TECHGEEKS

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SV COLLEGE OF ENGINERRING

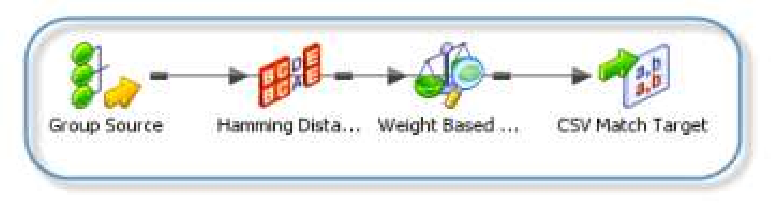
VOLUME I JAN-JUN 2019

INSIDE THIS ISSUE:

Hamming Cut Matching Algorithm

we discuss the details regarding the information about how the iris is located, to distinguish it from other parts of the eye, how the scanner scans the whole pattern of the iris while enrolling and matching and how the scanned patterns are converted into 256 bytes of data so that it can be stored in the database. We compare the iris codes of the current person who wants to access the database and gives the matched results to the user accordingly.

As the iris recognition technology produces very low false rate when compared to the other biometrics results it is very preferable in many systems such as airports, banks, defense, etc.., where the security plays one of the major role. But in the case of fields where the database is huge, the comparison time is very high.



This paper includes the implementation of HAMMING-CUT-MATCHING algorithm which reduces the comparison time for matching the iris code with database so that we can use iris recognition in case of huge databases like voting system.

BIOMETRIC SYSTEMS

The determination, measuring, and codification of the unique characteristic traits that each of us is born with is known as the science of biometrics. Various forms of computer-based biometrics for personal authentication have been around for the past twenty years, but not until recently have some reached maturity and a quality/reliability that has enabled their widespread application. In the past, hand geometry enjoyed the advantage of very small templates (codes containing the biometric data), but with modern computers this is no longer the main issue and iris based solutions are steadily gaining ground.

Retinal, iris, and fingerprint recognition are mature technologies with the most reliable performance. Of the three methods, iris recognition is the least intrusive (unwanted involvement) with greater accuracy.

In addition to reliable performance some of the other advantages of using biometrics are:

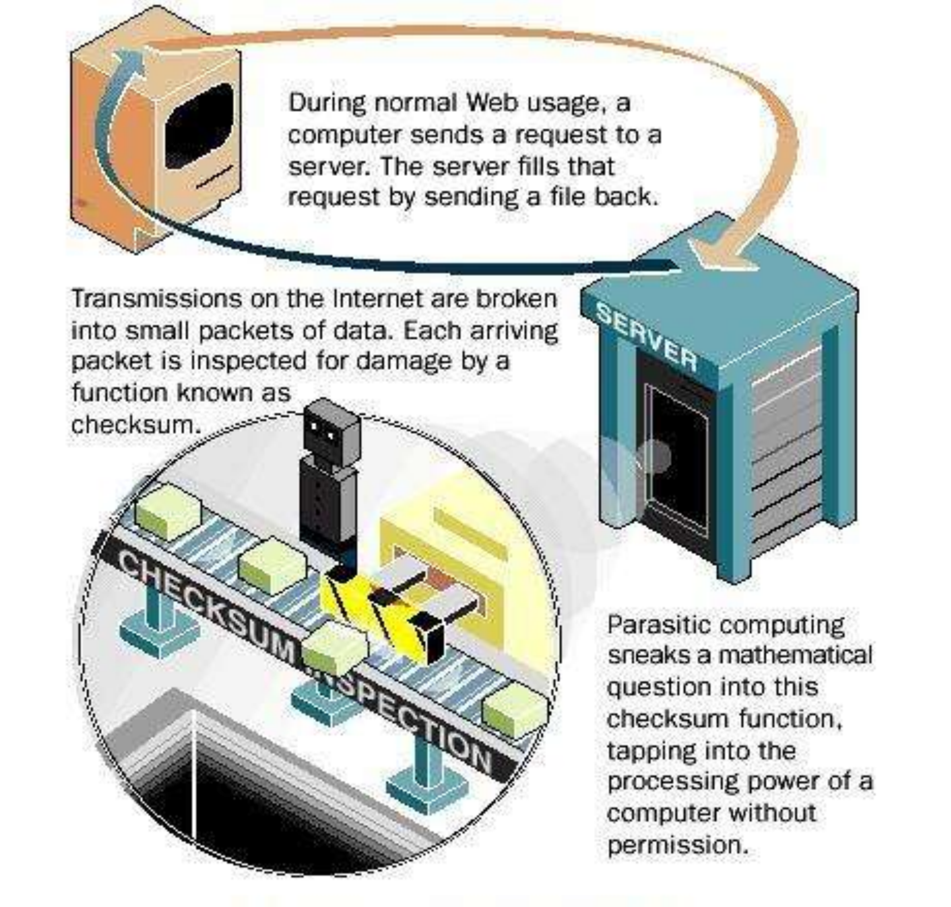
High security: It is based on physical characteristics, which cannot be lost or stolen.

