DIGIT

Department of Computer Science & Enginering

Anantha Lakshmi Institute of Technology & Sciences

Volume 08 Jul-Dec 2022

Inside this issue:

VISION & MISSION

VISION : To produce technically competent computer science professionals with high quality education in cutting edge technologies and professional ethics.

MISSION :

M1: Impart quality technical education in design and implementation of IT applications through innovative teaching - learning practice.

M2: Provide state-of-art computing infrastructure to enable practical learning experience that foster problem solving and technical communication skills.

M3: Provide quality learning experiences through experiential learning for students and faculty to carry out multidisciplinary research projects with innovative ideas and professional ethics for sustainable development.

PROGRAM EDUCTIONAL OBJECTIVES

PEO 1 : **Demonstrate proficiency in fundamental concepts and advanced technologies of computer science in their careers and/or obtain a higher degree.**

PEO 2 : **Analyze complex computing problems in multidisciplinary area and creatively solve them with analytical decision making and programming skills**

PEO 3 : **Recognize ethical dilemma in work environment and apply professional code of Ethics to excel as successful software professional, researcher and entrepreneur.**

PROGRAM SPECIFIC OUT COMES

PSO 1 : Apply the knowledge of programming languages, data structures, algorithms and standard software engineering principles to develop viable solutions for complex computing problems.

PSO 2 : Design and develop efficient Web and Mobile based applications under realistic constraints.

PSO3 : Apply theoretical principles of core and advanced computer science to solve engineering problems.

PROGRAM OUTCOMES

PO 1	**Engineering Knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
PO 2	**Problem Analysis:** Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
PO 3	**Design/Development of Solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
PO 4	**Conduct Investigations of Complex Problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
PO 5	**Modern Tool Usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
PO 6	**The Engineer and Society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
PO 7	**Environment and Sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
PO 8	**Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
PO 9	**Individual and Team Work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
PO 10	**Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
PO 11	**Project Management and Finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
PO 12	**Life-long Learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Cloud Computing : Architecture & Services of Cloud

Cloud computing refers to any situation in which computing is done in a remote location (out in the clouds) rather than your portable device or desktop wherein the computing power is tapped over an internet connection. At a basic level cloud computing is simply a means of delivering IT resources as services. Almost all IT resources can be delivered as a cloud service: applications, compute power, storage capacity, networking, programming tools, communication services even collaboration tools. Cloud computing began as large-scale internet service providers such as Google, Amazon, and others built out their infrastructure. A new architecture emerged: A massively scaled, horizontally distributed system resources, abstracted as virtual IT services and managed as continuously configured pooled resources. This new model was applied to internet services.

The architecture of Cloud Computing

When talking about a cloud computing system, it is helpful to divide it into three sections: the front end, the central system, and the back end. They connect to each other through a network, usually the Internet via a set of protocols. The front end is the side the computer user, or client. The back end is the "cloud" section of the system.

The front end includes the client's computer and the application required to access the cloud computing system. This could include services like accessing social networking accounts via web browsers, Salesforce (CRM application), Zuora (subscription business model), etc.

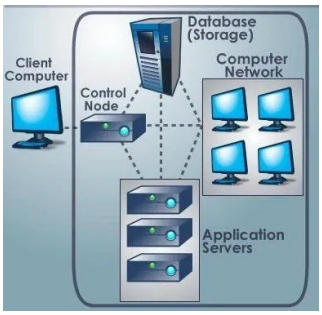
A central server administers the system, monitoring traffic and client demands to ensure everything runs smoothly. It follows a set of rules called protocols and uses integration software called middleware. Middleware allows networked computers to communicate with each other via web services or REST APIs. Middleware software can run on-premise or on the cloud. The best example for an on-premise middleware is Tibco software and for cloud-based, there are many like Oracle Fusion Middleware, Mulesoft, Red Hat JBoss Fusee, etc. Most of the cloud-supported software support on-premise too.

On the back end of the system are the various computers, servers, and data storage systems that create the "cloud" of computing services. In theory, a cloud computing system could include practically any computer program you can imagine, from data processing to video games. Usually, each application will have its own dedicated server.

So when a customer creates an account in the Salesforce system (front-end application) the account details are sent to Middleware software like Mulesoft via a set of protocols. Next, the account details are pushed end systems like other CRM systems, cloud database, etc.

In the initial days, only the front-end system was available on the cloud and middleware would run on-premise. This architecture would slower the data processing. In recent days, middleware systems are also being pushed to the cloud to achieve better results in data processing and fasten up response time to end users.

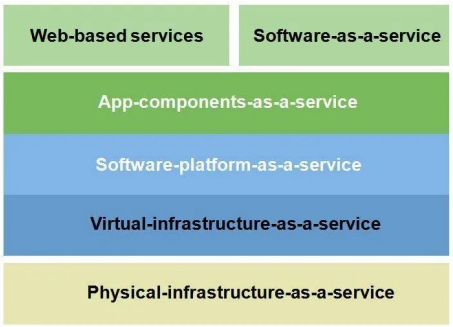
To secure client's data, a cloud computing system must make a copy of all its clients' information and store it on different servers as a backup. The copies enable the central server to access backup machines to retrieve data that otherwise would be unreachable.



