International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Review Paper Volume-9, Issue-12, 2022 Regular Edition E-ISSN: 2349-7084

A Study of Heterogeneity Characteristics over Wireless Sensor Networks

K. Sandhya Rani

Associate Professor, Department of CSE

G. Pullaiah College of Engineering and Technology, Kurnool

Received: 28/10/2022, Revised: 21/11/2022, Accepted: 24/12/2022, Published: 30/12/2022

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.
Low-energy adaptive clustering hierarchy (LEACH) by Heinemann addressed efficient clustering and node energy constraints in a homogenous environment [11].

LEACH is an adaptive and self-organizing clustering algorithm that selects the cluster heads randomly based on the residual energy. LEACH prolongs the network's lifespan by significantly reducing energy utilization. LEACH protocol execution has two steps, namely the setup and study state phases. In the setup phase, each node is organized and forms a cluster by selecting one cluster head. In each round, the possibility of the node becoming the cluster head is 1/total number of rounds, and the cluster head will change the node's energy balance, which prolongs the network's lifetime. LEACH, a dependable protocol, performs computations

© 2019 IJSRST | Volume 6 | Issue 1 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Capability of Multi Keyword investigation in Cloud Computing

K. Gayathri, Y. Supriya
G. Pullaiah College of Engineering and Technology, Department of CSE, Kurnool, Andhra Pradesh, India

ABSTRACT

Cloud computing is enormous technical development of this modern era which offers variety of services to satisfy the needs of multiple users. The Cloud service providers charge depending on the user's usage. Imposing confidentiality and scalability on cloud data increases the complexity of cloud computing. Cloud technology has various advantages such as high availability, storage, fast data retrieval, it still has a limitation to overcome which is known as security as sensitive information is centralized into the cloud, and this information must be encrypted and uploaded to cloud for the data privacy and efficient data utilization. As the data becomes complex and number of users are increasing searching of the files must be allowed through multiple keyword of the end users interest. The traditional searchable encryption schemes allows users to search in the encrypted cloud data through keywords, which support only search, i.e., whether a keyword exists in a file or not, without any relevance of data files and the queried keyword. Searching of data in the cloud using Single keyword ranked search results too coarse output and the data privacy is opposed using server side ranking based on order-preserving encryption. In this paper, an efficient clustering technique is used to retrieve encrypted cloud data for multiple related keywords.

Keywords : Cloud Computing, Attribute-Based Encryption, File Hierarchy Document Retrieval.

I. INTRODUCTION

An ever increasing number of individuals and endeavours are inspired to re-appropriate their nearby archive the executives frameworks to the cloud which is a promising data system (IT) to process the unstable extending of information In spite of the benefits of cloud administrations, releasing the delicate data, for example, individual data, organization money related information and government archives, to people in general is a major danger to the information proprietors. Moreover, to make full utilization of the information on the cloud, the information clients need to get to them adaptable and effectively. An instinctive methodology is scrambling the records first and after that re-appropriating the encoded archives to the cloud.

Ranked search can also elegantly eliminate unnecessary network traffic by sending back only the most relevant data, which is highly desirable in the "pay-as-you use" cloud paradigm. For privacy rotation, such ranking operation, however, should not leak any keyword related information. On the other hand, to improve search result accuracy as well as to enhance the user searching experience, it is also crucial for such ranking system to support multiple keywords search, as single keyword search often yields far too coarse result. As a common practice indicated by today's web search engines (e.g., Google search), users may tend to provide a set of keywords instead of only one as the indicator of their search interest to retrieve the most relevant data. Searchable encryption schemes usually build up an index for

Study of Query Optimization in Cloud

Y. Supriya
DV Srilakshmi, Husna Fatima, DSVN Ramya
G. Pullaiah college of Engineering and Technology, Department of CSE, Kurnool, Andhra Pradesh, India

ABSTRACT

Cloud computing in very simple terms, is basically where a company uses someone else's computing services (usually over the internet) instead of having to run that software on their own computers. Today, cloud computing plays an important role in service-oriented technologies. The main purpose of cloud computing is, it allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access and it allow users to easily and efficiently calculate and save resources. The recent approach is to process data expression and search. To improve cloud performance, it is necessary to optimize the processing time. Our research provides a comprehensive overview of the different models and methods used to optimize queries to reduce execution time and improve resource utilization. We conducted various query optimization research activities for the classic SQL and Map Reduce platforms.

Keywords : Cloud Computing, Map-Reduce, Service Level Agreement, Query optimization, Conventional SQL.

I. INTRODUCTION

Cloud computing is a very successful paradigm for service-oriented computing [1]. The most popular cloud services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Expanding this concept is a Database as a Service (DBaaS) or Storage as a Service. Cloud computing improves common computer and storage capacity for a number of database applications. "The observed number of applications that have affected multiple platforms in the clouds has greatly increased the amount of data generated and used by these applications" [2]. "Cloud is the basis for cloud computing applications and search algorithm and cloud organization and search algorithm." The new research topic was how to organize and manage this huge amount of data. Get users useful information about cloud computing "it's the core of the cloud application" [3] How to get data fast, accurate and secure Play an important role in a successful job data model in the cloud. In cloud computing, resources need to be automatically and quickly acquired and released during business hours to provide Service Level Agreements (SLAs) between the client and the cloud provider [4]. Using virtual machine clusters, cloud computing users can rent large amounts of resources for a short period of time to effectively execute large-scale complex queries [5]. Lease duration can be further reduced by using better query optimization techniques [6]. Therefore, it is necessary to investigate effective query optimization techniques to reduce query time and response time. It will also improve the use of computing resources in the cloud. "Query optimization leads to optimization of resource lease time in the cloud environment". Query optimization techniques in centralized and distributed platforms are extensively researched in conventional SQL and Map Reduce methods. An example of processing a request in the cloud is shown

© 2018 IJSRST | Volume 4 | Issue 8 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

An Effective QoS based Route Optimization Model in MANET using Machine Learning

M. Janardhan
Department of Computer Science and Engineering, G Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India

ABSTRACT

Mobile Ad hoc network is a network which is dynamic where the mobile nodes form a temporary network in the deficiency of centralized administration, i.e. A MANET is an autonomous group of distributed mobile nodes. Due to the absence of centralized administrator in a network, routing in mobile ad hoc network (MANET) becomes the primary issue which reduces the selection of an optimal path for routing. Specific performance parameters such as latency, overhead, and packet delivery ratio (PDR) are affected unfavorably for which various techniques such as Machine Learning approach are encouraged that enhances the selection of the efficient and stable path. In our, Proposed Research works our attempt is made to select the optimal route i.e. which supports to identify the pattern for Link failure in communication and Optimized routing path for better communication to achieve the QoS for MANET environment using knowledge-based learning algorithm. The optimal path will possess the highest average sum of relay nodes and will be considered as the most optimal and reliable path. We also anticipated that analysis of throughput and PDR is better as compared to the traditional methods.

Keywords : Routing Protocols, Internal Attacks, External Attacks, Manets

I. INTRODUCTION topology and produces better throughput and low delay variance. Again flooding of route request

There are research contribution exist in routing may potentially reach all nodes in the network, so mechanisms of MANETS by considering the QoS bandwidth wastage increases and efficiency parameters. degrades. Besides this, it is a collision and

- ✓ Ant Colony Based QoS Routing Algorithm for contention prone routing protocol. Thus, packet Mobile AdHoc Networks is an on-demand QoS delivery ratio decreases, congestion increases and routing algorithm [1] proposed by throughput also become very poor in case of P.Deepalakshmi. This algorithm is adaptive in multimedia. The routing overhead is also nature and reduces the end to end delay in high increased.

  mobility cases. But the other QoS constraints i.e. ✓ An on-demand routing protocol Ant-E [3] is other network layer or link layer metrics like introduced by Srinivas Sethi which is based on energy, jitter, link stability etc. are not considered Blocking Expanding Ring Search (Blocking-ERS) here. Furthermore, here link failure is not handled to control the overhead and local retransmission properly. to improve the reliability. It resumes its route
- ✓ Metrics in Mobile Ad Hoc Networks proposed by Discovery process to discover a route to the R. Asokan [2] and it performs well in route destination node from the place where it ended in discovery phase with dynamically changing

QOS Based Route Optimization Model in Manet

K. Lakshmi

Assistant Professor, Department of Computer science and Engineering, G. Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India

ABSTRACT

The primary objective of this paper is to develop specific evolutionary algorithms using Machine learning approach to enhance the selection of efficient and stable optimized routing path in MANET with a guarantee on QoS parameters. The primary QoS constraints considered include delay delay - jitter, bandwidth and packet loss rate for computing the possible network route. The essential characteristics of this routing process such as the accuracy, interpretability, robustness and versatility have been considered while calculating the workable routing path for MANETs. To attain this Machine learning techniques play vital, role in identify patterns such as optimized routing path and node-link failure detection which leads other than QoS and energy efficiency, security which attracts many researchers.

1. To develop an innovative mechanism for the feasible path selection of the given network with a guarantee on QoS metrics.
2. To identify the optimized routing patterns using Machine learning Approach to achieve an effective routing mechanism for dynamic, scalable networks.
3. To Identify the Pattern for Node link failure among MANET by Machine Learning to handle the link failure in dynamic networks which establish the communication efficiency .
4. Develop a secure authentication mechanism for improving the security in MANETs

Keywords : MANET, QOS, Routing Mechanism, Machine Learning Techniques.

I. INTRODUCTION

Mobile Ad hoc network is a network which is dynamic where the mobile nodes form a temporary network in the deficiency of centralized administration, i.e. A MANET is an autonomous group of distributed mobile nodes. Due to the absence of centralized administrator in a network, routing in mobile ad hoc network (MANET) becomes the primary issue which reduces the selection of an optimal path for routing. Specific performance parameters such as latency, overhead, and packet delivery ratio (PDR) are affected unfavourably for which various techniques such as Machine Learning approach are encouraged that enhances the selection of the efficient and stable path. In our, Proposed Research works our attempt is made to select the optimal route i.e. which supports to identify the pattern for Link failure in communication and Optimized routing path for better communication to achieve the QoS for MANET environment using knowledge-based learning algorithm. The optimal path will possess the highest average sum of relay nodes and will be considered as the most optimal and reliable path. We also anticipated that analysis of throughput and PDR is better as compared to the traditional methods.

II. RELATED WORK

The following are the contribution exists in routing mechanisms of MANETS by considering the QoS parameters.

Machine Learning for internet of Thing: Smart City

D. Jayanarayana Reddy
C.Abhinay ,K.Vamshi ,G.Dinesh

G . Pullaiah College Of Engineering and Technology,
Andhra Pradesh ,Kurnool,India.

Pakistan; munir@ncbae.edu.pk (M.A.); syedshehryar@live.com (S.S.A.)
- Department of Business Administration, Faculty of Economics and Administrative Sciences, The Hashemite University, Zarqa 13115, Jordan; barween@hu.edu.jo
- Department of Information Systems, College of Computing and Informatics, University of Sharjah, Sharjah 27272, United Arab Emirates; iakour@sharjah.ac.ae

* Correspondence: haitham.alzubi@skylineuniversity.ac.ae

Abstract: Smart city is a collective term for technologies and concepts that are directed toward making cities efficient, technologically more advanced, greener and more socially inclusive. These concepts include technical, economic and social innovations. This term has been tossed around by various actors in politics, business, administration and urban planning since the 2000s to establish tech-based changes and innovations in urban areas. The idea of the smart city is used in conjunction with the utilization of digital technologies and at the same time represents a reaction to the economic, social and political challenges that postindustrial societies are confronted with at the start of the new millennium. The key focus is on dealing with challenges faced by urban society, such as environmental pollution, demographic change, population growth, healthcare, the financial crisis or scarcity of resources. In a broader sense, the term also includes nontechnical innovations that make urban life more sustainable. So far, the idea of using IoT-based sensor networks for healthcare applications is a promising one with the potential of minimizing inefficiencies in the existing infrastructure. A machine learning approach is key to successful implementation of the IoT-powered wireless sensor networks for this purpose since there is large amount of data to be handled intelligently. Throughout this paper, it will be discussed in detail how AI-powered IoT and WSNs are applied in the healthcare sector. This research will be a baseline study for understanding the role of the IoT in smart cities, in particular in the healthcare sector, for future research works.

Keywords: smart cities; IoT; machine learning; sensor networks; artificial intelligence; healthcare

---

Future Internet **2021**, *13*, 218. https://doi.org/10.3390/fi13080218 https://www.mdpi.com/journal/futureinternet The work of specialists, for example, that of a radiologist, will also change as a result. Especially with imaging processes that can be easily evaluated and standardized technically, the technology is already doing a remarkable job. Since it has evaluated millions of cases, it can judge with greater accuracy than the treating doctor with the naked eye. Even if the decision-making authority will always remain with the doctor, thanks to artificial intelligence he will receive a valuable second opinion that can underpin his own anamnesis or add further aspects.

The more data the system has from the patient himself and the more other cases it knows, the more certain the statements and recommendations for action will be. It will therefore be desirable in the future to have as much data as possible available and to evaluate it, considering all anonymization measures. In general, data from wearables in everyday diagnostics will support the patient and the treating doctor in making the right decisions more quickly and making recommendations for action. For example, a patient who wakes up in the morning with an increased pulse and blood pressure can better decide whether to see a doctor or whether the malaise is likely to go away on its own in the course of the morning.

The challenge we face today is that we are struggling with various interfaces between medical subsystems that have to ensure interoperability with one another. With the help of a blockchain, patient data records can be standardized, reliably exchanged, evaluated and stored in a forgery-proof manner. This means that those responsible for medical data do not have to harmonize several different systems in parallel, but can rely on a reliable standard [1]. A blockchain as a basic technology will also be used in other industries and sectors where the exchange of reliable, unchangeable data is important. We would be an important step closer to the digital patient file,

ISSN: e-ISSN: 2395-0056

IOT Based Weather Monitoring

D. Jayanarayana Reddy
C.Abhinay Sunny ,K.Vamshi Krishna ,G.Sai Vishal.

**G . Pullaiah College Of Engineering and Technology,
Andhra Pradesh ,Kurnool,India**

Girija C
Department of Electronics and Communication, NIEIT, Mysuru

Andreanna Grace Shires
Department of Electronics and Communication, NIEIT, Mysuru

***Abstract*- The system proposed in this paper is an advanced solution for monitoring the weather conditions at a particular place and make the information visible anywhere in the world. The technology behind this is Internet of Things (IoT), which is an advanced and efficient solution for connecting the things to the internet and to connect the entire world of things in a network. Here things might be whatever like electronic gadgets, sensors and automotive electronic equipment. The system deals with monitoring and controlling the environmental conditions like temperature, relative humidity and CO level with sensors and sends the information to the web page and then plot the sensor data as graphical statistics. The data updated from the implemented system can be accessible in the internet from anywhere in the world.**

Keywords- Internet of Things (IoT) Embedded Computing System; Arduino Software, ESP8266, Smart Environment.

I. INTRODUCTION

The internet of Things (IoT) is viewedas an innovation and financial wave in the worldwide data industry after the Internet. The IoT is a wise system which associates all things to the Internet with the end goal of trading data and conveying through the data detecting gadgets as per concurred conventions. It accomplishes the objective of keen recognizing, finding, following, observing, and overseeing things . It is an augmentation and extension of Internet-based system, which grows the correspondence from human and human to human and things or things and things. In the IoT worldview, many articles encompassing us will be associated into systems in some shape . It is a current correspondence paradigm that envisions a near future, in which the objects of regular day to day existence will be outfitted with microcontrollers, handsets for computerized correspondence, and reasonable convention stacks that will make them ready to speak with each other and with the clients, turning into a vital piece of the Internet. The IoT idea,consequently, goes for making the Internet much more immersive and unavoidable.Moreover, by empowering simple get to and association with a wide assortment of gadgets, for example, for example, home apparatuses, reconnaissance cameras, checking sensors, actuators, showcases, vehicles, et cetera, the IoT will encourage the advancement of various applications that make utilization of the possibly gigantic sum and assortment of information created by such questions give new

Harshalatha H
Department of Electronics and Communication, NIEIT, Mysuru

Pushpalatha H P
Department of Electronics and Communication, NIEIT, Mysuru

administrations to subjects, organizations, and open organizations. Present innovations in technology mainly focus on controlling and monitoring of different activities. These are increasingly emerging to reach the human needs. Most of this technology is focused on efficient monitoring and controlling different activities. An efficient environmental monitoring system is required to monitor and assess the conditions in case of exceeding the prescribed level of parameters (e.g., noise, CO and radiation levels). When the objects like environment equipped with sensor devices, microcontroller and various software applications becomes a self-protecting and selfmonitoring environment and it is also called as smart

ISSN NUMBER:1076-5131

Industrial IOT in Education

D. Jayanarayana Reddy
C.Sai Sunny ,K.Krishna ,G.Vishal.

G . Pullaiah College Of Engineering and Technology, Andhra Pradesh ,Kurnool,India

***Abstract*—This paper is aimed to examine the adoption of the Internet of Things (IoT) in industry (so-called Industrial Internet of Things, shortly IIoT) and the requirements for higher education in the times of the fourth industrial revolution. The addition of the fourth letter, "I" in front of the "IoT" coins the name of the new concept, "IIoT" in relation with another term, "Industry 4.0". Because these concepts have no precise and widely accepted definitions, we presented some considered relevant by scientific literature. The paper also highlights the most important similarities and differences between these concepts. IIoT is a very dynamic concept and it will constantly bring changes in digital technologies, requirements and markets, and will also transform industries and business practices. According to manifold studies, currently, there is a skill gap which may widen in the future if no action is taken. Higher education must adopt the latest related technologies and must adapt to the new ways in which people, machines, services and data can interact. Consequently, employees, students, graduates, etc. have to be equally dynamic in learning and acquiring new skills. The transition from higher education to employment is a challenge that could be more easily addressed through the efforts of all stakeholders, from individuals to organizations, and from businesses to governments. As changes in higher education take time, all stakeholders will now have to act in preparing for the Industrial Internet of Things.**

Keywords—Industry 4.0; Industrial Internet of Things; Internet of Things; higher education; skills gap

I. INTRODUCTION

Industrial engineering is constantly bound to adapt to the many occurring changes, from progress in business models to the most advanced information and communications technologies; the purpose is to increase the overall quality of products and productivity, and also to reduce overall costs. Currently, we are witnessing the rise of a new digital industrial wave, namely the fourth industrial revolution (IR 4.0 or FIR), enabled by the widespread deployment of inexpensive smart sensors, processors, wireless sensor networks, embedded systems, but also by the advances in data storage, analytics, cloud infrastructure, and so on. Various worldwide surveys conducted in relation to the industry field reveal that the biggest current technological initiative for implementing this revolution is the Industrial Internet of Things (IIoT).

