1. Problem Statement:
2. Diagnosis of left ventricular hypertrophy using
3. convolutional neural network
4. Diagnosis of left ventricular hypertrophy using
5. convolutional neural network
6. Diagnosis of left ventricular hypertrophy using
7. convolutional neural network

Diagnosis of left ventricular hypertrophy using convolutional neural network

Conclusion:

Background: Clinically, doctors obtain the left ventricular posterior wall thickness (LVPWT) mainly by observing ultrasonic echocardiographic video stream to capture a single frame of images with diagnostic significance, and then mark two key points on both sides of the posterior wall of the left ventricle with their own experience for computer measurement. In the actual measurement, the doctor's selection point is subjective, and difficult to accurately locate the edge, which will bring errors to the measurement results. Material/Methods: In this paper, a convolutional neural network model of left ventricular posterior wall positioning was built under the TensorFlow framework, and the target region images were obtained after the positioning results were processed by non-local mean filtering and opening operation. Then the edge detection algorithm based on threshold segmentation is used. After the contour was extracted by adjusting the segmentation threshold through prior analysis and the OTSU algorithm, the design algorithm completed the computer selection point measurement of the thickness of the posterior wall of the left ventricle. Results: The proposed method can effectively extract the left ventricular posterior wall contour and measure its thickness. The experimental results show that the relative error between the measurement result and the hospital measurement value is less than 15%, which is less than 20% of the acceptable repeatability error in clinical practice. Conclusions: Therefore, the method proposed in this paper not only has the advantage of less manual intervention, but also can reduce the workload of doctors.

2. Problem Statement:

Prediction of Office Building Rental upon Spatiotemporal Data

Conclusion:

This paper presents a study on effectively predicting office building rentals based on the surrounding spatiotemporal data. During the planning, development, and construction stages of an office building, the stakeholders of the building may have one question to be answered, i.e., what the potential value of the office building is. The potential value of office buildings may be hard to be measured directly, however, it can be reflected in the rental after the office is put into operation. An accurate prediction of the office building rental will provide the solid base for the corresponding stakeholders to make business decisions. The rental of office buildings is affected by many factors, such as its location, floors, number of parking spots, the convenience of transportation, as well as the activities of the surrounding business. To support the rental prediction, we collect the datasets from different data sources in Shanghai. The linear regression, the decision tree, and the random forest models are employed in the computational experiments to predict the office building rentals and the most suitable prediction methodology for predicting the office building rental is suggested upon the experiments.

3. Problem Statement:

Product Innovation through Knowledge Management and Social Media Strategies

Conclusion:

Product Innovation through Knowledge Management and Social Media Strategies is an authoritative reference source for the latest scholarly research on the application of social networking platforms to enhance knowledge sharing and innovative practice within organizations. Highlighting pertinent theories and techniques for improving communication and ensuring successful product development, this book is ideally designed for corporate managers, organizational leaders, researchers, and professionals interested in the value of knowledge sharing and social media tools in modern organizations. Companies competing on a global scale must endeavor to launch new initiatives, products, and services aimed to set them apart from their competitors. Integrating technology and knowledge management strategies into the product development process is one solution to remaining relevant in a highly competitive marketplace.

4. Problem Statement:

Securing Enterprise from Malicious Attacks on their Networks

Conclusion:

Routers interconnect networks of various enterprises, and the more secure the entry or exit points are made, the more robust the security of these enterprises is. These routers become the first direct targets and are vulnerable to security attacks. If these routers are not tightly protected, the attackers get an edge to intrude the system. In order to ensure the security of these routers, Secure Access Control Lists (ACLs) Filtering-Based Enterprise Networks (SAFE-Nets) are proposed in this chapter. In this scheme, routers are configured with Access Control Lists (ACL) that are used to filter in the intended packets and filter out the dangerous malicious packets from network traffic. This consolidates security deployment over the entire network on top of anti-virus software, weak passwords, latent software vulnerabilities, and other related secure measures. This can help network technicians working for various enterprises manage security at low costs.

# 5. Problem Statement:

# Twitter bot detection using supervised machine learning

Conclusion:

In the world of Internet and social media, there are about 3.8 billion active social media users and 4.5 billion people accessing the internet daily. Every year there is a 9% growth in the number of users and half of the internet traffic consists of mostly bots. Bots are mainly categorized into two categories: good and bad bots; good bots consist of web crawlers and chat bots whereas bad bots consist of malicious bots which make up 20% of the traffic, the reason they are not good is that they are used for nefarious purposes, they can mimic human behavior, they can impersonate legal traffic, attack IoT devices and exploit their performance. Among all these concerns, the primary concern is for social media users as they represent a large group of active users on the internet, they are more vulnerable to breach of data, change in opinion based on data. Detection of such bots is crucial to prevent further mishaps. We use supervised Machine learning techniques in this paper such as Decision tree, K nearest neighbors, Logistic regression, and Naïve Bayes to calculate their accuracies and compare it with our classifier which uses Bag of bots’ word model to detect Twitter bots from a given training data set.