Services of Cloud Computing

- **Software as a Service(SaaS):**

It is at the highest layer and features a complete application offered as a service, on-demand, via multi-tenancy, meaning a single instance of the software runs on the provider's infrastructure and serves multiple client organizations. SaaS represents a number of licensing and pricing models for the vendors to choose from that includes pay-as-you-go, subscription-based, revenue-based, transaction-based and other. Some even go as far as offering complete services free of charge preferring to monetize with ads only.



Platform as a Service(PaaS):

The middle layer is the encapsulation of a development environment abstraction and the packaging of a payload of services. PaaS is an integrated platform to build, test and deploy custom applications.

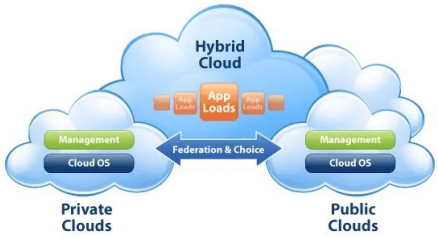
- **Hardware as a Service(HaaS):**

HaaS is at the lowest level and is a means of delivering basic storage and compute capabilities as standardized services over the network. Servers, storage systems, switches, routers, and other systems are pooled (through virtualization) to handle specific types of workloads from batch processing to server augmentation during peak loads.

Different modes of Cloud Computing

Public:

Public clouds are run by third parties, and jobs from many different customers may be mixed together and the servers, storage systems, and other infrastructure within the cloud. End users don't know who else's job may be running on the server, network, or disk as their own jobs.



Private:

Private clouds are a good option for companies dealing with data protection and service-level issues. Private clouds are on-demand infrastructure owned by a single customer who controls which applications run and where. They own the server, network, and disk and can decide which users are allowed to use the infrastructure.

Hybrid:

Hybrid clouds combine public and private cloud models. You own parts and share other parts, though in a controlled way. Hybrid clouds offer the promise of on-demand, externally provisioned scale, but add the complexity of determining how to distribute applications across these environments.

Submitted By :
M LAHARI
192G1A05B9

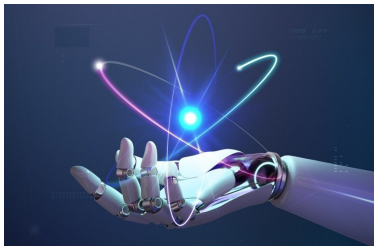
What is Artificial Intelligence? How AI is Affecting our lives Positively

Artificial Intelligence best suits the phrase **"Simplify Human Work"**. Building new machines, applications, smart infrastructure, and software – all these innovations are to simplify or reduce human work. Artificial Intelligence is all about feeding intelligence to machines or software to get the desired output and to automate things so that less human intervention is required.

Artificial intelligence (AI) is an ever-evolving field that is constantly improving and introducing new and innovative techniques to the world. In recent years, AI has made incredible strides, thanks to advances in machine learning, deep learning, and natural language processing. A recent innovation is a chatbot, ChatGPT developed by OpenAI which is capable of generating articles, language translations, engaging in conversations, and many more as it is further developed and trained.

John McCarthy an American computer scientist, and a Stanford University graduate known to be one of the founders of Artificial Intelligence used the term Artificial Intelligence for the first time in 1956. But, It took decades to experience the wonders that AI can do. The present era is only dominated by AI. Today AI is everywhere, be it online shopping, online search, factory automation, healthcare, education, robotics, metaverse, cybersecurity, virtual assistants – you name an industry AI is already there.

Innovations in Artificial Intelligence



In recent years, there have been several significant innovations in AI that have the potential to transform the way we live and work:

GPT-3

GPT-3 (Generative Pre-trained Transformer 3) is an artificial intelligence language model developed by OpenAI. It is one of the most advanced AI language models to date, with the ability to generate human-like text with unprecedented accuracy. GPT-3 has been used to develop a wide range of applications, including chatbots, language translation, and content creation.

Neuralink

Neuralink is a startup founded by Elon Musk that is developing implantable brain-computer interfaces (BCIs). BCIs are devices that allow humans to control computers and other devices using their thoughts. Neuralink's technology has the potential to revolutionize the way we interact with machines and could even help people with disabilities regain lost functions.

DeepMind AlphaFold

AlphaFold is an AI system developed by DeepMind, a subsidiary of Alphabet Inc. AlphaFold uses deep learning algorithms to predict the three-dimensional structures of proteins. This has the potential to revolutionize the field of protein folding, which is essential for developing new drugs and understanding diseases.

Generative Adversarial Networks

Generative Adversarial Networks (GANs) are a type of AI algorithm that allows machines to generate synthetic data that is similar to real-world data. GANs have been used to develop applications such as photorealistic image generation and video game development.

Autonomous vehicles

Autonomous vehicles are another area where AI is making significant strides. Companies such as Tesla and Google are developing self-driving cars that use AI algorithms to navigate roads and make decisions in real-time. This technology has the potential to revolutionize the way we travel and could significantly reduce accidents caused by human error.

Quantum Machine Learning

Quantum Machine Learning is an emerging field that combines quantum computing and AI. This technology has the potential to significantly speed up AI algorithms and enable machines to process vast amounts of data much faster than traditional computing systems. Quantum Machine Learning is still in its early stages, but it has the potential to revolutionize AI and many other fields.

