FORM 2

THE PATENTS ACT 1970

39 OF 1970

&

THE PATENT RULES 2003

COMPLETE SPECIFICATION

(SEE SECTIONS 10 & RULE 13)

1. TITLE OF THE INVENTION

ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS

2. APPLICANTS (S)

NAME	NATIONALITY	ADDRESS
Dr.B.Nageswara Rao	Indian	Associate professor Lendi Institute of Engineering and Technology (Autonomous) Jonnada, Vizinagaram, Pin: 535005 Andhra Pradesh India
Dr.T NAGA NIRMALA RANI	Indian	ASSOCIATE PROFESSOR TELLAKULA JALAYYA POLISETTY SOMASUNDARAM COLLEGE,OPP. JUTE MILL RING ROAD, GUNTUR Pin:522002 ANDHRA PRADESH INDIA
Dr.M. Senthil	Indian	Professor

		QIS College of Engineering and Technology, Vengamukkalapalem, Ongole Prakasam Pin: 523272 Andhra Pradesh India
Mr. Y Srinivas	Indian	Prof. & HOD Nalla Narsimha Reddy Education Society's Group of Institutons Korremula X Road, Ghatkesar(M), Medchal Malkajgiri Pin: 500088 Telangana India
Mrs. BHARGAVI KOTA	Indian	Lecture in Computer Science Vaagdevi Degree & PG College, Hanamkonda Pin: 506001 Telangana India
P.Sathish Kumar	Indian	Assistant Professor Soet ,SPMVV,Tirupati Tirupati Pin: 517502 Andhra Pradesh India
Dr. Vineet Kumar	Indian	Assistant Professor Dr. Yashwant Singh Parmar Govt. P. G. College Nahan, Sirmour (H.P.) Pin:173001 Himachal Pradesh India
Mr. Ch.kishore kumar	Indian	Assistant Professor Vaagdevi degree and pg college Krishnapura Hanamkoda Warangal Pin:506371 Telangana

		India
Ms. Ghazala Ansari	Indian	Assistant Professor Department of ECE, SRM Institute of Science and technology, Sikri Kalan, Modinagar Ghaziabad Pin: 201204 Uttar Pradesh India
Dr. Vijay Kumar Salvia	Indian	Director/Professor Research Innovation StartUp University Regd, Indore Pin:452018 Madhya Pradesh India
Mr. Y. M. MAHABOOBJOHN	Indian	ASSISTANT PROFESSOR MAHENDRA COLLEGE OF ENGINEERING MINNAMPALLI, SALEM Pin: 636106 TAMILNADU INDIA
Dr. Harikumar Pallathadka	Indian	Director and Professor Manipur International University, Ghari, Imphal, Imphal West, Imphal Pin: 795140 Manipur India

2. PREAMBLE TO THE DESCRIPTION

COMPLETE SPECIFICATION

The following specification particularly describes the invention and the manner in which it is to be performed

ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS

Abstract:

As more individuals acquire access to the internet, cyberattacks have risen substantially. As individuals become more concerned about cybersecurity, there is also a drive to secure systems and activities. It is easy to understand why cybersecurity professionals seek inspiration from artificial intelligence. Given the current state of cybersecurity, it is easy to understand why things are how they are. Fuzzy neural networks are a type of hybrid design that may recognise patterns in a number of situations, such as mistake detection and unusual behaviour. Finding and classifying patterns is one example. This article explores how to apply a model of artificial intelligence based on the interaction between fuzzy logic and artificial neural network training to detect problems with financial transactions in computer networks and cyberattacks. Massive datasets were utilised to develop fuzzy rules, which were then included into expert systems and used to validate the model's accuracy. The learned rules permit the creation of high-level, intelligent algorithms that can detect online purchases that breach the restrictions. The dependability of the trials also shows that fuzzy neural networks could be utilised in highly secure computer networks as anomaly detectors.