In a report [1], Accenture estimates that the Industrial Internet of Things could add $14.2 trillion to the global economy by 2030. The global Industrial Internet of Things market is anticipated to expand at a CAGR of +24% during the 2018-2022 [2]. A McKinsey report [3] anticipates that by 2025, the percentage of factories adopting IIoT will reach 65%-90% in advanced economies and 50%-70% in developing economies.

Researchers estimate that the IIoT development will impact different sectors, influencing both the industry and the labor market, leading to the creation of new jobs, but also to the elimination of some existing ones. Thus, various studies on technology uptake conducted in different countries reveal that the adoption of new technologies is expected to have a significant impact on the employment landscape. For example, according to [4], ―in many industries and countries, the most in-demand occupations or specialties did not exist 10 or even five years ago, and the pace of change is set to accelerate‖. The same report estimates that ―65% of children entering primary school today will ultimately end up working in completely new job types that don't yet exist‖. This is also the case of the Industrial Internet of Things. Various publications have focused their attention on this new concept, analyzing, among others, both the multiple possible benefits and challenges generated by the application of this paradigm across different economies. In addition to the technological barriers, the widespread and accelerated adoption of the Internet of Things (IoT) paradigm in the industrial field is hampered by the skills gap. According to manifold studies, currently, there is a skills gap which may widen in the future if no action is taken. For example, an analysis from Deloitte [5] reveals that over the next decade, there will be 3.5 million job openings in manufacturing, but only enough skilled labor to fill less than half of them. And as IIoT growth takes hold, the need for skilled workforce will intensify. One solution to reduce the skills gap lies in education, for example through effective skills, re- and up-skilling programmes. IIoT is a very dynamic concept and it will constantly bring changes in digital technologies, requirements and markets, and will also transform industries and business practices. Consequently, employees, students, graduates, etc. have to be equally dynamic in learning and acquiring new skills. Higher education must adopt the latest related technologies and must adapt to the new ways in which people, machines, services and data can interact.

This paper is concerned specifically with the importance of higher education in supporting the development of the skills and competencies required for the Industrial Internet of Things era. Currently, the pictures of Internet of Things, Industrial Internet of Things and Industry 4.0 are still quite blurry. Although IoT, IIoT and Industry 4.0 are closely related concepts, they cannot be interchangeably used. So far, there is no generally accepted definition for each of these terms and in an attempt to understand these concepts, this paper tries to clarify them. The literature in the field proposes several definitions, some of them being presented in a section of this

Enhancing Social Media Services using Machine Learning

M. Janardhan

Department of Computer Science and Engineering
G. Pullaiah College of Engineering and Technology, Kurnool,
Andhra Pradesh-India

Abstract: Network analysis aids management in reducing overall expenditures and maintenance workload. Social media platforms frequently use neural networks to suggest material that corresponds with user preferences. Machine learning is one of many methods for social network analysis. Machine learning algorithms operate on a collection of observable features that are taken from user data. Machine learning and neural network-based systems represent a topic of study that spans several fields. Computers can now recognize the emotions behind particular content uploaded by users to social media networks thanks to machine learning. This study examines research on machine learning and neural networks, with an emphasis on social analysis in the context of the current literature.

Keywords: social media; artificial neural networks; machine learning; social networks

1. Introduction

Machine learning is a process of autonomous learning that occurs through the processing of typically very large data sets according to a statement by L'heureux et al. [1]. The techniques of the past, referred to as "symbolic artificial intelligence (AI)," were based on algorithms consisting of logical sets of instructions for encoding a given output (typically referred to as the target) for all potential inputs. In contrast, the new machine learning algorithms "learn" directly from data and estimate mathematical functions that discover representations of an input or learn to link one or more inputs to one or more outputs to make predictions using new data [2].

In recent years, the application of machine learning has gained traction across various disciplines in the social sciences. For instance, in the field of economics, researchers such as Varian [3], Blumenstock et al. [4], Athey and Imbens [5], and Mullainathan and Spiess [6] have incorporated machine learning methods into their studies. Similarly, in political science, Bonikowski and DiMaggio [7] have explored the use of machine learning techniques. In sociology, scholars such as Baldassarri and Abascal [8] and Evans and Aceves [9] have applied machine learning in their research. Communication science has also embraced machine learning with studies conducted by Bail [10]. Furthermore, machine learning has found practical applications in the public administration sector (Athey [5] and Berk et al. [11]), as well as in the operations of private companies.

Kleinberg et al. [12] state that machine learning encompasses a wide variety of approaches and instruments. The function of user-generated content, which is also subject to feedback from other users [13,14], is expanding as a result of the proliferation of social media. Given that social networking sites (SNSs) offer abundant opportunities for social comparison [15], researchers have begun to investigate their implications for psychological health [16]. By spending a great deal of time observing the posts of others, users are inevitably drawn into the process of social comparison, particularly when using SNSs devoted to visual content, such as Instagram [17]. Social comparison research investigates

International Journal of Scientific Research in Science and Technology

Artificial Intelligence in the Field of Medicine

M Janardhan

C Jayanthi, G Roopa, H Nandini

Department of Computer Science and Engineering

G Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India

ABSTRACT

Background: Artificial intelligence (AI) is the term used to describe the use of computers and technology to simulate intelligent behavior and critical thinking comparable to a human being. John McCarthy first described the term AI in 1956 as the science and engineering of making intelligent machines. **Objective:** This descriptive article gives a broad overview of AI in medicine, dealing with the terms and concepts as well as the current and future applications of AI. It aims to develop knowledge and familiarity of AI among primary care physicians. **Materials and Methods:** PubMed and Google searches were performed using the key words 'artificial intelligence'. Further references were obtained by cross-referencing the key articles. **Results:** Recent advances in AI technology and its current applications in the field of medicine have been discussed in detail. **Conclusions:** AI promises to change the practice of medicine in hitherto unknown ways, but many of its practical applications are still in their infancy and need to be explored and developed better. Medical professionals also need to understand and acclimatize themselves with these advances for better healthcare delivery to the masses.

Keywords: Artificial intelligence, future of medicine, machine learning, neural networks, robots

Introduction

Alan Turing (1950) was one of the founders of modern computers and AI. The "Turing test" was based on the fact that the intelligent behavior of a computer is the ability to achieve human level performance in cognition related tasks.[1] The 1980s and 1990s saw a surge in interest in AI. Artificial intelligent techniques such as fuzzy expert systems, Bayesian networks, artificial neural networks, and hybrid intelligent systems were used in different clinical settings in health care. In 2016, the biggest chunk of investments in AI research were in healthcare applications compared with other sectors.[2]

AI in medicine can be dichotomized into two subtypes: Virtual and physical.[3] The virtual part ranges from applications such as electronic health record systems to neural network-based guidance in treatment decisions. The physical part deals with robots assisting in performing surgeries, intelligent prostheses for handicapped people, and elderly care.

The basis of evidence-based medicine is to establish clinical correlations and insights via developing associations and patterns from the existing database of information. Traditionally, we used to employ statistical methods to establish these patterns and associations. Computers learn the art of diagnosing a patient via two broad techniques - flowcharts and database approach.

The flowchart-based approach involves translating the process of history-taking, i.e. a physician asking a series of questions and then arriving at a probable diagnosis by combining the symptom complex presented. This requires feeding a large amount of data into machine-based cloud networks considering the wide range of symptoms and disease processes encountered

in routine medical practice. The outcomes of this approach are

Load Balancing in a Networking

M. Janardhan
A. Pooja, B. Pavani, B. Likitha
Department of Computer Science and Engineering
G. Pullaiah College of Engineering & Technology, Kurnool,
Andhra Pradesh - India

ABSTRACT
Load balancing is a way to spread tasks out over multiple resources. By processing tasks and directing sessions on different servers, load balancing helps a network avoid annoying downtime and delivers optimal performance to users. There are virtual load balancing solutions that work in a manner similar to virtual applications or server environments. There are also physical load balancing hardware solutions that can be integrated with a network. The method used depends entirely upon the team implementing the solution and their particular needs. **Network Load Balancing (NLB)** is a clustering technology offered by Microsoft as part of all Server and Windows Server 2003 family operating. NLB uses a distributed algorithm to load balance network traffic across a number of hosts, helping to enhance the scalability and availability of mission critical, IP -based services, such as Web, virtual private networking, streaming media, terminal services, proxy and so on. It also provides high availability by detecting host failures and automatically redistributing traffic to operational hosts. This paper describes the detailed architecture of network load balancing, various types of addressing and the various performance measures. ***Keywords:-*** Addressing, Load balancing, Network, performance.

I. INTRODUCTION

Network load balancing is an efficient and cost-effective solution designed to enhance the availability and scalability of Internet applications by allowing system administrators to build clusters, which are load balanced with incoming client requests. During NLB, clients cannot distinguish the cluster from a single server. Server programs are also unaware that a cluster is running.

As a result of this setup, NLB allows for greater overall control, including remote cluster management from any network point. Administrators can tailor clusters to services with port-defined controls. Cluster hosts and software may be modified without service interruption.
NLB sends regular messages, allowing all cluster members to monitor the other hosts' presence. Host failures and recovery are handled automatically and quickly. NLB's software implementation requires extremely low overhead to handle network traffic. The process delivers excellent performance scaling, which is limited only by subnet bandwidth.

Network Load Balancing provides scalability and high availability to enterprise-wide TCP/IP services, such as Web, Terminal Services, proxy, Virtual Private Networking (VPN), and streaming media services. Network Load Balancing brings special value to enterprises deploying TCP/IP services, such as e-commerce applications, that link clients with transaction applications and back-end databases.
Network Load Balancing servers (also called *hosts*) in a cluster communicate among themselves to provide key benefits, including:

- **Scalability:** Network Load Balancing scales the performance of a server-based program, such as a Web server, by distributing its client requests across multiple servers within the cluster. As traffic increases, additional servers can be added to the cluster, with up to 32 servers possible in any one cluster.

- **High availability:** Network Load Balancing provides high availability by automatically detecting the failure of a server and repartitioning client traffic among the remaining servers within ten seconds, while providing users with continuous service.

  Network Load Balancing distributes IP traffic to multiple copies (or *instances*) of a TCP/IP service, such as a Web server, each running on a host within the cluster. Network Load Balancing transparently partitions the client requests among the hosts and lets the client's access the cluster using one or more "virtual" IP addresses [1]. From the client's point of view, the cluster appears to be a single server that answers these client requests. As enterprise traffic increases, network administrators can simply plug another server into the cluster.

  For example, the clustered hosts in Fig. 1 below work together to service network traffic from the Internet.
  Each server runs a copy of an IP-based service, such as Internet Information Services 5.0 (IIS), and Network Load Balancing distributes the networking workload among them.

Hindawi
Journal of Healthcare Engineering
Volume 2023, Article ID 6992441, 11 pages
https://doi.org/10.1155/2023/6992441

Research Article

Clinical Decision Support System for Diabetic Patients by Predicting Type 2 Diabetes Using Machine Learning Algorithms

Rakibul Islam,[1] **Azrin Sultana**,[1] **Md. Nuruzzaman Tuhin**,[1] **Md. Sazzad Hossain Saikat**,[1] **and Mohammad Rashedul Islam**[2,3]

[1]*Department of Computer Science, American International University-Bangladesh, Dhaka 1229, Bangladesh*
[2]*Department of Research & Training Monitoring, Bangladesh College of Physicians and Surgeons, Dhaka 1212, Bangladesh*
[3]*Department of Health Informatics, Bangladesh University of Health Sciences, Dhaka 1216, Bangladesh*

Correspondence should be addressed to Rakibul Islam; rakibulislam.cse21@gmail.com

Received 5 September 2022; Revised 29 December 2022; Accepted 17 February 2023; Published 30 May 2023

Academic Editor: Kuruva Lakshmanna

Diabetes is one of the most serious chronic diseases that result in high blood sugar levels. Early prediction can significantly diminish the potential jeopardy and severity of diabetes. In this study, different machine learning (ML) algorithms were applied to predict whether an unknown sample had diabetes or not. However, the main significance of this research was to provide a clinical decision support system (CDSS) by predicting type 2 diabetes using different ML algorithms. For the research purpose, the publicly available Pima Indian Diabetes (PID) dataset was used. Data preprocessing, K-fold cross-validation, hyperparameter tuning, and various ML classifiers such as K-nearest neighbor (KNN), decision tree (DT), random forest (RF), Naïve Bayes (NB), support vector machine (SVM), and histogram-based gradient boosting (HBGB) were used. Several scaling methods were also used to improve the accuracy of the result. For further research, a rule-based approach was used to escalate the effectiveness of the system. After that, the accuracy of DT and HBGB was above 90%. Based on this result, the CDSS was implemented where users can give the required input parameters through a web-based user interface to get decision support with some analytical results for the individual patient. The CDSS, which was implemented, will be beneficial for physicians and patients to make decisions about diabetes diagnosis and offer real-time analysis-based suggestions to improve medical quality. For future work, if daily data of a diabetic patient can be put together, then a better clinical support system can be implemented for daily decision support for patients worldwide.

1. Introduction

A CDSS can be a blessing in the field of chronic diseases like diabetes. The capacity, complexity, and dynamic behavior of clinical info are a challenge for doctors and other health professionals. CDSS seeks to favor the physicians as well as the patients by providingreal-time feedback regarding health conditions [1].

Diabetes is a chronic metabolic condition marked by a recurrent rise in blood glucose levels. It is a global health priority that affects 463 million people, or one out of every eleven adults. This figure is anticipated to grow to 578 million by 2030 [2]. Diabetes is caused by several different pathogenic mechanisms. These can range from autoimmune death of pancreatic beta cells, resulting in insulin shortage, to anomalies that lead to insulin resistance. Due to the poor impact of insulin on target tissues, diabetes produces abnormalities in glucose, lipid, and protein metabolism. Insulin deficiency happens when the body does not make enough insulin and/or when tissues do not respond well enough to insulin at one or more points along the complicated path of hormone action. In many patients, reduced insulin secretion and impaired insulin movement coexist, and it is tough to inform which condition, if either, is the essential supply of hyperglycemia [3]. Diabetes is a category of metabolic disorders marked by hyperglycemia caused by

Zero-Injection: A Collaborative Filtering Recommender System for Exploiting Uninterested Items

B. Vijaya Lakshmi
Department of Computer Science and Engineering
G Pullaiah College of Engineering and Technology, Kurnool,
Andhra Pradesh, India

Abstract—We develop a novel framework, named as l-injection, to address the sparsity problem of recommender systems. By carefully injecting low values to a selected set of unrated user-item pairs in a user-item matrix, we demonstrate that top-N recommendation accuracies of various collaborative filtering (CF) techniques can be significantly and consistently improved. We first adopt the notion of pre-use preferences of users toward a vast amount of unrated items. Using this notion, we identify uninteresting items that have not been rated yet but are likely to receive low ratings from users, and selectively impute them as low values. As our proposed approach is method-agnostic, it can be easily applied to a variety of CF algorithms. Through comprehensive experiments with three real-life datasets (e.g., Movielens, Ciao, and Watcha), we demonstrate that our solution consistently and universally enhances the accuracies of existing CF algorithms (e.g., item-based CF, SVD-based CF, and SVD++) by 2.5 to 5 times on average. Furthermore, our solution improves the running time of those CF methods by 1.2 to 2.3 times when its setting produces the best accuracy. The datasets and codes that we used in the experiments are available at: https://goo.gl/KUrmip.

Index Terms—Recommender systems, collaborative filtering, data sparsity, uninteresting items, pre-use preference, post-use preference

1 Introduction

The goal of recommender systems (RS) is to suggest appealing items (e.g., movies, books, or news articles) to a user by analyzing her prior preferences. As a large number of online applications use RS as a core component, improving the quality of RS becomes a critically important problem to businesses. Among existing solutions in RS, in particular, collaborative filtering (CF) methods (e.g., [2], [3], [4], [5], [6], [7]) have been shown to be widely effective. Based on the past behavior of users such as explicit user ratings and implicit click logs, CF methods exploit the similarities between users' behavior patterns.

However, when the fraction of known ratings in a rating matrix R is overly small (so-called data sparsity problem), CF methods tend to suffer. For an R with m users and n items, if we assume that each user has rated k items on average, the fraction of rated items incally, such a fraction of rated items inR is $_{n}^{k}$R(=is extremely small$_{m=n}^{m=k}$Þ. Asymptoti-

(i.e., k n). It is common for an e-business to sell millions of items with a very long tail, and many users rate very few items (i.e., cold-start users). The goal of this work is to mitigate such a data sparsity problem to improve top-N recommendation accuracies of CF methods. Our proposal is based on the following hypothesis in CF:

Hypothesis 1. Filling some values into empty cells, i.e., unrated items, in a rating matrix R can improve the accuracy of CF methods for top-N recommendation.

We first argue that ratings in R be often a reflection of the satisfaction of users. Therefore, users tend to rate (high) only the items that they like, and those who are dissatisfied tend not to rate items in R. Corroborating this point, Table 1 illustrates severe imbalance between low (i.e., 1 or 2) and high (i.e., 3, 4, or 5) ratings from three real-life datasets that we used in our experiments. Note that only a small fraction (i.e., 10-17 percent) of ratings are low values. Then, a natural question to raise is: how can we identify the unknown opinions of those users who were dissatisfied with and did not leave ratings for items ?

To answer this question, note that unrated items in R can be classified into three different types: (1) unrated items whose existence users were not aware of, (2) unrated items that users knew and purchased but did not rate, and (3) unrated items that users knew but did not like and thus did not purchase. We note that the unrated items of the third type, called uninteresting items (denoted by I^{un}), clearly indicate users' latent negative preferences on them. Therefore, it is better not to recommend those uninteresting items.

J. Lee is with the Department of Software, Sungkyunkwan University,Suwon-si, Gyeonggi-do, Republic of Korea. E-mail: jongwuklee@skku.edu.

W.-S. Hwang, J. Parc, Y. Lee, and S.-W. Kim are with the Department ofComputer and Software, Hanyang University,Seongdong-gu, Seoul, Republic of Korea. E-mail: {hws23, crystaldia, utopianami, wook}@hanyang.ac.kr.

D. Lee is with the College of Information Sciences and Technology, ThePennsylvania State University, PA 16801. E-mail: dongwon@psu.edu.