Artificial Intelligence in Healthcare

AI is changing the landscape of the healthcare sector by helping in Disease detection and diagnosis, Personalized treatment plans, Remote patient monitoring, and Drug discovery and development. AI has the potential to automate health operations in the time to come. Read in detail about the impact of Artificial Intelligence in the Healthcare sector.

What is Artificial Intelligence? How AI is Affecting our lives Positively

Artificial Intelligence in Marketing

Artificial Intelligence in marketing is a technique that uses data and machine learning to provide campaigns that help companies achieve their goals more successfully. AI can help to build stronger customer relationships, determine your target audience, semantic research, promote your business, promote your business, digital advertising, and content creation. Read in detail about Artificial Intelligence in Marketing.

AI in Metaverse

Metaverse is all about creating an imaginary world by using Virtual Reality and Augmented Reality (AR) technologies. Artificial Intelligence (AI) and Machine Learning (ML) technologies help to create intelligent and responsive virtual environments and characters in the metaverse. Read in detail about Metaverse.

AI in Robotics

Artificial intelligence-based robots are already widely employed in health, manufacturing, and engineering and more innovations are awaited in robotics. With AI it has become possible to replicate human brains and activities. Advanced humanoid robots are capable of multiple activities that are mere reflexes of a human being. Read in detail about humanoid robots.

AI in Cybersecurity

AI is becoming an increasingly important tool in cybersecurity, helping organizations to identify and respond to threats in real-time, study malware detection, study user behavior analytics, and stay one step ahead of cybercriminals. Read more about cybercrime and cybersecurity.

Major Branches of AI

- **Robotics:** This branch of AI involves the creation of intelligent machines that can perform tasks autonomously. Robotics combines AI with mechanical engineering, computers, and other disciplines.

- **Computer Vision:** This branch of AI involves teaching machines to recognize and interpret visual information from the world around them. Computer vision is used in applications like facial recognition and self-driving cars.

- **Natural language processing:** This branch of AI focuses on understanding and generating human language. It includes tasks like language translation, sentiment analysis, and speech recognition.

- **Machine Learning:** This branch of AI involves developing algorithms that can learn from data and make predictions or decisions based on that data.

- **Neural Networks:** Computer that can act like or simulate the functioning of the brain.

- **Expert system:** These are AI systems that are designed to mimic the decision-making ability of a human expert in a particular field. Expert systems are used in areas like medicine, law, and finance. For example – an expert system helps doctors in diagnosing diseases.

- **Cognitive Computing**: This branch of AI aims to create machines that can think and reason like humans. Cognitive computing systems are designed to understand complex problems and develop solutions based on that understanding.

Submitted By :
G DEEPA
192G1A0575

The Urgent Need to Improve Cybersecurity in the Education System

The education sector is considered to be highly vulnerable to cyber threats. The 2018 Education Cybersecurity Report, suggests that education institutions are struggling with various things like application security, endpoint security, and patching cadence. With this, the education industry is ranked the worst at cybersecurity out of 17 major industries. This implies that there is a need for preventive measures to Improve Cybersecurity in the Education System.

According to a report by the U.S Education department, students browsing the internet for information and such learning purposes are prone to dangerous cyberattacks. Educational institutions are facing huge pressure to safeguard the sensitive information of students with the rising issue of cybersecurity.

Lately, schools have started using technological methods to store data, but many schools are still not adhering to monitoring and protecting network infrastructure. Institutions are now becoming digitalized in compiling a massive amount of data including assessment information, learning tool data, educator observations, attendance data, instructor feedback, and summative evaluations.

Meanwhile, as the Internet of Things (IoT) gain momentum, students are using more than one device in classrooms, where all of them are not secured. Educational institutions are underestimating the need for a protective solution across all institution networks.

There is an urgent need to deal with cyber frauds in India, as schools collect an incredible amount of personal data. In order to escape from cybercrime, understand the common mistakes that lead to cybercrime.

Educational institutions have become more prone to cyber hacks due to:

Financial gain: The core idea of every hacker is to gain personal data or financial credentials to withdraw money. With schools and colleges handling a large number of student fees, they are susceptible to cyberattacks.

Data theft: What else than hacking personal information and sending them to the third party? Well, this is what hackers do! Since schools are incompetent in handling a huge amount of sensitive details of children during admission, they become a prime target for cyber frauds in India.

According to me, a lack of proper resources and poor knowledge of cybersecurity in schools and colleges is a serious concern for the education sector. It is the responsibility of the school to protect information and secure the network to overcome this menace.

Before moving forward, let me give you an insight into the three weaknesses faced by this industry:

Application security: Many schools are relying on online applications for data collection, testing, and analysis. Any slight change observed in your network should be taken seriously. Thus, schools and universities need to build application security into their system, incorporate vulnerability scans, penetration tests, etc. to prevent security flaws.

Endpoint security: Vulnerable endpoints are on the rise with students and staff using multiple personal devices. Children are seen connecting their devices to the same home network that are not secured.

Schools need to choose endpoint security software that can easily detect vulnerabilities and unify network management. Enrolling children and faculty into cybersecurity training programs will create awareness about cybersecurity.

