Android Development : The future scope

Varaprasad.R varap@gmail.com, Dept. of CSE, G. Pullaiah college of engineering &
Technology, Kurnool, A.P

Abstract: Android accounts for approximately 85% of all devices sold today. Android Application Development simply means developing new applications that can run on the devices powered by android operating system. Google states that "**Android applications can be written using Kotlin** (an alternate programming language for developing android applications. Many renowned technology firms have started using Kotlin for developing their android applications such as Pinterest, Uber, Atlassian, Pivotal etc.), Java, and C++ languages" using the Android software development kit, while using other languages is also possible. When thinking about the scope of Android Application Development in India (one of the fastest growing nations in the world as far as IT market is concerned) -- one of the major benefits of choosing android application development is astonishing job opportunities associated with it. Many IT firms and startups require android application developers who can create cost effective apps that are capable of delivering best user experience.

Keywords: Android; Smartphones; Architecture; Applications; App Developers.

"I think right now it's a battle for the mindshare of developers and for the mindshare of customers, and right now iPhone and Android are winning that battle."

– Steve Jobs

Review

Machine learning for autism: promising

,

Dr.K.Seshadri Ramana , seshu45@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract: Early and objective autism spectrum disorder (ASD) assessment, as well as early intervention are particularly important and may have long term benefits in the lives of ASD people. ASD assessment relies on subjective rather on objective criteria, whereas advances in research point to up-to-date procedures for early ASD assessment comprising eye-tracking technology, machine learning, as well as other assessment tools. This systematic review, the first to our knowledge of its kind, provides a comprehensive discussion of 30 studies irrespective of the stimuli/tasks and dataset used, the algorithms applied, the eye-tracking tools utilised and their goals. Evidence indicates that the combination of machine learning and eye-tracking technology could be considered a promising tool in autism research regarding early and objective diagnosis. Limitations and suggestions for future research are also presented.

Keywords: machine learning; eye-tracking technology; ASD; autism; assessment; classification

Citation: Kollias, K.-F.; Syriopoulou-Delli, C.K.; Sarigiannidis, P.; Fragulis, G.F. The Contribution of Machine Learning and Eye-Tracking Technology in Autism Spectrum Disorder Research: A Systematic Review. *Electronics* **2021**, *10*, 2982. https://doi.org/10.3390/electronics10232982

Academic Editors: Tomasz Trzcinski and Hyunjin Park

Received: 9 October 2021
Accepted: 27 November 2021
Published: 30 November 2021

1. Introduction

The Diagnostic and Statistical Manual of Mental Disorders defines autism spectrum disorder (ASD) as a highly complicated neurodevelopmental disorder with complex etiological causes [1] characterised by social communication/interaction difficulties and repetitive behaviours/interests [2], prevalent in 1% of the world's population [3]. It was first introduced by Kanner [4], who described it as involving "resistance to change" and "need for sameness". Asperger in [5] defined ASD as "autistic psychopathy," meaning autism (self) and psychopathy (personality). ASD reaches a high male-to female ratio, attaining an average of 4:1, a steep increase to 10:1 in "high functioning autism" or Asperger syndrome and a fall to 2:1 in people presenting comorbidity with moderate-to-severe intellectual disability [6].

In addition to reduced social interaction and communication, restricted, repetitive, and stereotyped behaviour, people with ASD tend to show a deficit in eye gaze, a characteristic which cannot cause autism [2] but which constitutes an important item in several diagnostic tests [7]. Eye gaze deficits of ASD people are related both to social and non-social stimuli. As far as social and facial stimuli are concerned, individuals with ASD are likely to have difficulties to preferentially attend both biological motion, i.e., gestures of the body, expressions of the face, as well as the eyes of others [8]. In other words, individuals with ASD tend to show visual differences in visual attention to faces, compared to typically developing ones. Regarding non-social stimuli, individuals with ASD appear to show

Article

Predicting Mental disorder using Machine Learning Algorithms: A review

M. Srilakshmi , lakshmigpcet@gmail.com,Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract: Autism spectrum disorder (ASD), characterized by social, communication, and behavioral abnormalities, affects 1 in 36 children according to the CDC. Several co-occurring conditions are often associated with ASD, including sleep and immune disorders and gastrointestinal (GI) problems. ASD is also associated with sensory sensitivities. Some individuals with ASD exhibit episodes of challenging behaviors that can endanger themselves or others, including aggression and self-injurious behavior (SIB). In this work, we explored the use of artificial intelligence models to predict behavior episodes based on past data of co-occurring conditions and environmental factors for 80 individuals in a residential setting. We found that our models predict occurrences of behavior and non-behavior with accuracies as high as 90% for some individuals, and that environmental, as well as gastrointestinal, factors are notable predictors across the population examined. While more work is needed to examine the underlying connections between the factors and the behaviors, having reasonably accurate predictions for behaviors has the potential to improve the quality of life of some individuals with ASD.

Keywords: autism spectrum disorder; challenging behavior; machine learning

check for updates

Citation: Ferina, J.; Kruger, M.; Kruger, U.; Ryan, D.; Anderson, C.; Foster, J.; Hamlin, T.; Hahn, J. Predicting Problematic Behavior in Autism Spectrum Disorder Using Medical History and Environmental Data. *J. Pers. Med.* **2021**, *13*, 1513. https://doi.org/10.3390/jpm13101513

Academic Editors: Kenneth Blum and Rajendra D Badgaiyan

Received: 11 August 2021
Revised: 16 October 2021
Accepted: 19 October 2021
Published: 21 October 2021

1. Introduction

Autism spectrum disorder (ASD) is a neurodevelopmental condition that is defined by difficulty in communication, social interaction, and restricted repetitive behaviors. ASD is estimated to affect about 1 in 36 children in the United States by age 8 according to the CDC [1]. Despite being categorized and diagnosed by a set of behavioral criteria [2,3], ASD is known to often be associated with several co-occurring conditions that affect a multitude of physiological systems [4,5]. Three major areas of ASD-associated comorbidities include sleep disorders [6], gastrointestinal (GI) problems [7], and immune disorders [8]. These comorbidities have the potential to cause an individual pain or discomfort, which may affect their behavior. While many atypical behaviors are associated with ASD, the focus of this paper is on two behaviors that can pose danger to the affected individual and/or others around them: aggression and self-injury. Aggressive behavior can have severe consequences for the individual, their peers, and caregivers [9,10], while self-injurious behavior (SIB) can cause serious harm to the individual [11].

Aggression has been shown to be associated with sleep abnormalities [12–14]. Aggression is also associated with several other behaviors, including SIB [14,15], ritualistic,

IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A COMPARISON OF CLASSICAL MACHINE LEARNING

M. Janardhan, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P
Janardhan12@gmail.com

ABSTRACT: Deep learning and machine learning are increasingly being utilized to evaluate medical pictures and address machine intervention difficulties. While existing deep-learning and machine learning technologies are adaptive, they need medical image analysis-specific capabilities and need substantial research before they can be applied in this sector. Consequently, several research teams have built incompatible infrastructure and spent critical time repeating their work. This article offers several medical pictures for various conditions that may be used to use machine learning and deep learning approaches. Images of the heart, chest, lungs, musculoskeletal system, eye, breast, and skin are used for comparison. Comparisons between deep learning and machine learning for the same illnesses using various images and approaches are primarily studied, and the findings of the research are made available to the public so they can be utilized, improved, and developed upon.

Keywords- Deep learning, machine learning and medical images.

1. INTRODUCTION

Researchers developed automatic analysis techniques as soon as medical images could be processed and submitted. Medical image processing throughout the 1970s and 1990s included successively applying low-level imaging techniques (edge and line detection filters, region expansion) and mathematical modeling (fitting lines, circles, and ellipses) to solve specific issue s. Expert systems that used if-then-else statements were standard in Intelligence at the time. In the late 1990s, medical image classification increasingly embraced supervised techniques, in which a machine-learning model is employed to build a system. Examples include active shape models (for segmentation), atlas techniques (fitted atlases using data for training), extraction and classification, and statistical classifiers (for computer-aided detection and diagnosis). This classification methodology, also known as machine learning, is still widely utilized in many computer-aided diagnostic categorization systems. As a result, we have seen a shift from human-designed to computer-trained systems that use example data to extract feature vectors. The

Estimation of software quality parameters for hybrid agile model

Lalband Neelu, neelugpcet@gmail.com,Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Summary
Software metrics are required to measure quality in terms of software performance and reliability related characteristics like dependencies, coupling and cohesion etc. It provides a way to measure the progress of code during development and having direct relationship with cost and time incurred in the software design and development at their later stages. These major issues must be checked and informed early in the development stage, so that reliability of any software product could be ensured for any large and complex software project. Object oriented software metrics directly focuses on the issues like complexity, reliability and robustness of the software developed using object oriented design methodologies. It reflects the time, cost and effort that would be incurred in development at later stage. While the software in its development stage, it is desirable that the complexity levels at every stage should be minimized to make the end product more reliable and manageable. Object oriented metrics provides all parameters through which one can estimate the complexities and quality related issues of any software at their early stages of development. In this paper, authors have studied three object oriented metrics namely MOOD Metrics, CK Metrics, and QMOOD Metrics and given a case study to show, how these metrics are useful in determining the quality of any software designed by using object oriented paradigm.

Key words:
Software Quality, JAVA RMI, MOOD Metrics, CK Metrics, QMOOD Metrics

1. Introduction

Software Metrics can be defined by measuring property or characteristic or quality of a software objects related to any large and complex software project. In a broader term, it is a degree up to which a system object can hold a particular attribute or characteristics. Object oriented approach is capable of classifying the problem in terms of objects and provide many paybacks like reliability, reusability, decomposition of problem into easily understood object and aiding of future modifications [19].

Object-Oriented Metrics are useless if they are not mapped to software quality parameters. Many number of quality models are proposed to map parameters of the Object Oriented software like Extensibility, Reusability, efforts, manageability and cost [1, 2, 3]. To know more about the internal structure of the product one should know more about the interdependencies of parameters of metrics and Software quality parameters. Figure 1 shows the interdependencies of the metrics parameters and software quality parameters by measuring Object Oriented Metrics [15].

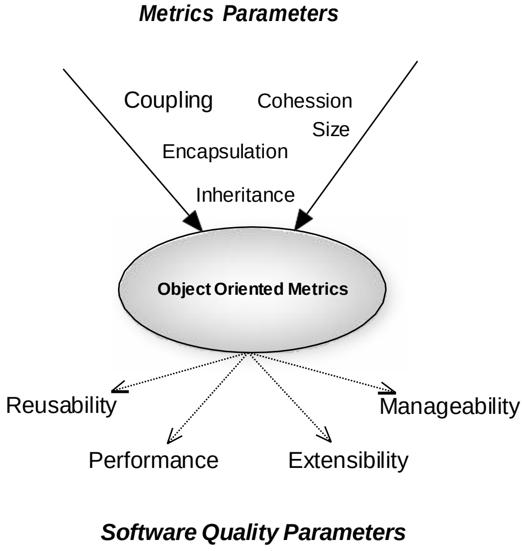


Fig. 1 Relationship between metrics and quality parameters

L.H. Rosenberg proposed various attributes related to object oriented metrics. They have proposed nine metrics for object oriented suite, which are depicted in table I. These metrics include three traditional metrics and six object-oriented metrics [4]. A metric should have a one to one relationship with structures that is being measured or analyzed by that metric.

Metrics proposed by Rosenberg, uses traditional metrics and it is structure based, prescribed for object oriented systems. Here one can see that first three metrics are the examples of traditional metrics and applied onto the

Manuscript received April 5, 2021
Manuscript revised April 20, 2021

ARTIFICIAL INTELLIGENCE IN HEALTHCARE: A REVIEW

T.Aditya Sai Srinivas

adi7g@gmail.com, *Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P*

ABSTRACT:

Artificial intelligence (AI) is the systems or machines that mimic intelligence to perform tasks and can iteratively improve themselves based on the information they collect. AI is being effectively utilized in a multitude of setting such as hospitals, and clinical laboratories as well as in research approaches. The basic or salient feature of AI in the medical field is treatment management as well as its diagnosis. AI systems in health care are succeeding because of the advanced algorithms for learning numerous characteristics from a huge amount of health care data that helps in problem-solving is achieved at a rate and amount futile for humans. The algorithms can be furnished with auto-learning to improve performance and accuracy. AI systems are utilized to facilitate physicians with advanced medical knowledge about journals, clinical papers to brief patient care and medical textbooks. AI can offer fewer diagnostic as well as therapeutic errors. For the learning process, it can make use of medical data, particularly from the patient population. There are different types of AI which can be used in the healthcare field like biomarkers, natural language processing, rule-basedexpert system, and physical robotics. AI is used in treatment design, disease progression, diagnosis aid, and health monitoring.

KEYWORDS: Artificial Intelligence, Healthcare, Robotic Process Automation

Role based access control in cloud computing methods: A case study

K Lakshmi ,lakshmigpcet@gmail.com, Dept. of CSE, G. Pullaiah college of engineering &Technology, Kurnool, A.P

ABSTRACT

This paper deals with various access control mechanisms that are present in cloud computing. Cloud computing is the emerging technology where resources are available pay as you go basis. Cloud storage technology provides the large pool of storage capacity to the cloud users. Providing security to the data stored in cloud is the major concern. So Security can be enhanced by providing access control to the authorized users. Access control gives the authorization to the users which gives the access privileges on data and other resources. Access control can be enabled in most of the computing environment such as Peer to Peer, Grid and Cloud. Cloud storage services are accessed through a cloud storage gateway. We present various types of access control mechanisms that are used in cloud computing environment.

General Terms

Cloud Computing, Access control.

Keywords

Discretionary access control, Mandatory access control, Role Based Access control , Conventional RBAC, dRBAC, Cloud Optimized RBAC.

1. INTRODUCTION

Cloud computing is said to be usage of computing resources such as hardware and software that can be delivered as a service over the internet. There are various number of resources available such as SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service).

End users can access the resources through a web enabled desktop and mobile. Giving access to those resources through the web is major concern and it enhances the security. Access control gives the authorization to the users to access resources that are publicly available to the users. In the earlier there was various access control mechanisms has been introduced for the secure data access. Access control relies on the security of the system and gives the access to the object.

Traditional access control mechanisms are DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control) .The purpose of access control in cloud is to prevent the access on object in cloud by unauthorized users of that particular cloud which will enhance security in the cloud environment. Accesscontrol mechanisms used to mediates the each and every attempt of particular users to the object based on the access privileges given to the system. Traditional access control considers reference monitor that has the authorization database. This database considers the authorization of user [1]. It can be widely used especially in computer science and automation. However the security of information is major concern in cloud. The security of information system directly or indirectly affects the organizations.

Access control is generally said to be policy or procedure that allows, denies or restricts access to a system [2]. It also identifies when the unauthorized users trying to access the system. The mostly used access control methods are identity based access control models [2]. Access control in cloud depends on the cloud storage and its data security and the access option becomes very necessary option in cloud. Access control is very important part in the data center of government and business. It is also important to understand that access control alone not a solution for securing data so the encryption of data also important. There will be a difference between policy decision and mechanism. Access policies are an always high level decision that determines how access are controlled and access decisions are made.

The various types of access control mechanisms are discussed below. In section 2.1 we will discuss Discretionary access control and its performance and in section 2.2 we will discuss Mandatory access control and its performance metrics and in section 2.3 we will discuss about role based access control and dRBAC, coRBAC , ABAC also discussed further.

2. ACCESS CONTROL METHODS

2.1 Discretionary Access Control

This is the traditional access control in which user has the complete control over all the programs. DAC is based on giving access to the user on the basis of user identity and authorization which is defined for open policies.

DAC owns and executes and also it determines permissions to the particular user to the object. DAC policies considers the access of users to the object which is based on the user's identity and authorization that specifies for each user's access method and object that is requested by user. Each individual request to access an object that has been checked. In DAC access method flexibility will be good. In this method most of the authorization is specified explicitly and also authorizations

Data Management in Real time transactions in bank sector

Dr.S. Prem Kumar, Dept. of CSE, prem123@gmail.com, G. Pullaiah college of engineering & Technology, Kurnool, A.P

ABSTRACT

The popularity of the Mobile Database is increasing day by day as people need information even on the move in the fast changing world. This database technology permits employees using mobile devices to connect to their corporate networks, hoard the needed data, work in the disconnected mode and reconnect to the network to synchronize with the corporate database. In this scenario, the data is being moved closer to the applications in order to improve the performance and autonomy. This leads to many interesting problems in mobile database research and Mobile Database has become a fertile land for many researchers. In this paper a survey is presented on data and Transaction management in Mobile Databases from the year 2000 onwards. The survey focuses on the complete study on the various types of Architectures used in Mobile databases and Mobile Transaction Models. It also addresses the data management issues namely Replication and Caching strategies and the transaction management functionalities such as Concurrency Control and Commit protocols, Synchronization, Query Processing, Recovery and Security. It also provides Research Directions in Mobile databases.

KEYWORDS

Architecture, Transaction Models, Concurrency Control, Replication, Synchronization, Caching, Query Processing, Recovery, Security, Issues and Research Directions.

1. INTRODUCTION

The usage of mobile database has increased rapidly because of the continuous growth of the Hardware devices with greater storage capacity and more powered CPU along with the fast development of the Wireless technology. Mobile devices are gradually more used for database driven applications like Sales Order Entry, Product Inventory Tracking and Customer Relationship Management. The way in which mobile applications access the data and manage them is changed completely due to these applications. In these applications data are moved closer to them to improve the efficiency and autonomy instead of storing them in a central database. This new style creates many motivating issues in mobile database research. In this paper we survey the issues related only to the data and transaction management and briefly present the state-of-the-art of data and transaction management in Mobile databases.

DOI: 10.5121/ijdms.2020.4501

IJCERT

International Journal of Computer Engineering in Research Trends

Multidisciplinary, Open Access, Peer-Reviewed and fully refereed

Review Paper Volume-9, Issue-12 E-ISSN: 2349-7084

A Study of Heterogeneity Characteristics over RPC using cloud platforms

Dr. S. Premkumar Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Prem4e@gamil.com

Abstract: Wireless Sensor Networks (WSNs) have the potential to build novel IOT applications to monitor and track the physical activities in the fields of wild life, smart homes, disaster recovery, battle fields, and so on. WSNs are purely application-specific; by behavior, they broadly classify into two categories, namely homogeneous and heterogeneous. All sensor nodes in homogeneous networks are the same type, have the same energy and link capabilities, and so on, whereas in heterogeneous networks, these parameters vary depending on the application. In this paper, we primarily focus on the elimination of overlapping results from existing surveys and propose extensive survey results in terms of the potential performance of various clustering and routing protocols in heterogeneous WSNs. The overall survey was carried out based on the three types of heterogeneity, namely link, energy, and computational and evaluated protocol capability with various network parameters, which are presented in the survey results.