Certainty/accountability: A specific person, not just a holder of a token or somebody who knows a PIN/password, has been authenticated. Users need not worry about someone using their token or PIN code without their knowledge.

Easeof administration: The problems of handling forgotten PINs/passwords and lost/stolen keys or access cards are eliminated, the benefit is a lot of time and resources saved.

Submitted by
K.NIKHILA RANI
17KH1A0530
CSE

Parasitic Computing


During normal Web usage, a computer sends a request to a server. The server fills that request by sending a file back.
SERVER
Transmissions on the Internet are broken into small packets of data. Each arriving packet is inspected for damage by a function known as checksum.
CHECKSUM INSPECTION
Parasitic computing sneaks a mathematical question into this checksum function, tapping into the processing power of a computer without permission.

HOW PARASITIC COMPUTING WORKS

Parasitic computing is a concept by which one can use the resources of machines that are connected on the Internet. This technology exploits open Internet protocols to use the resources of remote machines. As the name suggests, the machine that requires the services of others does not need to be authorized by the latter. Any machine, which is connected to the Internet, has to carry out minimum processing of any packet they receive without any authorization.

This concept is exploited by parasitic computing in order to make use of computing powers of remote machines and web servers all around the globe. So one cannot really stop their machines from being utilized in this manner.

Parasitic computing can be a very effective technique when it comes to solve NP complete problems such as Circuit SAT, 3 SAT, etc. These problems are currently considered as some of world's most complex and time consuming problems. These problems generally have a set of solutions which itself is a subset of a set of possible solutions.

HOW PARASITIC COMPUTING WORKS

Although any possible solution to such problems can be verified quickly, there is no known efficient way to identify a solution in the first place. In fact, the most notable characteristic for such problem is that there is no fast solution. The time required to solve such problem is exponentially proportional to the size of the problem. So, as the size of the problem grows, the time required to find all solutions of the problem grows exponentially. In fact, time required to solve a moderately large NP-Complete problem can easily reach billions if not trillions of years using any kind of modern computing technology we have available today. For this reason, even just determining whether there is a fast solution to such problems or not is one of the principal unsolved problems of computer science.