Make sure you don't forget to integrate an endpoint segmentation!

Patching cadence: As known to all, updating your system regularly can keep cyber threats at bay. Patching involves determining vulnerabilities in the system and knowing the number of critical vulnerabilities that need to be patched. There are several security companies like McAfee that helps in identifying the vulnerabilities and provides temporary fixes until an IT member completes the patch.

The next question is, what are the reasons for these cyber-attacks:

Lack of budget or resources

The education sector is not financially stable to invest in a cybersecurity team or software.

Cultural differences

Schools and universities without a secured MDM solution can open the door for cyber attacks.

No policy in place

Set strict policies for using a protected network and implement it effectively across the school campus.

The Urgent Need to Improve Cybersecurity in the Education System

In various schools, Children bring their own devices which can increase the difficulty of securing a wider network without any protection. This can infect devices and eventually turns to be a favorable hub for a data breach. Head down to know how this can be prevented through some basic steps.

Preventive Measures to be taken by the Education Sector

I recommend a few top tips to protect oneself from the prey of cyberattacks. Go through it.

- **Ensure strong password protection for all devices**

Never forget to secure your password and refrain from sharing information among peers or other staff members. Make your passwords strong by using characters and changing them annually.

- **Network security training is necessary**

Data breaches are a result of human errors that can be avoided by providing a basic security training regimen for students and staff. You can also introduce cybersecurity training to mitigate risks.

Training can be given on how to differentiate between safe and unsafe sites while browsing, educating them about cybersecurity and its types, identifying suspicious behavior, and motivating all to use antiviruses and malware.

- **Invest in the best firewalls**

Having a mitigation strategy in place works well wherein you can avoid risk by early detection. Isn't it great if you know where your vulnerabilities are? Develop clear and strict rules so that everyone follows it. Having cybersecurity policies or a formal audit can help in validating whether the institution is following the rules set.

These audits are performed by a third party who will help in the assessment of technology infrastructure, organizational policies, and user training to understand the risks. What can be done now?

Act Fast!

Keep all your networks free from malware by shifting to portable antivirus software. Understand the causes of cybercrime and preventive measures.

With the huge volume of data owned by these institutions and the increase in connected devices, this sector urgently requires cybersecurity. It is important to move from the traditional anti-virus solutions, and manual practices and step into the modern world.

Cybersecurity is no longer a problem just for the IT sector, it has to be treated through collaborative effort before it turns out to be a global problem. All sectors need to join hands to combat this issue. Take a step against cyber frauds in India by shifting to automation tools!

Submitted By :
T GOWSIYA
192G1A0575

Detection of digital photo image forgery

Digital image forgery is the process of manipulating photographic images using image-processing tools like digital photo editing software to produce a digital image as evidence to the court; there is a need to identify the authenticity of the image. Digital Image forgery can be classified as the forgery with copy move and without copy move. In case of copy move type, some part of the image is cut and pasted somewhere in the image so that there are no manipulations like rotation, scaling etc. In the other case, due to the above-mentioned types, the data becomes highly correlated. The advent of the modern digital technology has not only brought about the prominent use of digital images in our daily activities but also the ease of creating image forgery using public accessible and user friendly image processing tools such as Photoshop. Hence the need for image authenticity assurance and detection of image forgery such as photomontage becomes increasingly acute as digital images takes role as news photographs, legal evidence and digital financial document.

A comparative study of the existing algorithms helps to investigate new methods. It opens up new avenues of research. It also helps the real world to overcome the problems being faced due to photomontage and forgery.

The literature survey has revealed that a substantial amount of work has been done in the field of digital image forgery and forensic science. Various algorithms and mathematical models were developed for detecting digital image forgery and various digital image forgery prevention methodologies, tools and techniques.

Manipulation of early photographic images was not an easy task, requiring a high level of technical expertise and specialized equipment. Alterations had to be made to the negatives, thus, if access could be obtained to the negatives, the authenticity or otherwise of the image could be determined by visual examination.

Tampering with photographic images dates back almost to the time when permanent photographic images were first created. One of the earliest instigators of photographic image tampering was Vladimir Ilyich Lenin, who, for political reasons, instructed that certain individuals be removed from photographs

Submitted By :
K PRAVEEN KUMAR
192G1A0589

Digital Jewelry

Mobile computing is beginning to break the chains that tie us to our desks, but many of today's mobile devices can still be a bit awkward to carry around. In the next age of computing, there will be an explosion of computer parts across our bodies, rather than across our desktops. Jewelry is worn for many reasons – for aesthetics, to impress others, or as a symbol of affiliation or commitment. Basically, jewelry adorns the body and has very little practical purpose. The combination of microcomputer devices and increasing computer power has allowed several companies to begin producing fashion jewelry with embedded intelligence i.e. Digital jewelry.

What is Digital jewelry?

Digital jewelry is fashion jewelry with embedded intelligence. It can best be defined as wireless, wearable computers that allow you to communicate by way of e-mail, voicemail, and voice communication.

In this post, we shall go through how various computerized jewelry (like earrings, necklace, ring, bracelet, etc.,) will work with mobile embedded intelligence.