Keywords: WSN's, Heterogeneity, IOT (Internet of Things), Low-energy adaptive clustering hierarchy

1. Introduction

Wireless sensor networks (WSN) are a collection of homogeneous and heterogeneous sensor nodes that are spatially scattered to observe an environmental or physical condition such as sound, pressure, temperature, etc. [1] [2]. These sensors collect information from the environment and forward the data to the nearest nodes, where it finally reaches the base station. Sensor nodes are equipped with a small battery and limited memory and processing capability. For sending and receiving data, sensor nodes consume resources like energy, storage, and computational capacity. Typical wireless sensor network applications are natural calamity relief operations, biodiversity mapping, smart buildings, industrial surveillance, precision horticulture, and health care [3–6]. One of the major research challenges is developing efficient clustering and routing algorithms to maintain large-scale sensor networks. Some of the current research challenges are real-time data scheduling, energy management, protocol programming abstraction, privacy and security, and localization aspects [7]. As per functional and technical metrics, wireless sensor networks are broadly classified into two types, namely homogeneous and heterogeneous, as extensively presented in [8-10].In homogeneity, all sensor nodes have the same type, energy, link capability, and other characteristics, whereas in heterogeneity, these characteristics vary depending on the application. Many researchers in previous decades concentrated on and contributed efficient techniques for homogeneous conditions, which lagged in heterogeneous conditions. Efficient clustering, energy optimization, scalable routing, node deployment strategies, and data fusion and aggregation are the major research goals, and some are still open issues.

The remaining paper is organized as follows: Section 2 represents a literature review; Section 3 presents a proposed model; Section 4 presents a result analysis; and Section 5 presents concussion.

2. Related Work

We investigated the properties of cluster-based routing protocols under heterogeneous conditions in this paper.

https://doi.org/10.22362/ijcert/2022/v9/i12/v9i1204

Review Article

ECG sensors using brainware better protection and security

R.VARAPRASAD, varan@gmail.com **,**Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool,

This paper presents the effectiveness of bioelectrical signals such as the electrocardiogram (ECG) and the electroencephalogram (EEG) for biometric applications. Studies show that the impulses of cardiac rhythm and electrical activity of the brain recorded in ECG and EEG, respectively; have unique features among individuals, therefore they can be suggested to be used as biometrics for identity verification. The favourable characteristics to use the ECG or EEG signals as biometric include universality, measurability, uniqueness and robustness. In addition, they have the inherent feature of vitality that signifies the life signs offering a strong protection against spoof attacks. Unlike conventional biometrics, the ECG or EEG is highly confidential and secure to an individual which is difficult to be forged. We present a review of methods used for the ECG and EEG as biometrics for individual authentication and compare their performance on the datasets and test conditions they have used. We illustrate the challenges involved in using the ECG or EEG as biometric primarily due to the presence of drastic acquisition variations and the lack of standardization of signal features. In order to determine the large-scale performance, individuality of the ECG or EEG is another challenge that remains to be addressed.

1. Introduction

1.1. Bioelectrical Signals. Bioelectrical signals are very low amplitude and low frequency electrical signals that can be measured from biological beings, for example, humans. Bioelectrical signals are generated from the complex self-regulatory system and can be measured through changes in electrical potential across a cell or an organ. The bioelectrical signals of our interest are in particular, the electrocardiogram (ECG) and the electroencephalogram (EEG). An ECG measures the electrical manifestation of the ionic potential of the heart while an EEG measures the electrical activity evoked along the scalp of the brain. The ECG and the EEG are recorded using standard equipments in the noninvasive fashion. The researchers of multiple disciplines have shown their greater interest in analyzing the ECG and the EEG to understand the high level features an individual is producing. However, the interdisciplinary analysis of bioelectrical signals not only helps in assessing the individuals state of health but also it suggests that the bioelectrical signals can be used as the candidate of biometrics for identity verification.

1.2. Characteristics of Bioelectrical Signals as Biometrics. Biometrics aim to facilitate an identity management system for achieving a higher level of accuracy while it uses the anatomical and behavioral characteristics of individuals which are unique and measurable. Anatomical parts of body and signaling methods include face, fingerprint, hands, eyes, ears, veins and voice while behavioural characteristics include handwritten signature, keystroke and gait [1]. The limitations using the conventional biometrics include that they are unique identifiers but they are not confidential and neither secret to an individual. For example, people leave their physical prints of finger on everything they touch, iris patterns can be observed anywhere they look, faces are visible, and voices

Artificial Intelligence with applications in Cyber Security issues

C. Ayesha sheriff
ayeshagp@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract. Without substantial automation, individuals cannot manage the complexity of operations and the scale of information to be utilized to secure cyberspace. Nonetheless, technology and software with traditional fixed implementations are difficult to build (hardwired decision-making logic) in order to successfully safeguard against security threats. This condition can be dealt with using machine simplicity and learning methods in AI. This paper provides a concise overview of AI implementations of various cybersecurity using artificial technologies and evaluates the prospects for expanding the cybersecurity capabilities by enhancing the defence mechanism. We may infer that valuable applications already exist after the review of current artificial intelligence software on cybersecurity. First of all, they are used to protect the periphery and many other cybersecurity areas with neural networks. On the other hand, it was clear that certain cybersecurity problems would only be overcome efficiently if artificial intelligence approaches are deployed. In strategic decision making, for example, comprehensive information is important, and logical decision assistance is one of the still unanswered cybersecurity issues.

Keywords: Artificial Intelligence, Intelligent Agents, Neural networks, Smart Cyber Security methods.

1. Introduction

This is clear that only smart technologies can help defend against sophisticated cyber devices, with the sophistication of malware and cyber-arms increasing exponentially in the past two years. The following case of "On 15 January 2009, Conficker corrupted "Ultramar" the French Navy computer network. The service has then been quarantined, and flights at different airbases have been forced to land because they've not been able to update their flight schedules [1]. The United Kingdom Defence Ministry confirmed contamination of some of its key devices and computers. The virus has dispersed through government offices, Navy Star / N * desk departments and hospitals in the town of Sheffield have confirmed infections to more than 800 machines. In a report on 2 February 2009, over a hundred of their machines were compromised by the Bundeswehr, the Federal Republic of Germany's united armed forces. In January 2010, the Information Network of the Greater Manchester Police triggered a pre-emptive disconnection of the Police Central Database for three days. Staff had to contact certain forces to carry out regular searches on cars and individuals [2]. Cyber incidents are particularly hazardous with Network Centric Warfare (NCW), and cyber defence alterations are urgently needed. The use of artificial intelligence techniques and knowledge-intensive tools would be vital in new offensive methods like dynamic installation of protected perimeters and integral crisis management, fully automated reactions to attacks in networks [3].

ImageNet specifications with deep interactive Neural Networks in advanced issues

P.Siva Kumar.
sivagepcet@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

KEY WORDS: Semantic Segmentation, Deep Neural Networks, Interactive, Aerial Images, Optical imagery, Human-in-the-loop

ABSTRACT:

This paper presents an interactive approach for multi-class segmentation of aerial images. Precisely, it is based on a deep neural network which exploits both RGB images and annotations. Starting from an initial output based on the image only, our network then interactively refines this segmentation map using a concatenation of the image and user annotations. Importantly, user annotations modify the inputs of the network - not its weights - enabling a fast and smooth process. Through experiments on two public aerial datasets, we show that user annotations are extremely rewarding: each click corrects roughly 5000 pixels. We analyze the impact of different aspects of our framework such as the representation of the annotations, the volume of training data or the network architecture.
Code is available at this address[†].

1. INTRODUCTION

Computer vision has seen tremendous progress in the last few years thanks to the emergence of powerful deep learning algorithms. This results in almost mature algorithms which are now used in industry. However, the devil is in the details and it is often not possible to reach the precision expected by industrial end-users. To fully automate computer vision tasks, a human supervision is still often necessary to assert the quality of the results. We focus in this paper on semantic segmentation of aerial images. This task consists in image classification at the pixel level and is useful in remote sensing and Earth observation to monitor man-made architectures or natural phenomena. Using deep learning tools, it has been first addressed with fully convolutional networks in (Long et al., 2015) and is now efficiently tackled with powerful convolutional neural networks (CNNs) such as Deeplabv3+ (Chen et al., 2018). Under appropriate conditions (e.g. when a large enough training dataset is available), one might say that semantic segmentation is nearly achieved. Indeed, these segmentation algorithms lack only a few percents of precision to reach perfect scores on public benchmarks. However, these few percents can visually make a big difference and therefore not be tolerable in practice. Besides, it often gets worse in real-life datasets due to a variety of factors (complex data, lack of well-annotated ground-truth, various usage domains, ...). This paper proposes a fast procedure to iteratively refine the segmentation maps with a human in the loop. It consists in a neural network pre-trained with simulated human annotations and which does not require any retraining during the interactive process.

In order to concretely motivate our approach, let us consider two famous aerial image datasets in remote sensing. On the INRIA Aerial Image Labelling Dataset (Maggiori et al., 2017), a building segmentation dataset, the current best networks reach an Intersection over Union (IoU) around 0.8 and a pixel accuracy around 97% on the test set. On the ISPRS Potsdam multi-class segmentation dataset (Rottensteiner et al., 2012), the state-of-the-art approaches almost reach a pixel accuracy of 92% on the test set. While these performances are incredibly high, there might still remain some misclassified areas unacceptable for an end-user. Besides, these optimal results are obtained using top notch neural networks which have required many specific refinements (Yue et al., 2019). An off-the-shelf neural network still yields good results but, as the baselines show, a drop of performance between 5 and 10% can be expected. Moreover, these performances decrease quickly when the networks are faced to the domain shift issues inherent to machine learning. Therefore, the segmentation masks output by these neural networks have to be manually reviewed to meet the expectations of a potential end-user.

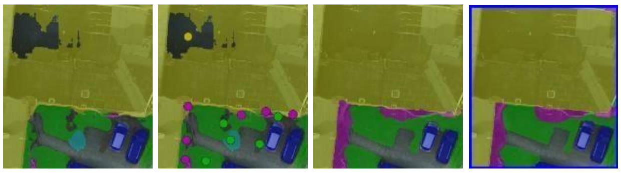


Figure 1. Example of the proposed interactive semantic segmentation approach on the ISPRS Postdam multi-class dataset (Rottensteiner et al., 2012)

Let us also consider a practical application for which current approaches still yield imperfect results. Drones are increasingly used to monitor different environments like crop fields, railroads or quarries. In this context, semantic segmentation can be extremely useful for different tasks such as defects detection, volumes computation or crop monitoring. However, due to the complexity and the high variety of the acquisitions, results are usually not as good as on public datasets while a high precision is necessary for these tasks. Therefore, the operators often have to manually refine the segmentation maps which is a slow process.

To address these issues, we propose to adopt an interactive semantic segmentation approach, as sketched in Figure 1. Indeed, a human in the loop can easily spot the misclassified areas and correct them thanks to a more complex yet intuitive analysis. The difficulty then is to reach optimal classification while keeping the whole process swift and engaging enough.

Our present contribution is as follows.

1. We propose an **interactive segmentation framework for aerial images using deep learning**. Once the classic train-

[*] Corresponding author
[†] https://github.com/delair-ai/DISIR

This contribution has been peer-reviewed. The double-blind peer-review was conducted on the basis of the full paper.
https://doi.org/10.5194/isprs-annals-V-2-2020-877-2020 | © Authors 2020. CC BY 4.0 License.

Playing Go with deep Neural networks in Tree search technologies

R. Varaprasad
Assistant Professor, Dept. of CSE
varaprasadcse@gmail.com

R. Lohitha
Assistant Professor, Dept of CSE
lohithacse@gmail.com

G. Pullaiah College of Engineering and Technology

Abstract

We present the first deep learning model to successfully learn control policies directly from high-dimensional sensory input using reinforcement learning. The model is a convolutional neural network, trained with a variant of Q-learning, whose input is raw pixels and whose output is a value function estimating future rewards. We apply our method to seven Atari 2600 games from the Arcade Learning Environment, with no adjustment of the architecture or learning algorithm. We find that it outperforms all previous approaches on six of the games and surpasses a human expert on three of them.

1 Introduction

Learning to control agents directly from high-dimensional sensory inputs like vision and speech is one of the long-standing challenges of reinforcement learning (RL). Most successful RL applications that operate on these domains have relied on hand-crafted features combined with linear value functions or policy representations. Clearly, the performance of such systems heavily relies on the quality of the feature representation.

Recent advances in deep learning have made it possible to extract high-level features from raw sensory data, leading to breakthroughs in computer vision [11, 22, 16] and speech recognition [6, 7]. These methods utilise a range of neural network architectures, including convolutional networks, multilayer perceptrons, restricted Boltzmann machines and recurrent neural networks, and have exploited both supervised and unsupervised learning. It seems natural to ask whether similar techniques could also be beneficial for RL with sensory data.

However reinforcement learning presents several challenges from a deep learning perspective. Firstly, most successful deep learning applications to date have required large amounts of hand-labelled training data. RL algorithms, on the other hand, must be able to learn from a scalar reward signal that is frequently sparse, noisy and delayed. The delay between actions and resulting rewards, which can be thousands of timesteps long, seems particularly daunting when compared to the direct association between inputs and targets found in supervised learning. Another issue is that most deep learning algorithms assume the data samples to be independent, while in reinforcement learning one typically encounters sequences of highly correlated states. Furthermore, in RL the data distribution changes as the algorithm learns new behaviours, which can be problematic for deep learning methods that assume a fixed underlying distribution.

This paper demonstrates that a convolutional neural network can overcome these challenges to learn successful control policies from raw video data in complex RL environments. The network is trained with a variant of the Q-learning [26] algorithm, with stochastic gradient descent to update the weights. To alleviate the problems of correlated data and non-stationary distributions, we use

Human level control and coordination through deep learning methods

R Vara prasad
Assistant Professor, Dept of CSE
varaprasadcse@gmail.com
G. Pullaiah College of Engineering and Technology.

Shaik Rasiq
Assistant Professor, Dept of CSE
Rasiqcse@gmail.com
G. Pullaiah College of Engineering and Technology.

Abstract

We present the first deep learning model to successfully learn control policies directly from high-dimensional sensory input using reinforcement learning. The model is a convolutional neural network, trained with a variant of Q-learning, whose input is raw pixels and whose output is a value function estimating future rewards. We apply our method to seven Atari 2600 games from the Arcade Learning Environment, with no adjustment of the architecture or learning algorithm. We find that it outperforms all previous approaches on six of the games and surpasses a human expert on three of them.

1 Introduction

Learning to control agents directly from high-dimensional sensory inputs like vision and speech is one of the long-standing challenges of reinforcement learning (RL). Most successful RL applications that operate on these domains have relied on hand-crafted features combined with linear value functions or policy representations. Clearly, the performance of such systems heavily relies on the quality of the feature representation.

Recent advances in deep learning have made it possible to extract high-level features from raw sensory data, leading to breakthroughs in computer vision [11, 22, 16] and speech recognition [6, 7]. These methods utilise a range of neural network architectures, including convolutional networks, multilayer perceptrons, restricted Boltzmann machines and recurrent neural networks, and have exploited both supervised and unsupervised learning. It seems natural to ask whether similar techniques could also be beneficial for RL with sensory data.

However reinforcement learning presents several challenges from a deep learning perspective. Firstly, most successful deep learning applications to date have required large amounts of hand-labelled training data. RL algorithms, on the other hand, must be able to learn from a scalar reward signal that is frequently sparse, noisy and delayed. The delay between actions and resulting rewards, which can be thousands of timesteps long, seems particularly daunting when compared to the direct association between inputs and targets found in supervised learning. Another issue is that most deep learning algorithms assume the data samples to be independent, while in reinforcement learning one typically encounters sequences of highly correlated states. Furthermore, in RL the data distribution changes as the algorithm learns new behaviours, which can be problematic for deep learning methods that assume a fixed underlying distribution.

This paper demonstrates that a convolutional neural network can overcome these challenges to learn successful control policies from raw video data in complex RL environments. The network is trained with a variant of the Q-learning [26] algorithm, with stochastic gradient descent to update the weights. To alleviate the problems of correlated data and non-stationary distributions, we use

The Ethernet Evolution . A local Area Network Data link layer

Dan Dove, Applied Micro

P Rama Rao
Assistant Professor, Dept of CSE
ramaraocse@gmail.com
G. Pullaiah College of Engineering and Technology.

Shaik Anees Fathima
Assistant Professor, Dept of CSE
aneesfathimacse@gmail.com
G. Pullaiah College of Engineering and Technology.

ABSTRACT

Ethernet is constantly evolving, adapting to the needs of the networking world, addressing the requirements of both operators and end users, while making sure that the resulting technology is cost-efficient, reliable, and operates in a plug-and-play manner. The IEEE 802.3 Working Group has been working for the last 30+ years, pushing the boundaries on the speed and capacity of wireline Ethernet links, migrating from shared medium CSMA/CD systems to switched point-to-point Ethernet and then introducing multilane technology and point-to-point emulation over shared media of passive optical networks. In this article, we look at the latest projects adding new features and capabilities to the family of wired Ethernet standards, enabling the exponential growth of the Ethernet ecosystem, driven by technical maturity, cost effectiveness, and broad market support.

INTRODUCTION

The total amount of data created or replicated on the planet in 2010 exceeded 1 zettabyte (1 zettabyte is 10^{21} bytes), or 143 Gbytes for each of the 7 billion people on the planet [1]. This volume of information requires high-speed links between server farms, cloud storage, and end users to make sure that it can be processed in a timely and reliable fashion. The relentless growth of the number of end stations connected to the network, whether permanent or nomadic (computer terminals, mobile devices, automated devices generating machine-to-machine traffic), has led to explosive growth in the volume of information exchanged at all levels of the networking infrastructure. The popularity of Ethernet and its widespread use in access, aggregation, transport, core networks, and data centers, combined with the unprecedented demand for advanced data connectivity services, fuel the development of new Ethernet standards, providing higher-speed links to address the market demand.

Ethernet is also venturing into brand new application areas, and is adding support for synchronization protocols or even potentially becoming a de facto standard for in-vehicle data networks, providing a common transport platform for control and multimedia applications.