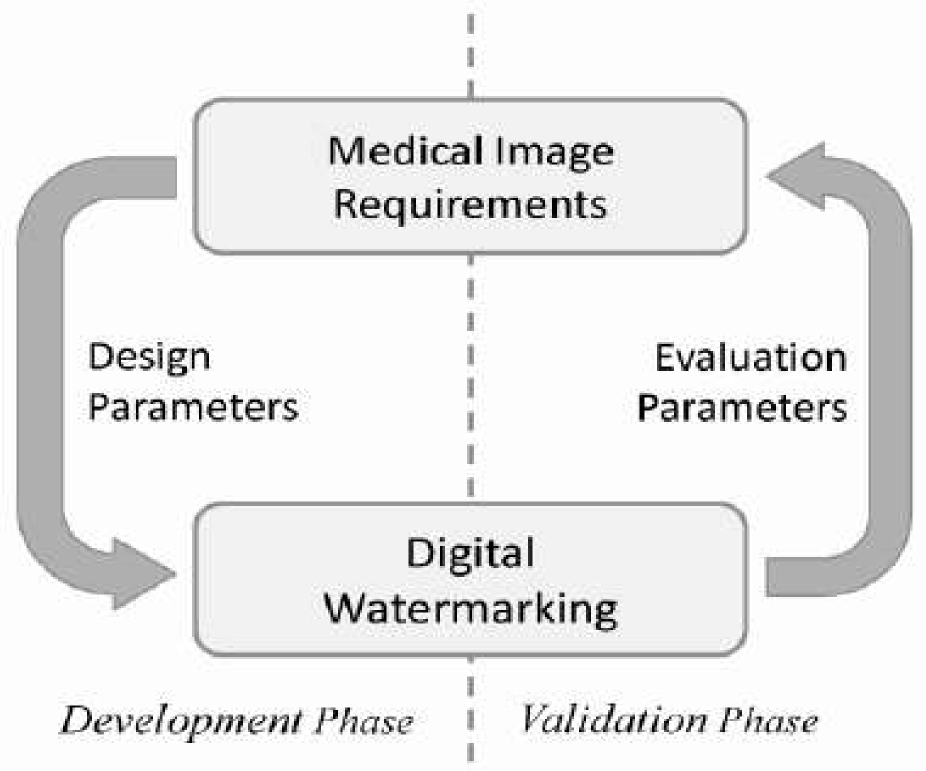
The parasitic computer starts the process by transmitting specially generated messages to number of targeted web servers consisting of arithmetic and logic unit (ALU) and a network interface (NIF). The packet carrying one of possible solutions to the problem is inserted into the IP level bypassing the parasitic node's TCP. The parasitic computer generates a message in such a way that if the solution is not valid, it will fail the TCP checksum on the destination machine and the packet will be dropped.

Submitted by
SHAIK HAFEEZA
17KH1A0549
CSE

Crypto Watermarking Method for Medical Images

Online content delivery faces massive hurdles in the absence of a secure framework for protecting valuable data. Digital watermarking a technology that can be used for control, media identification, tracing and protecting content owner's rights provides the solution

This paper presents overview on digital watermarking and a new method that combines image encryption and watermarking technique for safe transmission purpose. This method is based on the combination of public private keys and secret key ciphering, and watermarking. The encryption algorithm with secret key is applied to the image. We encrypt the secret key with an encryption method based on public-private keys. Then, this secret key is embedded in the encrypted image. We apply and show the results of our method to medical images. The amount of digital medical images has increased rapidly in the Internet. The necessity of fast and secure diagnosis is vital in the medical world. Nowadays, the transmission of images became a daily routine and it is necessary to find an efficient form to transmit them over the net. In this paper we propose a new technique to encrypt an image for safe transmission.



Our research deals with image encryption and watermarking. There are several methods to encrypt binary or grey level images. Watermarking can be an answer to make secure image transmission. For applications dealing with images, the watermarking objective is to embed invisibly message inside the image data. The length of the transmitted message can be relatively important, in fact, longer that just for identification. Insertion can be made in a different way according to the length of message or desired robustness. The combination in the spatial and frequency domains for the image watermarking is also possible.