Introduction

The latest computer craze has been to be able to wear wireless computers. Best examples are Red Tacton technology, wearable biosensors, smart watches etc. The "Digital Jewelry" looks to be the next sizzling fashion trend of the technological wave. In the next wave of mobile computing devices, our jewelry might double as our cell phones, personal digital assistants (PDAs) and GPS receivers.

The combination of shrinking computer devices and increasing computer power has allowed several companies to begin producing fashion jewelry with embedded intelligence. Today, manufacturers can place millions of transistors on a microchip, which can be used to make small devices that store tons of digital data. Digital Jewelry appears to be one of the biggest growing promotions of its time. Imagine being able to email your boss just by talking into your necklace. The whole concept behind this is to be able to communicate to others by means of wireless appliances. The other key factor of this concept market is to stay fashionable at the same time.

Digital jewelry, can help you solve problems like forgotten passwords and security badges. These devices have a tiny processor and unique identifiers that interact with local sensors. Digital jewelry, is a nascent catchphrase for wearable ID devices that contain personal information like passwords, identification, and account information. They have the potential to be all-in-one replacements for your drivers' license, key chain, business cards, credit cards, health insurance card, corporate security badge, and loose cash. They can also solve a common dilemma of today's wired world the forgotten password.

How does Digital Jewelry work?

Soon, cell phones will take a totally new form, appearing to have no form at all. Instead of one single device, cell phones will be broken up into their basic components and packaged as various pieces of digital jewelry or other wearable devices. Each piece of jewelry will contain a fraction of the components found in a conventional mobile phone. Together, the digital-jewelry cell phone should work just like a conventional cell phone.

The various components that are inside a cell phone are Microphone, Receiver, Touchpad, Display, Circuit Board, Antenna, Battery.

IBM has developed a prototype of a cell phone that consists of several pieces of digital jewelry that will work together wirelessly, possibly with Bluetooth wireless technology, to perform the functions of the above components.

Here are the pieces of computerized-jewelry phone and their functions:

- **Earrings** – Speakers embedded into these earrings will be the phone's receiver.
- **Necklace** – Users will talk into the necklace's embedded microphone.
- **Ring** – Perhaps the most interesting piece of the phone, this "magic decoder ring, is equipped with light-emitting diodes (LEDs) that flash to indicate an incoming call. It can also be programmed to flash different colors to identify a particular caller or indicate the importance of a call.

Digital Jewelry

With a jewelry phone, the keypad and dialing function could be integrated into the bracelet, or else dumped altogether – it's likely that voice-recognition software will be used to make calls, a capability that is already commonplace in many of today's cell phones. Simply say the name of the person you want to call and the phone will dial that person. IBM is also working on a miniature rechargeable battery to power these components.

In addition to changing the way we make phone calls, digital jewelry will also affect how we deal with the ever-increasing bombardment of e-mails. Imagine that the same ring that flashes for phone calls could also inform you that e-mail is piling up in your inbox. This flashing alert could also indicate the urgency of the e-mail. Two of the most identifiable components of a personal computer are the mouse and monitor. These devices are as familiar to us today as a television set.

The mouse-ring that IBM is developing will use the company's Track Point technology to wirelessly move the cursor on a computer monitor display. You're probably most familiar with Track Point as the little button embedded in the keyboard of some laptops. IBM Researchers have transferred Track Point technology to a ring, which looks something like a black pearl ring. On top of the ring is a little black ball that users will swivel to move the cursor, in the same way, that the Track Point button on a laptop is used.

This Track Point ring will be very valuable when monitors shrink to the size of the watch face. In the coming age of ubiquitous computing, displays will no longer be tied to desktops or wall screens. Instead, you'll wear the display like a pair of sunglasses or a bracelet. Researchers are overcoming several obstacles facing these new wearable displays, the most important of which is the readability of information displayed on these tiny devices.

Charmed Technology is already marketing its digital jewelry, including a futuristic-looking eyepiece display. The eyepiece is the display component of the company's Charmed Communicator, a wearable, wireless, broadband-Internet device that can be controlled by voice, pen or handheld keypad. The Communicator can be used as an MP3 player, video player and cell phone. The Communicator runs on the company's Linux-based Nanix operating system.

Similar Designs available:

Garnet-Ring

JavaRing

Submitted By :
P SAJIDA
192G1A0542

Importance of Data Mining and Predictive Analytics

Have you ever heard of personal data theft for the data analysis? Must have heard of **Facebook–Cambridge Analytica data scandal?** Cambridge Analytica was a British political consulting firm which managed to collect millions of Facebook user's personal data and it is said to be a major influencer in the USA elections 2016. It is one of the biggest scandals of recent times. Data Mining and Predictive Analytics are all about dealing with such huge data and its analysis. Apache Hadoop is one of the well-known tools to deal with massive amounts of data.

Even if you're not really sure what kind of data big tech companies are mining from you, you've probably noticed some things that make you wonder who is "watching" you and what kind of information they're storing. For example, if you're on Facebook, ads for things that you've recently viewed on another site may pop up. Or if you're reading a news website, you might notice a link to a shirt that you had your eye on. It's almost like your computer is retrieving all that information and recording it.