6. Problem Statement:

Informed Machine Learning - A Taxonomy and Survey of Integrating Prior Knowledge into Learning Systems

Conclusion:

Despite its great success, machine learning can have its limits when dealing with insufficient training data. A potential solution is the additional integration of prior knowledge into the training process which leads to the notion of informed machine learning. In this paper, we present a structured overview of various approaches in this field. We provide a definition and propose a concept for informed machine learning which illustrates its building blocks and distinguishes it from conventional machine learning. We introduce a taxonomy that serves as a classification framework for informed machine learning approaches. It considers the source of knowledge, its representation, and its integration into the machine learning pipeline. Based on this taxonomy, we survey related research and describe how different knowledge representations such as algebraic equations, logic rules, or simulation results can be used in learning systems. This evaluation of numerous papers on the basis of our taxonomy uncovers key methods in the field of informed machine learning.

7. Problem Statement:

Web user identification based on browser fingerprints using machine learning methods

Conclusion:

The article developed a method for identifying users on the network based on browser fingerprints using machine learning methods. The resulting method is a modification of the user identification method based on a digital footprint, which can be more efficient due to two components. First, the selection of attributes for a digital footprint is made from a limited set of attributes to form a user browser fingerprint. Secondly, the identification accuracy can be increased through the combined use of classification methods and the probabilistic-statistical approach. To check the successful operation of the method, a computational experiment is carried out on real data, which consists in solving the problem of classifying a user based on his browser fingerprint using the K nearest neighbors method.

8. Problem Statement:

The Development of a Data Collection and Browser Fingerprinting System

Conclusion:

The urgent need to protect user privacy and security has emerged as the World Wide Web has become an increasingly necessary part of daily life. Browser fingerprinting is a very interesting topic in the industry of technology security. New technology will always raise new security issues and browser fingerprinting will undoubtedly follow the same process. It has become one of the most popular topics in online privacy because, to date, there is still no exact solution as to how to stop it entirely. The majority of solutions just aim to reduce the likelihood of obtaining a browser fingerprint. Research on browser fingerprinting is unquestionably required since it is essential to educate users, developers, policymakers, and law enforcement about it so that they can make strategic choices based on knowledge. Browser fingerprinting must be recognised in order to defend against privacy problems. A browser fingerprint is described as data gathered by the receiving server to identify a distant device, and it is different from cookies. Websites frequently utilize browser fingerprinting to obtain information about the type and version of the browser, as well as the operating system, and other current settings. It has been known that even when cookies are disabled, fingerprints can be used to fully or partially identify users or devices. In this communication paper, a new insight into the challenge of browser fingerprint is encouraged as a new venture. Thus, the initial way to truly understand the browser fingerprint is the need to collect browser fingerprints. In this work, the process of data collection for browser fingerprinting through scripting, to offer a complete all-in-one fingerprinting test suite, has been thoughtfully divided into appropriate sections and grouped with key information to be carried out. The objective is to gather fingerprint data with no personal identification information and make it an open source of raw datasets in the industry for any future research purposes. To our best knowledge, there are no open datasets made available for browser fingerprints in the research field. The dataset will be widely accessible by anyone interested in obtaining those data. The dataset collected will be very raw and will be in the form of a text file. Thus, the main contribution of this work is to share an open dataset of browser fingerprints along with its collection methodology.

9. Problem Statement:

End-User Browser-Side Modification of Web Pages

Conclusion:

The increasing volume of content and actions available on the Web, combined with the growing number of mature digital natives, anticipate a growing desire of controlling the Web experience. Akin to the Web2.0 movement, webies’ desires do not stop at content authoring but look for controlling how content is arranged in websites. By content, we mainly refer to HTML pages, better said, their runtime representation: DOM trees. The vision is for users to “prune” (removing nodes) or “graft” (adding nodes) existing DOM trees to improve their idiosyncratic and situational Web experience. Hence, Web content is no longer consumed as canned by Web masters. Rather, users can remove content of no interest, or place new content from somewhere else. This vision accounts for a post-production user-driven Web customization (referred to as “Web Modding”). Being user driven, appropriate abstractions and tools are needed. The paper introduces a set of abstractions (formalized in terms of a domain-specific language) and an IDE (realized as an add-on from Google Chrome) to empower non-programmers to achieve HTML rearrangement. The paper discusses the technical issues and the results of a first validation.

10. Problem Statement:

Incremental Cost-Sensitive Support Vector Machine With Linear-Exponential Loss

Conclusion:

Incremental learning or online learning as a branch of machine learning has attracted more attention recently. For large-scale problems and dynamic data problem, incremental learning overwhelms batch learning, because of its efficient treatment for new data. However, class imbalance problem, which always appears in online classification brings a considerable challenge for incremental learning. The serious class imbalance problem may directly lead to a useless learning system. Cost-sensitive learning is an important learning paradigm for class imbalance problems and widely used in many applications. In this paper, we propose an incremental cost-sensitive learning method to tackle the class imbalance problems in the online situation. This proposed algorithm is based on a novel cost-sensitive support vector machine, which uses the Linear-exponential (LINEX) loss to implement high cost for minority class and low cost for majority class. Using the half-quadratic optimization, we first put forward the algorithm for the cost-sensitive support vector machine, called CSLINEX-SVM\*. Then we propose the incremental cost-sensitive algorithm, ICSL-SVM. The results of numeric experiments demonstrate that the proposed incremental algorithm outperforms some conventional batch algorithms except the proposed CSLINEX-SVM\*.