This article will examine the evolution of Ethernet standards taking place in the IEEE 802.3 Working Group. There are a number of exciting new projects, pushing the boundaries of Ethernet into new application areas and markets.

EVOLUTION OF ETHERNET STANDARDS

The IEEE Std 802.3 Ethernet standard was first published in 1985, specifying a half-duplex carrier sense multiple access with collision detection (CSMA/CD) medium access control (MAC) protocol operating at 10 Mb/s, and a medium attachment unit (MAU) for operation on a coaxial cable medium, supporting a bus topology between the attached end stations.

Amendments to the IEEE 802.3 standard then added specifications for, among other items, a repeater to extend topologies supported, MAUs for operation over fiber optic cabling, a MAU for operation over twisted pair cabling, 10BASE- T, and layer management. In 1995 amendment IEEE Std 802.3u was published adding operation at 100 Mb/s (fast Ethernet). This included a number of physical layer (PHY) specifications for operation over fiber optic and twisted pair cabling (100BASE-TX).

Amendment IEEE Std 802.3x published in 1997 added full duplex operation to the MAC and a flow control protocol to take advantage of the full duplex capable medium, such as twisted pair and fiber, for which PHYs were already specified in IEEE 802.3, as well as support switching, which was becoming more cost effective due to increased device integration.

In 1998 amendment IEEE Std 802.3z was

0163-6804/13/$25.00 © 2013 IEEE

A review of measurements measurements of internet backbone Traffic bottelenecks

U Supriya
Assistant Professor, Dept of CSE
supriyacse@gmail.com,
G. Pullaiah college of engineering & Technology

S.Nandini
Assistant Professor, Dept of CSE
nandinicse@gmail.com
G. Pullaiah college of engineering & Technology

Abstract – We design and implement Netdiff, a system that enables detailed performance comparisons among ISP networks. It helps customers and applications determine, for instance, which ISP offers the best performance for their specific workload. Netdiff is easy to deploy because it requires only a modest number of nodes and does not require active cooperation from ISPs. Realizing such a system, however, is challenging as we must aggressively reduce probing cost and ensure that the results are robust to measurement noise. We describe the techniques that Netdiff uses to address these challenges.

Netdiff has been measuring eighteen backbone ISPs since February 2007. Its techniques allow it to capture an accurate view of an ISP's performance in terms of latency within fifteen minutes. Using Netdiff, we find that the relative performance of ISPs depends on many factors, including the geographic properties of traffic and the popularity of destinations. Thus, the detailed comparison that Netdiff provides is important for identifying ISPs that perform well for a given workload.

1 Introduction

Knowledge of the performance characteristics of ISP networks is highly valuable. It can enable customers and applications to make informed choices regarding which ISP(s) to use for their traffic. These choices are important because the performance of distributed applications depends heavily on the network paths that are used.

Shedding light on ISP performance can also improve overall network infrastructure. Application performance in the Internet depends collectively on multiple ISPs. Unfortunately, the inability to differentiate individual ISPs' performance creates little incentive for ISPs to resolve problems and promote internal innovation [24]. In response, researchers have proposed radical network architectures based on ISP accountability, overlays or customer-directed routing [2, 5, 6, 24, 32, 41]. However, we believe that simply providing visibility into ISPs' performance creates the right incentives. For instance, no particular ISP is motivated to act if studies report that the average latency in the Internet is 60 ms. If instead, stud-ies report that the average latency for the customers of anISP is twice that for the customers of competitors, marketforces will motivate the ISP to improve its performance.It is thus surprising that the problem of systematically understanding how well various ISPs deliver traffic has received little attention, especially in the research community. To our knowledge, there has been only one commercial effort [20], whose limitations we discuss in the next section. Today, customers of ISP networks are oftenin the dark about which ISPs are better and if the higher price of a particular ISP is justified by better perfor- mance [25, 26, 35, 42]. A common method for customersto obtain this information is by asking each other about their experiences [25, 26, 42]. Similarly, distributed ap- plications are unaware of how the choice of ISP impactsperformance. Even if they use measurements to learn this [3, 14], they cannot predict the performance for ISPsto which they do not directly connect.

Motivated by the observations above, we consider the task of comparing the performance of ISP networks, both in the recent past and over longer time periods. We focus on large ISPs that form the backbone of the Internet. Collectively, these ISPs carry most of the application traffic in the Internet. Their customers include content providers, enterprises, universities, and smaller ISPs.

We first identify the important requirements for a system to compare ISPs. These requirements govern how the measurements should be conducted and analyzed. A key requirement is to quantify performance in a way thatis relevant to customers and applications. This implies, for instance, that we measure the performance of paths that extend to destination networks, rather than stoppingwhere the paths exit the ISP's network. The latter is com-mon in service level agreements (SLAs) of ISPs today, but it is less useful because application performance de- pends on the performance of the entire path. Other re- quirements include enabling a fair comparison among ISPs, by taking into account the inherent differences in their sizes and geographic spreads, as well as helping ISPs improve their networks.

International Journal of Computer Engineering in Research Trends

Multidisciplinary, Open Access, Peer-Reviewed and fully refereed

Review Paper E-ISSN: 2349-7084

Gradient based shematic methods of Learning Apllied to document Recognition

T.N Balakrishna
Assistant Professor, Dept of CSE
balacse@gmail.com
G. Pullaiah college ofengineering & Technology

U.Susmitha
Assistant Professor, Dept of CSE
susmithacse@gmail.com

G. Pullaiah college of engineering & Technology

Abstract: Wireless Sensor Networks (WSNs) have the potential to build novel IOT applications to monitor and track the physical activities in the fields of wild life, smart homes, disaster recovery, battle fields, and so on. WSNs are purely application-specific; by behavior, they broadly classify into two categories, namely homogeneous and heterogeneous. All sensor nodes in homogeneous networks are the same type, have the same energy and link capabilities, and so on, whereas in heterogeneous networks, these parameters vary depending on the application. In this paper, we primarily focus on the elimination of overlapping results from existing surveys and propose extensive survey results in terms of the potential performance of various clustering and routing protocols in heterogeneous WSNs. The overall survey was carried out based on the three types of heterogeneity, namely link, energy, and computational and evaluated protocol capability with various network parameters, which are presented in the survey results.

Keywords: WSN's, Heterogeneity, IOT (Internet of Things), Low-energy adaptive clustering hierarchy

1. Introduction

Wireless sensor networks (WSN) are a collection of homogeneous and heterogeneous sensor nodes that are spatially scattered to observe an environmental or physical condition such as sound, pressure, temperature, etc. [1] [2]. These sensors collect information from the environment and forward the data to the nearest nodes, where it finally reaches the base station. Sensor nodes are equipped with a small battery and limited memory and processing capability. For sending and receiving data, sensor nodes consume resources like energy, storage, and computational capacity. Typical wireless sensor network applications are natural calamity relief operations, biodiversity mapping, smart buildings, industrial surveillance, precision horticulture, and health care [3–6]. One of the major research challenges is developing efficient clustering and routing algorithms to maintain large-scale sensor networks. Some of the current research challenges are real-time data scheduling, energy management, protocol programming abstraction, privacy and security, and localization aspects [7]. As per functional and technical metrics, wireless sensor networks are broadly classified into two types, namely homogeneous and heterogeneous, as extensively presented in [8-10].In homogeneity, all sensor nodes have the same type, energy, link capability, and other characteristics, whereas in heterogeneity, these characteristics vary depending on the application. Many researchers in previous decades concentrated on and contributed efficient techniques for homogeneous conditions, which lagged in heterogeneous conditions. Efficient clustering, energy optimization, scalable routing, node deployment strategies, and data fusion and aggregation are the major research goals, and some are still open issues.

The remaining paper is organized as follows: Section 2 represents a literature review; Section 3 presents a proposed model; Section 4 presents a result analysis; and Section 5 presents concussion.

2. Related Work

We investigated the properties of cluster-based routing protocols under heterogeneous conditions in this paper.

https://doi.org/10.22362/ijcert/2022/v9/i12/v9i1204

A study about machine learning and Artificial Intelligence

G Sreenivasulu
Assistant Professor, Dept of CSE
sreenugpcet@gmail.com,
G. Pullaiah college of engineering & Technology

T.komali
Assistant Professor, Dept of CSE
komscse@gmail.com
G. Pullaiah college of engineering & Technology

ABSTRACT-

It is the science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable. While no consensual definition of Artificial Intelligence (AI) exists, AI is broadly characterized as the study of computations that allow for perception, reason and action. *Today, the amount of data that is generated, by both humans and machines, far outpaces humans' ability to absorb, interpret, and make complex decisions based on that data. Artificial intelligence forms the basis for all computer learning and is the future of all complex decision making.* This paper examines features of artificial Intelligence, introduction, definitions of AI, history, applications, growth and achievements.

KEYWORDS- ***machine learning,deep learning,neural networks,Natural Language Processing and Knowledge Base System***

INTRODUCTION-

Artificial Intelligence (AI) is the branch of computer science which deals with intelligence of machines where an intelligent agent is a system that takes actions which maximize its chances of success. It is the study of ideas which enable computers to do the things that make people seem intelligent. The central principles of AI include such as reasoning, knowledge, planning, learning, communication, perception and the ability to move and manipulate objects. It is the science and engineering of making intelligent machines, especially intelligent computer programs

ARTIFICIAL INTELLIGENCE METHODS:

Machine Learning-

It is one of the applications of AI where machines are not explicitly programmed to perform certain tasks; rather, they learn and improve from experience automatically. Deep Learning is a subset of machine learning based on artificial neural networks for predictive analysis. There are various machine learning algorithms, such as Unsupervised Learning, Supervised Learning, and Reinforcement Learning. In Unsupervised Learning, the algorithm does not use classified information to act on it without any guidance. In Supervised Learning, it deduces a function from the training data, which consists of a set of an input object and the desired output. Reinforcement learning is used by machines to take suitable actions to increase the reward to find the best possibility which should be taken in to account.

Natural Language Processing(NLP)

It is the interactions between computers and human language where the computers are programmed to process natural languages. Machine Learning is a reliable technology for Natural Language Processing to obtain meaning from human languages. In NLP, the audio of a human talk is captured by the machine. Then the audio to text conversation occurs, and then the text is processed where the data is converted into audio. Then the machine uses the audio to respond to humans. Applications of Natural Language Processing can be found in IVR (Interactive Voice Response) applications used in call centres, language translation applications like Google Translate and word processors such as Microsoft Word to check the accuracy of grammar in text. However, the nature of human languages makes the Natural Language Processing difficult because of the rules which are involved in the passing of information using natural language, and they are not easy for the computers to understand. So NLP uses algorithms to recognize and abstract the rules of the natural languages where the unstructured data from the human languages can be converted to a format that is understood by the computer.

Automation & Robotics-

The purpose of Automation is to get the monotonous and repetitive tasks done by machines which also improve productivity and in receiving cost-effective and more efficient results. Many organizations use machine learning, neural networks, and graphs in

The functionalities of complex network topologies inOSI

K. Gayatri
Assistant Professor, Dept of CSE
gayatrigpcet@gmail.com,
G. Pullaiah college of engineering & Technology

T.Lalitha
Assistant Professor, Dept of CSE
lalithacse@gmail.com
G. Pullaiah college of engineering & Technology

ABSTRACT: Topology refers to the process of ordering, arranging, or linking things in a certain way. As a result, network topology refers to the process of organising, arranging, or connecting several devices in a network. The many ways in which devices can be connected to one another are referred to as network topology. These network topologies have been divided into sections depending on how devices are connected and how data flows between them. The topologies of star, ring, hybrid, mesh, tree, and bus are some of the topologies that are utilised in various industries for system layout. The merits and disadvantages of these topologies based on connections and data flow have been explored in this study. This article discusses the importance of network topology. This article discusses the growing demand for these topologies in numerous start-ups and global corporations. It highlights how the future of topologies is bright since every organisation needs to set up a network that must be properly organised, resulting in increased use of network topologies.

KEYWORDS: Cable, Data, Network, System, Topology.

1. INTRODUCTION

Networking topology is the process of arranging several elements (such as links and nodes) of a network. It can be referred as a geometric representation of how several systems can be linked and communicate with each other[1].

1.1 Importance of network topology:

The network layout is critical for a variety of causes. Above all, it is important for any network's operation and performance. Picking the correct topology for operational model of any company can increase performance while also it makes it simpler to discover errors, rectify mistakes, and allocate resource more effectively through the network to make sure best network health[2].

A software-created network topology diagram is widely used to demonstrate and alter the architecture and structure of a network. The most significant reason for these diagrams is that they may give visual representations of both physical and logical layouts, helping managers to comprehend the relationships between devices during troubleshooting[3].

An efficient and correctly managed topology can boost energy and efficiency of data that can assist to minimise operating and maintaining of expenses. The manner a network is structured may make or break functioning of network, connection, and protection from downtime. To guarantee that any network is efficient and healthy, effective network administration and monitoring necessitates a thorough understanding of both the logical and physical topology[4].

1.2 Types of Topologies:

Figure 1 shows several types of network topologies used for arrangement of systems. There are several types of topologies that are used for arranging systems. These are discussed below.

computers

MDPI

Review

A schematic study on the latest trends in deep learning methods

K Sandhya Rani
Assistant Professor, Dept of CSE
sandhyaranicse@gmail.com
G. Pullaiah College of Engineering and Technology.

Shaik Hidayathulla
Assistant Professor, Dept of CSE
hidayathullacse@gmail.com
G. Pullaiah College of Engineering and Technology.

Abstract: In recent years, deep learning (DL) has been the most popular computational approach in the field of machine learning (ML), achieving exceptional results on a variety of complex cognitive tasks, matching or even surpassing human performance. Deep learning technology, which grew out of artificial neural networks (ANN), has become a big deal in computing because it can learn from data. The ability to learn enormous volumes of data is one of the benefits of deep learning. In the past few years, the field of deep learning has grown quickly, and it has been used successfully in a wide range of traditional fields. In numerous disciplines, including cybersecurity, natural language processing, bioinformatics, robotics and control, and medical information processing, deep learning has outperformed well-known machine learning approaches. In order to provide a more ideal starting point from which to create a comprehensive understanding of deep learning, also, this article aims to provide a more detailed overview of the most significant facets of deep learning, including the most current developments in the field. Moreover, this paper discusses the significance of deep learning and the various deep learning techniques and networks. Additionally, it provides an overview of real-world application areas where deep learning techniques can be utilised. We conclude by identifying possible characteristics for future generations of deep learning modelling and providing research suggestions. On the same hand, this article intends to provide a comprehensive overview of deep learning modelling that can serve as a resource for academics and industry people alike. Lastly, we provide additional issues and recommended solutions to assist researchers in comprehending the existing research gaps. Various approaches, deep learning architectures, strategies, and applications are discussed in this work.

Keywords: machine learning (ML); deep learning (DL); recurrent neural network (RNN); convolutional neural networks (CNN) artificial intelligence (AI)

check for updates

Citation: Taye, M.M. Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions. *Computers* **2020**, *12*, 91. https://doi.org/10.3390/computers12050091

Academic Editors: M. Ali Akber Dewan and Aditya Kumar Sahu

Received: 11 February 2020
Revised: 19 April 2020
Accepted: 22 April 2020
Published: 25 April 2020

1. Introduction

Machine learning is used to make computers execute activities that humans can perform more effectively [1]. Using computer algorithms, machine learning enables the machine to access data automatically and with enhanced experience as it learns. It has simplified life and become an indispensable instrument in several industries, such as agriculture [2], banking [3], optimisation [4], robotics [5], structural health monitoring [6], and so on. It may be utilised in cameras for object detection, picture, colour, and pattern recognition, data collection, data sorting, and audio-to-text translation [7].

Deep learning [8] is one of the machine learning methods that dominate in various application areas. Machine learning functions similarly to a newborn infant. There are billions of linked neurons in the brain, which are engaged when a message is sent to the brain. When a baby is shown a vehicle, for instance, a specific set of neurons are active. When the infant is shown another automobile of a different model, the same set of neurons plus some extra neurons may be triggered. Thus, humans are trained and educated during childhood, and during this process, their neurons and the pathways linking them are modified.

Deep Learning : a Probabilistic Perspective

David Donald
Assistant Professor, Dept of CSE
daviddonaldcse@gmail.com
G. Pullaiah College of Engineering and Technology

Pavel Izmailov
Assistant Professor, Dept of CSE
pavelizmailovcse@gmail.com
G. Pullaiah College of Engineering and Technology

Abstract

The key distinguishing property of a Bayesian approach is marginalization, rather than using a single setting of weights. Bayesian marginalization can particularly improve the accuracy and calibration of modern deep neural networks, which are typically underspecified by the data, and can represent many compelling but different solutions. We show that deep ensembles provide an effective mechanism for approximate Bayesian marginalization, and propose a related approach that further improves the predictive distribution by marginalizing within basins of attraction, without significant overhead. We also investigate the prior over functions implied by a vague distribution over neural network weights, explaining the generalization properties of such models from a probabilistic perspective. From this perspective, we explain results that have been presented as mysterious and distinct to neural network generalization, such as the ability to fit images with random labels, and show that these results can be reproduced with Gaussian processes. We also show that Bayesian model averaging alleviates double descent, resulting in monotonic performance improvements with increased flexibility.

1 Introduction

Imagine fitting the airline passenger data in Figure 1. Which model would you choose: (1) $f_1(x) = w_0 + w_1 x$, (2) $f_2(x) = \sum_{j=0}^{3} w_j x^j$, or (3) $f_3(x) = \sum^{10^4} w \; x^j$? Put this way, most audiences overwhelmingly favour choices (1) and (2), for fear of overfitting. But of these options, choice (3) most honestly represents our beliefs. Indeed, it is likely that the ground truth explanation for the data is out of class for any of these choices, but there is some setting of the coefficients $\{w_j\}$ in choice (3) which provides a better description of reality than could be managed by choices (1) and (2), which are special cases of choice (3). Moreover, our beliefs about the generative processes for our observations, which are often very sophisticated, typically ought to be independent of how many data points we observe.

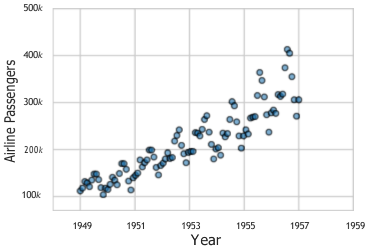


Figure 1: Airline passenger data.