Not to scare you, but that's because it is. But it's not necessarily all bad. Companies are retrieving a lot of information about you – gigantic swaths of data. Luckily (or maybe not) for all of us, they haven't quite figured out what to do with it. Once they do – and once you do for your own company – you're going to be fast into the world of data mining and predictive analytics, and that's where things get interesting.

Of course, experts already know that those two topics – data mining and predictive analytics – aren't the same things. The first is pretty easy to understand, and you'll start to see how companies mine your data throughout the day (and also how you can mine your customer's data). For example, they'll start by trying to collect your email to sign you up for rewards. They would want you to use that rewards number whenever you buy something because if you do, they can start to record what you're buying and when you're buying it.

On the surface, that's just data, nothing more. It's important, but it's what companies do with the data that matters. If they're smart, they're going to take it to the next step of data mining, which is figuring out patterns and organizing methods for that data. It helps you understand what time of day to market to them, of course, and what days of the week they like to visit a site, to name just two examples.

The next step, of course, follows data mining and that's **predictive analysis**. This process puts the data to work – who are you and what are you going to do now and in the future? Are you going to grow your spending, and what information can a company provide to you to encourage you to do that? If companies can figure that out, then they can forecast the future of sales – beyond just you, of course. More examples of how data can be used to predict the end result are explained here.

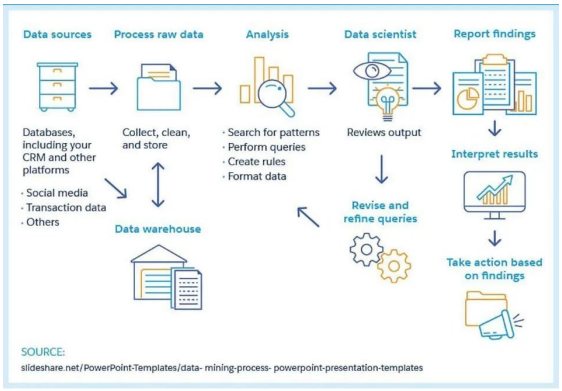
You may not realize it, but you've probably already been subject to predictive analysis. Think about applying for a credit card or a mortgage. Your credit score is a collection of data, and the approval or denial of the loan or credit card is a predictive analysis the financial institution makes on your behalf.

Thefollowing infographics explain what are data mining and predictive analytics and how these both can be combined to

get better results:

What is data mining?

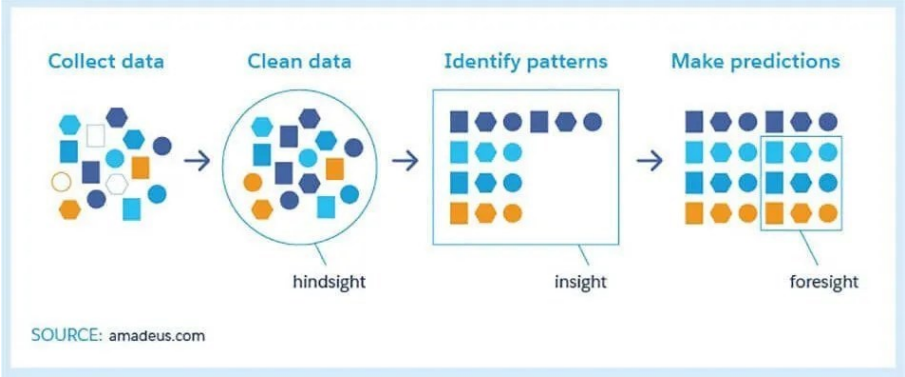
Data mining is the process of discovering useful data or patterns in large data sets. The below image explains the process of data mining. It starts with a data warehouse where the large data is stored usually and then cleaning, analyzing, applying algorithms (ML), interpreting results are performed.



Importance of Data Mining and Predictive Analytics

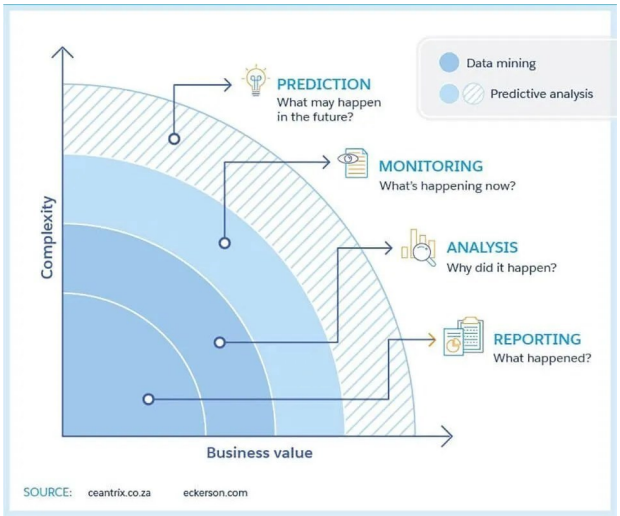
What is Predictive Analytics?

Predictive analysis is the continuation of data mining where a predictive score is assigned to the identified patterns. This helps in prioritizing the data based on the importance.



What is Data Mining and Predictive Analytics?