Manuscript received 11 Sept. 2016; revised 7 Mar. 2017; accepted 15 Apr. 2017. Date of publication 27 Apr. 2017; date of current version 5 Dec. 2018. Recommended for acceptance by W. Lehner, J. Gehrke, and K. Shim. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below.
Digital Object Identifier no. 10.1109/TKDE.2017.2698461

EEG Sensors using Brain Waves for Ease of use and Better Security

C. Ayesha Shariff
G Meghana, B Ashritha, D Ramya
G. Pullaiah college of Engineering and Technology,
Department of CSE, Kurnool, Andhra Pradesh, India

Abstract:

Electroencephalography (EEG)-based brain-computer interfaces (BCIs), particularly those using motor-imagery (MI) data, have the potential to become groundbreaking technologies in both clinical and entertainment settings. MI data is generated when a subject imagines the movement of a limb. This paper reviews state-of-the-art signal processing techniques for MI EEG-based BCIs, with a particular focus on the feature extraction, feature selection and classification techniques used. It also summarizes the main applications of EEG-based BCIs, particularly those based on MI data, and finally presents a detailed discussion of the most prevalent challenges impeding the development and commercialization of EEG-based BCIs

1. INTRODUCTION

A complete picture of the brain structure will provide new insights into how the human brain functions and may facilitate new treatments and drug discovery for brain disorders. Recent advances in intact brain imaging, such as the CLARITY and MAP (Magnified Analysis of the Proteome) tissue clearing techniques, make it possible to collect large volumetric images of brain tissue at cellular and sub-cellular resolutions. The high throughput and high-resolution brain imagery, however, poses a challenge for efficient processing and analysis. We have developed an automated dense axonal fibber tracing pipeline that can track long-range fibbers and construct 3D connectivity maps, which include not only the vertices and edges of a network graph, but also the 3D location information associated with each fibres track.

In addition to typical graph analysis, we are interested in identifying long-range neuron fibres connections and fibres crossings, both of which could reveal informative patterns when analyzed at cellular resolution and at long range (≥ 1 mm). Brain graphs offer a framework to represent the structural or functional topology at multiple levels. A number of software tools exist for analysing topology of brain networks using graph theory. Few are designed for high throughput dense and long-range neuron analysis at the cellular level, which is critical for understanding brain circuits and for comparing healthy and diseased brains.

Mind reading and remote communication have their unique fingerprint in numerous fields such as educational, self-regulation, production, marketing, security as well as games and entertainment. It creates a mutual understanding between users and the surrounding systems. This paper shows the application areas that could benefit from brain waves in facilitating or achieving their goals. We also discuss major usability and technical challenges that face brain signals utilization in various components of BCI system. Different solutions that aim to limit and decrease their effects have also been reviewed.

2. LITERATURE SURVEY

2.1 THE NIH BRAIN INITIATIVE

Movie Recommendation System

B. Kalyani

Gopanna Meghana Snigdha Reddy, B. Naga Ashritha

[1]*Professor, Dept. of Computer Science and Engineering, G Pullaiah College of Engineering and Technology, Andhra Pradesh, India*

[2]*Student, Dept. of Computer Science and Engineering, G Pullaiah College of Engineering and Technology, Andhra Pradesh, India*

[3]*Student, Dept. of Computer Science and Engineering, G Pullaiah College of Engineering and Technology, Andhra Pradesh, India*

Abstract – *Recommendation systems have been around for a while now with the advent of websites for movies, books, products, music, etc. There are various techniques used in the core of a recommender engine but the end-user does not have any say in it. In this movie recommender system, we have implemented two such techniques which are collaborative filtering and content-based filtering. The users can choose between the two and customize the parameters affecting the recommendations according to their preferences.*

***Key Words*: Recommender System, Machine Learning, Collaborative Filtering, Content based Filtering**

1. INTRODUCTION

Recommender systems are have become a staple in this era of the internet economy. They help in reducing the overload of information by providing customized information access. Modeling, programming, and deploying these recommender systems have allowed businesses to enhance revenues and retain customers. These systems include customized search engines, personalized shopping agents, and handcrafted content indices. The scope of personalization and use of these systems extends to many different areas, not just web pages. The algorithm and concepts used in recommender systems can range from keyword matching in user profiles, content-based filtering, collaborative filtering, to more sophisticated techniques of data mining such as clustering server logs. Recommendation systems filter data using various concepts and approaches and recommend the most relevant items to users based on customizable criteria. It first captures the past behaviour of a customer and recommends products based on that. This proves to be beneficial to the user and clients as users only see relevant content and are not bombarded with unnecessary products and clients get better engagement. Hence it has become imperative for businesses nowadays to build smart recommendation systems and make use of the past behavior of their users.

2. DOMAIN OVERVIEW

2.1 Content-based filtering

The content-based filtering approach tries to study the liking of a user given the movies' features, which the user reacts positively to. Content refers to the features or attributes of the movies the user likes. The gist of this technique of recommendation is to compare movies using specific attributes, understand what the user has already liked, predicting what he may like, and recommend a few movies from the database with the most similar attributes. These attributes can be fixed or specified by the user himself. This method of recommendation uses movie features to recommend other similar movies to what the user has already liked.

This technique involves the calculation of the cosine similarity matrix which is done using the movie's feature vectors and the user's preferred feature vectors from the user's previous records. Then, the top few movies which are most similar are recommended to the user.

User's feedback and its significance in recommendation:

Implicit Feedback: The user's likes are recorded based on actions like clicks, searches, etc.

Explicit Feedback: The users specify their liking by actions like reacting to an item, marking it as their favorite, or rating it. In our system, the user marks certain movies as 'favorites' and also gives ratings to movies. The ratings given are used for collaborative filtering.

Cosine Similarity:
It is a concept used to measure how similar one movie is to every other movie in the dataset. It measures the cosine of the angle between two vectors projected in a multidimensional space.[6] Even if the two similar movies are far apart by means of the Euclidean distance, they may still be oriented closer together. [5]

computers

MDPI

ISSN: 2395-602X

QOS FOR NETWORKING

R. Vara Prasad
Assistant Professor, Dept of CSE
G. Pullaiah College of Engineering and Technology.

P. V. Jyotshna
Assistant Professor, Dept of CSE
G. Pullaiah College of Engineering and Technology.

Abstract: This study presents the proposed testbed implementation for the Advanced Technology Training Center (ADTEC) Batu Pahat, one of Malaysia's industrial training institutes. The objectives of this study are to discover the issues regarding network congestion, propose a suitable method to overcome such issues, and generate output data for the comparison of the results before and after the proposed implementation. The internet is directly connected to internet service providers (ISPs), which neither impose any rule nor filter the traffic components; all connections comply on the basis of the base effort services provided by the ISP. The congestion problem has been raised several times and the information technology (IT) department has been receiving complaints about poor and sometimes intermittent internet connection. Such issues provide some ideas for a possible solution because the end client is a human resource core business. In addition, budget constraints contribute to this problem. After a comprehensive review of related literature and discussion with experts, the implementation of quality of service through add-on rules, such as traffic policing on network traffic, was proposed. The proposed testbed also classified the traffic. Results show that the proposed testbed is stable. After the implementation of the generated solution, the IT department no longer receives any complaints, and thus fulfills the goal of having zero internet connection issues.

Keywords: best-effort service; classification; traffic policing; QoS; LAN

1. Introduction

Network technology users practice a variety of methods for searching for information, such as reading books from the library or reading an online article through internet access. Users need a unique id called an internet protocol (IP) address when they gather data from the internet. However, when billions of users try to gain simultaneous internet access to the same data, congestion traffic occurs. This phenomenon also happened in our training institute, which experiences congested internet connectivity during peak or non-peak hours. P.K. Dey et al. mentioned that the solution for increasing network traffic without it becoming congested is increasing the amount of bandwidth [1]. However, increasing the amount of bandwidth would increase our monthly cost. M. Marcon et al. mentioned that using a method that will yield a traffic-shaping network can resolve traffic congestion issues [2]. This proposal, however, will, affect voice and video transmissions because real-time communication is necessary for such processes [3]. After comparing related works and considering the institutional budget constraints, this study has

Yan et al. Journal of Cloud Computing (2023) 12:61
https://doi.org/10.1186/s13677-023-00444-4

Journal of Cloud Computing:
Advances, Systems and Applications

ISSN: 2395-602X

RESEARCH Open Access

Attribute Based Encryption Access Control for Cloud Computing

R. Vara Prasad
Assistant Professor, Dept of CSE.
G. Pullaiah college of engineering and technology.
S. Anees Fathima
Assistant Professor, Dept of CSE.
G. Pullaiah college of engineering and technology.

Abstract

With the rapid development of cloud computing technology, how to achieve secure access to cloud data has become a current research hotspot. Attribute-based encryption technology provides the feasibility to achieve the above goal. However, most of the existing solutions have high computational and trust costs. Furthermore, the fairness of access authorization and the security of data search can be difficult to guarantee. To address these issues, we propose a novel access control scheme based on blockchain and attribute-based searchable encryption in cloud environment. The proposed scheme achieves fine-grained access control with low computation consumption by implementing proxy encryption and decryption, while supporting policy hiding and attribute revocation. The encrypted file is stored in the IPFS and the metadata ciphertext is stored on the blockchain, which ensures data integrity and confidentiality. Simultaneously, the scheme enables the secure search of ciphertext keyword in an open and transparent blockchain environment. Additionally, an audit contract is designed to constrain user access behavior to dynamically manage access authorization. Security analysis proves that our scheme is resistant to chosen-plaintext attacks and keyword-guessing attacks. Theoretical analysis and experimental results show that our scheme has high computational and storage efficiency, which is more advantageous than other schemes.

Keywords Access control, Attribute-based encryption, Blockchain, Secure search, Attribute revocation

Introduction

With the connection of the global mobile Internet and the rapid development of cloud computing, more and more communication academia and industry are committed to shaping a safe and effective resource sharing method in the cloud environment [1]. Cloud storage technology has been widely used due to its high performance and low cost. To ensure the security of private data, data is usually stored in cloud services in encrypted form. However, the traditional public key encryption technology has been unable to meet the current needs of cloud data privacy protection. In this context, how to achieve access authorization and accurate retrieval of encrypted cloud data has become a new challenge.

Access control (AC) is a key technology to maintain data security and privacy [2]. The AC provides a solution to the above problem by constraining user access rights to ensure legitimate access to sensitive data. Attribute-based searchable encryption based on ciphertext policy not only enables fine-grained access control of encrypted data, but also supports users to retrieve ciphertext based on keywords. Ciphertext Policy Attribute-Based Encryp- tion Algorithm. (CP-ABE) [3, 4] allows data owners to autonomously set data access policies according to a set of attributes, and associate data access policies with ciphertexts. When the user's attribute set satisfies the access policy, the ciphertext can be decrypted using the

ISSN: 2395-602X

Dynamic Clustering Approaches in Hetergenous Sensor Nodes WSN Survey

R. VaraPrasad
Department of Computer Science and Engg.
G. Pullaiah College of
Engineering and Technology

Z. Yashmin
Department of Computer Science and Engg.
G. Pullaiah College of
Engineering and Technology

***Abstract*— the previous few years have seen an enlarged interest in the prospective utilize of wireless sensor networks (WSNs) in different fields like: - disaster management, battle ground surveillance, and border security surveillance. In such applications, a huge number of sensor nodes are deployed, which are frequently unattended and work separately. Clustering is a key technique used to expand the lifetime of a sensor network by reducing energy consumption. It can also raise network scalability. Researchers in all fields of wireless sensor network think that nodes are homogeneous, but some nodes may be of dissimilar energy to extend the lifetime of a WSN and its dependability. In this paper, we presented heterogeneous model for Wireless Sensor Network and clustering algorithms proposed in the literature for heterogeneous wireless sensor networks (HWSNs).**

Keywords-; Intruction Detection.,Reliability.,Security

I. INTRODUCTION

Wireless Sensor networks have become the one of the most attractive areas of research in the past few years. A Wireless Sensor Network is collected of a number of wireless sensor nodes that form a sensor field and a sink. These huge numbers of nodes, having the capability to sense their surroundings, perform limited calculation and communicate wirelessly appearance the WSNs. Specific functions such as sensing, tracking, and alerting as described. It can be obtained through collaboration among these nodes. These functions build wireless sensors very useful for monitoring usual phenomena, environmental changes, controlling security, estimating traffic flows, monitoring military application, and tracking friendly forces in the battlefields. These tasks need high reliability of the sensor networks. To create sensor networks extra reliable, the concentration to research on heterogeneous wireless sensor networks has been rising in recent past [1]. A sensor network can be ended scalable by assembling the sensor nodes into groups i.e. cluster. Every cluster has a leader, often referred to as the cluster head (CH). A Cluster Head may be elected by the sensors in a cluster or preassigned by the network trendy. The cluster relationship may be fixed or variable. A number of clustering algorithms have been specially designed for Wireless Sensor Networks (WSNs) for scalability and well-organized statement. The idea of cluster based routing is also exploited to present energy efficient routing in Ware less sensor networks (WSNs). In a hierarchical architecture, higher energy nodes (cluster heads) may be used to procedure and send the information even as low energy nodes may be used to achieve the sensing. Some of routing protocols in this group are: LEACH, PEGASIS, TEEN and APTEEN.

Clustering has many advantages: Some of these, which are presenting below:-

1. Clustering reduces the size of the routing table stored at the entity nodes by localizing the route set up within the cluster.
2. Clustering can preserve communication bandwidth since it restrictions the scope of inter cluster interactions to CHs and avoids superfluous exchange of messages among sensor nodes.
3. The Cluster Head (CH) can extend the battery life of the individual sensors and the network lifetime as well by implementing optimized management strategies.
4. Clustering cuts on topology preservation overhead. Sensors would care only for connecting with their Cluster Heads (CHs).
5. A CH can present data aggregation in its cluster and decrease the number of redundant packets.
6. A CH can reduce the rate of energy consumption by scheduling activities in the cluster.

Researchers generally suppose that the nodes in wireless sensor networks are homogeneous, but in reality, homogeneous sensor networks scarcely exist. Even homogeneous sensors have different Capabilities like different levels of preliminary energy, reduction rate, etc. In heterogeneous sensor networks, typically, a large number of reasonably priced nodes perform sensing, even as a few nodes having comparatively more energy perform data filtering, fusion and transport. This escort to the research on heterogeneous networks where two or more types of nodes are considered. Heterogeneity in wireless sensor networks can be used to extend the life time and reliability of the network. Heterogeneous sensor networks are popular, predominantly in real deployments as described by Freitas [2] and Corchado [3]. Most of the recent energy efficient protocols designed for heterogeneous networks are stands on the clustering technique, that are effectual in scalability and energy saving for WSNs.

ISSN 2348-6848

Access Policy Enforcement in a Cloud Computing Environment

R. Vara Prasad
Assistant professor, Dept of CSE
G. Pullaiah College of Engineering and Technology.

Shaik Rasiq
Assistant Professor, Dept of CSE
G. Pullaiah College of Engineering and Technology.

***Abstract*—Cloud computing has become a widely used paradigm in many IT domains such as e-health. It offers several advantages to the users, e.g. elasticity, flexibility and the rapid sharing of a huge set of digital data. However, many security and privacy concerns still pose significant challenges. In particular, the most identified problem is how to enforce the user's security policy in the access control of the outsourced data. In fact, cloud environments does not provide facilities to support high level defined security policies. For instance, the swift storage component of openstack supports only fine grained access control to execute a specific action on a specific defined object. In this paper, we designed and implemented a middleware to provide high level security policies while using such swift fine grained primitives. An e-health collaborative application dedicated for remote diagnosis is used to illustrate the suggested approach.**

***Keywords*-Cloud storage, access control, security policy, Openstack swift storage, curl library.**

I. Introduction

Cloud computing has provided many advantages to its users through different services such as storage. The storage consists of two parts: the physical data location and their access control policies. However, the current cloud architecture does not provide to the users the possibility to define their own access control policies (high level control policies). For instance, *Openstack* is a widely used cloud open source that offers the storage service via *Swift*. Although the swift component supports a fine-grained access control to objects, it remains specific and low level control. Hence, there is a need to introduce facilities in the Cloud layers to support access control policies specification at a high level. For instance in a collaborative e-health application for remote diagnosis, doctors from different hospitals collaborating through a cloud environment, need to access, exchange and share objects. Therefore each collaborative organization needs to specify its global access control policies. These kind of policies permit to regulate the access to the objects by users in other organizations. However, the underlying cloud does not provide ways to enforce high level policies. In fact, there is a need to develop a middleware that facilitates this enforcement using the cloud object access primitives while being conform to the specification of access control policies.

In this paper we propose a middleware that provides high level security policy verification using a swift fine-grained access control requests. This guarantees to the owner of data to impose its own security policy and manage the access to its resources while sharing it with others. Our approach aims to enforce the security policy without affecting the user's request. In fact the user can send an access request which is then received by a middleware denoted *curlX* [1] that translates it into an XACML request. This later will be sent to the XACML policy mechanism (containing the set of defined policies) to decide whether the user is allowed to access the data or not. For the validation of our approach, we implemented such middleware using openstack object storage (swift). For the policy and the case study, we consider a reference scenario of stroke accident [2]. This scenario consists of a collaboration between three kinds of medical organizations in order to group several relevant competencies in order to contribute to obtain a diagnosis as precise and correct as possible. Each organization outsourced its medical data to a cloud provider (openstack in our case) and imposes a set of security rules to manage their accesses.

This work was supported by the Moroccan-German project PMARs

The contribution of this work can be summarized as follows:

- We propose an approach to enforce access control policies to a set of data stored in the cloud.
- We implement, under openstack, a middleware that uses the proposed process enforcement.

The rest of this paper is organized as follows: Section II presents related work. Section III presents an overview of the swift object storage of Openstack. Section IV discusses the policy enforcement process. Section V introduces the curlX middleware: architecture and functionality. In section VI, we describe the implementation. Finally section VII concludes the paper.

II. Related Work

Despite of the advantages offered by the cloud (storage, flexibility, elasticity), it has many security challenges [3]: access control, confidentiality and integrity of data. Many researches have shown interest to solve these problems.

For confidentiality issues, current proposed solutions were based on a cryptography layer ([4], [5] and [6]), combining fragmentation and cryptography [7] or mainly using fragmentation [8]. In [4], the authors propose a domain-specific

Fraud Less Voting using Blockchain

P.Rama rao , Dr. J. W. Bakal , Ganesh Nanasaheb Dabade , Shubham Sanjay Mahto

Submitted:19-02-23 **Revised:**25/10/23 **Accepted:**10/11/23

***Abstract* - The rise of technology has brought about various societal improvements, particularly in conducting our elections. With the advent of electronic voting (e-voting), we have seen a significant increase in voter participation and reduced election-related fraud. However, as with any technology, e-voting has its challenges, particularly when it comes to ensuring the integrity and security of the voting procedure. Blockchain technology It is being proposed to address some of the issues associated with digital voting, such as scam prevention. This paper provides a comprehensive review of the current literature on the study of e-voting and fraud prevention using blockchain technology. It explores the potential benefits of blockchain technology since e-voting, the challenges that still need to be overcome, and It was proposed to address some of the issues associated with digital polling, such as fraud prevention. blockchain technology in improving the protection and integrity of the e-voting procedure.**

Key Words: Block-chain technology, Fraud Prevention, Security.