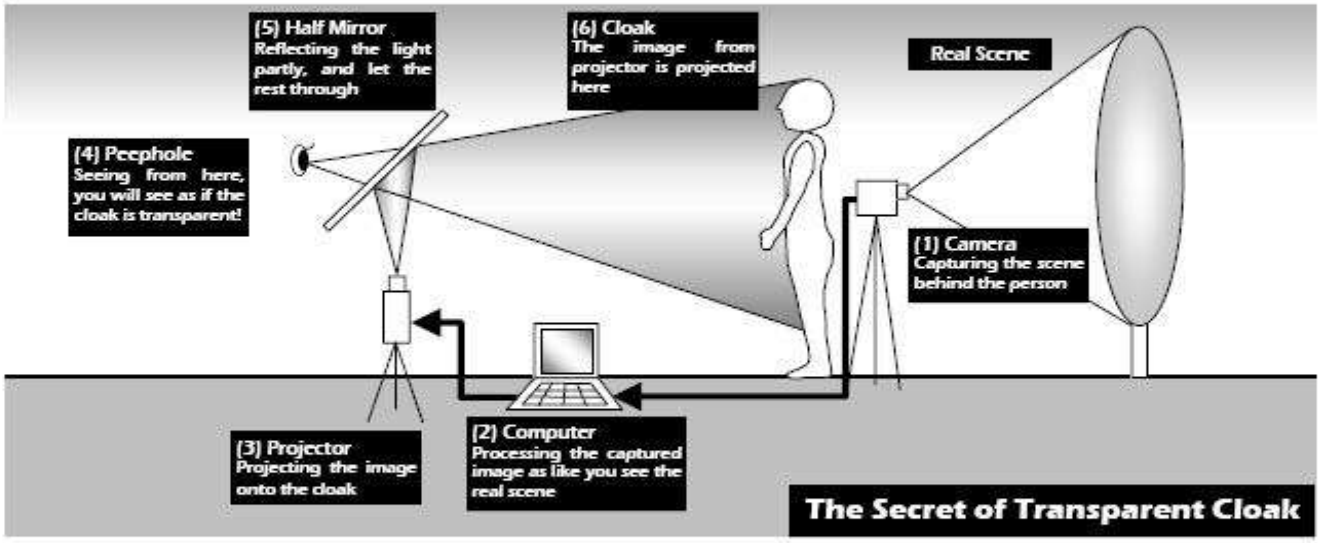
An encryption method which depends on the secrecy of the encryption algorithm is not considered to be a true encryption method. In the same way, watermarking algorithms are well-known.

The encryption can be done by block or by stream. But the encryption block methods have presented two inconvenient applied to image. The first one was when you have homogeneous zones; all blocks of this kind are encrypted on the same manner. The second problem was that block encryption methods are not robust to noise. The stream cipher method is robust to moderate noise like JPEG compression with high quality factor. To embed the encrypted secret key in the image we have used a new DCT-based watermarking method. We have chosen to work in the frequency domain because of the robustness to JPEG compression of the stream cypher method. An important application is the secure transfer of medical image.

Submitted by
KATTA SAI KUMAR
17KH1A0527
CSE

Optical Camouflage

Have you seen the movies predator, ghost in the shell or almost any sci-fi series? at least you might have seen tom n jerry show in cartoon network right, then you know what is clocking. It is bending of light around an object, or displaying the image behind an object on the other side so as to give the illusion of there being nothing in the way. It's kind of being invisible so that a person standing in front of you, can see the scene behind you. This process of invisibility basically relates to an upcoming technology called "Optical Camouflage".


(5) Half Mirror
Reflecting the light partly, and let the rest through
(6) Cloak
The image from projector is projected here
Real Scene
(4) Peephole
Seeing from here, you will see as if the cloak is transparent!
(1) Camera
Capturing the scene behind the person
(3) Projector
Projecting the image onto the cloak
(2) Computer
Processing the captured image as like you see the real scene
The Secret of Transparent Cloak

Optical Camouflage delivers a similar experience to Harry Potter's invisibility cloak, but using it requires a slightly more complicated arrangement. First, the person who want be invisible (let's call her person A) dons a garment that resembles a hooded raincoat. The garment is made of a special material. Next, an observer (Person B) stands before a person A at a specific location. At that location, instead of seeing person A wearing a hooded raincoat, person B sees right through the cloak, making person A appear to be invisible. If person B were viewing from a slightly different location, he would simply see person A wearing a silver garment. Still, despite its limitations, this is a cool piece of technology.