And in modern practice, we are implicitly favouring choice (3): we often use neural networks with millions of parameters to fit datasets with thousands of points. Furthermore, non-parametric methods such as Gaussian processes often involve infinitely many parameters, enabling the flexibility for universal approximation [40], yet in many cases provide very simple predictive distributions. Indeed, parameter counting is a poor proxy for understanding generalization behaviour.

From a probabilistic perspective, we argue that generalization depends largely on *two* properties, the *support* and the *inductive biases* of a model. Consider Figure 2(a), where on the horizontal axis we have a conceptualization of all possible datasets, and on the vertical axis the Bayesian *evidence* for a

34th Conference on Neural Information Processing Systems (NeurIPS 2020), Vancouver, Canada.

Review

A survey on Deep Neural networks on the cognitive approaches

V. Sravani
sravanicse@gmail.com
Dept.of.CSE,G.Pullaiah College Of Engineering & Technology

Abstract: The rapid development of financial technology not only provides a lot of convenience to people's production and life, but also brings a lot of risks to financial security. To prevent financial risks, a better way is to build an accurate warning model before the financial risk occurs, not to find a solution after the outbreak of the risk. In the past decade, deep learning has made amazing achievements in the fields, such as image recognition, natural language processing. Therefore, some researchers try to apply deep learning methods to financial risk prediction and most of the results are satisfactory. The main work of this paper is to review the predecessors' work of deep learning for financial risk prediction according to three prominent characteristics of financial data: heterogeneity, multi-source, and imbalance. We first briefly introduced some classical deep learning models as the model basis of financial risk prediction. Then we analyzed the reasons for these characteristics of financial data. Meanwhile, we studied the differences of commonly used deep learning models according to different data characteristics. Finally, we pointed out some open issues with research significance in this field and suggested the future implementations that might be feasible.

Keywords: risk prediction; deep learning; financial data; risk assessment; bankruptcy prediction; financial distress prediction; financial security

JEL Codes: C45, C5, C1, C38

1. Introduction

The 1997 Asian financial crisis, the dot-com bubble burst of the late 1990s and the financial crisis of 2007–2008 caused serious damage to China's economy, which directly led to the bankruptcy of a large number of companies and the unemployment of a great quantity of workers. Since then, the

EPJ Web of Conferences **248**, 01012 (2021) https://doi.org/10.1051/epjconf/202124801012
MNPS-2020

Gradient-Based Learning subjected to Documentation recognition Techniques

S.Shashikala
Assistant Professor, Dept of CSE
shashikalacse@gmail.com
G. Pullaiah College of Engineering and Technology.

Tanju Shaik
Assistant Professor, Dept of CSE
tanjushaikcse@gmail.com
G. Pullaiah College of Engineering and Technology.

Abstract. The research conducted in this paper is in the field of machine learning. The main object of the research is the learning process of an artificial neural network in order to increase its efficiency. The algorithm based on the analysis of retrospective learning data. The dynamics of changes in the values of the weights of an artificial neural network during training is an important indicator of training efficiency. The algorithm proposed in this work is based on changing the weight gradients values. Changing of the gradients weights makes it possible to understand how actively the network weights change during training. This knowledge helps to diagnose the training process and makes an adjusting the training parameters. The results of the algorithm can be used to train an artificial neural network. The network will help to determine the set of measures (actions) needed to optimize the learning process by the algorithm results.

1. Introduction

Artificial neural networks are the most promising method of machine learning and are widely used for solving various applied problems such as image [1], text [2] and speech [3] recognition, semantic analysis [4], forecasting [5] and others.

One of the long-standing priority problems for the authors is monitoring and forecasting the implementation of priority areas of scientific and technological development in Russia. To solve this problem, experts need to analyze large amounts of information including collections of scientific publications and patent documents.

The use of artificial neural networks allows building in an automated mode semantic models of subject areas based on the extraction of actual objects of scientific research from textual information and the detection of their relationship. However, the result of such an application depends on the quality of training an artificial neural network, which requires consideration of the optimization of the training process to increase its efficiency and, thus, the overall accuracy of the network. That is why the work is largely focused on the learning process. The algorithm proposed in this work makes it possible to expand the information used in the analysis of learning an artificial neural network, which greatly simplifies the introduction of adjustments and increases both learning efficiency and accuracy of the artificial neural.

2. Training an artificial neural network

In the course of training an artificial neural network, it is necessary to change the weights of the network to minimize the error in its operation. Incorrectly chosen parameters of training an artificial neural network can lead to situations in which the global minimum of the error function will not be reached. It will negatively affect the accuracy of the network. The gradient property is usually used for training networks. It allows determining the direction of maximum decrease in the value of the error function. The proposed algorithm is also based on the values of the gradients of the weights of an artificial neural network and allows you to track its change during the training process.

2.1 Artificial neural network learning process

Neural network training is the search for the best set of weights to obtain the minimum network error and, as a consequence, the maximum solution accuracy. During training, it is required to change the weighting coefficients of the network so as to minimize the error of its operation on the sequence of training data.

Idealized training of an artificial neural network boils down to choosing the optimal direction of movement and step at each iteration. After a some number of iterations, the global minimum of the loss function (error) must be reached. The loss function characterizes the loss due to poor decision making on input data. The direction of movement during ideal learning should not change significantly. However, this cannot be guaranteed because of the complex relief of the loss function and the fact that adjustments to the weights during training are often made based on the operation of the network not on the full set of data for training, but only on a part of it (batch). The data batch has own global minimum, which in most cases differs from the global minimum of all training data.

* Corresponding author: starodub_a_v@mail.ru

A Delay-MANET network architecture for challenged network layer

Ameen Yasmeen
Assistant Professor, Dept of CSE
ameenyasmeencse@gmail.com
G. Pullaiah College of Engineering and Technology.

T. Bhuvana
Assistant Professor, Dept of CSE
bhuvanacse@gmail.com
G. Pullaiah College of Engineering and Technology.

Abstract

With the advancement of technology and wireless communications, Mobile Ad-hoc Networks (MANETs) have increasingly been the subject of investigation for researches. Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. "MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an —infrastructure less network" [1]. "A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure" [2]. The purpose of this study is to assess some performance issues and challenges of mobile ad-hoc networks on a given set of metrics and protocols. The output of which is a MANET paradigm as a result of the performance evaluation under given circumstances. A paradigm was developed based on previous studies under similar subject matter.

Keywords: Mobile Ad-hoc Network, metric, protocols, paradigm

Introduction

The advancement of technology along the area of computing, telecommunications and broadcasting through the years have led to the increasingly widespread usage and application of wireless technology. "Mobile ad-hoc networks, also known as short-lived networks, are autonomous systems of mobile nodes forming network in the absence of any centralized support. These are collection of wireless nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure"[3] .

"The set of applications for MANETs is diverse, ranging from largescale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management because of these vulnerabilities, MANET is more prone to malicious attacks" [4].

The purpose of this study was to assess some performance issues and challenges of mobile ad-hoc networks. The output of which is a MANET paradigm as a result of the performance evaluation under given circumstances. A paradigm was developed which will be based on previous studies under similar subject matter.

Related Literature

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links [5].

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid- to late 1990s. Many academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures [6].

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad hoc

Wireless Network Energy saving in the topology control method

Dr. K Sreenivasulu
Assistant Professor, Dept of CSE
sreenivasulucse@gmail.com
G. Pullaiah College of Engineering and Technology.

T. Komali Harshitha
Assistant Professor, Dept of CSE
komaliharshithacse@gmail.com
G. Pullaiah College of Engineering and Technology.

Keywords: Wireless sensor network (WSN), a complex network, small-world networks and scale-free feature

Abstract: The placement of the wireless sensor networks in the wild or the unpopulated area makes it difficult for energy supplement, and vulnerable to damage, so it is of great importance to improve the overall network energy efficiency and prolong the maximum life cycle. In consideration of the energy consumption existed in the wireless sensor networks, a wireless sensor networks model featured by small world effect is put forward in the paper by introducing hyperlink through the addition of super nodes to the wireless sensor networks, based on the characteristics of the complex small-world networks. From the perspective of complex network, the influence of adding super nodes to the sensor networks on the energy efficiency is analyzed. Simulation studies show that the proper addition of super nodes to the wireless sensor networks exerts a clear improvement on network transmission and energy efficiency.

1. Introduction

Wireless sensor is a distributed self-organization networks composed of a large quantity of ubiquitous micro sensor nodes with wireless communication and computing capabilities, which has been widely applied to the fields: disaster rescue, medical rescue, forest fire alarm, volcano detection, environmental monitoring and military.

Small-world phenomenon(small-world effect) is also known as Six Degrees of Separation, which is characterized as small average path length and large clustering coefficient.

Based on the characteristics of complex small-world networks, the paper introduces a super node with higher energy, storage capacity and data processing capacity, which makes up a super link that is a reliable way to communicate with the sink node, and puts forwards a network model based on small world effect in wireless sensor networks. Still, in consideration of the parameters, like: the average path length, the change rate of the average path length and the network energy saving ratio, the paper makes a simulation analysis and test of the appropriate addition of the super nodes to construct the super link that makes the wireless sensor networks have the the following characteristics: the small world effect, the reduced data transmission delay and the improved energy efficiency.

2. Background

Small world phenomenon is often seen in many real networks, such as the Internet, scientist cooperation networks, social relation networks and WWW network, etc., and is also widely used in the field of P2P systems and neural networks[1-2]. Real networks can be divided into two categories. One is the relation network, in which the distance between the nodes is not dependent on the network topology and node location, but on the calculation of hop count. The other one is the spatial network, in which the connection between the nodes is closely related to the distance between the nodes. The usual study on complex networks belongs to the study of relation schema in which relation networks are taken from the social relations or the technical networks, while wireless networks and wireless sensor networks, due to the limitation of its transmission radius, is the spatial network, which belongs to the study of space map. The topological structure of spatial network is closely related to the connectivity and transmission radius. Recent studies have indicated that "small

A Study on ImageNet Classification with deep CNN

R. Varaprasad
Assistant Professor, Dept of CSE
varaprasadcse@gmail.com
G. Pullaiah College of Engineering and Technology.

Shaik Faizullah
Assistant Professor, Dept of CSE
faizullahcse@gmail.com
G. Pullaiah College of Engineering and Technology.

Abstract

We trained a large, deep convolutional neural network to classify the 1.2 million high-resolution images in the ImageNet LSVRC-2010 contest into the 1000 different classes. On the test data, we achieved top-1 and top-5 error rates of 37.5% and 17.0% which is considerably better than the previous state-of-the-art. The neural network, which has 60 million parameters and 650,000 neurons, consists of five convolutional layers, some of which are followed by max-pooling layers, and three fully-connected layers with a final 1000-way softmax. To make training faster, we used non-saturating neurons and a very efficient GPU implementation of the convolution operation. To reduce overfitting in the fully-connected layers we employed a recently-developed regularization method called "dropout" that proved to be very effective. We also entered a variant of this model in the ILSVRC-2012 competition and achieved a winning top-5 test error rate of 15.3%, compared to 26.2% achieved by the second-best entry.

1 Introduction

Current approaches to object recognition make essential use of machine learning methods. To improve their performance, we can collect larger datasets, learn more powerful models, and use better techniques for preventing overfitting. Until recently, datasets of labeled images were relatively small — on the order of tens of thousands of images (e.g., NORB [16], Caltech-101/256 [8, 9], and CIFAR-10/100 [12]). Simple recognition tasks can be solved quite well with datasets of this size, especially if they are augmented with label-preserving transformations. For example, the current-best error rate on the MNIST digit-recognition task (<0.3%) approaches human performance [4]. But objects in realistic settings exhibit considerable variability, so to learn to recognize them it is necessary to use much larger training sets. And indeed, the shortcomings of small image datasets have been widely recognized (e.g., Pinto et al. [21]), but it has only recently become possible to collect labeled datasets with millions of images. The new larger datasets include LabelMe [23], which consists of hundreds of thousands of fully-segmented images, and ImageNet [6], which consists of over 15 million labeled high-resolution images in over 22,000 categories.

To learn about thousands of objects from millions of images, we need a model with a large learning capacity. However, the immense complexity of the object recognition task means that this problem cannot be specified even by a dataset as large as ImageNet, so our model should also have lots of prior knowledge to compensate for all the data we don't have. Convolutional neural networks (CNNs) constitute one such class of models [16, 11, 13, 18, 15, 22, 26]. Their capacity can be controlled by varying their depth and breadth, and they also make strong and mostly correct assumptions about the nature of images (namely, stationarity of statistics and locality of pixel dependencies). Thus, compared to standard feedforward neural networks with similarly-sized layers, CNNs have much fewer connections and parameters and so they are easier to train, while their theoretically-best performance is likely to be only slightly worse.

Review on mobile edge networks in computing environments

Dr. Seshadri Ramana
Assistant Professor, Dept of CSE
seshadriramanacse@gmail.com
G. Pullaiah College of Engineering and Technology.

S. Madiha
Assistant Professor, Dept of CSE
madihacse@gmail.com
G. Pullaiah College of Engineering and Technology.

Abstract—As the explosive growth of smart devices and the advent of many new applications, traffic volume has been growing exponentially. The traditional centralized network architecture cannot accommodate such user demands due to heavy burden on the backhaul links and long latency. Therefore, new architectures which bring network functions and contents to the network edge are proposed, i.e., mobile edge computing and caching. Mobile edge networks provide cloud computing and caching capabilities at the edge of cellular networks. In this survey, we make an exhaustive review on the state-of-the-art research efforts on mobile edge networks. We first give an overview of mobile edge networks including definition, architecture and advantages. Next, a comprehensive survey of issues on computing, caching and communication techniques at the network edge is presented respectively. The applications and use cases of mobile edge networks are discussed. Subsequently, the key enablers of mobile edge networks such as cloud technology, SDN/NFV and smart devices are discussed. Finally, open research challenges and future directions are presented as well.

Index Terms—Mobile edge computing, mobile edge caching, D2D, SDN, NFV, content delivery, computational offloading.

I. INTRODUCTION

DURING the past several decades, mobile cellular networks have been evolving steadily and significantly from the 1st generation (1G) voice only systems to current 4th generation (4G) all-IP based LTE-Advanced networks. The system capacity and average data rate have improved greatly with the technology advancements in physical layer such as WCDMA, OFDMA, MIMO, CoMP and in network layer such as heterogeneous network (HetNet) and cloud radio access network (C-RAN). According to a recent report from Cisco [1], the mobile data traffic has grown 4000-fold during the past 10 years and will continue grow at a rate of 53 percent annually from 2015 to 2020. In particular, mobile video traffic accounts for more than half of total mobile data traffic and this percentage keeps increasing. Besides, mobile devices are getting smarter in their computing capabilities, and new machine type devices appear such as wearable devices and sensors in addition to human type devices. This leads to massive M2M connections in next generation mobile networks.

Machine type communications (MTC) bring a wide range of new applications and services in wireless networks. The authors in [2] presented the current status and challenges of MTC for cellular systems. The most important challenges include massive number of MTC devices, small data bursts, low-latency, and low power consumption. Various solutions have been proposed to accommodate these challenges [3], [4]. Since the processing capabilities of MTC devices are constrained, one promising solution is to offload their tasks to places that have powerful processing capabilities. The ubiquitous connectivity of MTC leads to the strong heterogeneous networking paradigm. Research efforts have been made to accommodate such MTC applications from 4G to the emerging 5G systems [5].

The preliminary mobile computing scheme adopted a 2-level hierarchy which originally called "servers" and "clients" [6]. Later on, The terminology "cloud" was used to represent a collection of servers with computational and information resources, which leads to the research on mobile cloud computing (MCC). Mobile cloud computing considers various mobile-related factors compared to the traditional computation offloading techniques, such as device energy, bandwidth utilization cost, network connectivity, mobility, context awareness and location awareness [7], [8]. Various survey articles have been published focusing on different aspects of MCC. In [9] and [10], the authors presented generic issues on mobile cloud computing including architecture, technical challenges and applications. In [11], existing works on mobile cloud platforms and access schemes were discussed. The authors compared two mobile cloud platforms, the Hyrax platform [12] and virtual machine (VM) based cloudlets [13], and then reviewed intelligent access schemes utilizing the user’s location and context [14]. The authors in [7] elaborated the entities affecting computation offloading decision and presented detailed application models classification and the latest mobile cloud application models. The authors in [15] presented a detailed taxonomy of mobile cloud computing based on the key issues and the approaches to tackle them, such as operational issues, end user issues, service level issues, security, context-awareness and data management. User authentication is significant in securing cloud-based computing and communications. In [16], the authors surveyed the state-of-the-art authentication mechanism in MCC and compare it with that in cloud computing. The merits of MCC can be summarized as follows. Firstly, it can provide sufficient resources for mobile devices and has great flexibility. Secondly, the cost of MCC can be reduced due to centralized management of resources. Finally, since all

S. Wang, X. Zhang, L. Wang, J. Yang and W. Wang are with the School of Information and Communications Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China (e-mail: wangsh@bupt.edu.cn; zhangx@ieee.org; wanglin121@gmail.com; yangjuwo@163.com; wbwang@bupt.edu.cn).

Y. Zhang is with University of Oslo, Norway (e-mail: yanzhang@ieee.org).

This work is supported by the National Science Foundation of China (NSFC) under grant 61372114, 61571054 and 61631005, by the New Star in Science and Technology of Beijing Municipal Science & Technology Commission (Beijing Nova Program: Z151100000315077).

SciEn
Journal of Engineering Advancements Vol. 01(04) , pp 170-182 https://doi.org/10.38032/jea.2020.04.008

A Strategy for evaluating security issues in network protocols

M. Srilakshmi
Assistant Professor, Dept of CSE
srilakshmicse@gmail.com
G. Pullaiah College of Engineering and Technology.

P. Vyshnavi
Assistant Professor, Dept of CSE
vyshnavicse@gmail.com
G. Pullaiah College of Engineering and Technology.

ABSTRACT

Internet of things (IoT) is the epitome of sustainable development. It has facilitated the development of smart systems, industrialization, and the state-of-the-art quality of life. IoT architecture is one of the essential baselines of understanding the widespread adoption. Security issues are very crucial for any technical infrastructure. Since IoT comprises heterogeneous devices, its security issues are diverse too. Various security attacks can be responsible for compromising confidentiality, integrity, and availability. In this paper, at first, the IoT architecture is described briefly. After that, the components of IoT are explained with perspective to various IoT based applications and services. Finally, various security issues, including recommended solutions, are elaborately described and the potential research challenges and future research directions.