INTRODUCTION

EFPB– Electronic voting (E-voting) is a fairly new technology recently gaining fashionability. E-voting is designed to give a more effective, secure, and transparent way of conducting choices. Still, as with any technology-voting is not without its challenges. One of the most significant challenges associated with E-voting is icing the integrity and security of the voting process. Election-related fraud has been a long-standing problem, and traditional voting styles are not vulnerable. The preface of E-voting has only made the issue more complex. Blockchain technology has surfaced as an implicit result of the challenges associated with E-voting, particularly regarding fraud since installment.

Blockchain technology is a distributed tally that allows since secure and transparent record-keeping. It utilizes a peer-to-peer (P2P) network and uses cryptographic ways to ensure that data stored on the web is tampered with- evidence and inflexible. The goal of this article is to conduct a thorough analysis of the current literature on the study of e-voting and fraud since its implementation using blockchain technology. This paper will explore the implicit benefits of blockchain technology since-voting, the challenges that still need to be overcome, and the current state of exploration in this area. By furnishing perceptivity into the eventuality of blockchain technology since perfecting the security and integrity of the thee-voting process, this paper aims to contribute to the ongoing discussion on using technology in choices.

RELATED WORKS

Several researchers have explored the potential of blockchain technology in the context of e-voting and fraud prevention. Crosby et al. (2016) suggest that blockchain technology could offer a tamper-proof and transparent voting system that enables secure and anonymous voting. Similarly, Kshetri (2018) discusses the potential since Blockchain to enhance transparency and traceability in supply chain management, which could also be applied to the voting process. Mylrea and McCoy (2018) propose a blockchain-based system since African social innovation that could improve access to voting since underrepresented populations.

In addition to these theoretical ideas, there have been some actual applications of Blockchain-based computerized voting systems. One notable example is the Sierra Leone presidential election in 2018, where a blockchain-based e-voting system was used to increase the transparency and security of the election process

[1]*Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; rmamraocse@gmail.com*

[2]*Associate Professor-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; jwbakalcse@gmail.com*

[*3]*Associate Professor-ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India ; nanasahebcse@gmail.com**

[4,5,6]*UG Scholar-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; shubhamcse@gmail.com,*

Secure Data Deduplication of Cloud Computing

P. Rama Rao
Kavya, Jayathi, Ramya
G. Pullaiah college of Engineering and Technology, Department of CSE, Kurnool, Andhra Pradesh, India

Abstract

Data redundancy is a significant issue that wastes plenty of storage space in the cloud-fog storage integrated environments. Most of the current techniques, which mainly center around the static scenes, for example, the backup and archive systems, are not appropriate because of the dynamic nature of data in the cloud or integrated cloud environments. This problem can be effectively reduced and successfully managed by data deduplication techniques, eliminating duplicate data in cloud storage systems. Implementation of data deduplication (DD) over encrypted data is always a significant challenge in an integrated cloud-fog storage and computing environment to optimize the storage efficiently in a highly secured manner. This paper develops a new method using Convergent and Modified Elliptic Curve Cryptography (MECC) algorithms over the cloud and fog environment to construct secure deduplication systems. The proposed method focuses on the two most important goals of such systems. On one side, the redundancy of data needs to be reduced to its minimum, and on the other hand, a robust encryption approach must be developed to ensure the security of the data. The proposed technique is well suited for operations such as uploading new files by a user to the fog or cloud storage. The file is first encrypted using the Convergent Encryption (CE) technique and then re-encrypted using the Modified Elliptic Curve Cryptography (MECC) algorithm. The proposed method can recognize data redundancy at the block level, reducing the redundancy of data more effectively. Testing results show that the proposed approach can outperform a few stateof-the-art methods of computational efficiency and security levels.

Keywords: Convergent encryption (CE), Modified elliptic curve cryptography (MECC), Edge computing, Integrated cloud and fog networks, Hash tree. Secure hash algorithm (SHA)

Introduction

The data gathered through different sources and the Emergence of the Internet of Things in all aspects of applications increases data volume from petabytes to yottabytes, necessitating cloud computing paradigm and fog networks to process and store the data. Cloud computing (CC) produces a network-centered environment vision to users which provides access to the internet, to a collective pool of programmable grids, servers, software, storage, and amenities that could be quickly freed, with less supervision and communication to the cloud service provider. Data processing in all ways is carried out remotely in the cloud server with the help of internet connectivity. Fog computing provides the local infrastructure to process the application locally and then connects to the cloud. The fog environment reduces delay when compared to the application connected to the cloud for processing. The application developed to process and store the data needs end-to-end security, communication protocols, and resources to access information stored in the cloud and fog environments. Smart applications are built with the help of sensors and actuators, and the data is stored in the cloud environment; and edge computing facilities are also used along with the local infrastructure, termed as fog, to process the data without delay. Internet of Things does not end up with an information system but tries to build a cyberphysical system [1]. Edge computing provisions the feature of mobility for the user to process and store data on the move. Mobile edge computing provides seamless integrity among multiple applications, vendors, mobile subscribers, and enterprises [2].

* Correspondence: Abbasi@basu.ac.ir
4 Department of Computer Engineering, Engineering Faculty, Bu-Ali Sina University, Hamedan 65178-38695, Iran
Full list of author information is available at the end of the article

Indonesian Journal of Electrical Engineering and Computer Science
Vol. 23, No. 1, July 2021, pp. 510~518
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v23.i1.pp510-518

Efficient multi-keyword similarity search over encrypted cloud computing

M.Sri Lakshmi, D. jagannath, A. Nandini
srilakshmicse@gmail.com Department of Computer Science, GPCET India

Article Info

Article history:

Received Feb 19, 2023
Revised Apr 12, 2023
Accepted Jun 16, 2023

Keywords:

Cloud computing
Multi-keywords ranking search
Privacy preserving
Searchable encryption

ABSTRACT

Many organizations and individuals are attracted to outsource their data into remote cloud service providers. To ensure privacy, sensitive data should be encrypted before being hosted. However, encryption disables the direct application of the essential data management operations like searching and indexing. Searchable encryption is a cryptographic tool that gives users the ability to search the encrypted data while being encrypted. However, the existing schemes either serve a single exact search that loss the ability to handle the misspelled keywords or multi-keyword search that generate very long trapdoors. In this paper, we address the problem of designing a practical multi-keyword similarity scheme that provides short trapdoors and returns the correct results according to their similarity scores. To do so, each document is translated into a compressed trapdoor. Trapdoors are generated using key based hash functions to ensure their privacy. Only authorized users can issue valid trapdoors. Similarity scores of two textual documents are evaluated by computing the Hamming distance between their corresponding trapdoors. A robust security definition is provided together with its proof. Our experimental results illustrate that the proposed scheme improves the search efficiency compared to the existing schemes. Furthermore, it shows a high level of performance.

1. INTRODUCTION

Cloud computing is a promising technology that supports cost-effective solutions for storing and processing large datasets. For this reason, individuals and organizations with constrained-resource machines tend to outsource their data collections to such professional power servers. However, such outsourced service may raise main concerns towards users privacy, where personal data should be preserved [1]. Such data may include E-mail, medical information, private videos, and photos. Therefore, users employ encryption to protect the privacy of their confidential data. Unfortunately, encryption disables traditional keyword search operations on remote data. Searchable encryption schemes allow preforming search over encrypted data at the server side without decryption. Like search over plaintext data, searchable encryption methods build a searchable index from the entire dataset, such that during the search, only trapdoors generated using a secret keys can match index entries to get relevant results. Index contents should reveal nothing to the adversary server. Index-based search not only enhances search efficiency, but also isolates data and index encryption schemes. Under the setting of searchable symmetric encryption (SSE) schemes, the encrypted data are uploaded and retrieved by the

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2015; 1(9): 396-399
www.allresearchjournal.com
Received: 19-02-2023
Accepted: 05-07-2023

Image Processing and Object Detection

P. Kiran Rao[1] K. Raju[2] L. Koushik[3]
kiranraocse@gmail.com

Abstract
With the advancement of modern technologies areas related to robotics and computer vision, real time image processing has become a major technology under consideration. So I tried a novel approach for capturing images from the computer web cam in real time environment and process them as we are required. By using *open source computer vision library* (OpenCV for short), an image can be captured on the bases of its *hue, saturation* and color *value* (HSV) range. The basic library functions for image handling and processing are used. Basic library functions are used for loading an image, creating windows to hold image at run time, saving images, and to differentiate images based on their color values. I have also applied function to threshold the output image in order to decrease the distortion in it. While processing, the images are converted from their basic scheme *Red, Green,* and *Blue* (RGB) to a more suitable one that is HSV.

Keywords: OpenCV, HSV, RGB, threshold

1. Introduction
The research purpose of computer vision aims to simulate the manner of human eyes directly by using computer. Computer vision is such kind of research field which tries to percept and represent the 3D information for world objects. Its essence is to reconstruct the visual aspects of 3D object by analyzing the 2D information extracted accordingly [1]. Real life 3D objects are represented by 2D images.

The process of *object detection* analysis the input image and to determine the number, location, size, position of the objects. Object detection is the base for object tracking and object recognition, whose results directly affect the process and accuracy of object recognition. The common object detection method is: color-based approach, detecting objects based on their color values. The method is strong adaptability and robustness, however, the detection speed needs to be improved, because it requires test all possible windows by exhaustive search and has high computational complexity.

2. Introduction to OpenCV
OpenCV is an open source computer vision library. The library is written in C and C++and runs under Linux, Windows and provides interfaces for Python, Ruby, Matlab and other languages. OpenCV library contains abundant advanced math functions, image processing functions, and computer vision functions that span many areas in vision.

A. *Basic Class*-

OpenCV 1.0 includes the following five modules [2]:

1) *CxCore:* Some basic functions (various data types and basic operations, etc.).
2) *CV:* Contains image processing and computer vision function(image processing, structure analysis, motion analysis, and object tracking, pattern recognition, and camera calibration).
3) *CvAux:* Some experimental functions (View Morphing, Three-dimensional Tracking, PCA, HMM).
4) *HighGUI:* Contains user interface GUI and image/video storage and recall
5) *CvCam:* Camera interface (After OpenCV 1.0 version, CvCam will be completely removed.).

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Secure Data Deduplication in Cloud Storage

Rama Rao, Dr. S. Rasiq , Dr. S. Hidayatullah , Dr. S. Faizullah

Submitted : *19/03/2023* ***Revised :*** *25/10/2023* ***Accepted :*** *10/11/2023*

Abstract - *In today's digitally evolving world, the very thing that is of utmost importance is the security of data. Cloud Computing has emerged as a popular and effective tool to manage data for administrations. Each day, around 2.5 quintillion bytes of data is generated on internet and to store this large amount of data, we need servers which can deduplicate data efficiently so as to avoid wastage of storage thus minimizing expenses. In this paper, we will be looking onto various techniques and methods to achieve this deduplication. The results depict that redundant data is always mapped onto same hash code and thus it does not get uploaded on the cloud servers thus ensuring successful deduplication. It saves storage as well as saves bandwidth by eliminating duplicate data. In this project, data gets stored in the cloud server named drivehq and numerous efforts have been taken to ensure complete data access. With effective deduplication, ensuring data confidentiality is also very important thus data is always stored in the cloud in an encrypted format. It is achieved with the help of Advanced Encryption Standard(AES) algorithm .*

Key Words: Cloud Computing, deduplication, data confidentiality, data access, Advanced Encryption Standard.

1. INTRODUCTION

As we move towards a more technological driven era, saving data in cloud servers is the need of the hour. Huge amount of data gets uploaded onto the internet every day , preservation and security of this data is becoming more and more challenging with every second. Preservation of data is very important and in this business era, it is even mandated by the law[1][2].To secure such huge amount of data, Cloud Computing is the most effective tool in our hands. Cloud Computing is a practice of using a network of remote servers which are hosted on the internet to store , manage and process data, rather than to store on a local server.

Every cloud has limited storage and if we start uploading redundant files to cloud, the storage is at loss and data redundancy will be a big problem to tackle. To counter this, researchers have been exploring various methods and the best solution is deduplication of data. Data deduplication is a technique evolved to optimize storage. This technique today is used by various cloud service providers such as Dropbox[3], Amazon S3[4], Google Drive[5].It ensures that duplicate data is never uploaded to the cloud more than once.

Big administrations and organizations usually buy a third party cloud for storage of client data. But giving valuable information in the hands of a third party is like an invitation to risk. Researchers have been exploring this issue and the best solution is to guard the outsourced data with cipher text. So, once the data is uploaded to a cloud server, it is in an encrypted format. When the data is downloaded, it is decrypted and is then visible to the client. In encryption strategies, data is converted into another form called cipher text but if encryption is done with different keys, it may result in different cipher text making deduplication less feasible. Thus, encryption is necessary to secure data. So, deduplication and encryption must work in a co-ordination to ensure data security. Various techniques for deduplication over encrypted data is studied in this paper.

2. BACKGROUND

2.1 DEDUPLICATION

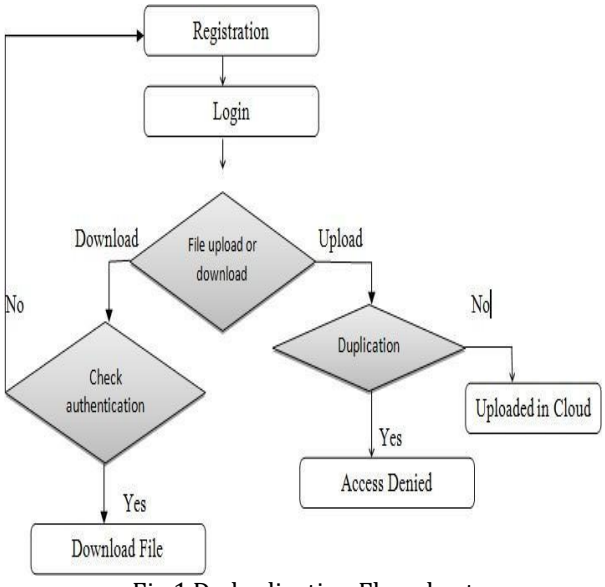


Fig 1.Deduplication Flowchart

Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; ramaraocse44@gmail.com, Sri Krishna College of Engineering and Technology, Coimbatore, India; hiddu1122@gmail.com

E-ISSN: 2582-2160

Secure in Cloud Computing

M. Sri Lakshmi
Assistant Professor
Dept of CSE
G. Pullaiah College of Engineering and Technology

S.Dada Ibrahim
Assistant Professor
Dept of CSE
G. Pullaiah College of Engineering and Technology

Abstract – Cloud Computing is a type of internet based computing which provides services via the internet and accesses the resources within the user enterprise either in a private-own-cloud or on a third-party server On Demand. The model is characterized by three attributes: scalability, pay-per-use, self-services. Many industries such as banking, healthcare, Retail, Education, Manufacturing and business are adopting this cloud technique due to efficiency of services provided by pay-per-use pattern which helps in accessing the networks, storage, servers, services and applications, without physically acquiring them [3]. The circumscribed control over the data may cause various security issues in cloud computing like Data crash, Misuse and reprehensible use of cloud computing, Insecure API, Wicked Insiders, Shared technology issues/multi-tendency nature, Account services and Traffic Hijacking. There are many new technologies, improvements and research proceedings happening every day in order to develop the security and to provide assurance for users [2]. This research paper brings a framework on what cloud computing is, main security risks and issues that are currently present in the field of cloud computing, research challenges, importance in key industries and also the personal hypothesis on future advances in the field of cloud security.

Index Terms – Security issues, Cloud Security, Cloud Architecture, Challenges, Automation of IT industry.

1. INTRODUCTION

Cloud Computing has become a compelling force in the world of Information Technology. It is considered as one of the key features for data storage, security, access, reliable nature on costs. Due to the advancement in technology, the usage of internet has been increased in a wide range and so the cost of the hardware and software too. In order to abate the cost of hardware and software by providing services when user demands over the internet, the cloud computing concept has been successful and gained a lot of popularity in a very little time period.

One main reason for the managements to move towards IT is not a new concept, it has recently become a paradigm of solutionsiscloudcomputing,astheyarerequiredtopaythe billings for the resources of only how much they consume. Though it distributed computing. In the year 1969 [4][5], L. Kleinrock predicted that, As of now, computer networks are still in their

International Journal of Cognitive Computing in Engineering 2 (2021) 229–241

Contents lists available at ScienceDirect

International Journal of Cognitive Computing in Engineering

E-ISSN: 2582-2160

A Smart Decision Support System to Predict Diabetes Disease Using Machine Learning Techniques

K. Tarakeshwar
Assistant Professor
Dept of CSE
G. Pullaiah College of Engineering and Technology.

Murtasim Khan
Assistant Professor
Dept of CSE
G. Pullaiah College of Engineering and Technology.

Nazin Ahmed[a], Rayhan Ahammed[a], Md. Manowarul Islam[a,*], Md. Ashraf Uddin[a], Arnisha Akhter[a], Md. Alamin Talukder[a], Bikash Kumar Paul[b]

[a] *Department of Computer Science and Engineering, Jagannath University, Dhaka, Bangladesh*
[b] *Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Bangladesh*

article info

Keywords:
Diabetes prediction
Machine learning
Flask
Accuracy
Random Forest (RF)
Support Vector Machines (SVM)
Logistic regression (LR)
Gradient boosting (GB)
k-nearest neighbor (k-NN)

abstract

Diabetes is a very common disease affecting individuals worldwide. Diabetes increases the risk of long-term complications including heart disease, and kidney failure among others. People might live longer and lead healthier lives if this disease is detected early. Different supervised machine learning models trained with appropriate datasets can aid in diagnosing the diabetes at the primary stage. The goal of this work is to find effective machine-learning-based classifier models for detecting diabetes in individuals utilizing clinical data. The machine learning algorithms to be trained with several datasets in this article include Decision tree (DT), Naive Bayes (NB), k-nearest neighbor (KNN), Random Forest (RF), Gradient Boosting (GB), Logistic Regression (LR) and Support Vector Machine (SVM). We have applied efficient pre-processing techniques including label-encoding and normalization that improve the accuracy of the models. Further, using various feature selection approaches, we have identified and prioritized a number of risk factors. Extensive experiments have been conducted to analyze the performance of the model using two different datasets. Our model is compared with some recent study and the results show that the proposed model can provide better accuracy of 2.71% to 13.13% depending on the dataset and the adopted ML algorithm. Finally, a machine learning algorithm showing the highest accuracy is selected for further development. We integrate this model in a web application using python flask web development framework. The results of this study suggest that an appropriate preprocessing pipeline on clinical data and applying ML-based classification may predict diabetes accurately and efficiently.

