**SECURE COMPUTING**

A security system identifies and mitigates the system vulnerabilities, by either removing them, or restricting access to them, to a very small group. The competition between inventing new security measures to protect data and inventing hacking techniques in conjunction with discovering and leveraging pre-existing vulnerabilities is infinite. Therefore, securing data and resources is becoming more and more challenging day by day. Nevertheless, there exist several different techniques to secure the data being transferred over a network and also that on a user machine. Specializes in securing data in motion through the use of the patented REL-ID based mutual authentication scheme. SSL is one such tool to secure data sent over a network, using cipher text. Using SSL data is kept confidential and message integrity is maintained.

However, recently there have been network security breaches, including the famous “HEARTBLEED” bug. But, the question that remains is “what if the user machine itself is hacked? .it can be used to ensure that the end user is secured as well as the tunnel. It also uses techniques of authentication to assure to each end user that it is communicating with an authorized user and not a fake one. Such security measures are used to secure data in motion, meaning data that has been shared between computers. They may prove to be of minimum value, if the operating system on which it resides is compromised. It is therefore crucial to understand and remove the security flaws in the operating system itself. We, on the other hand, are trying to secure data at rest, by coming up with various approaches, one of which is application white listing.

Hardening is a technique to reduce vulnerabilities of the existing operating system. It aims to eliminate security risks in an operating system. This is done by turning off all those services of the operating system which are not used are risky and allowing only those which are secure for user’s data. Thus, this environment becomes a kind of locked down or reduce version of a fully-fledged operating system. Operating system hardening is a technique which allows us a security on the machine level. A hardened operating system can be considered as a smaller version of an otherwise compromised operating system. Secondly, we implement a technique called as application white-listing. It is the technique of preparing a list of all applications that are safe to execute. All applications that excluded from this list are disallowed to spawn.

**METHODS**

**Hardening**

For operating system hardening we may try to reformat the operating system and install only those parts of the operating system which are required for the users program to run. Hence hardening is depend upon the particular application for which it was done in the first place. We may also consider disabling guest login as an added security measure. This is done because even if the guest user is not authorized, some kinds of penetration are always possible. Also we may consider turning off services such as resource sharing, file sharing, printer sharing.

**Whitelisting**

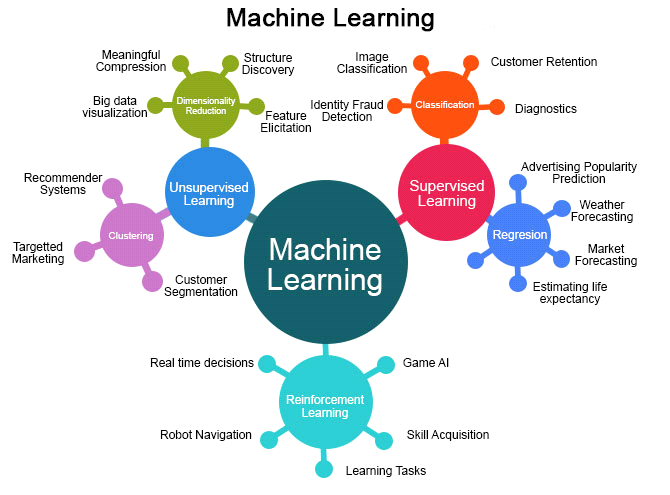
In white-listing all applications that are found to be suspicious, or might be containing possible back-doors are denied permission to execute. This minimizes the threats to operating system. This may start by preparing a list of names of applications which are safe to execute and checking the name of each spawned application against this list. If a match occurs we need not take any action. If the application name does not match with any of the supposed white-listed application, it is killed immediately. On a higher level, it should not be allowed to spawn in the first place.

**MACHINE LEARNING**

**OVERVIEW**

Machine learning is an application of Artificial Intelligence (AI) that provides systems the ability to automatically learn and improve experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves. The primary aim is to allow the computer to learn automatically without human intervention or assistance and adjust actions accordingly.

The test for a machine learning model is a validation error on new data not a theoretical test that proves a null hypothesis. Because this often uses an iterative approach to learn from data, the learning can be easily automated.