Descriptions

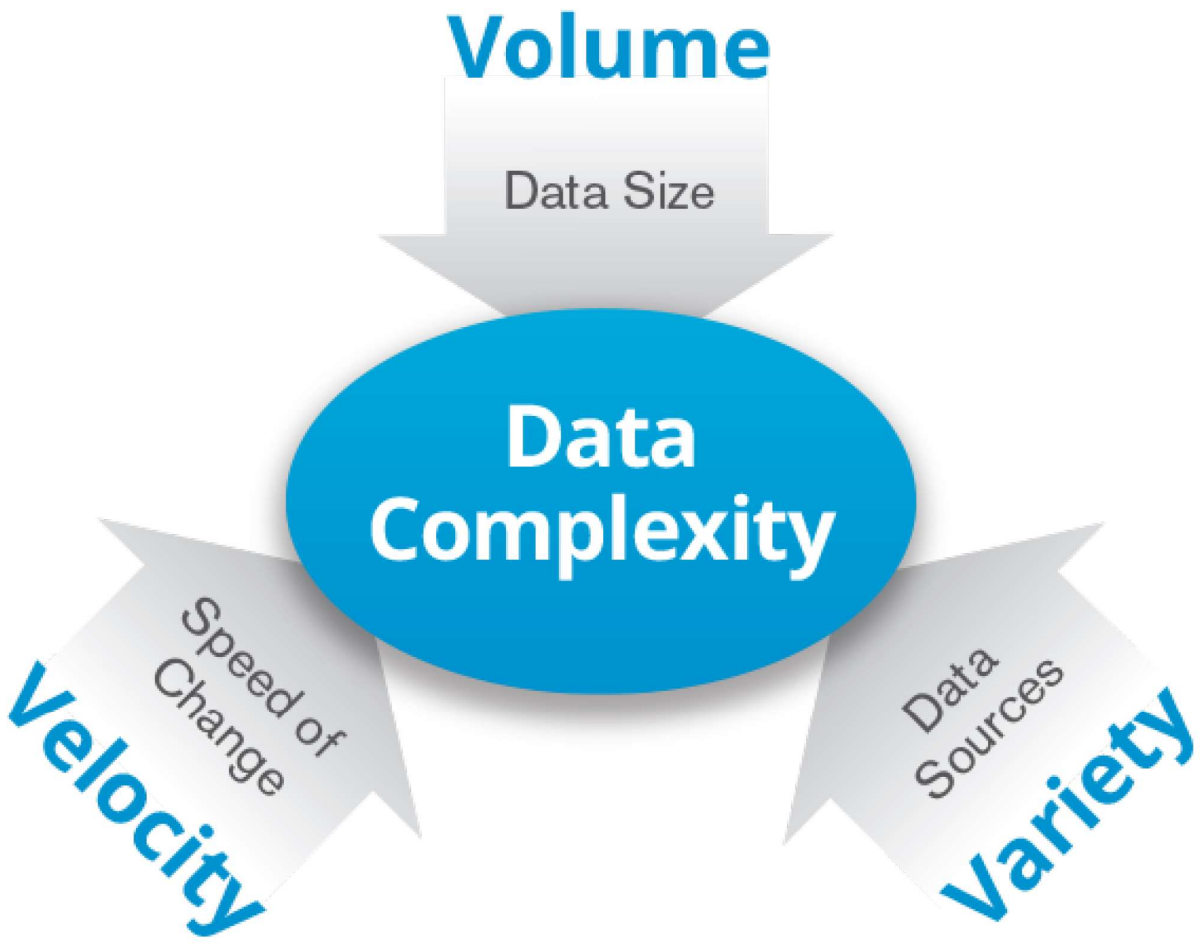
According to the White House, a number of federal organisations are already utilising AI. This is also true in the commercial sphere, where numerous industries and organisations are already employing artificial intelligence. Why? Why? If AI could quickly analyse organised data while also evaluating and researching unstructured data, statistics, voice patterns, and language, it could save a great deal of time and money. This is easy and quick to perform. It is possible that artificial intelligence may protect both government funds and sensitive information. In addition, they are separated by spaces. The hackers are looking for vulnerabilities in our systems that they can exploit to obtain access. Unfathomable is the length of time between a data breach and the company's discovery of it. Both the hacker and whatever confidential information they obtained had vanished by that point. However, AI has little choice but to collect data while waiting for a hacker to wreak havoc. When a user creates an account or a password, AI searches for signs that the user may be a hacker. This can occur either when the password is initially created or when the user logs in. Artificial intelligence can identify subtle hints that might otherwise be overlooked. This prevents the hacker squad from advancing. Varughese was true in his assertion that any tool can be abused. Cybersecurity is analogous to chess: regardless of how sophisticated a system is, hackers will always seek out vulnerabilities. AI has a chance in the future so long as it remains under human control. AI is proficient at linking and analysing data, but it can only perform tasks that it has been instructed to do. If criminals are to be prevented from seizing entire control of AI systems, their creators must instal additional security measures. There will always be cat-and-mouse games, but applying artificial intelligence to safeguard private information is a