When you use both data mining and predictive analysis together it can create wonders. The important data can be filtered in seconds. The output of data mining acts as input to the predictive analysis i.e. the predictive analysis acts on the patterns identified by the data mining and the predictive score is assigned to the patter



Submitted By :
V VANDANA
202G1A05A7

Honeypot

A honeypot is used in the area of computer and Internet security. It is a security resource, whose value lies in being probed, attacked, or compromised. They are special decoy servers to catch the Blackhats (people with evil and illegal intents). Honeypots attract hackers to attack a vulnerable computer system, which is under observation, by a security team. All the information about the attackers is logged and monitored. A honeypot is a relatively new concept in network security and researchers all over the world, are making it more independent and secure. Compared to an Intrusion Detection System (IDS) or Firewalls, honeypots have the big advantage that they do not generate false alerts as each observed traffic is suspicious because no productive components are running on the system. This paper aims at giving a detailed description of honeypots, their types, other advantages of honeypots over currently existing IDS.

Introduction:

Global communication is getting more important every day. At the same time, computer crimes are increasing. Countermeasures are developed to detect or prevent attacks most of these measures are based on known facts, known attack patterns. It is important to know, what kind of strategy an attacker uses, what tools he utilizes and his intention. By knowing attack strategies, countermeasures can be improved and vulnerabilities can be fixed. To gather such information is one main goal of a honeypot.

A honeypot is primarily an instrument for information gathering and learning. Its purpose is not to be an ambush for the blackhat community to catch them in action. The focus lies on a silent collection of information about their attack patterns, used programs, purpose of attack and the blackhat community itself. All this information is used to learn more about the blackhat proceedings and motives, as well as their technical knowledge and abilities. There are a lot of other possibilities for a honeypot divert hackers from productive systems or catch a hacker while conducting an attack are few examples.

Types of Honeypots

1) Low-Involvement Honeypot

A low-involvement honeypot typically only provides certain fake services. In a basic form, these services could be implemented by having a listener on a specific port. For example a simple *netcat -l -p 80 > /log/honeypot/port 80.log* could be used to listen on port 80 (HTTP) and log all incoming traffic to a log file. In such a way, all incoming traffic can easily be recognized and stored. On a low involvement honeypot, there is no real operating system that an attacker can operate on. This will minimize the risk significantly because the complexity of an operating system is eliminated. On the other hand, this is also a disadvantage. It is not possible to watch an attacker interacting with the operating system, which could be really interesting.

Honeypot

2) Mid-Involvement Honeypot

A mid-involvement honeypot provides more to interact with but still does not provide a real underlying operating system. The fake daemons are more sophisticated and have deeper knowledge about the specific services they provide. At the same moment, the risk increases. Through the higher level of interaction, more complex attacks are possible and can, therefore, be logged and analyzed. The attacker gets a better illusion of a real operating system. He has more possibilities to interact with and probe the system. Developing a mid-involvement honeypot is complex and time-consuming. Special care has to be taken for security checks as all developed fake daemons need to be as secure as possible.

3) High-Involvement Honeypot

A high-involvement honeypot has a real underlying operating system. This leads to a much higher risk as the complexity increases rapidly. At the same time, the possibilities to gather information, the possible attacks as well as the attractiveness increase a lot. One goal of a hacker is to gain root and to have access to a machine, which is connected to the Internet. A high involvement honeypot does offer such an environment. A high involvement honeypot is very time-consuming. The system should be constantly under surveillance. By providing a full operating system to the attacker, he has the possibilities to upload and install new files. This is where a high-involvement honeypot can show its strength, as all actions can be recorded and analyzed. Unfortunately, the attacker has to compromise the system to get this level of freedom. He will then have root rights on the system and can do everything at any moment on the compromised system. This system is no longer secure.

Advantages of Honeypots

Small Data Sets

Honeypots only collect data when someone or something is interacting with them. Organizations that may log thousands of alerts a day may only log a hundred alerts with honeypots. This makes the data honeypots collect much easier to manage and analyze.

Reduced False Positives

Honeypots dramatically reduce false positives. Any activity with honeypots is by definition unauthorized, making it extremely effective at detecting attacks. This allows organizations to quickly and easily reduce, if not eliminate, false alerts, allowing organizations to focus on other security priorities, such as patching.

Catching False Negatives

Honeypots can easily identify and capture new attacks or actions against them. Any activity with the honeypot is an anomaly, making new or unseen attacks easily stand out.

Minimal Resources

Honeypots require minimal resources, even on the largest of networks. A simple Pentium computer can monitor literally millions of IP addresses on an OC-12 network.

Encryption

It does not matter if an attack is encrypted, the honeypot will capture the activity.

Protocol Independent

It does not matter which IP protocol an attacker uses, honeypots will detect, capture, and log all IP activity. In one documented case, a Solaris honeypot detected and captured an attack where attackers attempted to hide their communications using IPv6 tunneling within IPv4. On the other hand, there are almost no NIDS (Network intrusion detection system) technologies that can decode IPv6 or IPv6-tunneled traffic.

Intelligence Gathering

Honeypots can gather a lot of valuable information about the attackers, and also the nature of their attacks, which can be used to take appropriate action against them. A honeypot is a valuable resource, especially to collect information about the proceedings of attackers as well as their deployed tools.