1. Introduction

The disease “Diabetes Mellitus” is one of the most common critical diseases in the world. According to the World Health Organization (WHO), diabetes affects 8.5% of adults over the age of 18 and is responsible for 1.6 million deaths worldwide (World Health Organization, 2021). Although the rate of diabetes-related premature death in many developing countries fell from 2000 to 2010, the statistics again increased between 2010 and 2016. The four primary diseases, namely cardiovascular diseases, cancer, chronic respiratory diseases, and diabetes, kill over 18% of people worldwide and have become a serious public health concern. For example, in 2000, deaths from diabetes climbed by 70%, and in 2020, mortality among males are expected to grow to 80%. Diabetes mellitus can result from obesity, age, lack of exercise, lifestyle, hereditary diabetes, high blood pressure, poor diet, etc. Over time, people with diabetes have a high risk of diseases such as heart disease, stroke, kidney failure, nerve damage, eye issues, etc.

Cloud Computing: Security Aspects

K. Tarakeswar
Computer Science and Engineering
G. Pullaiah College of Engineering and Technology

A. Rishith
Computer Science and Engineering

ABSTRACT
Security issue in cloud computing is an active area of research. Thousands of users are connecting to a cloud daily for their day to day work. Unfortunately they are ignorant about the risk involved while doing transactions on the internet. End user systems as well as cloud based data centers must be able to overcome the threats due to Viruses, Trojan and Malware etc. This paper highlights the major security threats in cloud computing system and introduce the most suitable countermeasures for these threats. Threats are classified according to different perspectives, providing a list of threats. In this article some effective countermeasures are enlisted and discussed.

General Terms
Network security, Cloud security.

Keywords
Cloud computing, security, vulnerabilities/threats and countermeasures.

1. INTRODUCTION
Cloud computing is a domain of using a network where remote servers are hosted to store, manage, and process data at very large scale. It is used for services to provide improved reliability, availability and scalability. The main goal of cloud computing from supplier's point is combination of hardware & software connected to reduce interruption on devices over network without changing user's context. It has a layering mechanism between software, networking and storage, such that every portion can be easily designed, executed, verified and run independently from consequent layers [1]. Figure 1 shows typical infrastructure of cloud computing.

Why enterprises should use cloud computing? [2]
- It has ability to scale up on demand IT capacity
- It has ability for managing large data sets
- It aligns IT resources directly with cost
- It helps in improving IT effectiveness by reducing operational cost
- It places business volatility into single domain

Why enterprises should be careful about cloud? [2]
- Due to nature and level of security threats involved in cloud environment
- It may cause lock-in due to proprietary technology
- It may cause network latency by using internet to use some cloud applications
- In some cases cloud provider may cost more than onpremises systems
- It may be problematic while integrating on-premise system and cloud based system

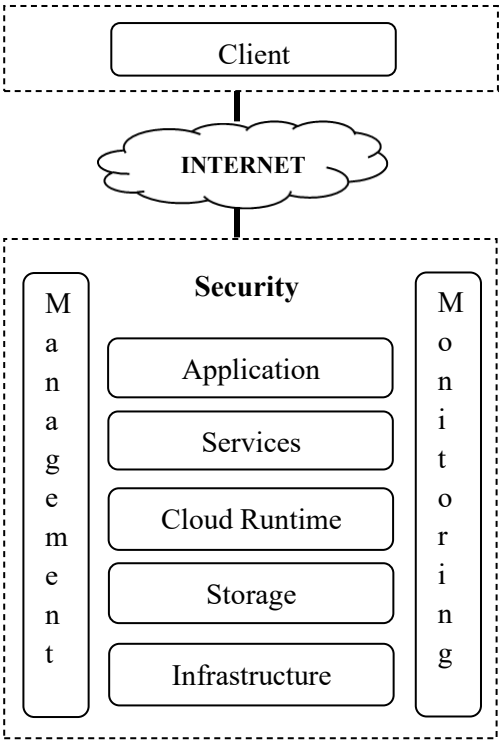


Fig 1: Infrastructure of cloud computing

However cloud computing must provide better utilization of resources by making use of virtualization. Also, it could help to take as much work load from clients even though it is having security related issue. The underlying technology that is used by cloud computing itself provides foremost security risk. This paper describe various security threats along with countermeasures in cloud computing environment. Section 1 gives overview of infrastructure of cloud computing environment. Section 2 deals with security aspects to be focused in cloud computing. Section 3 deals with security threats and challenges in cloud computing. Section 4 deals with security countermeasures. Section 5 delivers a conclusion for the paper.

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Big Data: Privacy and Security Aspects

K. Tarakeshwar , Dr. M. Vinit Kumar , Dr. Smd. Zaid , Dr. S. Shahool Hamid

Submitted : *19/03/2023* ***Revised :*** *25/10/23* ***Accepted :*** *10/11/23*

Abstract - *In the ever-growing era of technology and commercialization, data has been a very important research topic for techno-savvy people. 'Data' is something that is processed by one party and provided by another party. On a commercial level, companies and consumers are the two parties in which the exchange of data occurs as per the benefits and requirements of the company and the consumer. Hence, on different stages and scales, various transactions and exchanges of data lead to concern about the privacy and security of the data. At the company level, a lot of data having complex information, high variety, increased volume, and having high velocity is exchanged among multiple parties. This data is called 'Big Data '. Such huge and complex data makes the exchange to be complicated and the preservation of privacy and security of big data requires various mechanisms. This review paper puts light on the various concerns about the protection of privacy and security of big data. The infrastructure, the mechanisms of protection, and the cycle of big data are discussed in this paper.*

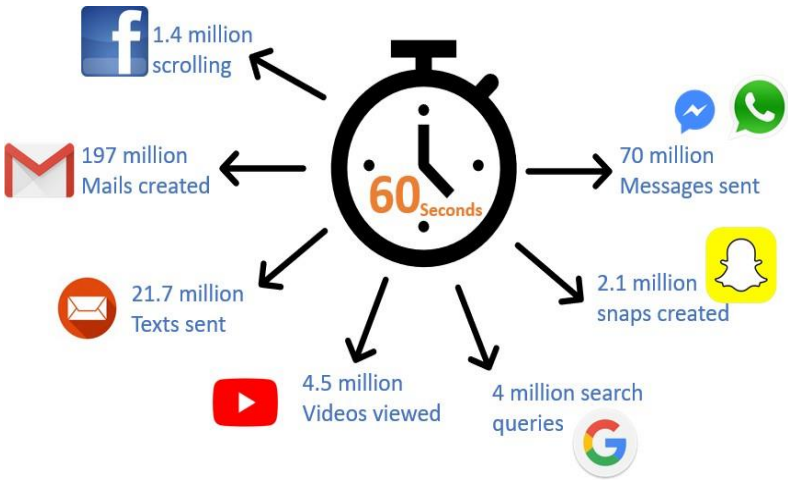
***Key Words*:** Big data; Privacy; Security; Information Security: Mechanisms; Security Protection; Infrastructure; the cycle of big data; Data Analysis; Social Applications.

1. INTRODUCTION

In the last few years, data has become a prime significant factor for businesses, companies, governments, the medical sector, engineering sector to name a few. Data is an essential asset for these companies and organizations to carry out their business plans, marketing strategies and to make decisions. A single smartphone user generates approximately 40 Exabytes of data every month. Existence of this data is in the form of pictures, emails, music and songs, texts, videos, searches, etc. The number of users of smartphones is in the millions and thus data generated is quite a lot of traditional computing systems to process and analyze it. This collection of large and complex sets of data is termed "Big Data". As we live in the era of big data, we need to go through all the important aspects of big data. So how do we classify a set of data as Big Data? This can be explained with velocity, volume, variety, value and veracity. Big data is super beneficial once it is processed and analyzed properly.

From a privacy and security perspective, a glance is to be taken on the fact that, for marketing purposes, making business strategies and research; many companies use data collected from consumers but they may not provide a future economic profit to consumers on a significant level. Instead this collected data may be misused to track the irrelative history of a consumer. Many businesses, companies and organizations use petabytes of data about their customers and company. These companies use technology to store and analyze data. Classification of this information (extracted from analyzed data) becomes even more critical. These issues of big data are related not only to variety and volume but also to security and privacy. A balance between data privacy and information needs is to be maintained. Hence, this review paper focuses on Big data - privacy and security solutions.

1Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; tarakeshwar44@gmail.com 2Associate Professor-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; vinitkumar1247@gmail.com *3Associate Professor-ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India ; zaid115@gmail.com* 4,5,6UG Scholar-ECE, Sri Krishna College* of Engineering and Technology, Coimbatore, India; shahool145@gmail.com, shaikhiddu19@gmail.com



Ambient Intelligence in Every Day Environment

K. Tarakeshwar

Department of Computer Science and Engineering

G Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India

Abstract

Ambient intelligence is an emerging discipline that brings intelligence to our everyday environments and makes those environments sensitive to us. Ambient intelligence (AmI) research builds upon advances in sensors and sensor networks, pervasive computing, and artificial intelligence. Because these contributing fields have experienced tremendous growth in the last few years, AmI research has strengthened and expanded. Because AmI research is maturing, the resulting technologies promise to revolutionarize daily human life by making people's surroundings flexible and adaptive.
In this paper, we provide a survey of the technologies that comprise ambient intelligence and of the applications that are dramatically affected by it. In particular, we specifically focus on the research that makes AmI technologies "intelligent". We also highlight challenges and opportunities that AmI researchers will face in the coming years.

Introduction

Computer science is a relatively new branch of science and as such it has gone through rapid and yet important transformations during the first decades of its existence. Those transformations have produced a very interesting mix of available experiences, and expectations which are making possible the creation and deployment of technology to ultimately improve the way our environments help us. This technical possibility is being explored in an area called Ambient Intelligence. Here we survey the field of Ambient Intelligence. Specifically, we review the technologies that led to and that support research in AmI. We also provide an overview of current uses of AmI in practical settings, and present opportunities for continued AmI research.

The European Commission first charted a path for AmI research in 2001 [1]. A significant factor in this birth of the field of AmI is the evolution of technology. Computers were initially very expensive as well as difficult to understand and use. Each computer was a rare and precious resource. A single computer would typically be used by many individuals (see Fig. 1). In the next evolutionary step, many users no longer needed to take turns to use a computer as many were able to access it simultaneously. The PC revolution in the 80s changed the ratio to one user per computer. As industry progressed and costs dropped, one user often was able to access more than one computer. The type of computational resources that we have at our disposal today is dramatically more varied than a few decades ago.

Today, access to multiple computers does not necessarily just mean owning both a PC and a laptop. Since the miniaturization of microprocessors, computing power is embedded in familiar objects such as home appliances (e.g., washing machines, refrigerators, and microwave ovens), they travel with us outside the home (e.g., mobile phones and PDAs), and they help guide us to and from our home (e.g., cars and GPS navigation). Computers that perform faster computation with reduced power and tailor the computation to accomplish very specific tasks.

LEAF DISEASE DETECTION USING IMAGE PROCESSING

[1] K. Seshadri ramana , [2] Surbhi Lanjewar, [3] Shubhangi Daduriya,

Abstract : Image retrieval is a poor stepchild to other forms of information retrieval (IR). Image retrieval has been one of the most interesting and research areas in the field of computer vision over the last decades. Content-Based Image Retrieval (CBIR) systems are used in order to automatically index, search, retrieve, and browse image databases. Colour, shape and texture features are important properties in content-based image retrieval systems. In this paper, we have mentioned detailed classification of CBIR system. We have defined different techniques as well as the combinations of them to improve the performance. We have also defined the effect of different matching techniques on the retrieval process.

Most content-based image retrievals (CBIR) use color as image features. However, image retrieval using color features often gives disappointing results because in many cases, images with similar colors do not have similar content. Color methods incorporating spatial information have been proposed to solve this problem, however, these methods often result in very high dimensions of features which drastically slow down the retrieval speed. In this paper, a method combining color, shape and texture features of image is proposed to improve the retrieval performance. Given a query, images in the database are firstly ranked using color features. Then the top ranked images are re-ranked according to their texture features. Results show the second process improves retrieval performance significantly.

Keywords: **Image acquisition, pre-processing, features extraction, classification, neural network.**

I. INTRODUCTION

India is an agriculture country. 70% of India economy depends on agriculture. Due to environmental changes like huge rain fall, drastic changes in temp, the crops get infected. And that can be characterized by spots on the leaf, dryness of leaf, colour changes in leaf and defoliation. The maximum people cannot be able to identify the disease easily and accurately. For that purpose we need experts that identify the disease. But this is more time consuming process and quite expensive. The proposed project leaf infection detection is made through image processing technique image because image from important data and information in biological science digital image processing and image analysis technology based on advance in micro electronics and computer has many applications in biology.

1.1 Basic Idea

For increasing growth and productivity of crop field, farmers need automatic monitoring of disease of plants instead of manual. Manual monitoring of disease do not give satisfactory result as naked eye observation is old method requires more time for disease recognition also need expert hence it is non effective. So in this, we introduced a modern technique to find out disease related to both leaf and fruit. To overcome disadvantages of traditional eye observing technique, we used digital image processing technique for fast and accurate disease detection of plant. In our proposed work, we developed k-means clustering algorithm with multi SVM algorithm in MATLAB software for disease identification and classification. The old and classical approach for detection and recognition of plant diseases is based on naked eye observation, which is very slow method also gives less accuracy.

1.2 History of Project

Image segmentation is the process of separating or grouping an image into different parts. There are currently many different ways of performing image segmentation, ranging from the simple thresholding method to advanced color image segmentation methods. These parts normally correspond to something that humans can easily separate and view as individual objects. Computers have no means of intelligently recognizing objects, and so many different methods have been developed in order to segment images. The segmentation process is based on various features found in the image. This might be color information, boundaries or segment of an image. We use Genetic algorithm for color image segmentation

[1]*Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; sheshadricse@gmail.com*

[2]*Associate Professor-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; lanjewarcse@gmail.com*

[*3]*Associate Professor-ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India , daduriyacse@gmail.com*

Rescue Robot in Coal Mines

Dr K.Sreenivasulu , Mr. Venkatesh Lotlikar , Prof. Anisha Cotta

Department of Computer Science and Engineering
GPCET

Abstract

Coal mine is a hazardous place in which numerous lethal variables are risky for human life, particularly when impacts happen. Rescue team typically doesn't have a clue about the real circumstance of the mine passage. Accordingly, it might be exceptionally risky for rescuers to go into mine passages to inquiry survivors without distinguishing ecological data previously. To tackle this issue, robot is created for helping individuals to do the rescue work. The robot is used for detecting the explosion environment of coal mine. We developed a prototype of a fully autonomous robot which can be used to indicate presence of harmful gases inside a mine for mine rescue operations in case of emergencies caused by natural calamities such as explosion. Coal mine rescue robot is a sort of portable robot. It can go into blast environment and discover gas content.

Keywords: Coal Mine, Hazardous, Rescue

I. INTRODUCTION

A coal mine is an underground tunnel system. There only a few pitheads on ground. If there are some accidents, people are easily trapped in tunnel and often cannot escape from it. It has dangerous accidents as collapse, gas explosion, CO, CO2 poison gas, low O2 content, high temperature, smoke, coal dust, fire, water, etc. All these accidents can kill people easily.

CH4 gas is intergrown with coal. When coal is mined, CH4 gas is released. Gas is pushed off by forced ventilating system. But if the ventilating system is faulty or gas is leaked from coal layer, gas diffuses throughout the tunnel. A flame current can cause a heavy gas explosion. Mine tunnel passageway is narrow, so the explosion wave can destroy any thing in the tunnel. All devices and people may be affected, and the gas of CH4, CO, CO2 and coal dust are filled in the tunnel, and the environment of the tunnel comprises of low O2 content and high temperature. Besides, the forced ventilate system has been damaged, the gases cannot be pushed out and gets accumulated in tunnel. A fire may cause a second explosion. People in tunnel could be poisoned by CO, stifled by CO2 and low O2 content, high temperature and coal dust. Rescuers on ground cannot go into mine tunnel because situation is not known and they may be killed by second explosion. So, detection of mine tunnel situation is the first mission. A Robot is an ideal tool in coal mine disaster. The robot used in coal mine tunnel must have many special characteristics which are different from other robots on ground.

II. PROBLEM STATEMENT

The mobile robot is designed so that it can run in explosive environment, climb over uneven surface areas, check gas contents and perform live surveillance using a camera.

[1]*Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; sreenivasulucse@gmail.com*

[2]*Associate Professor-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; venkateshcse@gmail.com*

[*3]*Associate Professor-ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India ;Anishacse@gmail.com**

International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

A Comparative Survey of Various Cryptographic Techniques

Dr K.Sreenivasulu[1] , Viny Jain[2]

Submitted:19/02/23 **Revised:25/02/23 Accepted:10/11/23**

Department of Computer Science and Enginnering

Abstract - *Now a days world that is characterized by the rapid rise in the number of attacking or hacking issues and more especially using more superior methods, it is prudent that a lot of IT research be intended for finding answer to the rising threats to the online or internet system , including the network itself and data and the information that carries and store from one location to another. Thus, information is a very important asset and must be kept confidential, have integrity and become available in order to be worth its name and be credible. The thought of information security lead to the development of Cryptography. In other words, Cryptography is the science of keeping information secure. It includes encryption and decryption of data or messages. Cryptography, in addition to providing confidentiality, also provides Integrity, Authentication and Non-repudiation. Based totally on the key distribution, cryptography is categorized into two important types-Symmetric Key Cryptography and Asymmetric Key Cryptography. In this paper, we've surveyed the conventional algorithms, based on their benefits and drawbacks. We additionally have in comparison the significance of each these cryptographic techniques. This paper also offer an appropriate future opportunity related to these cryptographic techniques.*

Key Words: *Man In The Middle Attack ; Biometric Sender Authentication; Diffie Hellman (DH) Key Exchange Algorithm; Speech and Message Encryption and Decryption;*

[1]*Associate Professor, Department of Computer Science and Engineering, G.Pulllaiah College of Engineering and Technology, Kurnool, India; sreenivasulucse@gmail.com*

[2]*Associate Professor-ECE, Sri Krishna College of Engineering and Technology, Coimbatore, India; venkateshcse@gmail.com*

[*3]*Associate Professor-ECE, Dr.N.G.P. Institute of Technology, Coimbatore, India ;Anishacse@gmail.com**

1. INTRODUCTION

In Cryptography is the art of science or collection of techniques or tools used to protect the data and information during its transmission over the network .