Optical camouflage is a kind of active camouflage which completely envelopes the wearer. It displays an image of the scene on the side opposite the viewer on it, so that the viewer can "see through" the wearer, rendering the wearer invisible. Optical camouflage doesn't work by way of magic. It works by taking advantage of something called

Augmented-reality technology -- a type of technology first pioneered in the 1960s by Ivan Sutherland and his students at Harvard University and the University of Utah. Optical camouflage is a hypothetical type of active camouflage currently only in a very primitive stage of development. The idea is relatively straightforward: to create the illusion of invisibility by covering an object with something that projects the scene directly behind that Object. Although optical is a term that technically refers to all forms of light, most proposed forms of optical camouflage would only provide invisibility in the visible portion of the spectrum. Prototype examples and proposed designs of optical camouflage devices range back to the late eighties at least, and the concept began to appear in fiction in the late nineties.

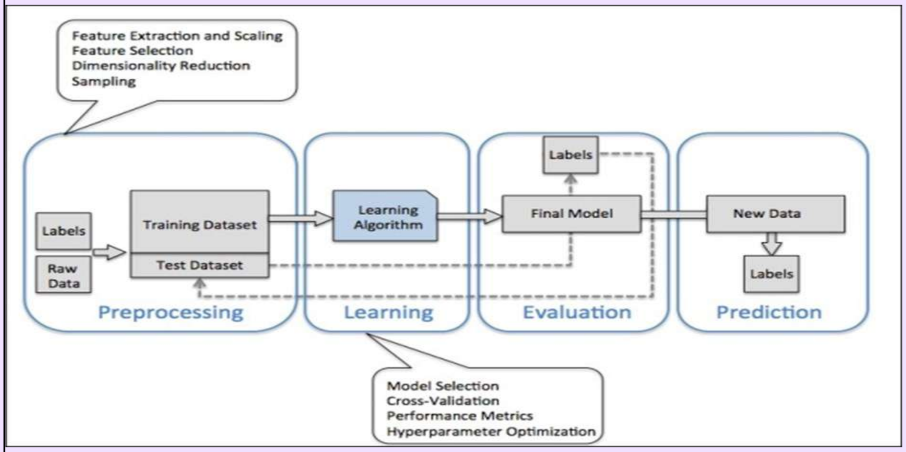
WORKING:

Optical camouflage doesn't work by way of magic. It works by taking advantage of something called Augmented-reality technology.Most augmented-reality systems require a user to look through a special viewing apparatus to see a real-world scene enhanced with synthesized graphics.

Submitted by
C SAI MEGHANA
17KH1A0512
CSE

Machine learning

Machine Learning is a new trending field these days and is an application of artificial intelligence. Machine learning uses certain statistical algorithms to make computers work in a certain way without being explicitly programmed. The algorithms receive an input value and predict an output for this by the use of certain statistical methods. The main aim of machine learning is to create intelligent machines which can think and work like human beings. Machine Learning is a branch of **artificial intelligence** that gives systems the ability to learn automatically and improve themselves from the experience without being explicitly programmed or without the intervention of human. Its main aim is to make computers learn automatically from the experience.



Requirements of creating good machine learning systems

So what is required for creating such machine learning systems? Following are the things required in creating such machine learning systems:

Data – Input data is required for predicting the output.

Algorithms – Machine Learning is dependent on certain statistical algorithms to determine data patterns.

Automation – It is the ability to make systems operate automatically.