Submitted By :
G G VARSHITHA
202G1A0520

Open Source Technology

Free and open source software has had a major impact on the computer industry since the late 1990s and has changed the way software is perceived, developed and deployed in many areas. Free and open source technology or software, is typically developed in a collaborative fashion and the majority of contributors are volunteers. Even though this collaborative form of development has produced a significant body of software, the development process is often described as unstructured and unorganized.

This dissertation studies the FOSS phenomenon from a quality perspective and investigates where improvements to the development process are possible. In particular, the focus is on release management since this is concerned with the delivery of a high quality product to end-users. The biggest downside of closed source software is that you have no idea how it was made.

Introduction

Open source technology is an often-misused term, it is not just a synonym for 'free'. With the relatively recent rise of the internet and the human dependncy on the internet, the amount of new applications/software being developed has also risen. The most widely used operating system for smartphones, android is also a freeware. A lot of people contribute their work to the android market. Linux operating system was one of the famous software that was announced open source in the early days.

The Apache Software Foundation (ASF) is the world's largest open source foundation. Some of the the world-famous software by ASF are Apache HTTP Server, Apache Hadoop, Apache Lucene, Apache OpenOffice and many more. The following are the highlights of the ASF's contribution as listed on its website.

What is Open Source?

Open source technology is defined as the production and development philosophy of allowing end-users and developers to not only see the source code of software, but modify it as well.

Open source provides a transparent platform upon which anyone with the skills to do so can add to the development and production of the software either for release as a new incarnation of the software for others to use or for strictly in-house development only.

One issue that has come up repeatedly in open source has to do with the copyrights assigned to the original software and any modifications made to it. As outlined in most open source license agreements, ownership of the software can never transfer to anyone who modifies the software.

Most money made from open source software comes in the form of support for the software technology and its many additions, add-ons, and modifications that often ensue.

Need for Open Source

All software has source code. Open source software grants every user access to that code. Freedom means choice. Choice means power. That's why we believe open source is inevitable. It returns control to the customer. You can see the code, change it, and learn from it. Bugs are found and fixed quickly. And when customers are unhappy with one vendor, they can choose another without overhauling their entire infrastructure. No more technology lock-in. No more monopolies.

In the proprietary model, development occurs within one company. Programmers write code, hide it behind binaries, and charge customers to use the software–then charge them more to fix it when it breaks. The problem worsens when you become tied to a company's architecture, protocols, and file formats. Bruce Perens calls this the addiction model of software procurement. And we think a model that puts customers at such a fundamental disadvantage is conceptually broken.

Criteria for Open Source

A. Free Redistribution

The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

B. Source Code

The program must include source code, and must allow distribution in source code as well as compiled form. Where some form of a product is not distributed with source code, there must be a well-publicized means of obtaining the source code for no more than a reasonable reproduction cost preferably, downloading via the Internet without charge. The source code must be the preferred form in which a programmer would modify the program. Deliberately obfuscated source code is not allowed. Intermediate forms such as the output of a preprocessor or translator are not allowed.

Open Source Technology

C. Derived Works

The license must allow modifications and derived works, and must allow them to be distributed under the same terms as the license of the original software.

D. Integrity of The Author's Source Code

The license may restrict source-code from being distributed in modified form only if the license allows the distribution of "patch files" with the source code for the purpose of modifying the program at build time. The license must explicitly permit distribution of software built from modified source code. The license may require derived works to carry a different name or version number from the original software.

E. No Discrimination Against Persons or Groups

The license must not discriminate against any person or group of persons.

F. No Discrimination Against Fields of Endeavor

The license must not restrict anyone from making use of the program in a specific field of endeavor. For example, it may not restrict the program from being used in a business, or from being used for genetic research.

G. Distribution of License

The rights attached to the program must apply to all to whom the program is redistributed without the need for execution of an additional license by those parties.

H. License Must Not Restrict Other Software

The license must not place restrictions on other software that is distributed along with the licensed software. For example, the license must not insist that all other programs distributed on the same medium must be open-source software.

I. License Must Be Technology-Neutral

No provision of the license may be predicated on any individual technology or style of interface is not free in the sense that the end user can do whatever he/she ***wants*** to it including selling it.

Submitted By
A SREENITHYA
202G1A0503

Anantha Lakshmi

Institute of Technology & Sciences

Address :
Near SK University,
Itukulapalli V),
Anantapur Dist. A.P. India-515721

Phone : 8328579395
8801110569

Email Id : alts.cse.hod@gmail.com

ABOUT THE DEPARTMENT

Computer Science and Engineering is at the core of the information age. To prepare our students for the tremendous opportunities in the field, the CSE Department is strongly committed to excellence in both education and research. Our majors are designed to provide a strong foundation in the core areas of Computer Science and Engineering.

Our majors are designed to provide a strong foundation in the core areas of Computer Science and Engineering. Our vibrant graduate programs prepare students for positions in industry and academia. Since its inception, the department has always been recognized for excellence in teaching. The Department provides an outstanding teaching environment complemented by superior teaching for its students to flourish in. Graduates from the department are recruited by both academia and industry.

The Department of Computer Science and Engineering with its cohesive team of faculty members offers a sound program at the UG as well as the PG levels. The curriculum is a blend of the conventional and the radical. It is updated regularly to keep up with the growing demands and the changing trends of the software industry and research laboratories.

College Code : ALTS

"