It involves encryption and decryption of messages. Encryption is the process of converting a plain text into cipher text and decryption is the process of getting back the original message from the encrypted text. Cryptography, in addition to providing confidentiality, also provides Integrity, Authentication and Non-repudiation. The crux of cryptography lies in the key involved and the secrecy of the keys used to encrypt or decrypt. Cryptography contains various abstraction levels of security mechanism .Network administrator provides authorized access over the network by implementing network security and adoption of its provisions and policies to prevent unauthorized access. Authorization has always been an integral part of the security mechanism. Cryptography has played a important role in curbing down most information threats such as the man in the middle and eavesdropping attacks that target data and information as it moves over the internet system. However, research carried out by professionals in the field indicates that there could be some gaps that need to be filled in the area of cryptography so as to attain a better security of data and information.

Blue Brain: The Name of the World's First Virtual Brain

N. Parashuram
Professor
G. Pullaiah College of Engineering and Technology
Nparsuramcse@gmail.com

Md Anees al Jari
Assisstant Professor
G. Pullaiah College of Engineering and Technology
aneescse@gmail.com

Abstract

Blue brain is a Virtual Brain it is the creation of synthetic brain by reverse engineering and recreates it at the cellular level inside a computer simulation. The concept of blue brain founded in May 2005 by Henry Markram at the EPFL in Lausanne, Switzerland. The aim of the project to gain a complete understanding of the brain and to enable better and faster development of brain disease treatments. No one can ever understand the complexity of human brain. It is more complex than any circuitry in the world. The scientists today are in research to create an artificial brain that can think, respond, take decision, and keep everything in memory. After the death of the body, we will not lose knowledge, intelligence, feelings and memory of that man and can be used for the welfare of human society.

Keywords: Blue Brain, Human Brain, Artificial Brain, Neurons, Knowledge Sharing

I. INTRODUCTION

The Blue Brain technology is a new and innovative project in the field of science and technology. It is the world's first ever virtual brain. The artificial brain which performs similar tasks of human brain [1]. The Human brain is considered to be full of complexities. The aim of Blue Brain technology is to upload the complete information existing in the brain in to a computer. With this technology we can preserve the knowledge and intelligence even after death of human body. The blue brain technology provides the comprehensive simulation of the essential internal connectivity of the cerebral parts with the external artificial intelligence network. This technology is showing the new path in the field of artificial intelligence. The intelligent neurons are a part existing in the human brain. The international computer giant, IBM has done a considerable research in this domain and has developed a virtual brain. The high performance computing support with blue brain technology is based on the current close connections between IBM and Blue Brain technology [4].

II. HISTORY

The Blue Brain is an attempt to create synthetic brain by reverse engineering which the human brain down to the molecular level. On July 2005, the Brain Mind Institute (BMI), Switzerland and International Business Machine (IBM) launched the blue brain project using the enormous computing powder of IBM's prototype Blue Gene/ L Super computer. An accurate replica of neocortical column is the essential first step to simulating the whole brain and also will provide the link between genetic, molecular and cognitive levels of brain function[4].

III. WHAT IS VIRTUAL BRAIN

A virtual brain is an artificial brain, which we are termed as Blue Brain. It can think like the natural brain, take decisions based on the past experience, and respond as the natural brain can. It is possible to do so by using supercomputers, with a huge amount of storage capacity, processing power and an interface between the human brain and this artificial one. Through this interface, the data stored in the natural brain can be uploaded into the computer. So the brain and the knowledge, intelligence of anyone can be preserved and used forever, even after the death of the person[1].

The Blue Brain Initiative is one of the best known trials to understand and organize brain data in a useful way. It is a neuroinformatics platform that tries to simulate the brain organization on the macroscopic level of detail. The neuroinformatics tool is based on the idea of taking advantage of available functional and structural brain data generated by imaging techniques such as MRI, functional MRI and trans-cranial magnetic stimulation.

Journal of Artificial Intelligence and Technology, 2022, 2, 39-41
https://doi.org/10.37965/jait.2022.0102

ISTP
GUEST EDITORIAL

Artificial Intelligence with Applications

M.Sri Lakshmi

(Received 29 March 2022; Revised 30 March 2022; Accepted 30 March 2022; Published online 05 April 2022)

Abstract: Artificial intelligence and machine-learning are widely applied in all domain applications, including computer vision and natural language processing (NLP). We briefly discuss the development of edge detection, which plays an important role in representing the salience features in a wide range of computer vision applications. Meanwhile, transformer-based deep models facilitate the usage of NLP application. We introduce two ongoing research projects for pharmaceutical industry and business negotiation. We also selected five papers in the related areas for this journal issue.

Key words: artificial intelligence; edge detection; machine learning; natural language processing; self-attention; transformer

I. INTRODUCTION

Artificial intelligence (AI) and machine-learning (ML) are inter-disciplinary domains that have found support and applications in all domains of science, technology, and engineering. They have transformed the traditional model-based design and development process to a data driven and learning process. On one side, AI is driven by the domains needs. On the other side, AI is applied in these domains to augment the performance and capacities of many applications.

II. AI IN COMPUTER VISION AND NATURAL LANGUAGE PROCESSING DOMAINS

For the computer vision-based applications, AI enables computers and systems to derive meaningful information from digital images, videos, and other visual inputs and take actions or make decisions based on the low-level visual stimulus. Backed by AI and ML, computers can mimic our human beings to see, observe, and understand.

Natural language processing (NLP) is also a branch of AI that focuses on helping computers to understand the way that humans write and speak. Real-world use case applications of NLP include but not limited to:

- Voice-controlled assistants like Siri and Alexa.
- Question answering by customer service chatbots.
- Streamlining the recruiting process by scanning through skills and experience listed in the resumes.
- Tools for correcting errors and making suggestions for simplifying writing.
- Language models that predict the next words in a text, based on what has already been typed.

In the following, one topic in computer vision and two NLP-based ongoing research applications are introduced.

A. EDGE DETECTION

Among many topics in the field of computer vision and image processing research, edge detection plays an important role in a wide range of fields from satellite imaging to medical screening, object recognition. It is an image processing technique to find boundaries/edges in a digital image with discontinuities that present a global view of an image with the most critical outline of the image. Robust edge-based shape features provide more concrete analysis for computer vision applications.

Traditional edge detection methods exploit low-level visual cues to construct hand-crafted features then classify the edge and nonedge pixels using threshold-based methods. The results of conventional approaches lack semantics at the object level. Nowadays, convolutional neural network-based approaches have become mainstream in the image processing domain. Among deep network-based edge detection methods, holistically nested edge detection (HED) [1] is one of the successful frameworks. It produces five intermediate side outputs and performs deep supervision along the network pathway. Its final fused result achieves performance within a 2% gap to human vision. Since then, several approaches use a similar architecture to further improve the accuracy. These efforts mainly focus on improving the quality of intermediate outputs or enhancing the deep supervision strategies. However, these approaches fuse intermediate layers without considering hierarchical edge importance within each side output. This poses the dilemma to the network: to include desired features, it has to accept many unwanted data and vice versa. Consequently, the result often contains more noise and thick edges while missing some key boundaries.

To tackle this issue, Scale-Invariant Salient Edge Detection (SISED) framework [2] can locate and extract the important Scale-Invariant Salient Edge (SISE) as the subset of each side output without increasing the network complexity. The normalized Hadamard Product is the key operation of SISED where a multiplicative operation is applied to promote mutually agreed features across multiscale side outputs while suppressing those with weak scale expression. SISED computes the edge importance hierarchically to enhance the edge results and reaches state-of-the-art performance.

).

EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Role-Based Access Control in Cloud Computing

K.Lakshmi
[1]Department of Computer Science and Application, G.Pullaiah College of Engineering and Technology, Kurnool, India

Abstract

The cloud reduces the user's burden to many folds. But cloud providers and cloud users with dynamic relationship, are in distinct security domains. Amongst various challenges with cloud, the crucial one is to detect and protect the user's data from unauthorized accesses. In cloud, users are not legendary by their predefined identities. Instead, they are providing accesses based on their characteristics and attributes. This work is focusing on available access control mechanisms and one that applicable for cloud environment. The paper also proposes an Efficient and Flexible Role-Based Access Control (EF-RBAC) mechanism for the cloud computing environment to achieve confidentiality and security. RBAC limits the accesses for resources within an organization to authorized users only and also guarantees that a user can solely access specific information they are authorized for by the organization policy. The proposed scheme adds flexibility to the RBAC for better cloud user's experience.

Keywords: Cloud Computing, Access control, Role-Based Access Control, Security, DDOS, Multimedia, Information Security.

Received on 08 September 2019, accepted on 01 November 2019, published on 18 November 2019

doi: 10.4108/eai.13-7-2018.161438

1. Introduction

Cloud computing creates several computing resources (computing centers, huge data centers, etc.) to work in a collaborative network system over the internet. Also, a secure, huge and fast network of data storage and computing is supported by the cloud for all kinds of users [1]. The three major cloud service delivery models are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

Although the cloud is providing numerous benefits but the main concern associated with both ends (i.e. consumer and provider) is security [2]. The consumer's concern is about maintaining the secrecy of their private data stored over the cloud servers [28]. However, the cloud provider's concern is that their services and resources remain accessible to authorized persons only. Thus, without proper access control policies, the cloud is always vulnerable to various threats and attacks. Organizations hesitate to adopt cloud for transfer of their multimedia storage and computations to cloud servers as they are not sure that whether they are 100% secure or not. As any access breach to user's personal multimedia data can be a matter of stake for them. In nutshell, the confidentiality and integrity of the user's data stored at the third party public cloud servers must not be compromised in any case [30]. Because of this, an effective mechanism for access control and management can play a crucial role as it is directly linked with the primary required characteristics those are authorization, confidentiality, availability, and integrity.

Cloud providers must ensure the basic functionalities for controlling unauthorized accesses or in other words providing secure access to the services based on the service level agreement (SLA), protecting access of one user's data from other users, providing a consistent state to consumer always, controlling users accesses based on their earlier defined privileges i.e. effectively maintaining and managing access control rules etc.

Traditionally access control mechanisms are of the following three categories:

*Corresponding Author: shilpi13n@gmail.com

Fine-grained Access Control for Cloud Computing

K.Lakshmi

Abstract: Fine-grained access control schemes are commonly used in cloud computing. In this type of schemes, each data item is given its own access control policy. The entity that wants to access the data item needs to provide its credentials to a policy enforcer. In a cloud environment, normally, the policy enforcer is not the owner of the data. The access control policies and the credentials might reveal some information that the policy enforcer is not entitled to know. This paper proposed a fine-grained access control scheme. It prevents the policy enforcers from comprehending the access control policies and the entities' credentials by using cryptographic techniques. Compared with the existing schemes, the proposed scheme provides higher level privacy.

1 Introduction

As cloud computing has helped many businesses increase their competitiveness (Narasimhan, 2011), many manufacturers are adopting the concept of cloud computing into their manufacturing process (Saito et al., 2011). Cloud manufacturing is being regarded as the future manufacturing model (Xu, 2012). In cloud manufacturing, manufacturers pool their resources together to form a cloud platform. A manufacturing process can be formed by integrating the services provided by the manufacturers in the cloud platform.

To ensure data security, it is important to provide fine-grained access control to the data in the cloud (Bethencourt et al., 2007; Song et al., 2012; Yu et al., 2010; Barhamgi et al., 2012). For example, when a company stores data in the cloud, the company would only allow its contractors to view the data that are relevant to the projects that the contractors are working on. Many fine-grained access control schemes have been developed, e.g. (Ye and Zhong, 2011). In these schemes, the access control policy for a data item is attached to the data item. The data's policy is transmitted with the data at the same time. Data are only sent to an entity if the entity's credentials satisfy the data's access control policy.

Cryptography has also been used to achieve fine-grained access control in cloud computing (Yu et al. 2010; Bethencourt et al., 2007; Zhou et al., 2011; Tian, 2012; Fan, 2012). In these approaches, attribute-based encryptions are used to encrypt data. The encrypted data can only be decrypted by the clients who possess the desired attributes. Encryption-based access control is designed for storing data on storage service providers. It assumes that the hosts of the data should not know the contents of the data. However, this assumption does not suit cloud manufacturing. For example, assume a company has two contractors working on a project. The company stores project-related data on the two contractors' sites. The two contractors are also expected to exchange project-related data between them. It can be seen that the data stored on the contractors' sites cannot be encrypted as the contractors need to access the contents of the data.

The problem with the existing fine-grained access control schemes is that the access control policies are not entirely hidden from the policy enforcers. Goyal et al. stated that it is important to hide the access control policies for some applica-

Data Management in IoT

Dr. S. Prem Kumar

***Abstract*—Internet of Thing (IoT) has been attracting the interest of researchers in recent years. Traditionally, only handful types of devices had the capability to be connected to internet/intranet, but due to the latest developments in RFID, NFC, smart sensors and communication protocols billions of heterogeneous devices are being connected each year. From smart phones uploading the data regarding location and fitness to smart grids uploading the data regarding energy consumption and distribution, these devices are generating a huge amount of data each passing moment. This research paper proposes a data management framework to securely manage the huge amount of data that is being generated by IoT enabled devices. The proposed framework is divided into nine layers. The framework incorporates layers such as data collection layer, fog computing layer, integrity management layer, security layer, data aggregation layer, data analysis layer, data storage layer, application layer and archiving layer. The security layer has been proposed as a background layer because all layers shall ensure the privacy and security of the data. These layers will help in managing the data from the point where it is generated by an IoT enabled device until the point where the data is archived at the data center.**

Keywords*—*IoT; Data Management; Cloud Computing; Big Data; Smart Devices; Interoperability; Privacy; Trust

I. INTRODUCTION

Internet of Things is one of the concepts, which tends to build a new future of computing by taking every smart object into a globally connected network capable of sensing, communicating, information sharing and performing smart analytics for different applications [1][7]. This is the result of rising technological evolution of computing devices and its use in different sectors like healthcare, automotive, education and sports. The excessive use of smart objects in human life has pushed the researchers towards the design and development of tools and techniques that can connect these smart devices to a global network. Emphasis has been to enhance the efficiency of these smart devices to generate less, but meaningful data that can be efficiently transported and analysed on a cloud before being stored. Last decade is a witness of the development of different network protocols, computing devices and storage devices that have helped in the rapid deployment of IoT enabled devices. [1][5][7][8][13].

Furthermore, it has been observed that this wave of smart devices is serving in different areas such as education, medical, military, research, sports and industries [5][15][17]. One of the application switches that IoT has made possible is a smart home concept. Smart home offers services like access control, home monitoring, safety and central control of numerous home appliances to its owner [4][11][15]. The basic idea of smart homes is to connect home appliances to network and employ the use of some standard protocols for communications. Smart sensors and cameras are utilised for this purpose [5] [15]. Another application that can be witnessed is smart agriculture where IoT exploits smart sensors and RFIDs to change the shape of traditional decision making regarding crops. IoT has enabled the farmers to be aware of information related to different field parameters like humidity, moisture, temperature and wind speed. This makes it possible for farmers to take timely and more accurate decisions for enhancing crop productivity and quality.

One more key application area is supply chain management where Internet of Thing term was coined for the very first time in 1991 [1][7]. IoT can provide supply chain system with real time insight of every process and transaction. The use of smart sensors and RFIDs will not only enable effective tracking of shipments as well as it will make it easy to control and manage mobile assets. It would also help in generating more business opportunities by producing analytical results on gathered information to sell goods based on this specific information.

It seems that these applications are just beginning of a big industry in computing. Moreover, this rapid development in applications shows that in the near future there will be a stable and steady stream of innovative applications and services in Internet of Things [2][3][25].

Internet of Things calls for to think beyond traditional computing. It demands small, smart and compact devices that could replace traditional computing capabilities. RFIDs, Wireless Sensor Networks, smart readers, mobile phones, laptops and portable devices are the major technologies that would work as basic computing units for such global network. RFIDs are one of the key players in IoT enabling technologies [17][25]. RFID brings into play microchips attached to any desired object for automatic identification, tracking and wireless information transmission [1]. RFIDs are used in applications of the supply chain, retail and ports for monitoring.

Image Processing for Security

Dr. Seshadri Ramana

G. Pullaiah College Of Engineering

Abstract

Using image stitching and image steganography security can be provided to any image which has to be sent over the network or transferred using any electronic mode. There is a message and a secret image that has to be sent. The secret image is divided into parts.The first phase is the Encrypting Phase, which deals with the process of converting the actual secret message into ciphertext using the AES algorithm. In the second phase which is the Embedding Phase, the cipher text is embedded into any part of the secret image that is to be sent. Third phase is the Hiding Phase, where steganography is performed on the output image of Embedding Phase and other parts of the image where the parts are camouflaged by another image using least significant bit replacement. These individual parts are sent to the concerned receiver. At the receivers end decryption of Hiding phase and Embedding Phase takes place respectively. The parts obtained are stitched together using k nearest method. Using SIFT features the quality of the image is improved.

Keywords

Cryptography, image steganography, image stitching.

1 Introduction

In today's world of growing technology security is of utmost concern. With the increase in cyber crime, providing only network security is not sufficient. Security provided to images like blue print of company projects , secret images of concern to the army or of company's interest, using image steganography and stitching is beneficial. As the text message is encrypted using AES algorithm and embedded in a part of the image the text message is difficult to find. More over since the secret image is broken down into parts and then sent to the receiver. This makes it difficult for the trespasers to get access to all the parts of the images at once. Thus increasing the security to a much needed higher level. This makes it becomes highly difficult for the the intruder to detect the and decode the document. There is no limitation on the image format that can be used right from bmp to a giff image can be used. It can be grey scale or coloured images.
The size of the message needs to be of only 140 characters.

2 Literature survey:

Current picture of the world says that everything that can be thought off can be done with the help of the internet. Right from shopping for clothes to buying a house. The transactions are all done using personal information, credit card numbers etc. With the amount of internet users hiking up

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

Smart Alert System For Garbage Clearance using IOT

Dr. Seshadri Ramana
Department of Data Science
G. Pullaiah College(Autonomous)

***Abstract*:- Internet of Things facilitates the realization of the sustainable growth of numerous smart systems and devices. Smart IoT based Garbage Monitoring System is an indispensable part in building clean college campuses. Garbage bins are kept at various places in the college campuses. Manual checking of each of these bins kept at various places inside the college campuses, might consume more time and energy sometimes leads to overflowing of garbage bins. Overflowing of garbage will cause air pollution which in turn will affect the historical college campus buildings. To overcome the drawbacks in the traditional way of garbage monitoring, SMARGAR -an IoT based SMARt GARbage Monitoring System is proposed to monitor the garbage bins constantly and to inform sweepers about the level of garbage collected in the garbage bins at regular intervals via a mobile app.**

Keywords—IoT; smart systems; Garbage Monitoring

1. INTRODUCTION

IoT based Garbage management is one of the most noteworthy concepts deployed for preserving the historical college campus buildings through intelligent monitoring. The effective remote monitoring of garbage levels anytime and anywhere is an important factor [1]. Excess garbage causes air pollution which in turn will affect the historical college campus buildings. The existing garbage collection and management system is not flawless. It depends on a vast amount of human resources and material resources. Poor monitoring and lack of efficient management policy lead to excessive piling up and even spillage. This phenomenon will not only cause air pollution, but also will affect the historical college campus buildings. As a result, it is significant to deploy an IoT based Smart Garbage Monitoring System for preserving historic College Campuses.