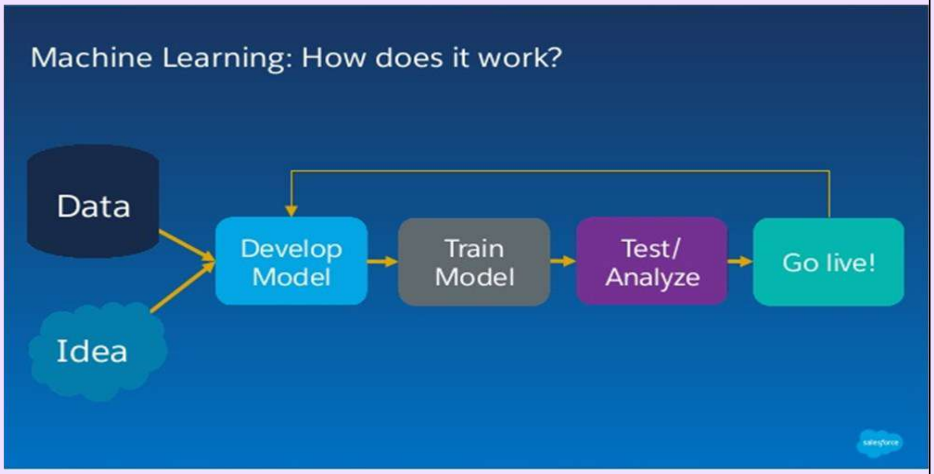
Iteration – The complete process is iterative i.e. repetition of process.

Scalability – The capacity of the machine can be increased or decreased in size and scale.

Modeling – The models are created according to the demand by the process of modeling.

Methods of Machine Learning Machine Learning methods are classified into certain categories. These are:

Supervised Learning – In this method, input and output is provided to the computer along with feedback during the training. The accuracy of predictions by the computer during training is also analyzed. The main goal of this training is to make computers learn how to map input to the output.


Machine Learning: How does it work?

Unsupervised Learning – In this case, no such training is provided leaving computers to find the output on its own. Unsupervised learning is mostly applied on transactional data. It is used in more complex tasks. It uses another approach of iteration known as deep learning to arrive at some conclusions.

Reinforcement Learning – This type of learning uses three components namely – agent, environment, action. An agent is the one that perceives its surroundings, an environment is the one with which an agent interacts and acts in that environment. The main goal in reinforcement learning is to find the best possible policy.

How does machine learning work?Machine learning makes use of processes similar to that of data mining. Machine learning algorithms are described in terms of target function(f) that maps input variable (x) to an output variable (y). This can be represented as:y=f(x)There is also an error e which is the independent of the input variable x. Thus the more generalized form of the equation is:y=f(x) + e

In machine the mapping from x to y is done for predictions. This method is known as predictive modeling to make most accurate predictions. There are various assumptions for this function.

Submitted by
GRANDE KAVYA SREE
17KH1A0519
CSE

Wavelet Transforms In Colored Image Steganography

Digital Steganography exploits the use of a host data to hide a piece of information in such away that it is imperceptible to a human observer. Wavelet transforms that map integers to integers allow perfect reconstruction of the original image. Hence, we proposed an algorithm that embeds the message bitstream into the LSB's of the integer wavelet coefficients of a true-color image. The algorithm also applies a preprocessing step on the cover image to adjust saturated pixel components in order to recover the embedded message without lose. Experimental results showed the high invisibility of the proposed model even with large message size.

Introduction

The appearance of the Internet is considered to be one of the major events of the past years; information become available on-line, all users who have a computer can easily connect to the Internet and search for the information they want to find. This increasing dependency on digital media has created a strong need to create new techniques for protecting these materials from illegal usage. One of those techniques that have been in practical use for a very long time is Encryption. The basic service that cryptography offers is the ability of transmitting information between persons in a way that prevents a third party from reading it.

Although, encryption protects content during the transmission of the data from the sender to receiver, after receipt and subsequent decryption, the data is no longer protected and is in the clear. That what makes steganography compliments encryption. Digital Steganography exploits the use of a host (container) data to hide or embed a piece of information that is hidden directly in media content, in such a way that it is imperceptible to a human observer, but easily detected by a computer.

The principal advantage of this is that the content is inseparable from the hidden message. In a blind image steganographic system, a message is embedded in a digital image by the stegosystem encoder which uses a key. The resulting stego-image is transmitted over a channel to the receiver where it is processed by the stegosystem decoder using the same key. In general, if the channel is monitored by someone who is allowed to modify the information flow between the two parties, he is called an active warden; but if he can only observe it, he is called a passive warden.