Keywords: IoT, Security, Privacy, Attacks, Vulnerability, Threats, Challenges.

1. Introduction

The Internet of Things (IoT) has gained popularity in recent times. It is an interconnected network of devices like sensors, actuators, electronics, and software. A network or correlation among those gadgets helps to collect and share data between them. Each and everything can be defined uniquely utilizing an embedded computing device but can communicate within the current Internet infrastructure. IoT makes it possible to monitor and sense using the network infrastructure [1] to create opportunities for more effective physical incorporation into computer-driven networks. Besides, to minimize human interference, increase performance, precision, and economic benefit [2],[3] the IoT devices play a vital role. Internet of Things facilitates smart human living, sustainability, and a greener lifestyle. Moreover, IoT devices used in the industrial environment increase efficient product management through proper monitoring and risk management [4],[5].

IoT comprises sensors and actuators. It is an example of a broader class of cyber-physical networks involving intelligent grids, smart buildings, VPP (Virtual Power Plants), smart transport, and smart cities. It has a significant impact on the medical sector also. Among the applications, a wide range of equipment such as cardiovascular implants, biochip transponders for farm animals, cameras for broadcasting wild animal live feed in coastal waters, vehicles with embedded captors, environmental DNA analysis, food, surveillance for pathogens [6], or on-site operations supports firefighters in search and rescue operations [7]. IoT has spread its domain in every sector of socio-economic sectors. Legal scholars propose "thing" as a combination of hardware, software, information.

Similar to every other technology IoT has several issues regarding security and privacy. Since the IoT network is a combination of devices, communication technologies, and various protocols, security issues regarding availability, data integrity, data confidentiality, and authentication exist [8]. These issues hamper operational inefficiency, robustness, and throughput. For a sustainable and robust IoT network, security and privacy issues need to be adequately addressed. The reasons mentioned above can be a very impactful motivation for a comprehensive study regarding leveraging various issues.

Being IoT an impactful technology of recent times, it needs to be studied vigorously. Several pieces of research are going on for improving IoT and removing the security threats. Moreover, IoT has a tremendous impact on the industry and recent smart city improvement. Considering all the factors, it is indispensable to study IoT and perform critical research analysis, including contemporary literature. The analysis can be used to outline a sophisticated piece of literature that can help those trying to initialize their career in IoT and existing researchers looking for research gaps and current research challenges.

The rest of the paper is organized as follows-

Section 2 comprises an architectural analysis of IoT that includes various IoT layers. Section 3 consists of various IoT components that make the IoT system. An extensive analysis of security and privacy issues, including their state of the art recommended solution, is outlined in Section 4 and 5. In addition to the recommended solutions, Section 5 also comprises a recent literature analysis about IoT privacy and security issues. Section 6 outlines the future research directions that can be helpful for researchers and scientists. Finally, the paper concludes with a conclusion in Section 7.

2. IoT Architectures

Software integrated hardware devices process raw data and turn it into a usable format. Furthermore, the data is transmitted, stored, recovered, and analyzed with advanced IoT-integrated computer devices. Only a dependable IoT architecture layer can ensure a steady, durable, and swift connection between information and communication technology. Researchers have proposed several different architectures for the IoT environment. However, the three-layer structure is the most popular type among researchers and publications [9].

2.1 The Three-Layer Architecture

One of the primary and significant IoT architectures is the three-layer architecture. It is one of the most functional,

To achieve the science of security and privacy in machine learning

M. Janardhan
Assistant Professor, Dept of CSE
G.pullaiah college of engineering and technolog

B.Jagadeeshwara reddy
Assistant Professor, Dept of CSE
G.pullaiah college of engineering and technology

ABSTRACT

This chapter revises the most important aspects in how computing infrastructures should be configured and intelligently managed to fulfill the most notably security aspects required by Big Data applications. One of them is privacy. It is a pertinent aspect to be addressed because users share more and more personal data and content through their devices and computers to social networks and public clouds. So, a secure framework to social networks is a very hot topic research. This last topic is addressed in one of the two sections of the current chapter with case studies. In addition, the traditional mechanisms to support security such as firewalls and demilitarized zones are not suitable to be applied in computing systems to support Big Data. SDN is an emergent management solution that could become a convenient mechanism to implement security in Big Data systems, as we show through a second case study at the end of the chapter. This also discusses current relevant work and identifies open issues.

Keywords: Big Data, Security, Privacy, Data Ownership, Cloud, Social Applications, Intrusion Detection, Intrusion Prevention.

INTRODUCTION

The Big Data is an emerging area applied to manage datasets whose size is beyond the ability of commonly used software tools to capture, manage, and timely analyze that amount of data. The quantity of data to be analyzed is expected to double every two years (IDC, 2012). All these data are very often unstructured and from various sources such as social media, sensors, scientific applications, surveillance, video and image archives, Internet search indexing, medical records, business transactions and system logs. Big data is gaining more and more attention since the number of devices connected to the so-called “Internet of Things” (IoT) is still increasing to unforeseen levels, producing large amounts of data which needs to be transformed into valuable information. Additionally, it is very popular to buy on-demand additional computing power and storage from public cloud providers to perform intensive data-parallel processing. In this way, security and privacy issues can be potentially boosted by the volume, variety, and wide area deployment of the system infrastructure to support Big Data applications.

As Big Data expands with the help of public clouds, traditional security solutions tailored to private computing infrastructures, confined to a well-defined security perimeter, such as firewalls and demilitarized zones (DMZs) are no more effective. Using Big Data, security functions are required to work over the heterogeneous composition of diverse hardware, operating systems, and network domains. In this puzzle-type computing environment, the abstraction capability of Software-Defined Networking (SDN) seems a very important characteristic that can enable the efficient deployment of Big Data secure services on-top of the heterogeneous infrastructure. SDN introduces abstraction because it separates the control (higher) plane from the underlying system infrastructure being supervised and controlled. Separating a network's control logic from the underlying physical routers and switches that forward traffic allows system administrators to write high-level control programs that specify the behavior of an entire network, in contrast to conventional networks, whereby administrators (if allowed to do it by the device manufacturers) must codify functionality in terms of low-level device configuration. Using SDN, the

A review of Data leakage Detection and prevention solutions

Lalband Neelu neelu45@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract – Data security is the major concern of every application in the distributed environment. The sensitive data protection from being leaked to the others is the ultimate aim of all organization. Many security procedures are followed to maintain the data confidentiality, which preserves the data according to the security policies and rules. However, due to the distributed nature, the confidential and sensitive data protection lack pro-activeness and has many complications. These results in serious consequences and the data can be leaked in various leaking channels. So the analysis and mitigation of these drawbacks using effective mechanism is important. This paper carried out a comprehensive survey on different data leakage detection and prevention techniques and suggests future direction to overcome the weakness of the current data leakage detection and prevention schemes.

Index Terms – Data Leakage Detection, Data Leakage Prevention, Sensitive data management, Information security.

1. INTRODUCTION

In the recent network Data Leakage is an important concern for the business organizations. Prevention of sensitive data from unauthorized entities and monitoring the data flow to avoid more security risks are the main goals of the security domain. Unauthorized disclosure may have serious consequences for an organization in both long term and short term. To prevent from the unwanted access and transaction from happening, an organized effort is needed to control the information flow inside and outside the organization. Data leakage detection and prevention process are the important research issue, which is not always possible because several reasons. Recent news and reports indicates 50 % of data's are leaked in the business sector either partially or fully [1]. This is very difficult to identify the exact details of leaked data and the leaker. However, the data leakage has many channels to leak. So monitoring every channel is an impossible task, and thus creates many serious issues. There is numerous detection and prevention schemes like Intrusion Detection System (IDS), firewall, and virtual private networks are the common security systems used to detect or prevent some unwanted access. These schemes can perform well if the rules are properly defined. However, the rules can be violated from different accessible channels like email, instant messaging, and via other social media attachments. To overcome this problem, Data Leakage Detection(DLD) systems and Data Leakage Prevention(DLP) systems are deployed. There are less adequate researches introduced to thwart the DLP issue, so there is a need and challenge to design and develop a new DLP mechanism with detection ability. Motivated by the DLP field of study, a survey on the Data Leakage Detection and Prevention approaches are presented in this paper. The paper provides the basic process of DLD and DLP along with the recent techniques under the data leakage process. The paper finally contributes the problem and challenges of the recent techniques with future work.

This paper is prepared as follows. Section 2 discusses the DLD and DLP standard. Section 3 describes the challenges facing DLDs and DLPs. Section 4 categorizes the current DLP methods and discusses the advantages and disadvantages of each method. Section 5 concludes the survey paper.

2. DATA LEAKAGE DETECTION AND PREVENTION STANDARDS

Numerous studies conducted to define the area of data leakage detection and prevention in the literature. But the definition of the data leak or information leak prevention is the process of content monitoring and protecting them from the misuse [2]. Although researches on data leakage prevention are rising, there is little research on the detection of data leakage from the perspective of user behavior [3]. Authors in [4] reviewed the DLP approaches and its problems with the appropriate definition. The DLD and DLP process contains three phases such as the data collection phase, analysis phase and the remedial action phase shown in Fig 1.0. The data collection is beginning with the user internet or intranet logs and the database sources. The collected data's are imported in the DLD and DLP analysis phase, which performs rule matching, policy verification, content and context verification processes. The context verification extracts the sender, source id, timings of the data access, format and size from the header information

The protection of information in computer system progressive approaches

T. Adithya sai sreenivas ,

sreenu727@gmail.com, Dept. of CSE,

G. Pullaiah college of engineering & Technology, Kurnool,A.P

Abstract

After thirty years of work on computer security, why are almost all the systems in service today extremely vulnerable to attack? The main reason is that security is expensive to set up and a nuisance to run, so people judge from experience how little of it they can get away with. Since there's been little damage, people decide that they don't need much security. In addition, setting it up is so complicated that it's hardly ever done right. While we await a catastrophe, simpler setup is the most important step toward better security.

In a distributed system with no central management like the Internet, security requires a clear story about who is trusted for each step in establishing it, and why. The basic tool for telling this story is the "speaks for" relation between principals that describes how authority is delegated, that is, who trusts whom. The idea is simple, and it explains what's going on in any system I know. The many different ways of encoding this relation often make it hard to see the underlying order.

1 Introduction

People have been working on computer system security for at least 30 years. During this time there have been many intellectual successes. Notable among them are the subject/object access matrix model [12], access control lists [19], multilevel security using information flow [6, 14] and the star-property [3], public key cryptography [16], and cryptographic protocols [1]. In spite of these successes, it seems fair to say that in an absolute sense, the security of the hundreds of millions of deployed computer systems is terrible: a determined and competent attacker could destroy most of the information on almost any of these systems, or steal it from any system that is connected to a network. Even worse, the attacker could do this to millions of systems at once.

The Internet has made computer security much more difficult than it used to be. In the good old days, a computer system had a few dozen users at most, all members of the same organization. It ran programs written in-house or by a few vendors. Information was moved from one computer to another by carrying tapes or disks.

Today half a billion people all over the world are on the Internet, including you. This poses a large new set of prob- lems.

- *Attack from anywhere*: Any one on the Internet can take a poke at your system.
- *Sharing with anyone*: On the other hand, you may want to communicate or share information with any other Internet user.
- *Automated infection*: Your system, if compromised, can spread the harm to many others in a few seconds.
- *Hostile code*: Code from many different sources runs on your system, usually without your knowledge if it comes from a Web page. The code might be hostile, but you can't just isolate it, because you want it to work for you.
- *Hostile physical environment*: A mobile device like a laptop may be lost or stolen and subject to physical attack.
- *Hostile hosts*: If you own information (music or movies, for example), it gets downloaded to your customers' systems, which may try to steal it.

All these problems cause two kinds of bad results. One is vandalism, motivated by personal entertainment or status-seeking: people write worms and viruses that infect many machines, either by exploiting buffer overrun bugs that allow arbitrary code to run, or by tricking users into running hostile code from e-mail attachments or web pages. These can disrupt servers that businesses depend on, or if they infect many end-user machines they can generate enough network traffic to overload either individual web servers or large parts of the Internet itself. The other bad result is that it's much easier to mount an attack on a specific target (usually an organization), either to steal information or to corrupt data.

On the other hand, the actual harm done by these attacks is limited, though growing. Once or twice a year an email virus such as "I love you" infects a million or two machines, and newspapers print extravagant estimates of the damage it does. Unfortunately, there is no accurate data about the cost of failures in computer security: most of them are never made public for fear of embarrassment, but when a public incident does occur, the security experts and vendors of antivirus software

blampson@microsoft.com, research.microsoft.com/Lampson

A Survey of Intrusion Detection systems in wireless sensor networks and MANETS

K. LAKSHMI, Assistant professor M.Janardhan

lakshmigpcet@gmail.com,Dept.ofCSE, janardhancse@gmail.com,Dept.of cse

G. Pullaiah college of engineering & Technology, Kurnool, A.P

***Abstract* - Intrusion detection in the computer networks has been a major research area from the past few years. Many new techniques have been evolved and compared with the existing approaches. The basis of comparison of such computer vulnerabilities have been the accuracy of detection and the and the failure rate. In the present paper several machine learning and other suitable approaches proposed to solve the problem of intrusion have been reviewed and conclusion on the basis of the performance parameters is drawn. In future the approach must be modified and results must be compared with the existing approaches.**

***Keyword* - Intrusion Detection System, Security**

INTRODUCTION

Networking is the practice of linking multiple computing devices together in order to share resources. These resources can be printers, CDs, files, or even electronic communications such as e-mails and instant messages. These networks can be created using several different methods, such as cables, telephone lines, satellites, radio waves, and infrared beams. Both traditional and modern forms of computer networking aim to provide users with the ability to share data amongst multiple gadgets, whether they be in the same building or across the globe. Traditional computer networking relied on Ethernet and fiber optic cables to connect various devices on a network. More modern technology has emerged that allows for wireless connections between electronics. These technologies include Wi-Fi and Bluetooth compatible devices.

Without the ability to network, businesses, government agencies, and schools would be unable to operate as efficiently as they do today. The ability for an office or school to connect dozens of computers to a single printer is a seemingly simple, yet extremely useful capability. Perhaps even more valuable is the ability to access the same data files from various computers throughout a building. This is incredibly useful for companies that may have files that require access by multiple employees daily. By utilizing networking, those same files could be made available to several employees on separate computers simultaneously, improving efficiency.

As the internet evolves and computer networks become bigger and bigger, network security has become one of the most important factors for companies to consider. Big enterprises like Microsoft are designing and building software products that need to be protected against foreign attacks. Anything from software, music and movies to books, games, etc. are stolen and copied because security is breached by malicious individuals. Today, most malicious users do not possess a high level of programming skills and instead make use of tools available on the Internet. There are several stages that an attacker has to pass through to successfully carry out an attack.

Network security refers to any activities designed to protect your network. Specifically, these activities protect the usability, reliability, integrity, and safety of your network and data. Effective network security targets a variety of threats and stops them from entering or spreading on your network. Network security is accomplished through hardware and software. The software must be constantly updated and managed to protect you from emerging threats. A network security system usually consists of many components. Ideally, all components work together, which minimizes maintenance and improves security.

IDS are one of many complementary layers of IT security technology. Several security layers exist because no one layer can provide all the security measures itself. IDS do several things that basic firewalls, for instance, cannot do: Identify anomalous packet content or patterns of traffic that are different from normal for any particular company’s network. Identify patterns, called signatures, of malicious content within packets coming into or leaving a company’s network.

The business benefit IDS provides is reducing the chance of missing security threats which could compromise confidentiality, integrity, privacy, or availability of mission critical assets and processes. An important consideration in lifecycle cost is managing and tuning out false positives generated by IDS. These activities are onerous and in my experience most network managers would rather outsource these tasks to experts. The next issue becomes selection of the appropriate IDS technology, which basically come in two flavours: network intrusion detection (NIDS or IDS) and host intrusion detection (HIDS). Network IDS sits on the network telecommunications media such as an Ethernet network or a wireless network, and passively monitors the contents of packets of information flowing in all directions. Host IDS is an entirely different ballgame. It has agents which reside on servers. It monitors several types of changes over time on servers which may indicate security problems.

Internet is a global public network. With the growth of the internet and its potential, there has been subsequent change in the business model of the organizations across the world. More and more people are getting connected to the internet every day to take advantage of the new business model popularly known as e-business. Internetwork connectivity has therefore become very critical aspect of today’s e-business. While an organization makes its information system available to harmless internet users, at the same time the information is available to the malicious users as well. Malicious users or hackers can get access to an

Reprinted with corrections from *The Bell System Technical Journal,*

A Mathematical Theory of Communication in health care diagnosis

Dr. S. Prem Kumar ,

premkumar@gmail.com,

Dept. of CSE, G. Pullaiah college of

engineering & Technology, Kurnool, A.P

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design. If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

I. It is practically more useful. Parameters of engineering importance such as time, bandwidth, number of relays, etc., tend to vary linearly with the logarithm of the number of possibilities. For example, adding one relay to a group doubles the number of possible states of the relays. It adds 1 to the base 2 logarithm of this number. Doubling the time roughly squares the number of possible messages, or doubles the logarithm, etc.

II. It is nearer to our intuitive feeling as to the proper measure. This is closely related to (1) since we intuitively measures entities by linear comparison with common standards. One feels, for example, that two punched cards should have twice the capacity of one for information storage, and two identical channels twice the capacity of one for transmitting information.

III. It is mathematically more suitable. Many of the limiting operations are simple in terms of the logarithm but would require clumsy restatement in terms of the number of possibilities.

The choice of a logarithmic base corresponds to the choice of a unit for measuring information. If the base 2 is used the resulting units may be called binary digits, or more briefly *bits,* a word suggested by J. W. Tukey. A device with two stable positions, such as a relay or a flip-flop circuit, can store one bit of information. N such devices can store N bits, since the total number of possible states is 2^N and $\log_2 2^N = N$. If the base 10 is used the units may be called decimal digits. Since

$$\begin{aligned}\log_2 M &= \log_{10} M = \log_{10} 2\\ &= 3:32 \log_{10} M;\end{aligned}$$

National Defence College E-Journal
E-ISSN: 2709-9016
https://ndcjournal.ndc.gov.bd/ndcj

Robotics and Autonomous systems in military application environment

Dr.S. Prem kumar

premgpcet@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract: To face the challenges of military defense, modernizing army and their tactical tools is a continuous process. In near future various kinds of missions will be executed by military robots to achieve 100% impact and 0% life risks. Defense robot engineers and companies are interested to automate various strategies for higher efficiency and greater impact as the demand of land defense robots is growing steadily. In this study, land-robots used in military defense system are focused and various types of land-robots are presented focusing on the technical specifications, control strategies, battle engagement, and purpose of use. Recent integration of land-robot technologies in the world military forces, its necessities, and contributions of various international defense companies to the world economy are also presented in this study indicating supremacy in the military automation and economic stability. Limitations and challenges of recent development, robot ethics, and moral impacts are also discussed here with some vital points related to robot security and some suggestions to overcome recent challenges for the future development.