SMARGAR – an IoT based Smart Garbage Monitoring System proposed in this paper will save historical resources and time. In Section 2, an overview of related works is presented. Section 3 presents the proposed SMARGAR – an IoT based Smart Garbage Monitoring System for preserving historic College Campuses. Section 4 elaborates the system requirements. In Section 5, architecture of the proposed An IoT based Smart Garbage Monitoring System for preserving historic College Campuses. Finally, Section 6 concludes the paper.

2. REVIEW OF LITERATURE

Yanglu et al. [1] proposed a wireless garbage monitoring system with IoT to monitor garbage at regular intervals remotely without human intervention. Himadri Nath Saha et al. [2] proposed the IoT based smart garbage monitoring and clearance alert system in which RGB led lights attached with the bins indicated the garbage level of bin at that moment and eventually reduced the human labour of monitoring. Saadia Kulsoom Memon et al. [3] developed an IoT based cost effective system that monitored garbage in real time by using smart technology with the help of WeMos and Ultrasonic sensors which consumed meagre resources of the waste management authorities. It was claimed that the proposed system monitored garbage inside garbage bins more accurately.

Chun-Yen Chung et al. [4] developed an integrated LoRaWAN communication networks developed using the Internet of Things with garbage sorting equipment to create a system used electrostatic capacitance-type proximity sensors to determine the types of garbage deposited in garbage cans. This system deployed a C# graphical monitoring interface to remind users to remove the garbage.Shashank Shetty et al. [5] presented a Smart Waste segregation and garbage level monitoring System which could be monitored remotely and built at a very low cost. Paavan Lakshmana Chowdary S et al. [6] proposed an IoT based Smart Garbage Alert System to trigger an alert message to the people concerned when the container was filled to avoid the over spilling of garbage. Amit Sundas et al. [7] discussed the state-of-art technologies that have been deployed for waste management. In this paper a novel architecture for waste management was proposed that utilized the concept of IoT and image processing. The proposed architecture acted as a surveillance monitoring system to monitor the overflow of the garbage and sent alert message to the concerned authorities to take the essential and instantaneous action. Aswin

Raaju et al. [8] presented a smart garbage collection management solution based on ZigBee technology. This system could read, collect, and transmit huge amount of data over the adhoc network to dynamically supervise garbage collection mechanism. Sudharani Ashok Ghadage et al. [9] proposed garbage management system made up of ultrasonic sensor, infrared sensor, Arduino UNO, microcontroller and Raspberry Pi for detecting the level of waste. In this system through the deployment of Global system for mobile (GSM), the concerned persons were informed through SMS.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 11, November-2021

Artificial Intelligence in Brain Informatics

Image Processing in brain tumor MRI

Dr. Seshadri Ramana

Article info

Article history:
Received 25 November 2021
Received in revised form 19 February 2022
Accepted 21 February 2022

ABSTRACT

Introduction: In modern days, checking the huge number of MRI (magnetic resonance imaging) images and finding a brain tumour manually by a human is a very tedious and inaccurate task. It can affect the proper medical treatment of the patient. Again, it can be a hugely time-consuming task as it involves a huge number of image datasets. There is a good similarity between normal tissue and brain tumour cells in appearance, so segmentation of tumour regions become a difficult task to do. So there is an essentiality for a highly accurate automatic tumour detection method.

Method: In this paper, we proposed an algorithm to segment brain tumours from 2D Magnetic Resonance brain Images (MRI) by a convolutional neural network which is followed by traditional classifiers and deep learning methods. We have taken various MRI images with diverse Tumour sizes, locations, shapes, and different image intensities to train the model well. Furthermore, we have applied SVM classifier and other activation algorithms (softmax, RMSProp, sigmoid, etc) to cross-check our work. We implement our proposed method using "TensorFlow" and "Keras" in "Python" as it is an efficient programming language to perform fast work.

Result: In our work, CNN gained an accuracy of 99.74%, which is better than the state of the result obtained so far.

Conclusion: Our CNN based model will help the doctors to detect brain tumours in MRI images accurately, so that the speed in treatment will increase a lot.

1. Introduction

Medical imaging refers to several techniques that can be used as non-invasive methods of looking inside the body [1]. The main use of medical image in the human body is for treatment and diagnostic purposes. So, it plays a significant role in the betterment of treatment and the health of the human.

Image segmentation is a crucial and essential step in image processing that determines the success of image processing at a higher level [2]. In this case we have mainly focused on the segmentation of the brain tumour from the MRI images. It helps the medical representatives to find the location of the tumour in the brain easily. Medical image processing encompasses the utilization and exploration of 3D image datasets of the physical body, obtained most typically from computed tomography (CT) or Magnetic Resonance Imaging (MRI) scanner to diagnose pathologies or guide medical interventions like surgical planning, or for research purposes. Medical image processing is applied by radiologists, engineers, and clinicians to understand the anatomy of either individual patients or population groups highly. Measurement, statistical analysis, and creation of simulation models which incorporate real anatomical geometries provide the chance for more complete understanding, as an example of interactions between patient anatomy and medical devices.

Tumour: The word "Tumour" is a synonym for the word "neoplasm" which is formed by an abnormal growth of cells. A tumour is significantly different from cancer [3].

1.1. Classification of tumour

There are three basic types of tumours: 1) Benign; 2) Pre-Malignant; 3) Malignant (cancer can only be malignant) [4].

1.1.1. Benign tumour

A Benign Tumour is not always Malignant or cancerous. It might not invade close tissue or unfold to alternative components of the body the way cancer can. In most cases, the outlook with

International Journal of Machine Learning and Cybernetics (2018) 9:1399–1417
https://doi.org/10.1007/s13042-018-0834-5

ORIGINAL ARTICLE

Machine learning Applications for Research to Internet of Things

R. Anil Kumar

Abstract

Internet of Things (IoT) has become an important network paradigm and there are lots of smart devices connected by IoT. IoT systems are producing massive data and thus more and more IoT applications and services are emerging. Machine learning, as an another important area, has obtained a great success in several research fields such as computer vision, computer graphics, natural language processing, speech recognition, decision-making, and intelligent control. It has also been introduced in networking research. Many researches study how to utilize machine learning to solve networking problems, including routing, traffic engineering, resource allocation, and security. Recently, there has been a rising trend of employing machine learning to improve IoT applications and provide IoT services such as traffic engineering, network management, security, Internet traffic classification, and quality of service optimization. This survey paper focuses on providing an overview of the application of machine learning in the domain of IoT. We provide a comprehensive survey highlighting the recent progresses in machine learning techniques for IoT and describe various IoT applications. The application of machine learning for IoT enables users to obtain deep analytics and develop efficient intelligent IoT applications. This paper is different from the previously published survey papers in terms of focus, scope, and breadth; specifically, we have written this paper to emphasize the application of machine learning for IoT and the coverage of most recent advances. This paper has made an attempt to cover the major applications of machine learning for IoT and the relevant techniques, including traffic profiling, IoT device identification, security, edge computing infrastructure, network management and typical IoT applications. We also make a discussion on research challenges and open issues.

Keywords Machine learning · IoT · Networking · Application

1 Introduction

Internet of Things (IoT) is becoming a new pervasive and ubiquitous network paradigm offering distributed and transparent services [1]. Through IoT, lots of smart devices are connected, such as sensors, mobile phones and other smart devices. These smart devices can communicate with each other and exchange information. According to the IDC statistical report, there are over 50 billion IoT devices in the world; they will produce over 60ZB data by 2020 [2–4]. By collecting the data of these IoT devices and analyzing these data to sense and understand the environment, the complex systems can be constructed to enhance the quality of life, such as diagnosis of machine condition, human body activities, health monitoring, localization, and structural monitoring.

As the popularity and widespread use of IoT, the massive sensors and devices are generating massive data and various IoT applications are developed to provide more

A Survey on Machine Learning

A Big Data - AI Integration Perspective

R.Anil Kumar

Abstract—Data collection is a major bottleneck in machine learning and an active research topic in multiple communities. There are largely two reasons data collection has recently become a critical issue. First, as machine learning is becoming more widely-used, we are seeing new applications that do not necessarily have enough labeled data. Second, unlike traditional machine learning, deep learning techniques automatically generate features, which saves feature engineering costs, but in return may require larger amounts of labeled data. Interestingly, recent research in data collection comes not only from the machine learning, natural language, and computer vision communities, but also from the data management community due to the importance of handling large amounts of data. In this survey, we perform a comprehensive study of data collection from a data management point of view. Data collection largely consists of data acquisition, data labeling, and improvement of existing data or models. We provide a research landscape of these operations, provide guidelines on which technique to use when, and identify interesting research challenges. The integration of machine learning and data management for data collection is part of a larger trend of Big data and Artificial Intelligence (AI) integration and opens many opportunities for new research.

Index Terms—data collection, data acquisition, data labeling, machine learning

1 Introduction

We are living in exciting times where machine learning is having a profound influence on a wide range of applications from text understanding, image and speech recognition, to health care and genomics. As a striking example, deep learning techniques are known to perform on par with ophthalmologists on identifying diabetic eye diseases in images [1]. Much of the recent success is due to better computation infrastructure and large amounts of training data.

Among the many challenges in machine learning, data collection is becoming one of the critical bottlenecks. It is known that the majority of the time for running machine learning end-to-end is spent on preparing the data, which includes collecting, cleaning, analyzing, visualizing, and feature engineering. While all of these steps are time-consuming, data collection has recently become a challenge due to the following reasons.

First, as machine learning is used in new applications, it is usually the case that there is not enough training data. Traditional applications like machine translation or object detection enjoy massive amounts of training data that have been accumulated for decades. On the other hand, more recent applications have little or no training data. As an illustration, smart factories are increasingly becoming automated where product quality control is performed with machine learning. Whenever there is a new product or a new defect to detect, there is little or no training data to start with. The na¨ıve approach of manual labeling may not be feasible because it is expensive and requires domain expertise. This problem applies to any novel application that benefits from machine learning.

Moreover, as deep learning [2] becomes popular, there is even more need for training data. In traditional machine learning, feature engineering is one of the most challenging steps where the user needs to understand the application and provide features used for training models. Deep learning, on the other hand, can automatically generate features, which saves us of feature engineering, which is a significant part of data preparation. However, in return, deep learning may require larger amounts of training data to perform well [3].

As a result, there is a pressing need of accurate and scalable data collection techniques in the era of Big data, which motivates us to conduct a comprehensive survey of the data collection literature from a data management point of view. There are largely three methods for data collection. First, if the goal is to share and search new datasets, then data acquisition techniques can be used to discover, augment, or generate datasets. Second, once the datasets are available, various data labeling techniques can be used to label the individual examples. Finally, instead of labeling new datasets, it may be better to improve existing data or train on top of trained models. These three methods are not necessarily distinct and can be used together. For example, one could search and label more datasets while improving existing ones.

An interesting observation is that the data collection techniques come not only from the machine learning community (including natural language processing and computer vision, which traditionally use machine learning heavily), but have also been studied for decades by the data management community, mainly under the names of data science and data analytics. Figure 1 shows an overview of

- *Y. Roh, G. Heo, and S. E. Whang are with the School of Electrical Engineering, KAIST, Daejeon, Korea.*
  E-mail: {yuji.roh, geon.heo, swhang}@kaist.ac.kr
- *Corresponding author: S. E. Whang*

International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 5, May-2022, Impact Factor: 7.957

Controlling Traffic Light Sequence with Python

P. Suman Prakash

ABSTRACT

With the increasing population of India, there is also an increase in vehicles which needs control to regulate the flow. The purpose of this paper is to control the traffic which is a big issue mainly in metropolitan cities. The idea is to implement a smart traffic controller using image processing. The system will detect vehicles through images instead of using electronic sensors embedded in the pavement. A camera will be used to capture the image which is kept alongside the traffic light. The sequence of the camera is analyzed using the object counting method; the density of the vehicles will be counted and given the required changes in the signal. In this feature extraction from the input image is done and the count is calculated by comparing these features values with cutoff values. These cutoff values are statically specified and used to calculate the density. In this paper, an automatic counting method is proposed to calculate the count of the object. The paper proposes an automated system to detect emergency cars from CCTV footage using the text reading technique.

Keyword: Image Processing, Emergency vehicles detection, Object detection.

INTRODUCTION

In day-to-day life we have to face many problems related to traffic congestion which is becoming more serious every day. It has become very difficult to manage the traffic congestion and high number of road accidents which is increasing day by day. This situation is affecting our life in many ways such as health issues and pollution. There are many negative impacts of traffic congestion which includes to wasting time, inability to forecast travel time, higher chance of collisions due to tight spacing and constant stopping. The highway and roads are incapable of meeting the requirement of increasing number of vehicles.

The major cause leading to traffic jam is the large number of vehicles which was caused by the population and the development of economy. Instead of working on roads to control the traffic on roads various techniques have been devised to control the traffic.The project is to detect the traffic by using image processing to get the density of the vehicles and helping the emergency vehicle to give a brief way by text reading. The project system can be capturing the image which is used for counting the density of the vehicles and an emergency vehicle can be detected by text reading from a distance of 100 meters and change the signals without having the vehicle to stick into the traffic. Image tracking of moving vehicles can give us quantitative description of traffic flow.

METHODOLOGY

There are many methods of detecting vehicles on road such as motion detection, installing lasers on both sides of the road [6], etc., which is tedious and involves large number of hardware. This method uses image processing techniques to count the number of vehicles on road and estimate the density. The number of vehicles found can be used for surveying or controlling the traffic signal. The methodology is based on two parts, vehicle detection using image processing and emergency vehicle detection using image text recognition through image.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

Energy Efficient Cluster Based Routing Protocols in Large Scale Wireless Sensor Networks

Dr. S. Prem Kumar

Abstract—**In wireless sensor networks (WSNs), an extension of the lifetime of the network is one of the primary concerns of every routing protocol design. A critical study on The Low Energy Adaptive Clustering Hierarchy (LEACH) revealed that the scheme uses a probabilistic approach in selecting cluster heads. This approach allows weak nodes to be chosen as cluster heads (CHs) which cannot transmit the sensed data to the Base station (BS) hence affecting the throughputs of the network. Also single hop communication method was adopted which limits the network coverage and unnecessary data transmission of the heads affecting the lifetime of the network. In this research work, a heterogeneous form of LEACH called Servant–LEACH is proposed. The new protocol modified the election probability of the nodes by considering two factors in selecting the heads. i) The distance between the nodes and the base station and ii) the residual energies of the nodes. The proposed scheme further implemented soft and hard thresholds and servant nodes concept. The simulation results of the new scheme showed that the proposed protocol outperformed Threshold Distributed Energy Efficient Clustering (TDEEC) protocol in terms of stability period, throughputs, residual energy and the lifetime of the network**

Keywords— S-LEACH; Servant nodes; Network lifetime; Residual energy; distance; Matlab simulation

I. INTRODUCTION

Wireless Sensor Network (WSN) consists of a large number of sensors. The sensor network by their nature, have low processing power, low energy consumption and short transmission range for monitoring a physical environment. WSN can be used in a wide variety of areas including environmental monitoring, health, home applications, control (object detection and tracking), and surveillance [1][2]. Generally, in order to reduce energy consumption in WSNs, the clustering method is mostly used. In this technique, the sensor nodes are put into groups called clusters in which each cluster is headed by a node called a Cluster Head (CH). The rest of the nodes in the cluster is referred to as cluster members. These cluster members are responsible for capturing data and transmitting the sensed data directly or indirectly to the Cluster Heads (CHs). The CHs then aggregate the data and send the report to the Base Station (BS) for further analysis [3].

LEACH protocol is one of the first homogeneous cluster-based routing protocols to be proposed by [4]. Several other protocols built on LEACH have also been proposed. Younis and Fahmy [5] proposed Hybrid Energy-Efficient Distributed Clustering (HEED). HEED improved the scheme of the LEACH algorithm by including remaining energy. This method balanced the load on sensor nodes and extend the lifetime of the network. The protocol also offered the guarantee that the maximum energy node will be the cluster head inside its cluster range. The protocol did not consider distance in CHs' selection. Therefore distant CHs will dissipate a lot of energy to send their data to the BS.

Ramesh et al. [6] described the modified R-LEACH protocol which allows an alternative node to get substituted in place of a node that loses its energy. This is to allow the protocol to prolong the lifetime of the entire network and avoids data loss. The results showed that the Packet Delivery Ratio (PDR) and energy level have been enhanced compared to LEACH. The challenge in this protocol is similar to HEED which distance is not considered as criteria in selecting CHs. This allows distant nodes to dissipate so much energy in order to send their data to the BS.

Yassein et al. [7] developed a new Version LEACH (V-LEACH) protocol which is an improvement of the original LEACH protocol by selecting vice-CH that takes over the role of the CH in case it dies. In this protocol, when a CH dies, the cluster becomes useless because all data gathered by sensors in the cluster will never reach the sink. In addition to electing CH, the vice-CH is also selected. This approach ensures that cluster nodes data will always reach the BS and there is no need to elect a new CH each time the CH dies. This has extended the lifetime of the wireless network. However, the protocol did not consider residual energy in selecting the CH. As a result, nodes with less energy can become CHs which cannot transmit data to the BS. Cheng et.al. [8] Presented their findings on Energy Efficient Weight Clustering (EWC) protocol as an extension to LEACH protocol in which residual energy, distance, and node degree are considered as metrics to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 05, May-2020

A Scalable and Distributed Architecture for IoT

Dr. S Prem Kumar

Abstract—The advent of Internet of Things (IoT) has boosted the growth in number of devices around us and kindled the possibility of umpteen number of applications. One of the major challenges in the realization of IoT applications is interoperability among various IoT devices and deployments. Thus, the need for a new architecture – comprising of smart control and actuation – has been identified by many researchers. In this article, we propose a *Distributed Internet-like Architecture for Things (DIAT)*, which will overcome most of the obstacles in the process of large scale expansion of IoT. It specifically addresses heterogeneity of IoT devices, and enables seamless addition of new devices across applications. In addition, we propose an usage control policy model to support security and privacy in a distributed environment. We propose a layered architecture that provides various levels of abstraction to tackle the issues such as, scalability, heterogeneity, security and interoperability. The proposed architecture is coupled with cognitive capabilities that helps in intelligent decision making and enables automated service creation. Using a comprehensive use-case, comprising elements from multiple-application domains, we illustrate the usability of the proposed architecture.

Index Terms—IoT distributed architecture, dynamic service creation, usage control policies.