.During the past few years, there has been a lot of research on developing techniques for the purpose of placing data in still images. Some techniques are more suited to dealing with small amounts of data, while others to large amounts. Some techniques are highly resistant to geometric modifications, , we expect a high level of robustness in return for low bandwidth.

Submitted by
T SURYA LIKHITHA
17KH1A0559
CSE

A Secure Dynamic Multi-keyword Ranked Search

Due to the increasing popularity of cloud computing, more and more data owners are motivated to outsource their data to cloud servers for great convenience and reduced cost in data management. However, sensitive data should be encrypted before outsourcing for privacy requirements, which obsoletes data utilization like keyword-based document retrieval. In this paper, we present a secure multi-keyword ranked search scheme over encrypted cloud data, which simultaneously supports dynamic update operations like deletion and insertion of documents. Specifically, the vector space model and the widely-used TF_IDF model are combined in the index construction and query generation.

We construct a special tree-based index structure and propose a “Greedy Depth-First Search” algorithm to provide efficient multi-keyword ranked search. The secure KNN algorithm is utilized to encrypt the index and query vectors, and meanwhile ensure accurate relevance score calculation between encrypted index and query vectors. In order to resist statistical attacks, phantom terms are added to the index vector for blinding search results. Due to the use of our special tree-based index structure, the proposed scheme can achieve sub-linear search time and deal with the deletion and insertion of documents flexibly. Extensive experiments are conducted to demonstrate the efficiency of the proposed scheme.

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

• On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

• Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

• Resource pooling: The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

• Rapid elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

• Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

Submitted by
B LAKSHMI BHAVANA
17KH1A0507
CSE

Brain controlled Robots

For robots to do what we want, they need to understand us. Too often, this means having to meet them halfway: teaching them the intricacies of human language, for example, or giving them explicit commands for very specific tasks. But what if we could develop robots that were a more natural extension of us and that could actually do whatever we are thinking? Using data from an electroencephalography (EEG) monitor that records brain activity, the system can detect if a person notices an error as a robot performs an object-sorting task. The team’s novel machine-learning algorithms enable the system to classify brain waves in the space of 10 to 30 milliseconds. While the system currently handles relatively simple binary-choice activities, the paper’s senior author says that the work suggests that we could one day control robots in much more intuitive ways.“Imagine being able to instantaneously tell a robot to do a certain action, without needing to type a command, push a button or even say a wordPast work in EEG-controlled robotics has required training humans to “think” in a prescribed way that computers can recognize. For example, an operator might have to look at one of two bright light displays, each of which corresponds to a different task for the robot to execute. The downside to this method is that the training process and the act of modulating one’s thoughts can be taxing, particularly for people who supervise tasks in navigation or construction that require intense concentration.

Talking to an android

We've all tried talking with devices, and in some cases they talk back. But, it's a far cry from having a conversation with a real person. Now, a research team from Kyoto University, Osaka University, and the Advanced Telecommunications Research Institute, or ATR, has significantly upgraded the interaction system for conversational android ERICA, giving her even greater dialog skills. ERICA is an android created by Hiroshi Ishiguro of Osaka University and ATR, specifically designed for natural conversation through incorporation of human-like facial expressions and gestures. The research team demonstrated the updates during a symposium at the National Museum of Emerging Science in Tokyo."When we talk to one another, it's never a simple back and forward progression of information," says Tatsuya Kawahara of Kyoto University's Graduate School of Informatics, and an expert in speech and audio processing. "Listening is active. We express agreement by nodding or saying 'uh-huh' to maintain the momentum of conversation. This is called 'back channelling,' and is something we wanted to implement with ERICA."The team also focused on developing a system for "attentive listening." This is when a listener asks elaborating questions, or repeats the last word of the speaker's sentence, allowing for more engaging dialogue. Deploying a series of distance sensors, facial recognition cameras and microphone arrays, the team began collecting data on parameters necessary for a fluid dialog between ERICA and a human subject.

Submitted by
K SESODHA REDDY
17KH1A0531
CSE