Keywords: *Land-robots; Military robots; Defense robots; Military defense engineering; Ground robots; UGV*

INTRODUCTION

To strengthen military defense system, significant development and increment of intelligent autonomous strategic capacity is necessary. Research on defense technology improvements is the priority in most of the first world countries to modernize the military defense. The characteristics of future warfare can be analyzed based on conflicts in various domains, such as: maritime, land, air, cyber,

A survey of socially interactive robots in farming.

R. Varaprasad, varan7772@gmail.com
Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract

Agriculture is both the site of development of important new technologies and a key area of application of technologies developed elsewhere. It is little wonder, then, that many thinkersbelieve that progress in the science and engineering of robotics may soon change the face offarming. This paper surveys the prospects for agricultural robotics, discusses its likely impacts, and examines the ethical and policy questions it may raise. Along with the environmental and economic impacts of robots, political, social, cultural, and security implications of the introduction of robots that have received little attention in the larger literature on agricultural robotics are considered. Key policy choices necessary to meet the ethical challenges likely to arise as agricultural robots start to become used more widely, andto maximise the social, environmental, and economic benefits of robots in agriculture, are highlighted.

Keywords: Agricultural robotics; precision farming; ethics; automation/autonomy;sustainability

Introduction:

In recent years, advancements in robotics and artificial intelligence have revolutionized various industries, and agriculture is no exception. With the global population steadily increasing and the demand for food surging, there's a growing need for innovative solutions to enhance agricultural productivity while addressing challenges such as labor shortages, efficiency, and sustainability. In this context, socially interactive robots (SIRs) have emerged as a promising technology with the potential to transform traditional farming practices.

Socially interactive robots are designed to engage with humans in a manner that mimics social behavior. These robots possess the ability to perceive, interpret, and respond to human actions and emotions, enabling seamless interaction between humans and machines. In farming, SIRs offer a range of functionalities that extend beyond traditional automation, including monitoring crops, managing livestock, and assisting with various agricultural tasks.

This survey aims to provide a comprehensive overview of the current state of socially interactive robots in farming, exploring their applications, benefits, challenges, and future prospects. By examining existing research, developments, and real-world implementations, this study seeks to elucidate the potential impact of SIRs on agriculture and identify key areas for further exploration and improvement.

A survey on Internet of Things (IOT): Architecture, Enabling technologies

C.Ayesha Shariff

Ayesha6gs@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

***Abstract*—With the Internet of Things (IoT) gradually evolving as the subsequent phase of the evolution of the Internet, it becomes crucial to recognize the various potential domains for application of IoT, and the research challenges that are associated with these applications. Ranging from smart cities, to health care, smart agriculture, logistics and retail, to even smart living and smart environments IoT is expected to infiltrate into virtually all aspects of daily life. Even though the current IoT enabling technologies have greatly improved in the recent years, there are still numerous problems that require attention. Since the IoT concept ensues from heterogeneous technologies, many research challenges are bound to arise. The fact that IoT is so expansive and affects practically all areas of our lives, makes it a significant research topic for studies in various related fields such as information technology and computer science. Thus, IoT is paving the way for new dimensions of research to be carried out. This paper presents the recent development of IoT technologies and discusses future applications and research challenges.**

Keywords—Internet of Things; IoT applications; IoT challenges; future technologies; smart cities; smart environment; smart agriculture; smart living

I. Introduction

The Internet can be described as the communication network that connects individuals to information while The Internet of Things (IoT) is an interconnected system of distinctively address able physical items with various degrees of processing, sensing, and actuation capabilities that share the capability to interoperate and communicate through the Internet as their joint platform [1]. Thus, the main objective of the Internet of Things is to make it possible for objects to be connected with other objects, individuals, at any time or anywhere using any network, path or service. The Internet of Things (IoT) is gradually being regarded as the subsequent phase in the Internet evolution. IoT will make it possible for ordinary devices to be linked to the internet in order to achieve countless disparate goals. Currently, an estimated number of only 0.6% of devices that can be part of IoT has been connected so far [2]. However, by the year 2020, it is likely that over 50 billion devices will have an internet connection.

As the internet continues to evolve, it has become more than a simple network of computers, but rather a network of various devices, while IoT serves as a network of various “connected” devices a network of networks [3], as shown in Fig. 1. Nowadays, devices like smartphones, vehicles, industrial systems, cameras, toys, buildings, home appliances, industrial systems and countless others can all share information over the Internet. Regardless of their sizes and functions, these devices can accomplish smart reorganizations, tracing, positioning, control, real-time monitoring and process control. In the past years, there has been an important propagation of Internet capable devices. Even though its most significant commercial effect has been observed in the consumer electronics field; i.e. particularly the revolution of smartphones and the interest in wearable devices (watches, headsets, etc.), connecting people has become merely a fragment of a bigger movement towards the association of the digital and physical worlds.

With all this in mind, the Internet of Things (IoT) is expected to continue expanding its reach as pertains the number of devices and functions, which it can run. This is evident from the ambiguity in the expression of “Things” which makes it difficult to outline the ever-growing limits of the IoT [4]. While commercial success continues to materialize, the IoT constantly offers a virtually limitless supply of opportunities, not just in businesses but also in research. Accordingly, the understudy addresses the various potential areas for application of IoT domains and the research challenges that are associated with these applications.

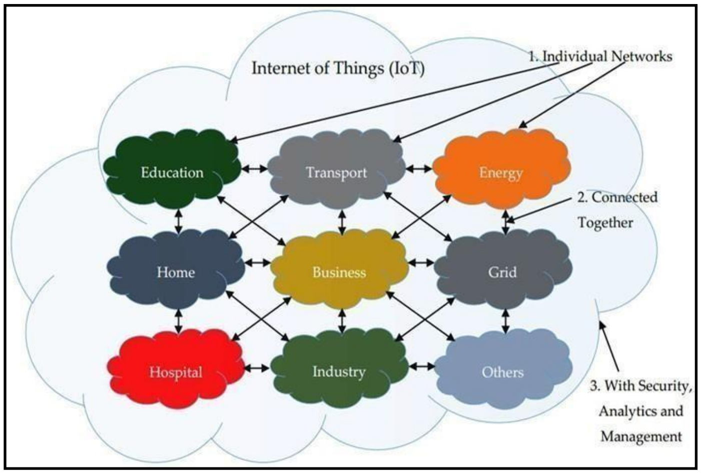


Fig. 1. IoT can be viewed as a Network of Networks [3].

II. Potential Application Domains of IoT

Potential applications of the internet of Things are not only numerous but also quite diverse as they permeate into virtually all aspects of daily life of individuals, institutions, and society. According to [5], the applications of IoT cover broad areas including manufacturing or the industrial sector, health sector, agriculture, smart cities, security and emergencies among many others.

ROLE OF BIG DATA IN INTERNET OF THINGS (IoT)

[1]P Siva Kumar, [2]Farheen Miraj Khan,

sivagpcet@gmail.com, Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

Abstract: The rate at which devices are connected to the internet which form IOT are increasing rapidly. All these devices produce huge amount of data. To process such voluminous amount of data is a challenging task. The big data management system has many tools which can be efficiently used for collection, processing and analytics of data. This review paper highlights the role of big data in IoT(Internet of Things) and recent advances in big data management and analytics in the IoT paradigm. As the number of devices and data generated by these devices are increasing rapidly, therefore it is challenging task to process, manage and analyze big data in scalable, cost-effective and distributed manner

IndexTerms - IoT,Big Data,Layered Architecure

I. INTRODUCTION

Due to the Internet and availability of network resources anyone can gather the required information easily and its usage is changing continuously with each and every second. The advent of new technologies, devices and convergence of wireless communication, digital electronics, and micro-electro- mechanical systems (MEMS) technologies have resulted in the emergence of Internet of Things (IoT) which in turn produces a huge amount of data. According to a recent Cisco report the number of devices connected to the Internet is more than the number of human beings in the world. Personal Computer (PC) users have produced almost 60 percent of the Internet traffic in 2014, but this count would reduce to 33 percent by 2019 [1]. IoT forms a network of interconnected devices such as PCs, laptops, WiFi, sensor enabled deices and household appliances which produces a big data and it is expected the this big data will increase from 22.9 billion in 2016 to 50 billion by 2020 and will continue to increase. Thus IOT is connected network in which communication and network resources are not only confined between users to users, but also extended to users to things and things to things. Most data collection tools in the IoT environment are sensor-fitted devices and sensors are used in nearly all industries, thus the IoT is expected to produce a huge amount of data. Fig.1 identifies different sources of producing different type and amount of data. IoT helps in reducing costs and increasing revenue, but at the cost of producing enormous data. In order to get benefits from IoT, organizations should design a platform that can process, manage and analyze huge amount of data in scalable and cost-effective manner [3]. Big data provides such a platform that can not only process voluminous and complex data sources, but also helps in accelerating the data integration. Organizations use various data analytics tools to manage a huge volume sensor-collected data into processed data.

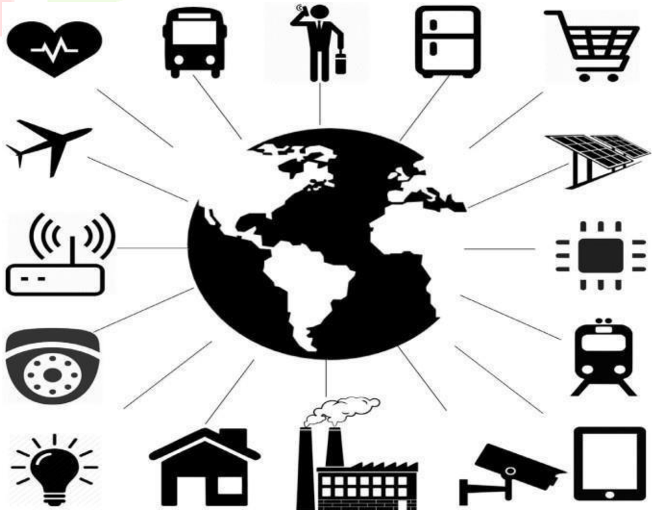


figure 1

A short survey of Security and Privacy Issues of Internet of Things

[1] M Srilakshmi , 2Sandhya rani

[1,2]Associate Professor, [3]Assistant Professor
Department of CSE,
lakshmi78@gmail.com
,sandhya@gmail.com
G Pullaiah College of Engineering & Technology, Kurnool

Abstract: **The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and wrist watches that share with your friends how far you have biked or run during the day. Which offers capabilities to identify and connect worldwide physical objects into a unified system? As a part of IoTs, serious concerns are raised over access of personal information pertaining to device and individual privacy. Security and privacy are the key issues for IoT applications, this survey summarizes the security threats and privacy concerns of IoT.**

***Index Terms* - Internet of Things (IoT), Threats, Security, Privacy**

I. INTRODUCTION

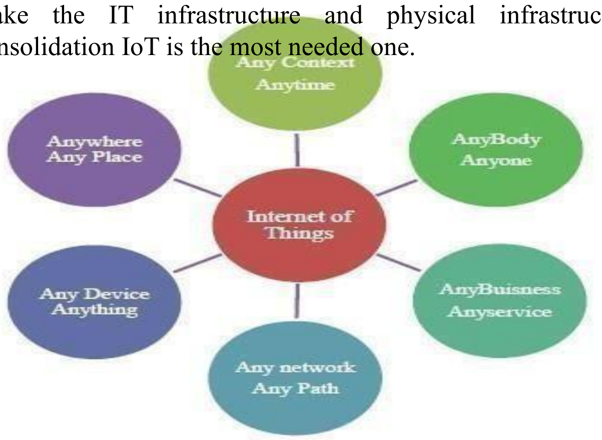
With the rapid development of Internet technology and communications technology, our lives are gradually led into an imaginary space of virtual world. People can chat, work, shopping, keeps pets and plants in the virtual world provided by the network. However, human beings live in a real world; human activities cannot be fully implemented through the services in the imaginary space. It is the limitation of imaginary space that restricts the development of Internet to provide better services. To remove these constraints, a new technology is required to integrate imaginary space and real- world on a same platform which is called as Internet of Things (IoTs). Based on a large number of low-cost sensors and wireless communication, the sensor network technology puts forward new demands to the Internet technology. It will bring huge changes to the future society, change our way of life and business models. Apart from benefits of IoTs, there are several security and privacy concerns at different layers viz; Front end, Back end and Network. In this paper, the survey is in security and privacy concerns related to Internet of Things (IoTs) by defining some open challenges. Nowadays, the concept of IoT is many-folded, it embraces many different technologies, services, and standards and it is widely perceived as the angular stone of the ICT market in the next ten years, at least.

From a logical viewpoint, an IoT system can be depicted as a collection of smart devices that interact on a collaborative basis to fulfill a common goal. At the technological floor, IoT deployments may adopt different processing and communication architectures, technologies, and design methodologies, based on their target. For instance, the same IoT system could leverage the capabilities of a wireless sensor network (WSN) that collects the environmental information in a given area and a set of smart phones on top of which monitoring applications run. In the middle, a standardized or proprietary middle-ware could be employed to ease the access to virtualized resources and services. The middleware, in turn, might be implemented using cloud technologies, centralized over- lays, or peer to peer systems.

II IOT OVERVIEW AND BACKGROUND

As shown in Fig. 1, the IoTs allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service. They are "Material objects connected to material objects in the Internet".

For example, through RFID, laser scanners, global writing system, infrared sensors and other information sensing devices are connected to any object for communication services and data exchange. At last, to reach the smart devices to be tracked, located, and monitored and to handle the network functions, to make the IT infrastructure and physical infrastructure consolidation IoT is the most needed one.



International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-3,
Article ID IRP1149, Pages 43-47
www.ijircst.org

A Method for obtaining Digital signatures and networks security matters

R Vara Prasad, varan45@gmail.com

Dept. of CSE, G. Pullaiah college of engineering & Technology, Kurnool, A.P

ABSTRACT- For secure and smart transactions over open networks, the Digital Signature Concept is necessary. It is having forms of programs with a view to make certain the integrity of information exchanged or saved and to show the identity of the originator to the recipient. Digital Signature techniques are usually used in cryptographic protocols to provide services like entity authentication, authenticated key delivery and authenticated key agreement. With using cellular devices as a client of internet, the risk of unauthorized and unauthenticated get admission to of crucial files (e.g. contracts, receipts, and so forth.) is growing every day. Although Digital Signature is supposed to be the solution for the unauthorized get right of entry to, its implementation isn't always good enough till now. The symmetric records transfer mechanism is used for the transfer of essential documents, but there's a want of a greater ready mechanism for safe transfer and verification of the documents. This Research paper presents a comprehensive study of Digital Signature and its benefits.

KEYWORDS- Authentication, Cryptography, Digital Signature, Verification

I. INTRODUCTION

Digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or report. A valid digital signature offers a recipient cause to agree with that the message became created by using a recognized sender, and that it turned into now not altered in transit. Digital signatures are normally used for software distribution, financial transactions, and in other instances wherein it's far critical to come across forgery or tampering. In our ordinary lifestyles Internet have become integral parts. Security is an important term in this regard. If serious attack occurs, communication, trade, transaction and other important functions will be affected. Public key cryptography is a shape of cryptography, which usually allows customers to talk securely without having prior access to a shared secret key. This is completed by way of the usage of a pair of cryptographic keys unique as public key and personal key. A public key is essentially like an e mail deal with, and a private key, just like the e mail deal with password. The public key is sent to the receiver, at the same time as the non-public key is not disclosed to absolutely everyone [1]. They are related mathematically. What has been encrypted with the first key can only be decrypted with the second - and vice versa [4]. Hence, if a desires to ship a comfortable e mail to B, A ought to encrypt it with B’s public key, so that when B receives the encrypted e-mail, he can decrypt it the usage of his own private key. When we say, A encrypts the report, what A in reality does is runs this file thru a hash function software. The hash characteristic software program produces a hard and fast duration of alphabets, numbers and logos for any report. This is known as the hash result. [5] [6]. The hash result is never the equal for two different documents. Any small alteration inside the file will generate a wholly extraordinary hash result. The hash function software will always produce the same hash result of a particular message. Thus, if there may be any doubt about the message being intercepted, all one should do is to examine the hash functions at each ends. Authentication of the digital record will be effected by the use of uneven crypto gadget (that's nothing but the public key cryptography system explained above) and hash function, which envelope and rework the preliminary digital record into any other digital document. A Digital Signature Certificate basically includes the public key of the person who holds it, alongside different details inclusive of contact details, and the most crucial component, this is the digital signature of the Certifying Authority [2][7]. The major reason of one of these certificates is to reveal that a trustable authority appointed and controlled by way of the Government, has attested the statistics contained in the Certificate.

A. *Benefits*

- While digital signatures have caught the fancy of many corporates and executives, what exactly is it? Simply positioned, a digital signature is your electronic fingerprint.
- It lets you sign a document electronically and it validates the signer.
- It is a mathematical code that authenticates the document from the sender and ensures the document remains unaltered in reaching the recipient.
- Fears about the security of digital signatures is reasonable, however, it uses an accepted format called a Public Key Infrastructure, which provide a very high level of security making it difficult to duplicate.
- Digital signatures make office paperwork far more efficient, but laws regarding this technology vary between countries.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 02,

A New method for Secure data Transmission using optical fiber in WNN

P Ramarao, ramaraogpcet@gmail.com
Dept. of CSE, G. Pullaiah college of engineering
& Technology, Kurnool, A.P

k.lakshmi,Lakshmi@gmail.com
dept of cse,GPCET

Abstract— **In this emerging world where individuals seem more valued and powerful, privacy might be under attack and security might be endangered. Security is essential while storing and transmission of information. Cryptography and steganography are two good techniques for data security. In this paper we are proposing a new technique for data security using distributed steganography and public key cryptography. In our proposed technique steganography is used to hide secure data in carrier video, Diffie - Hellman key exchange algorithm is used to produce the keys used for encryption and embedding process and AES is for encrypting the embedding data. The combination of steganography and public key cryptographic technique produces better results for securing the data.**

Keywords*— *Steganography, Distributed Steganography, Information Hiding, Public Key Cryptography, AES, Diffie and Hellman Key Exchange algorithm.