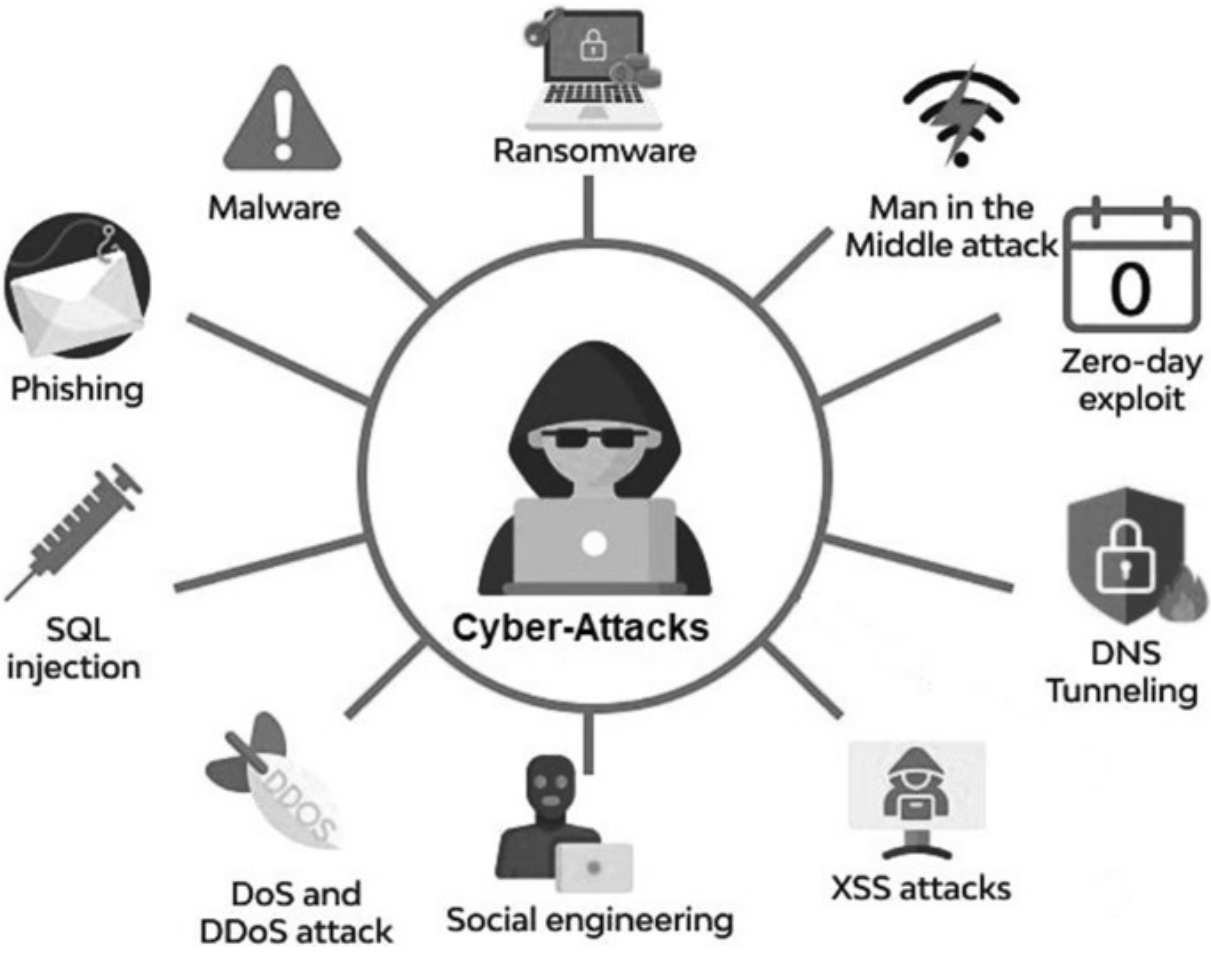
step in the right direction. Google created a graphical data learning approach using Tensor Flow to enhance machine learning. seek out a date 03.09.2019 Neural Structured Learning is an open-source framework designed to train neural network data sets and data structures using Neural Graph Learning. NSL stands for Neural Structured Learning in this context. NSL is intended for experienced users as opposed to those who have never utilised machine learning previously. It works with the Tensor Flow platform for machine learning. It can be used to visualise machine vision models, perform natural language processing, and project data from sources that are constantly changing, such as medical records and charts. As the volume and complexity of attacks continue to rise, security operations analysts are turning to artificial intelligence to help them stay one step ahead of prospective threats, despite shrinking resources. Machine learning and natural language processing are two AI technologies that can sort through the constant deluge of warnings and give useful information in a fraction of the time normally required. These systems employ threat intelligence obtained from millions of scholarly articles, blogs, and news items. In this video, you will learn how artificial intelligence (AI) may assist security analysts in identifying linkages between different security vulnerabilities. Users can work on a variety of projects, from research and development to marketing and sales, in a dynamic virtual environment. Cybersecurity defends data, networks, electronic devices, and servers against harmful attacks and unauthorised access. Cybersecurity practises include application security, identity management, network security, data security, end-user education, disaster recovery, and business continuity. Ransomware, phishing, malware, and social engineering are typical types of cyber attacks. Anti-virus and anti-malware software, firewalls, encryption tools, two-factor authentication, patches and updates, and two-factor authentication are some