11. Problem Statement:

Hybrid Machine Learning Model of Extreme Learning Machine Radial basis function for Breast Cancer Detection and Diagnosis; a Multilayer Fuzzy Expert System

Conclusion:

Mammography is often used as the most common laboratory method for the detection of breast cancer, yet associated with the high cost and many side effects. Machine learning prediction as an alternative method has shown promising results. This paper presents a method based on a multilayer fuzzy expert system for the detection of breast cancer using an extreme learning machine (ELM) classification model integrated with radial basis function (RBF) kernel called ELM-RBF, considering the Wisconsin dataset. The performance of the proposed model is further compared with a linear-SVM model. The proposed model outperforms the linear-SVM model with RMSE, R 2 , MAPE equal to 0.1719, 0.9374 and 0.0539, respectively. Furthermore, both models are studied in terms of criteria of accuracy, precision, sensitivity, specificity, validation, true positive rate (TPR), and false-negative rate (FNR). The ELM-RBF model for these criteria presents better performance compared to the SVM model. Keywords-hybrid machine learning, extreme learning machine (ELM), radial basis function (RBF), breast cancer, support vector machine (SVM).

12. Problem Statement:

Prognosis of Crop Yield Using Machine Learning Techniques

Conclusion:

Agriculture is the major occupation of many people in India. India was standing in the leading producer of agricultural goods. As the population of India increases gradually, the yield of the crop may be not sufficient in further days. Also, the Indian economy is based on agriculture. Using the technologies like Machine Learning, Deep Learning, and Artificial Intelligence we can prognosis the yield of the crop using some parameters like rainfall, temperature, crop to be cultivated, and pesticides. This prediction helps the farmers to know the yield before they cultivate

13. Problem Statement:

Application Layer DDOS Attack Detection and Defense Methods

Conclusion:

Nowadays in the cyberworld, the Internet has dramatically revolutionized many different fields and different public services globally. Due to any reason, unavailability of these services leads to enormous cost implications and it even affects society. A distributed denial of service (DDOS) attack is a major cybersecurity threat designed to deny services to legitimate users. These days, application-layer distributed denial of service attacks are the main threat on web servers. This paper addressed application layer DDOS attacks typical architecture, common detection mechanisms and defense methods. Numerous Application layer DDOS attack detection techniques have been developed, these can generally be described as detection methods based on the signature, anomalies and hybrids. In anomaly detection, we discussed statistical and machine learning-based methods by researchers. We classified defense mechanisms as defense methods and a combination of detection and defense methods.

14. Problem Statement:

A Survey on Machine Learning Techniques for Source Code Analysis

Conclusion:

The advancements in machine learning techniques have encouraged researchers to apply these techniques to a myriad of software engineering tasks that use source code analysis such as testing and vulnerabilities detection. A large number of studies poses challenges to the community to understand the current landscape. Objective: We aim to summarize the current knowledge in the area of applied machine learning for source code analysis. Method: We investigate studies belonging to twelve categories of software engineering tasks and corresponding machine learning techniques, tools, and datasets that have been applied to solve them. To do so, we carried out an extensive literature search and identified 364 primary studies published between 2002 and 2021. We summarize our observations and findings with the help of the identified studies. Results: Our findings suggest that the usage of machine learning techniques for source code analysis tasks is consistently increasing. We synthesize commonly used steps and the overall workflow for each task, and summarize the employed machine learning techniques. Additionally, we collate a comprehensive list of available datasets and tools useable in this context. Finally, we summarize the perceived challenges in this area that include availability of standard datasets, reproducibility and replicability, and hardware resources.

15. Problem Statement:

Machine-learning-assisted optimization and its application to antenna designs: Opportunities and challenges

Conclusion:

With the rapid development of modern wireless communications and radar, antennas and arrays are becoming more complex, therein having, e.g., more degrees of design freedom, integration and fabrication constraints and design objectives. While full-wave electromagnetic simulation can be very accurate and therefore essential to the design process, it is also very time consuming, which leads to many challenges for antenna design, optimization and sensitivity analysis (SA). Recently, machine-learning-assisted optimization (MLAO) has been widely introduced to accelerate the design process of antennas and arrays. Machine learning (ML) methods, including Gaussian process regression, support vector machine (SVM) and artificial neural networks (ANNs), have been applied to build surrogate models of antennas to achieve fast response prediction. With the help of these ML methods, various MLAO algorithms have been proposed for different applications. A comprehensive survey of recent advances in ML methods for antenna modeling is first presented. Then, algorithms for ML-assisted antenna design, including optimization and SA, are reviewed. Finally, some challenges facing future MLAO for antenna design are discussed.