I. Introduction

In today's connected world, there are several means of ephemeral communication amongst devices, e.g., Bluetooth, GSM, NFC, WiFi, ZigBee, etc. However, the idea now is not only to connect with other communicating devices opportunistically, but also to be aware of various real-world non-communicable objects in the surroundings. This paradigmatic shift opens up new futuristic services. An important aspect of these services can be captured by the words of Mark Weiser. In his seminal paper [1], he provided a vision – "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it". This vision, in fact, is the driving force behind today's miniaturized technologies and communication substrates. Thus, we are about to witness a future where there will be thousands of inanimate objects for each person that will seamlessly communicate with each other to support everyday life in a smart way. In general, this paradigm is referred to as the "Internet of Things" (IoT). The idea is to form an intelligent network of these humongous numbers of devices, systems and equipments. Further, the ambit of IoT is expanding to include any-'thing' that could be represented or identified in the cyber (virtual) world even without having any direct communication interfaces on those "things".

Many IoT applications have been identified, e.g., smart home, smart logistics, smart transportation, smart health care, smart agriculture, etc. [2]. A common factor in all such applications is the inherent *smartness*. Being part of a "smart" application, various devices within an application domain can automatically collect data, share information among themselves, and initiate and execute services with minimal human intervention. Some of the desired characteristics of IoT objects (devices)[1] as well as IoT applications are listed below [3].

- Automation: Automation is a key feature of any IoT device and application. Autonomous data collection, processing, contextual inference, collaborating with other IoT objects and decision making should be supported by any IoT infrastructure.
- Intelligence: Objects in IoT should act intelligently. Building intelligence into these objects and empowering them to operate adaptively based on different situations is an important aspect. Situation and context awareness are the key entities for an intelligent system, which can operate with minimal human intervention.
- Dynamicity: An object in a IoT ecosystem can move from one place to another place. The IoT ecosystem should be able to dynamically recognize and adapt these objects based on the environment. Thus, dynamic management and integration of these objects across different environments and applications is crucial for a unified IoT architecture.
- Zero-configurations: To support easy integration of devices in the IoT ecosystem, plug-and-play feature should be available. Zero-configuration support encourages an easy and decentralized growth of IoT systems [4].

The main challenge in IoT is to manage and maintain large number of devices and react smartly according to the data generated by them. Some answers addressing this challenge can be seen under the umbrella of Future Internet and in projects such as BUTLER [5], COMPOSE [6], FIND [7], FIRE [8], IoT-A [9], etc. They deal with large scale networking, cognitive networking, network of networks [10], as well as service-oriented architecture development for a converged communication and service infrastructure, to mention a few. In

C. Sarkar, A. U. Nambi and R. V. Prasad are with the Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, 2628 ZH, Netherlands (e-mail: chayan@ieee.org, akshay.narashiman@tudelft.nl, rvprasad@ieee.org).

A. Rahim is with CREATE-NET, Trento, Italy (e-mail: abdur.rahim@create-net.org).

R. Neisse and G. Baldini are with European Commission Joint Research Center (JRC), Italy (e-mail: ricardo.neisse@jrc.ec.europa.eu, gian-marco.baldini@jrc.ec.europa.eu).

[1]We use the terms IoT object and IoT device interchangeably.

Secure Computing Arithmetic Operations using Fully Homomorphic Encryption

K. Seshadri Ramana

ABSTRACT

Nowadays, more and more organizations move their data to the cloud. When it comes to cloud computing, which is common among different industries for its speed and efficiency, data has to be decrypted to allow mathematical operations to be applied to it. Thus, in this case, the original data is seen in its plain format by the third-party service, which introduces a problem of keeping the data secret to avoid data leakages. Fully Homomorphic Encryption schemes help to address this issue by making computation applicable over ciphertexts. Most of the existent solutions, while providing good data protection require huge computational resources and produce big keys and ciphertexts. In this paper, we propose a new compact fully homomorphic encryption scheme with keys and output data which are well suited for practical use.

CCS CONCEPTS

• **Information systems** → **Data encryption**; • **Security and privacy** → **Cryptography**; • **Computer systems organization** → Cloud computing;

KEYWORDS

fully homomorphic encryption, secure computation, modular arithmetic

ACM Reference Format:

Alisa Gazizullina. 2018. Fully Homomorphic Encryption Scheme for Secure Computation. In *Proceedings of 2nd International Conference on the Art, Science, and Engineering of Programming (<Programming'18> Companion).* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3191697.3213794

1 INTRODUCTION

Any computation done on a computer involves the use of a computational model. There are two existing models: the first one is based on binary arithmetic, the second one on modular arithmetic. Construction of a Fully Homomorphic Encryption Algorithm requires the computational model chosen in advance.

Papers of Gentry and his followers introduced a scheme based on binary logic [2]. It is difficult to construct an efficient implementation for it. Rivest R.L., Adleman L., Dertouzos M. L. in their early work[8] introduced modular arithmetic to FHE algorithm. However, that approach turned out to be non-persistent. J. Domingo-Ferrer continued to work in that direction [3]. The major drawback of the algorithm he proposed was the exponential growth of data caused by multiplication.

Most of the proposed schemes, while securing computation over data, suffer from not being efficient for a practical use. That defines our goal to develop a new efficient in terms of the memory requirements and complexity of computations fully homomorphic data encryption scheme.

The proposed algorithm is based on modular arithmetic in the meaning of computer model presented by Akushskii I. A., Yuditskii D.I. [5] and thus avoids an increase in data size. Also, it is efficiently implementable on digital machines, as we introduced the notion of multiplication tables for computations over ciphertexts.

<Programming'18> Companion, April 9–12, 2018, Nice, France

ACM ISBN 978-1-4503-5513-1/18/04…$15.00
https://doi.org/10.1145/3191697.3213794

2 BASICS

Let us start with the formal definition of **fully homomorphic encryption** [4]. Fully homomorphic encryption supports arbitrary computation over ciphertexts with no need to decrypt and perform computations over original data. Thus, FHE concerns an encryption algorithm E and a decryption algorithm D, such that:

$$C_1 = E(X_1),\ C_2 = E(X_2) \tag{1}$$

$$D(f(C_1, C_2)) = f(X_1, X_2) \tag{2}$$

where C_1 and C_2 are ciphertexts, X_1 and X_2 are plaintexts, f - arbitrary function.

To allow efficient computations, a cryptosystem has to be compact [9]. We used **modular arithmetic** and **multiplication tables** for computation over encrypted data for this purpose.

Also, we proved that the introduction of extra **randomly** chosen elements ("noise" vectors) to the ciphertext evaluation algorithm preserves the homomorphic nature of the overall scheme while bringing in additional complexity to the breaking scheme, what makes the cryptosystem more strong.

Set up:

(1) The algorithm is considered for the ring Z_M and modulus M

(2) The result of all the mathematical operations cannot exceed M

(3) Let original message X be the integer number, the size of X is t . For the purposes of unique decodability and correctness, the modulus M should be large enough to avoid overflow and should satisfy: $X \in [0, M-1]$, $M > 2^t$

3 PROPOSED CRYPTOSYSTEM

Proposed cryptosystem consists of three probabilistic polynomial time algorithms: Key Generator, Encryptor, Decrypter.

3.1 Key Generation

The secret key consists of modulus M, vector m of relatively prime moduli, the set of vectors $s_i \forall\ i = 1, \ldots, k$, permutation matrix P_C , the number r.

Artificial Intelligence in Brain Informatics

Image Processing in brain tumor MRI

K. Lakshmi

Article info

Article history:
Received 25 November 2021
Received in revised form 19 February 2022
Accepted 21 February 2022

ABSTRACT

Introduction: In modern days, checking the huge number of MRI (magnetic resonance imaging) images and finding a brain tumour manually by a human is a very tedious and inaccurate task. It can affect the proper medical treatment of the patient. Again, it can be a hugely time-consuming task as it involves a huge number of image datasets. There is a good similarity between normal tissue and brain tumour cells in appearance, so segmentation of tumour regions become a difficult task to do. So there is an essentiality for a highly accurate automatic tumour detection method.

Method: In this paper, we proposed an algorithm to segment brain tumours from 2D Magnetic Resonance brain Images (MRI) by a convolutional neural network which is followed by traditional classifiers and deep learning methods. We have taken various MRI images with diverse Tumour sizes, locations, shapes, and different image intensities to train the model well. Furthermore, we have applied SVM classifier and other activation algorithms (softmax, RMSProp, sigmoid, etc) to cross-check our work. We implement our proposed method using "TensorFlow" and "Keras" in "Python" as it is an efficient programming language to perform fast work.

Result: In our work, CNN gained an accuracy of 99.74%, which is better than the state of the result obtained so far.

Conclusion: Our CNN based model will help the doctors to detect brain tumours in MRI images accurately, so that the speed in treatment will increase a lot.

1. Introduction

Medical imaging refers to several techniques that can be used as non-invasive methods of looking inside the body [1]. The main use of medical image in the human body is for treatment and diagnostic purposes. So, it plays a significant role in the betterment of treatment and the health of the human.

Image segmentation is a crucial and essential step in image processing that determines the success of image processing at a higher level [2]. In this case we have mainly focused on the segmentation of the brain tumour from the MRI images. It helps the medical representatives to find the location of the tumour in the brain easily. Medical image processing encompasses the utilization and exploration of 3D image datasets of the physical body, obtained most typically from computed tomography (CT) or Magnetic Resonance Imaging (MRI) scanner to diagnose pathologies or guide medical interventions like surgical planning, or for research purposes. Medical image processing is applied by radiologists, engineers, and clinicians to understand the anatomy of either individual patients or population groups highly. Measurement, statistical analysis, and creation of simulation models which incorporate real anatomical geometries provide the chance for more complete understanding, as an example of interactions between patient anatomy and medical devices.

Tumour: The word "Tumour" is a synonym for the word "neoplasm" which is formed by an abnormal growth of cells. A tumour is significantly different from cancer [3].

1.1. Classification of tumour

There are three basic types of tumours: 1) Benign; 2) Pre-Malignant; 3) Malignant (cancer can only be malignant) [4].

1.1.1. Benign tumour

A Benign Tumour is not always Malignant or cancerous. It might not invade close tissue or unfold to alternative components of the body the way cancer can. In most cases, the outlook with

EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Role-Based Access Control in Cloud Computing

Dr.K.Sreenivasulu

[1]Department of Computer Science and Application, G.Pullaiah College of Engineering and Technology, Kurnool, India

Abstract

The cloud reduces the user's burden to many folds. But cloud providers and cloud users with dynamic relationship, are in distinct security domains. Amongst various challenges with cloud, the crucial one is to detect and protect the user's data from unauthorized accesses. In cloud, users are not legendary by their predefined identities. Instead, they are providing accesses based on their characteristics and attributes. This work is focusing on available access control mechanisms and one that applicable for cloud environment. The paper also proposes an Efficient and Flexible Role-Based Access Control (EF-RBAC) mechanism for the cloud computing environment to achieve confidentiality and security. RBAC limits the accesses for resources within an organization to authorized users only and also guarantees that a user can solely access specific information they are authorized for by the organization policy. The proposed scheme adds flexibility to the RBAC for better cloud user's experience.

Keywords: Cloud Computing, Access control, Role-Based Access Control, Security, DDOS, Multimedia, Information Security.

Received on 08 September 2019, accepted on 01 November 2019, published on 18 November 2019

doi: 10.4108/eai.13-7-2018.161438

1. Introduction

Cloud computing creates several computing resources (computing centers, huge data centers, etc.) to work in a collaborative network system over the internet. Also, a secure, huge and fast network of data storage and computing is supported by the cloud for all kinds of users [1]. The three major cloud service delivery models are Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS).

Although the cloud is providing numerous benefits but the main concern associated with both ends (i.e. consumer and provider) is security [2]. The consumer's concern is about maintaining the secrecy of their private data stored over the cloud servers [28]. However, the cloud provider's concern is that their services and resources remain accessible to authorized persons only. Thus, without proper access control policies, the cloud is always vulnerable to various threats and attacks. Organizations hesitate to adopt cloud for transfer of their multimedia storage and computations to cloud servers as they are not sure that whether they are 100% secure or not. As any access breach to user's personal multimedia data can be a matter of stake for them. In nutshell, the confidentiality and integrity of the user's data stored at the third party public cloud servers must not be compromised in any case [30]. Because of this, an effective mechanism for access control and management can play a crucial role as it is directly linked with the primary required characteristics those are authorization, confidentiality, availability, and integrity.

Cloud providers must ensure the basic functionalities for controlling unauthorized accesses or in other words providing secure access to the services based on the service level agreement (SLA), protecting access of one user's data from other users, providing a consistent state to consumer always, controlling users accesses based on their earlier defined privileges i.e. effectively maintaining and managing access control rules etc.

Traditionally access control mechanisms are of the following three categories:

*Corresponding Author: shilpi13n@gmail.com

IJSTE - International Journal of Science Technology & Engineering | Volume 4 | Issue 10 | April 2018
ISSN (online): 2349-784X

Rescue Robot in Coal Mines Using IoT

K. Tarakeshwer

Abstract

Coal mine is a hazardous place in which numerous lethal variables are risky for human life, particularly when impacts happen. Rescue team typically doesn't have a clue about the real circumstance of the mine passage. Accordingly, it might be exceptionally risky for rescuers to go into mine passages to inquiry survivors without distinguishing ecological data previously. To tackle this issue, robot is created for helping individuals to do the rescue work. The robot is used for detecting the explosion environment of coal mine. We developed a prototype of a fully autonomous robot which can be used to indicate presence of harmful gases inside a mine for mine rescue operations in case of emergencies caused by natural calamities such as explosion. Coal mine rescue robot is a sort of portable robot. It can go into blast environment and discover gas content.

Keywords: Coal Mine, Hazardous, Rescue

I. INTRODUCTION

A coal mine is an underground tunnel system. There only a few pitheads on ground. If there are some accidents, people are easily trapped in tunnel and often cannot escape from it. It has dangerous accidents as collapse, gas explosion, CO, CO2 poison gas, low O2 content, high temperature, smoke, coal dust, fire, water, etc. All these accidents can kill people easily.

CH4 gas is intergrown with coal. When coal is mined, CH4 gas is released. Gas is pushed off by forced ventilating system. But if the ventilating system is faulty or gas is leaked from coal layer, gas diffuses throughout the tunnel. A flame current can cause a heavy gas explosion. Mine tunnel passageway is narrow, so the explosion wave can destroy any thing in the tunnel. All devices and people may be affected, and the gas of CH4, CO, CO2 and coal dust are filled in the tunnel, and the environment of the tunnel comprises of low O2 content and high temperature. Besides, the forced ventilate system has been damaged, the gases cannot be pushed out and gets accumulated in tunnel. A fire may cause a second explosion. People in tunnel could be poisoned by CO, stifled by CO2 and low O2 content, high temperature and coal dust. Rescuers on ground cannot go into mine tunnel because situation is not known and they may be killed by second explosion. So, detection of mine tunnel situation is the first mission. A Robot is an ideal tool in coal mine disaster. The robot used in coal mine tunnel must have many special characteristics which are different from other robots on ground.

Coal mine tunnel is a special environment. The first problem is explosion gas is everywhere in tunnel. Any fire can cause an explosion. Robot must be designed as a flame-proof device to avoid malfunction of components. The second problem is the mine have narrow tunnel and rugged. The middle of the tunnel is railway. One side of the railway is belt transmission. The other side is a narrow road on coal. The mine passageway is filled with many obstacles and rugged coal road, so it is difficult to move inside the mine tunnel. But various obstacles must be crossed. Communication is another difficult problem in mine tunnel because electromagnetic wave is absorbed and echoed in a coal tube. Because of many corners in the tunnel, Wave cannot cross these corners easily.

II. PROBLEM STATEMENT

The mobile robot is designed so that it can run in explosive environment, climb over uneven surface areas, check gas contents and perform live surveillance using a camera.

Big Data Security and Privacy Issues

P. Rama Rao

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

P. G. *et al. Journal of Cloud Computing: Advances, Systems and Applications* (2020) 9:61
https://doi.org/10.1186/s13677-020-00214-6

Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH Open Access

Secure Data Deduplication of Cloud Computing

P. Rama Rao

Abstract

Data redundancy is a significant issue that wastes plenty of storage space in the cloud-fog storage integrated environments. Most of the current techniques, which mainly center around the static scenes, for example, the backup and archive systems, are not appropriate because of the dynamic nature of data in the cloud or integrated cloud environments. This problem can be effectively reduced and successfully managed by data deduplication techniques, eliminating duplicate data in cloud storage systems. Implementation of data deduplication (DD) over encrypted data is always a significant challenge in an integrated cloud-fog storage and computing environment to optimize the storage efficiently in a highly secured manner. This paper develops a new method using Convergent and Modified Elliptic Curve Cryptography (MECC) algorithms over the cloud and fog environment to construct secure deduplication systems. The proposed method focuses on the two most important goals of such systems. On one side, the redundancy of data needs to be reduced to its minimum, and on the other hand, a robust encryption approach must be developed to ensure the security of the data. The proposed technique is well suited for operations such as uploading new files by a user to the fog or cloud storage. The file is first encrypted using the Convergent Encryption (CE) technique and then re-encrypted using the Modified Elliptic Curve Cryptography (MECC) algorithm. The proposed method can recognize data redundancy at the block level, reducing the redundancy of data more effectively. Testing results show that the proposed approach can outperform a few state-of-the-art methods of computational efficiency and security levels.

Keywords: Convergent encryption (CE), Modified elliptic curve cryptography (MECC), Edge computing, Integrated cloud and fog networks, Hash tree. Secure hash algorithm (SHA)

Introduction

The data gathered through different sources and the Emergence of the Internet of Things in all aspects of applications increases data volume from petabytes to yottabytes, necessitating cloud computing paradigm and fog networks to process and store the data. Cloud computing (CC) produces a network-centered environment vision to users which provides access to the internet, to a collective pool of programmable grids, servers, software, storage, and amenities that could be quickly freed, with less supervision and communication to the cloud service provider. Data processing in all ways is carried out remotely in the cloud server with the help of internet connectivity. Fog computing provides the local infrastructure to process the application locally and then connects to the cloud. The fog environment reduces delay when compared to the application connected to the cloud for processing. The application developed to process and store the data needs end-to-end security, communication protocols, and resources to access information stored in the cloud and fog environments. Smart applications are built with the help of sensors and actuators, and the data is stored in the cloud environment; and edge computing facilities are also used along with the local infrastructure, termed as fog, to process the data without delay. Internet of Things does not end up with an information system but tries to build a cyber-physical system [1]. Edge computing provisions the

* Correspondence: Abbasi@basu.ac.ir
[4]Department of Computer Engineering, Engineering Faculty, Bu-Ali Sina University, Hamedan 65178-38695, Iran
Full list of author information is available at the end of the article