I. INTRODUCTION

Steganography is the art of concealing the secure messages in other messages [4, 5]. Steganography techniques uses different media like image files, audio files, video files and text files for secret communication [2, 3]. There are many parameters that affect steganography techniques. These parameters include hiding capacity, perceptual transparency (or security), robustness, complexity, survivability, and capability.

Distributed steganography is the process of distributing the secure message across multiple carrier signals or source messages[9]. For example a single text message would be broken into multiple blocks, each block hidden in a different image. The message blocked are permuted according to a key and stored in different carrier messages.

Cryptography is the method that allows information to be sent in a secure form in such a way that the only receiver will be able to retrieve this information [7, 8]. The main purpose of the cryptography is used not only to provide confidentiality, but also to provide solutions for other problem like: data integrity, authentication, non-repudiation. Cryptography is divided into two types depending on number of keys used. They are private key encryption techniques and public key encryption techniques. Private key encryption techniques use same key at sender and receiver side whereas public key encryption techniques uses two different keys, one for encryption and other for decryption.

Diffie and Hellman is a public key cryptography technique[10]. The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages. The algorithm itself is limited to the exchange of secret values. In this scheme, there are two publicly known numbers: a prime number q and an integer that is a primitive root of q. Suppose the users A and B wish to exchange a key. User A selects a random integer $X_A <$ q and computes $Y_A = \alpha^{X_A} \bmod q$. Similarly, user B independently selects a random integer $X_B <$ q and computes $Y_B = \alpha^{X_B} \bmod q$. Each side keeps the X value private and makes the Y value available publicly to the other side. User A computes the key as $K = (Y_B)^{X_A} \bmod q$ and user B computes the key as $K = (Y_A)^{X_B} \bmod q$. The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms.

AES standards for Advanced Encryption Standard [6]. Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14). These rounds are governed by the following transformations: (i) Byte sub transformation: Is a non linear byte Substitution, using a substitution table (s-box), which is constructed by multiplicative inverse and affine transformation. (ii) Shift rows transformation: Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes. (iii) Mix columns transformation: Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers. (iv) Add round key transformation: Is a simple XOR between the working state and the round key. This transformation is its own inverse.

Performance and usage of data analytics in health care

U Supriya

supriyacse@gmail.com
department of computer science and engineering.
g.pullaiah college o9f engineering and technology.

P pranav sai reddy

department of computer science and engineering.
g.pullaiah college o9f engineering and technology.

Abstract

The main aim of this paper is to provide a deep analysis on the research field of healthcare data analytics., as well as highlighting some of guidelines and gaps in previous studies. This study has focused on searching relevant papers about healthcare analytics by searching in seven popular databases such as google scholar and springer using specific keywords, in order to understand the healthcare topic and conduct our literature review. The paper has listed some data analytics tools and techniques that have been used to improve healthcare performance in many areas such as: medical operations, reports, decision making, and prediction and prevention system. Moreover, the systematic review has showed an interesting demographic of fields of publication, research approaches, as well as outlined some of the possible reasons and issues associated with healthcare data analytics, based on geographical distribution theme.

Keywords Healthcare, Data Analytics, Clinics, Systematic Review, Tools and Techniques.

1 INTRODUCTION

Today's healthcare industries are moving from volume-based business into value-based business, which requires an overwork from doctors and nurses to be more productive and efficient. This will improve healthcare practice, changing individual life style and driving them into longer life, prevent diseases, illnesses and infections.

Over the last few years, healthcare data has become more complex for the reason that large amount of data are being available lately, along with the rapid change of technologies and mobile applications and new diseases have discovered. Therefore, healthcare sectors have believed that healthcare data analytics tools are really important subject in order to manage a large amount of complex data, which can lead to improve healthcare industries and help medical practice to reach a high level of efficiency and work flow accuracy, if these data analytics tools applied correctly, but the questions are how healthcare organizations are applying these tools today, and how to think about it's future use? Also, what are the challenges they face when using such tools? And finally, what are the innovations can healthcare add to meet these challenges?

Sequence to Sequence Learning with Neural Networks in data analysis methods

Balakrishna
balakrishna@gmai.com
dept of cse,GPCET

saisimhareddy
saisimhacse@gmail.com
dept of cse,GPCET

Abstract

Deep Neural Networks (DNNs) are powerful models that have achieved excellent performance on difficult learning tasks. Although DNNs work well whenever large labeled training sets are available, they cannot be used to map sequences to sequences. In this paper, we present a general end-to-end approach to sequence learning that makes minimal assumptions on the sequence structure. Our method uses a multilayered Long Short-Term Memory (LSTM) to map the input sequence to a vector of a fixed dimensionality, and then another deep LSTM to decode the target sequence from the vector. Our main result is that on an English to French translation task from the WMT-14 dataset, the translations produced by the LSTM achieve a BLEU score of 34.8 on the entire test set, where the LSTM's BLEU score was penalized on out-of-vocabulary words. Additionally, the LSTM did not have difficulty on long sentences. For comparison, a phrase-based SMT system achieves a BLEU score of 33.3 on the same dataset. When we used the LSTM to rerank the 1000 hypotheses produced by the aforementioned SMT system, its BLEU score increases to 36.5, which is close to the previous state of the art. The LSTM also learned sensible phrase and sentence representations that are sensitive to word order and are relatively invariant to the active and the passive voice. Finally, we found that reversing the order of the words in all source sentences (but not target sentences) improved the LSTM's performance markedly, because doing so introduced many short term dependencies between the source and the target sentence which made the optimization problem easier.

1 Introduction

Deep Neural Networks (DNNs) are extremely powerful machine learning models that achieve excellent performance on difficult problems such as speech recognition [13, 7] and visual object recognition [19, 6, 21, 20]. DNNs are powerful because they can perform arbitrary parallel computation for a modest number of steps. A surprising example of the power of DNNs is their ability to sort N N-bit numbers using only 2 hidden layers of quadratic size [27]. So, while neural networks are related to conventional statistical models, they learn an intricate computation. Furthermore, large DNNs can be trained with supervised backpropagation whenever the labeled training set has enough information to specify the network's parameters. Thus, if there exists a parameter setting of a large DNN that achieves good results (for example, because humans can solve the task very rapidly), supervised backpropagation will find these parameters and solve the problem.

Despite their flexibility and power, DNNs can only be applied to problems whose inputs and targets can be sensibly encoded with vectors of fixed dimensionality. It is a significant limitation, since many important problems are best expressed with sequences whose lengths are not known a-priori. For example, speech recognition and machine translation are sequential problems. Likewise, question answering can also be seen as mapping a sequence of words representing the question to a

A Neural Conversation Model in security methods

G Sreenivasulu M VARALAKSHMI
Department of computer science and engineering
G.Pullaiah college of engineering and Technology
sreenivasulucse@gmail.com
varalakshmicse@gmail.com

Abstract

The prevalent use of social media leads to a vast amount of online conversations being pro- duced on a daily basis. It presents a concrete challenge for individuals to better discover and engage in social media discussions. In this paper, we present a novel framework to automatically recommend conversations to users based on their prior conversation behaviors. Built on neural collaborative filtering, our model explores deep semantic features that measure how a user's preferences match an ongoing conversation's context. Furthermore, to identify salient characteristics from interleaving user interactions, our model incorporates graph-structured networks, where both replying relations and temporal features are encoded as conversation context. Experimental results on two large-scale datasets collected from Twitter and Reddit show that our model yields better performance than previous state- of-the-art models, which only utilize lexical features and ignore past user interactions in the conversations.

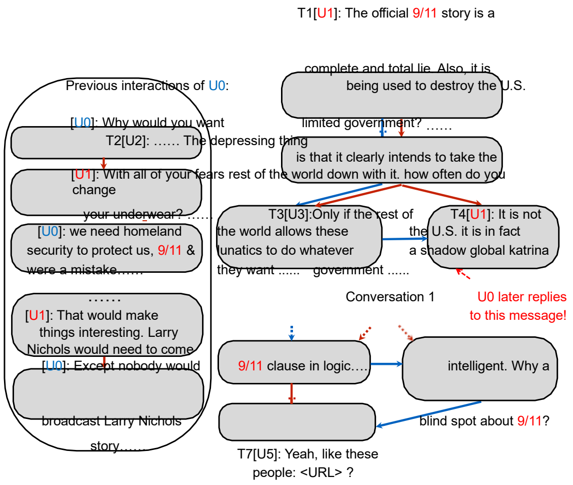

T1[U1]: The official 9/11 story is a
complete and total lie. Also, it is
being used to destroy the U.S.
limited government? ......
Previous interactions of U0:
[U0]: Why would you want
T2[U2]: ...... The depressing thing
is that it clearly intends to take the
[U1]: With all of your fears rest of the world down with it. how often do you
change
your underwear? ......
[U0]: we need homeland
security to protect us, 9/11 &
were a mistake......
T3[U3]:Only if the rest of
the world allows these
lunatics to do whatever
they want ...... government ......
T4[U1]: It is not
the U.S. it is in fact
a shadow global katrina
......
[U1]: That would make
things interesting. Larry
Nichols would need to come
[U0]: Except nobody would
broadcast Larry Nichols
story......
Conversation 1
U0 later replies
to this message!
9/11 clause in logic....
intelligent. Why a
blind spot about 9/11?
T7[U5]: Yeah, like these
people: <URL> ?
up for Hillary......
T5[U4]:No, there is a
users tend to be quiteT6[U5]:
Why? Reddit
Conversation 2

Figure 1: Two Reddit conversation snippets on the right. User U₀, whose historical interactions with another user U₁ shown on the left, only engages in Conversation 1 (which is initialized by U₁), but not Conversation 2 (U₁ does not participate in). Red arrows indicate in-reply-to relations, and blue arrows depict chronological orders.

1 Introduction

Social media has profoundly revolutionized people's social interactions, as many individuals now turn to online platforms to voice opinions and exchange ideas. Meanwhile, the abundance of information brings the problem of information explosion — the huge volume of online discussions produced every day has far outpaced any individual's capability of digesting them. It is hence difficult for one to discover online discussions that are potentially of interest. To address this issue, we study the problem of online conversation recommendation, with the goal of identifying conversations that fit a user's preferences, hence likely to result in the user's future engagement.

In previous studies, it has been shown that effective online conversation recommendation has the potential to produce more positive online social interaction experience (Chen et al., 2011; Zeng et al., 2018). Prior work on this subject has focused on post-level recommendation (Yan et al., 2012; Chen et al., 2012), or conversation-level suggestion with handcrafted features (Chen et al., 2011) and word co-occurrence patterns (Zeng et al., 2018). Nev- ertheless, they ignore the useful information em- bedded in replying relations, where the conversa- tion structure is formed via messages sent among users. In this work, we examine conversation context, and model the participants' interactions therein. This approach enables deep representa- tion learning that reflects personal interests and conversation preferences,

* This work was mainly conducted when Jing Li was af- filiated with Tencent AI Lab, Shenzhen, China.

Effective approaches to attention based Neural Machine translation in network passage

G Sreenivasulu
sreenivasulucse@gmail.com
G.pullaiah college of engineering and technology department of cse

rayyan hussain
rayyanece@gmail.com
Department of cse

Abstract

Automatic question generation aims to generate questions from a text passage where the generated questions can be answered by certain sub-spans of the given passage. Traditional methods mainly use rigid heuristic rules to transform a sentence into related questions. In this work, we propose to apply the neural encoder-decoder model to generate meaningful and diverse questions from natural language sentences. The encoder reads the input text and the answer position, to produce an answer-aware input representation, which is fed to the decoder to generate an answer focused question. We conduct a preliminary study on neural question generation from text with the SQuAD dataset, and the experiment results show that our method can produce fluent and diverse questions.

1 Introduction

Automatic question generation from natural language text aims to generate questions taking text as input, which has the potential value of education purpose (Heilman, 2011). As the reverse task of question answering, question generation also has the potential for providing a large scale corpus of question-answer pairs.

Previous works for question generation mainly use rigid heuristic rules to transform a sentence into related questions (Heilman, 2011; Chali and Hasan, 2015). However, these methods heavily rely on human-designed transformation and generation rules, which cannot be easily adopted to other domains. Instead of generating questions from texts, Serban et al. (2016) proposed a neural network method to generate factoid questions from structured data.

In this work we conduct a preliminary study on question generation from text with neural networks, which is denoted as the Neural Question Generation (NQG) framework, to generate natural language questions from text without pre-defined rules. The Neural Question Generation framework extends the sequence-to-sequence models by enriching the encoder with answer and lexical features to generate answer focused questions. Concretely, the encoder reads not only the input sentence, but also the answer position indicator and lexical features. The answer position feature denotes the answer span in the input sentence, which is essential to generate answer relevant questions. The lexical features include part-of-speech (POS) and named entity (NER) tags to help produce better sentence encoding. Lastly, the decoder with attention mechanism (Bahdanau et al., 2015) generates an answer specific question of the sentence.

Large-scale manually annotated passage and question pairs play a crucial role in developing question generation systems. We propose to adapt the recently released Stanford Question Answering Dataset (SQuAD) (Rajpurkar et al., 2016) as the training and development datasets for the question generation task. In SQuAD, the answers are labeled as subsequences in the given sentences by crowed sourcing, and it contains more than 100K questions which makes it feasible to train our neural network models. We conduct the experiments on SQuAD, and the experiment results show the neural network models can produce fluent and diverse questions from text.

2 Approach

In this section, we introduce the NQG framework, which consists of a feature-rich encoder and an

*Contribution during internship at Microsoft Research.

Mining Association Rules between Sets of Items in Large Databasesin deffetent algorithms

k gayathri *himanshu katri*

Department of computer science and engineering.
G . pullaiah college of engineering and technology.
gayatri@gmail.com alicse@gmail.com

Abstract

We are given a large database of customer transactions. Each transaction consists of items purchased by a customer in a visit. We present an efficient algorithm that generates all significant association rules between items in the database. The algorithm incorporates buffer management and novel estimation and pruning techniques. We also present results of applying this algorithm to sales data obtained from a large retailing company, which shows the effectiveness of the algorithm.

1 Introduction

Consider a supermarket with a large collection of items. Typical business decisions that the management of the supermarket has to make include what to put on sale, how to design coupons, how to place merchandise on shelves in order to maximize the profit, etc. Analysis of past transaction data is a commonly used approach in order to improve the quality of such decisions. Until recently, however, only global data about the cumulative sales during some time period (a day,a week, a month, etc.) was available on the computer. Progress in bar-code technology has made it possible to store the so called basket *data that stores items purchased on a per-transaction basis. Basket data type transactions do not necessarily consist of items bought together at the same point of time. It may consist of items bought by a customer over a period of time. Examples include monthly purchases by members of a book club or a music club.*

Several organizations have collected massive amounts of such data. These data sets are usually stored on tertiary storage and are very slowly migrating to database systems. One of the main reasons for the limited success of database systems in this area is that current database systems do not provide necessary functionality for a user interested in taking advantage of this information.

This paper introduces the problem of \mining" a large collection of basket data type transactions for association rules between sets of items with some minimum specified confidence, and presents an efficient algorithm for this purpose. An example of such an association rule is the statement that 90% of transactions that purchase bread and butter also purchase milk. The antecedent of this rule consists of bread and butter and the consequent consists of milk alone. The number 90% is the confidence factor of the rule.

The work reported in this paper could be viewed as a step towards enhancing databases with functionalities to process queries such as (we have omitted the confidence factor specification):

> *Find all rules that have \Diet Coke" as consequent. These rules may help plan what the store should do to boost the sale of Diet Coke.*
>
> *Find all rules that have \bagels" in the antecedent. These rules may help determine what products may be impacted if the store discontinues selling bagels.*
>
> *Find all rules that have \sausage" in the antecedent and \mustard" in the consequent. This query can be phrased alternatively as a request for the additional items that have to be sold together with sausage in order to make it highly likely that mustard will also be sold.*
>
> *Find all the rules relating items located on shelves A and B in the store. These rules may help shelf planning by determining if the sale of items on shelf A is related to the sale of items on shelf B.*

Current address: Computer Science Department, Rutgers University, New Brunswick, NJ 08903

Proceedings of the 1993 ACM SIGMOD Conference
Washington DC, USA, May 1993

Review Article

A Few useful things to know about Machine Learning in Healthcare

Dr k. Sreenivasulu **n saisimhareddy** **r vignesh**

G . pullaiah college of engineering and technology Kurnool.

Department of computer science and engineering .

Sreenivasulu@gmail.com saisimhareddycse@gmail.com rvigneshcse@gmail.com

In the present day, there are many diseases which need to be identified at their early stages to start relevant treatments. If not, they could be uncurable and deadly. Due to this reason, there is a need of analysing complex medical data, medical reports, and medical images at a lesser time but with greater accuracy. There are even some instances where certain abnormalities cannot be directly recognized by humans. In healthcare for computational decision making, machine learning approaches are being used in these types of situations where a crucial data analysis needs to be performed on medical data to reveal hidden relationships or abnormalities which are not visible to humans. Implementing algorithms to perform such tasks itself is difficult, but what makes it even more challenging is to increase the accuracy of the algorithm while decreasing the required time for the algorithm to execute. In the early days, processing of large amount of medical data was an important task which resulted in machine learning being adapted in the biological domain. Since this happened, the biology and biomedical fields have been reaching higher levels by exploring more knowledge and identifying relationships which were never observed before. Reaching to its peak now the concern is being diverted towards treating patients not only based on the type of disease but also their genetics, which is known as precision medicine. Modifications in machine learning algorithms are being performed and tested daily to improve the performance of the algorithms in analysing and presenting more accurate information. In the healthcare field, starting from information extraction from medical documents until the prediction or diagnosis of a disease, machine learning has been involved. Medical imaging is a section that was greatly improved with the integration of machine learning algorithms to the field of computational biology. Nowadays, many disease diagnoses are being performed by medical image processing using machine learning algorithms. In addition, patient care, resource allocation, and research on treatments for various diseases are also being performed using machine learning-based computational decision making. Throughout this paper, various machine learning algorithms and approaches that are being used for decision making in the healthcare sector will be discussed along with the involvement of machine learning in healthcare applications in the current context. With the explored knowledge, it was evident that neural network-based deep learning methods have performed extremely well in the field of computational biology with the support of the high processing power of modern sophisticated computers and are being extensively applied because of their high predicting accuracy and reliability. When giving concern towards the big picture by combining the observations, it is noticeable that computational biology and biomedicine-based decision making in healthcare have now become dependent on machine learning algorithms, and thus they cannot be separated from the field of artificial intelligence.

