mr. Syed Muqthadar Ali	Senior Assistant Professor, Department of Computer Science and Engineering CVR College of Engineering, Vastunagar, Mangalpalli (V), Ibrahimpatnam (M), Rangareddy (D), Telangana 501 510, India	India
Mr. Ganesh Naidu Ummadisetti	Assistant Professor, Department of Computer Science and Business system, B V Raju Institute of Technology, Narsapur, Medak – 502313, Hyderabad, Telangana, India	India

Abstract:

The security of the Internet of Things is attracting increasing attention from both academia and industry. In fact, IoT devices are vulnerable to various security attacks from denial of service (DoS) to network intrusions and data leaks. This work introduces a novel machine learning (ML)-based security framework that automatically ha growing security issues associated with the IoT domain. This framework uses both software-defined networking (SDN) and network functions virtualization (NFV) enal counter a variety of threats. This AI framework combines an AI-based monitoring agent and response agent using machine learning models broken down into networ analysis, along with anomaly-based intrusion detection in IoT systems. The framework uses supervised learning, the distributed data mining system, and the neural r achieve its goals. In particular, the propagation of attacks using the data mining approach is very successful in identifying attacks with high performance and low cost

Complete Specification

Description:FIELD OF INVENTION

Securing IoT devices is a growing challenge for manufacturers and consumers. Weak, default, or storing data online without a password are some of the major secu challenges identified by the researchers. IoT devices are often shipped with either default, easy to remember, or without any password. Hackers can very easily exp vulnerability by gaining access to these devices. Such vulnerability puts the consumers' privacy at risk and allows hackers to use IoT devices to launch large-scale att DDoS.

BACKGROUND OF INVENTION

The disruptive acceleration of Internet of Things (IoT) is drastically modifying the current ICT landscape with a massive number of cellular IoT devices expected to be deployed in the next few years. IoT devices are taking over a variety of aspects of our current lives, such as health care, transportation, and home environments. Th the massive growth in analytics and cloud computing technologies, they are expected to be able to provide relevant contextual data using their autonomous communication with each other without human interaction. All of these envisioned benefits are rapidly pushing the adoption of this technology. On the other side c spectrum, IoT nodes can be comprised by malicious attackers leveraging their resource constraints and relevant vulnerabilities. Accounting for their wide adoption, security threats can cause severe privacy problems and economical damage. As they are becoming an essential element in our daily lives, maintaining privacy, secu business operations/opportunities are of a very high priority. For instance, IoT devices could be used for various purposes and can be deployed in different places i home, health care and industrial environments. Thus, they can carry sensitive personal data, such as user information and daily activities. An attack against those Io devices could lead to sensitive information leakage and can cause an interruption in workflows, thus compromising the quality of the products

View Application Status