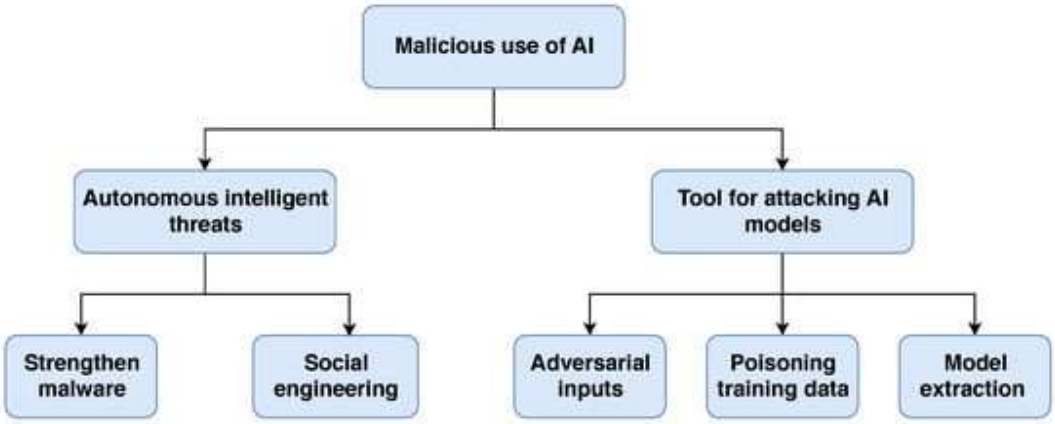
of the cybersecurity technologies that can guard against these attacks. Using these methods, it is impossible to monitor and protect cyberspace from a wide variety of online crimes. Cyber-threat defences must be versatile, dependable, and secure to detect a wide variety of alarms and make real-time decisions based on accurate data. Artificial intelligence is one way to facilitate this. Because fuzzy neural networks are used in this paper, we can say that they perform well as anomaly detectors. Due to the skewed nature of the problem and the fact that over 98% of the data came from the same group, the model performed exceptionally well in recognising outliers, identifying them in the great majority of tests. More than 98 percent of all samples belong to the same group. Some features of the collected information can be explored. All of the models presented for the cyber-attack categorization test performed wonderfully and contained a good balance of training and testing data, indicating that none of them were overfitted. The fuzzy neural network is the most promising model for detecting cyberattacks since it performed better in both training and testing. Training and testing required far less time when the cyber invasion exam was first developed. Because multilayered networks contain so much information, it takes longer to find solutions. The least successful models for identifying malicious cyber activity were those that could be executed in the smallest amount of time. This is due to the fact that the value of specificity, which indicates how accurately attacks can be predicted, is one of the most important measures of a model's performance when dealing with an unbalanced problem such as this one. As a result, the FNN had the best success rate, with over 98% accuracy. When the results of how simple it is to learn about attacks were paired with the results of the model given in this study, the evaluation indices produced the best results. It is essential to note, however, that the model described in this study produced the best results

despite its lengthy execution time. Methods for guarding against cyber threats that utilise the acquired knowledge. Information systems with logical programming and programmable electrical devices are examples of situations where fuzzy rules are simple to implement. Because the model can convert data from a database into a collection of linguistic rules, it can be considered as a technique for managing knowledge in Big Data. In other words, people outside the computer science industry are more likely to comprehend these norms. This strategy can aid in enhancing research and removing anomalies. It also facilitates the dissemination of efficient methods. In the future, it will be essential to identify methods for accelerating algorithm performance without reducing its ability to detect anomalies. Other fuzzy-making and training procedures can be investigated and compared to other intelligent models. This will allow you to assess and compare different AI situations. Future alterations to this study could incorporate utilising more current information to search for variances across a broad spectrum of cyberattacks.

DRAWINGS:


Volume
Data Size
Data Complexity
Speed of Change
Velocity
Data Sources
Variety


Ransomware
Malware
Man in the Middle attack
Phishing
Zero-day exploit
Cyber-Attacks
SQL injection
DNS Tunneling
DDOS
DoS and DDoS attack
Social engineering
XSS attacks


Malicious use of AI
Autonomous intelligent threats
Tool for attacking AI models
Strengthen malware
Social engineering
Adversarial inputs
Poisoning training data
Model extraction

CLAIMS

1. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said it provides a ground work for future research.

2. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said that in this paper, we discussed various aspects.

3. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said that in recent years, AI become a hot topic in the all sector.

4. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said that it is an effective tool.

5. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said that this research looks at all limitations and challenges.

6. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said that the research findings could benefit in the design and implementation of the next phase.

7. ARTIFICIAL INTELLIGENCE (AI) AND FUZZY NEURAL NETWORKS FOR THE IDENTIFICATION OF ABNORMALITIES IN LARGE-SCALE CYBERATTACKS of claim 1, wherein said that additionally, research may be undertaken frequently.