1. Introduction

Artificial Intelligence includes approaches and techniques like machine learning, machine reasoning, and robotics. In this review, the main concern will be given towards machine learning as it is the approach that is being applied using different techniques and algorithms in various healthcare activities. The use of machine learning to solve clinical problems is called revolutionary clinical decision making. When machine learning is being used in clinical decision

International Journal of Data Science and Analytics

Fast Algorithms for Mining Association Rules in industrial purposes

S. Shasikala
shashikala@gmail.com
Dept.of.CSE , G.Pullaiah College Of Engineering & Technology

Abstract

We consider the problem of discovering association rules between items in a large databaseof sales transactions. We present two new algorithms for solving this problem that are fundamentally different from the known algorithms. Experiments with synthetic as well as real-life data show that these algorithms outperform the known algorithms by factors ranging from three for small problems to more than an order of magnitude for large problems. We also show how the best features of the two proposed algorithms can be combined into a hybrid algorithm, called AprioriHybrid. Scale-up experiments show that AprioriHybrid scales linearly with the number of transactions. AprioriHybrid also has excellent scale-up properties with respect to the transaction size and the number of items in the database.

1 Introduction

Database mining is motivated by the decision support problem faced by most large retail organizations [S+93]. Progress in bar-code technology has made it possible for retail organizations to collect and store massive amounts of sales data, referred to as the basket data. A record in such data typically consists of the transaction date and the items bought in the transaction. Success- ful organizations view such databases as important pieces of the marketing infrastructure [Ass92]. They are interested in instituting information-driven marketing processes, managed by database technology, that enable marketers to develop and implement customized marketing programs and strategies [Ass90].

The problem of mining association rules over basket data was introduced in [AIS93b]. An example of such a rule might be that 98% of customers that purchase tires and auto accessories also get automotive services done. Finding all such rules is valuable for cross-marketing and attached mailing applications. Other applications include catalog design, add-on sales, store layout, and customer segmentation based on buying patterns. The databases involved in these applications are very large. It is imperative, therefore, to have fast algorithms for this task.

Visiting from the Department of Computer Science

Mining Frequent pattrens Without Candidate Generation In Education center

S Shasikala rakesh .m

G.pullaiah college of engineering and technology .

Department of computer science and engineering

shasikalacse@gmail.com rakesh@gmail.com

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: Mining of regular trends in group action databases, time series databases, and lots of different database types was popularly studied in data processing research. Most previous studies follow the generation-and-test method of associate degree Apriori-like candidate collection. In this study, we seem to propose a particular frequency tree like structure, which is associated degree of prefix-tree like structure that is extended to be used for compressed storage, crucial knowledge of the frequency pattern, associated degrees create an economic FP-tree mining methodology, FP growth, by the growth of pattern fragments for the mining of the entire set of frequent patterns. Three different mining techniques are used to outsize the information which is compressed into small structures such as FP-tree that avoids repetitive information scans, cost. The proposed FP-tree-based mining receives an example philosophy of section creation to stay away from the exorbitant age of several competitor sets, and an apportioning-based, separating and-overcoming technique is used to divide the mining task into a contingent knowledge base for restricted mining designs that effectively reduces the investigation field.

Keywords: Itemsets, FP-Tree, transactions, Conditional FP-Growth.

1. Introduction

Data mining may be a way of getting beneficial, previously unknown, and eventually understandable knowledge from the details. Association rules mining is one in every critical piece of information on information knowledge} mining and is used to look for interesting associations or connection relationships in mass data between item sets [1]. The discovery of frequent item sets could be a key technology and step within the application of the mining rules of the association. The primary illustrious rule is that Apriori implies within the algorithms of the discovery of frequent item sets by Agrawal. Apriori rule scans the details extracting solitary item sets by continuous association to search for all the frequent item sets in the information. However, the Apriori rule repeatedly scans the information in the mining system and generates an oversized variety of candidate itemsets affecting the mining running pace [2].

The FP-Growth (frequent-pattern growth) rule is an improved rule suggested by the Jiawei dynasty and then forward by the Apriori rule. It compresses information sets to an FP-tree, doubly scans the data, doesn't turn out the candidate, item sets in the mining process, and greatly enhances mining capacity. The FP-Growth rule must, however, generate an FP-tree containing all the information sets. The memory house is in high demand for this FP-tree. And scanning the information doubly together does not make the power of the FP-Growth rule strong. Then the compressed information is divided into a series of databases on condition (a special kind of prediction database) [3-5].

2. Working of FP-Growth Algorithm

Without generating candidate itemset, the FP-Growth the algorithm permits the frequent itemset to be found. The method mentioned below is a two-step one,

1) The primary step is to scan the information inside the information to look for the occurrences of the element sets. This process is the same as the beginning of Apriori. Inside the information the count of 1-itemsets is called 1-itemset help count or frequency [6].

2) Constructing the FP the tree is the second step. For that, produce the tree's base. The base is drawn by null [7].

A Survey of Data Mining Techniques for Social Network Analysis for sentiment analysis

Ameena Yasmeen,Gautam kumar

G.pullaiah college of engineering and technology Kurnool.

department of computer science andengineering

yasmin@gmail.com csegautam@gmail.com

Abstract. Social network has gained remarkable attention in the last decade. Accessing social network sites such as Twitter, Facebook LinkedIn and Google+ through the internet and the web 2.0 technologies has become more affordable. People are becoming more interested in and relying on social network for information, news and opinion of other users on diverse subject matters. The heavy reliance on social network sites causes them to generate massive data characterised by three computational issues namely; size, noise and dynamism. These issues often make social network data very complex to analyse manually, resulting in the pertinent use of computational means of analysing them. Data mining provides a wide range of techniques for detecting useful knowledge from massive datasets like trends, patterns and rules [44]. Data mining techniques are used for information retrieval, statistical modelling and machine learning. These techniques employ ***data pre-processing, data analysis, and data interpretation*** processes in the course of data analysis. This survey discusses different data mining techniques used in mining diverse aspects of the social network over decades going from the historical techniques to the up-to-date models, including our novel technique named ***TRCM.*** All the techniques covered in this survey are listed in the Table.1 including the tools employed as well as names of their authors.

Keywords: Social Network, Social Network Analysis, Data Mining Techniques

1. Introduction

Social network is a term used to describe web-based services that allow individuals to create a public/semi-public profile within a domain such that they can communicatively connect with other users within the network [22]. Social network has improved on the concept and technology of Web 2.0, by enabling the formation and exchange of User-Generated Content [46]. Simply put, social network is a graph consisting of *nodes* and *links* used to represent social relations on social network sites [17]. The *nodes* include entities and the relationships between them forms the *links* (as presented in Fig. 1).

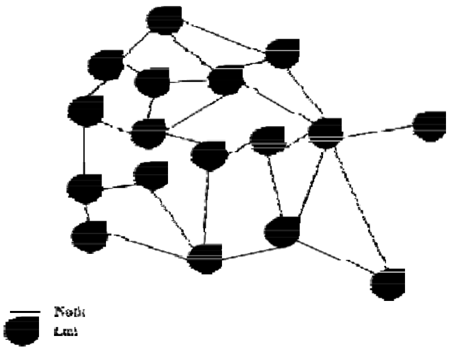


Fig. 1. Social Network showing nodes and links

A Comparative Analysis of Methodologies for Database Schema Integration in network architectures

R Varaprasad gmail:varaprasad@gmail.com

Dept.of.CSE, G.Pullaiah College Of Engineering & Technology

***Abstract*—Capturing uncertainty in object detection is indispensable for safe autonomous driving. In recent years, deep learning has become the de-facto approach for object detection, and many probabilistic object detectors have been proposed. However, there is no summary on uncertainty estimation in deep object detection, and existing methods are either built with different network architectures and uncertainty estimation methods, or evaluated on different datasets with a wide range of evaluation metrics. As a result, a comparison among methods remains challenging, as does the selection of a model that best suits a particular application. This paper aims to alleviate this problem by providing a review and comparative study on existing probabilistic object detection methods for autonomous driving applications. First, we provide an overview of practical uncertainty estimation methods in deep learning, and then systematically survey existing methods and evaluation metrics for probabilistic object detection. Next, we present a strict comparative study for probabilistic object detection based on an image detector and three public autonomous driving datasets. Finally, we present a discussion of the remaining challenges and future works. Code has been made available at https://github.com/asharakeh/pod_compare.git.**

***Keywords*—Uncertainty estimation, object detection, deep learning, autonomous driving**

I. IntRodUctIon

Capturing perceptual uncertainties is indispensable for safe autonomous driving. Consider a self-driving car operating *in snowy days,* when on-board sensors can be compromised by snow; *during the night-time*, when the image quality of RGB cameras is diminished; or *on an unfamiliar street*, where we encounter a motorized-tricycle, which can be often seen in Asian cities but are exceedingly rare in Western Europe. In these complex, unstructured driving environments, the perception module may make predictions with varied errors and increased failure rates. Determining reliable perceptual uncertainties, which reflect perception inaccuracy or sensor noises, could provide valuable information to introspect the perception performance, and help an autonomous car react accordingly. Further, cognitive psychologists have found that humans are good intuitive statisticians, and have a frequentist sense of uncertainties [1]. Therefore, reliable perceptual uncertainties could help humans better interpret the intention of autonomous cars, and enhance the development of trust in this rapidly evolving technology. As the machine learning methods (especially deep learning) have been widely applied to safety-critical computer vision problems [2], efforts to improve a network's self-assessment ability, reliability and interpretability with uncertainty estimation are steadily increasing [3], [4].

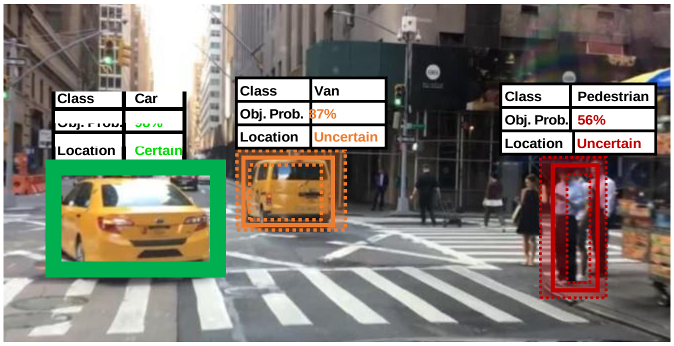


Fig. 1: A *conceptual* illustration of probabilistic object detection in an urban driving scenario. Each object is classified with a classification probability, and its bounding box is predicted with a confidence interval. The RGB camera image is from the BDD100k dataset [18].

In this paper, we focus on object detection, one of the most important perception problems in autonomous driving. An object detector is targeted to jointly classify and localize relevant traffic participants from on-board sensor data (e.g. RGB camera images, LiDAR and Radar points) in a frame-by-frame manner. When modeling probability in object detection, we need to estimate the probability an object belongs to the classes of interest (also called semantic uncertainty as introduced in [5]), as well as the probability distribution and the confidence interval of bounding box (i.e. spatial uncertainty [5]), as shown conceptually in Fig 1. In recent years, deep learning has become the de-facto approach in object detection, and many methods of modeling uncertainties in deep neural networks have been proposed [6]–[17]. However, to our knowledge, there is no work that provides a summary on uncertainty estimation in deep object detection, making it difficult for researchers to enter this field. Besides, existing probabilistic object detection models are often built with different network architectures, different uncertainty modeling approaches, and different sensing modalities. They are also tested on different datasets with a wide range of evaluation metrics. As a result, a comparison among methods remains challenging, as does the selection of the model that best suits a particular application.

[†] Di Feng and Ali Harakeh contributed equally to this work. Listing order is random.

[1] Institute of Measurement, Control and Microtechnology, Ulm University, 89081 Ulm, Germany.

[2] Toronto Robotics and Artificial Intelligence Laboratory, University of Toronto Institute for Aerospace Studies (UTIAS), Toronto, Canada.

Corresponding author: di.feng@uni-ulm.de

Article

Cloud Computing Security management in data analysis: A Survey

Dr K Seshadri Ramana, Abdallah , Muhammad Ajas

G.Pullaiah college of engineering and technology

E-Mail:seshadriramanacse@gmail.com department of computer science and engineering.
email : abdallahshaik@gmail.com

Abstract: Cloud computing is an emerging technology paradigm that migrates current technological and computing concepts into utility-like solutions similar to electricity and water systems. Clouds bring out a wide range of benefits including configurable computing resources, economic savings, and service flexibility. However, security and privacy concerns are shown to be the primary obstacles to a wide adoption of clouds. The new concepts that clouds introduce, such as multi-tenancy, resource sharing and outsourcing, create new challenges to the security community. Addressing these challenges requires, in addition to the ability to cultivate and tune the security measures developed for traditional computing systems, proposing new security policies, models, and protocols to address the unique cloud security challenges. In this work, we provide a comprehensive study of cloud computing security and privacy concerns. We identify cloud vulnerabilities, classify known security threats and attacks, and present the state-of-the-art practices to control the vulnerabilities, neutralize the threats, and calibrate the attacks. Additionally, we investigate and identify the limitations of the current solutions and provide insights of the future security perspectives. Finally, we provide a cloud security framework in which we present the various lines of defense and identify the dependency levels among them. We identify 28 cloud security threats which we classify into five categories. We also present nine general cloud attacks along with various attack incidents, and provide effectiveness analysis of the proposed countermeasures.

Attacks and Their Defensesin the Internet of Things :A Case Study

M.Sri Lakshmi ,Dept of *cse department,* poojitha

Email: srilakshmicse@gmail.com

***Abstract*—The emerging Internet-of-Things (IoT) are vulnerable to Sybil attacks where attackers can manipulate fake identities or abuse pseudoidentities to compromise the effectiveness of the IoT and even disseminate spam. In this paper, we survey Sybil attacks and defense schemes in IoT. Specifically, we first define three types Sybil attacks: SA-1, SA-2, and SA-3 according to the Sybil attacker's capabilities. We then present some Sybil defense schemes, including social graph-based Sybil detection (SGSD), behavior classification-based Sybil detection (BCSD), and mobile Sybil detection with the comprehensive comparisons. Finally, we discuss the challenging research issues and future directions for Sybil defense in IoT.**

***Index Terms*—Behavior classification, Internet of Things (IoT), mobile social network, social network, Sybil attack.**

I. Introduction

INTERNET-OF-THINGS (IoT), which can expand the traditional Internet to a ubiquitous network connecting objects in the physical world, starts an evolution to enhance the interaction among people and the objects. With the embedded sensors on objects, IoT can sense the information from the environments, the objects and our body (via sensor network, radio-frequency identification (RFID) technique, wearable devices, etc.) [1]–[3]. With the emerging wireless communication techniques, such as short-range wireless communications and WiFi, IoT can enable users to share information with others [4], [5] in social network and the Internet of connected vehicles [6], [7]. Furthermore, by integrating the sensing, communication, and computation capabilities [8], [9], IoT can offer diverse intelligent services [10] to form smart home [11], smart grid [12]–[14], smart community [15], and smart city [16], [17], as shown in Fig. 1. Therefore, as the advancement of IoT technology, these value-added applications flourish to facilitate people to interact with objects, people, and the world, and change the way we communicate with each other.

However, the emerging IoT is vulnerable to Sybil attacks where attackers can manipulate fake identities [18]–[20] or abuse pseudoidentities to compromise the effectiveness of the systems. In the presence of Sybil attacks, the IoT systems may generate wrong reports, and users might receive spam and lose their privacy. From a recent report [21] in 2012, a substantial number of user accounts are confirmed as fake or Sybil accounts in online social networks (OSNs), totally 76 million (7.2%) in Facebook, and 20 million fake accounts created in Twitter per week. These Sybil accounts not only spread spam and advertisements, but also disseminate malware and fishing websites to others to steal other users' private information. In addition, in a distributed vehicular communication system [22] and mobile social systems [23], Sybil attackers generate biased options with "legible" accounts. Without an effective detection mechanism, the collective results will be easily manipulated by the attackers. Since most Sybil attackers behave similarly to normal users, to find out whether an account is Sybil or not is extremely difficult, which makes Sybil defense of paramount importance in the IoT.

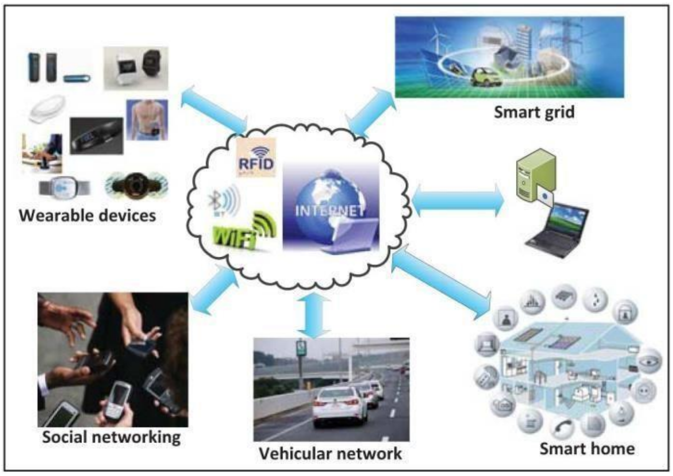


Fig. 1. Overview of IoT.

Recent research efforts [24], [25] have been focused on studying Sybil attacks and how to detect and defend them. SybilGuard [24], a social graph (network)-based Sybil detection scheme, explores random walk to partition the whole social graph into honest regions and Sybil one which contains Sybil nodes within it. SybilGuard relies on the assumption that Sybil nodes can only build a limited number of social connections with the honest nodes. Alternatively, according to different behaviors, such as clickstream, of normal and Sybil users, a behavior classification-based Sybil detection (BCSD) scheme is proposed in [26]. From the observation

Manuscript received March 01, 2014; revised June 29, 2014; accepted July 11, 2014. Date of publication July 30, 2014; date of current version October 21, 2014. This work was supported by the Natural Science and Engineering Research Council (NSERC) of Canada, under a research grant.

K. Zhang and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: k52zhang@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

X. Liang is with the Department of Computer Science, Dartmouth College, Hanover, NH 03755-3510 USA (e-mail: xiaohui.liang@dartmouth.edu).

R. Lu is with the School of Electrical and Electronics Engineering, Nanyang Technological University, 639798 Singapore (e-mail: rxlu@ntu.edu.sg).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JIOT.2014.2344013