**MACHINE LEARNING METHODS**

Some of the methods of Machine Learning algorithm are categorized as

**SUPERVISED LEARNING**

A Supervised learning algorithm learns from labelled training data, helps you to predict outcomes for unforeseen data. It is highly accurate and trustworthy method.

**UNSUPERVISED LEARNING**

Unsupervised learning algorithm is the type of self - organized with the help of previously unknown patterns in dataset without pre-existing labels.

**SEMI-SUPERVISED LEARNING**

Semi-supervised learning is the combination of both supervised and unsupervised which means labelled and unlabelled data.

**REINFORCEMENT MACHINE LEARNING**

Reinforcement machine learning is an area of machine learning concerned with how software agents ought to take actions in an environment so as to maximize some notion of cumulative reward.

**APPLICATIONS OF MACHINE LEARNING**

* + Video Surveillance
  + Social Media Services
  + Email Spam and Malware Filtering
  + Financial Services
  + Health Care
  + Retail
  + Transportation

**ADVANTAGES**

* + Computational property is cheaper and more powerful.
  + Affordable data storage.
  + It can analysis complex data quickly and automatically.
  + It produces more accurate results.

**BLOCK CHAN**

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.This allows the participants to verify and audit transactions independently and relatively inexpensively.A blockchain database is managed autonomously using a peer-to-peer network and a distributed time stamping server. They are authenticated by mass collaboration powered by collective self-interests. Such a design facilitates robust workflow where participants' uncertainty regarding data security is marginal. The use of a blockchain removes the characteristic of infinite reproducibility from a digital asset. It confirms that each unit of value was transferred only once, solving the long-standing problem of double spending. A blockchain has been described as a *value-exchange protocol*. This blockchain-based exchange of value can be completed quicker, safer and cheaper than with traditional systems. A blockchain can maintain title rights because, when properly set up to detail the exchange agreement, it provides a record that compels offer and acceptance.

**3.1 Methods**

**Block Chain Analytics:**

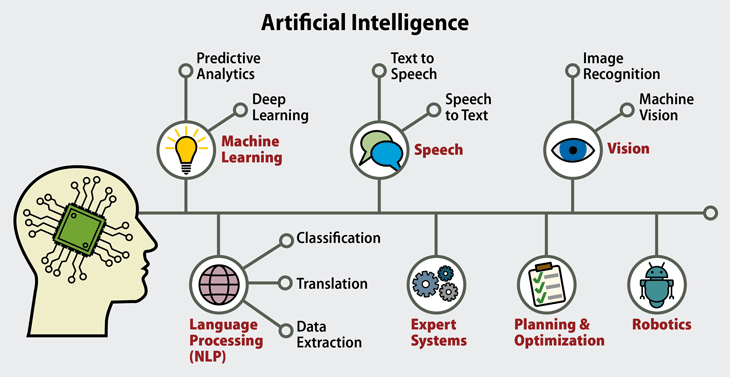
**Blockchain analysis** is the process of inspecting,identifying, [clustering](https://en.wikipedia.org/wiki/Data_Clustering), [modeling](https://en.wikipedia.org/wiki/Data_modeling" \o "Data modeling) and visually representing [data](https://en.wikipedia.org/wiki/Data) on a [cryptographic](https://en.wikipedia.org/wiki/Cryptographic_hash_function) distributed-ledger known as a [blockchain](https://en.wikipedia.org/wiki/Blockchain" \o "Blockchain). Data in most blockchains are public meaning that anyone can harness the addresses. By using common-spend clustering algorithms, it is possible to map the spending of certain entities on the [blockchain](https://en.wikipedia.org/wiki/Blockchain" \o "Blockchain). This is how criminals have been caught moving illicit funds using various crypto currencies The goal of blockchain analysis is discovering useful information about the different actors transacting in crypto currency. Analysis of public blockchains such as the [bitcoin](https://en.wikipedia.org/wiki/Bitcoin" \o "Bitcoin) and [ethereum](https://en.wikipedia.org/wiki/Ethereum" \o "Ethereum) is often conducted by private companies Bitcoin has long been associated with the trade of illegal goods on the [dark web](https://en.wikipedia.org/wiki/Dark_web); this has been the case since bitcoin became the standard currency on the now closed [Silk Road](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)). [Crypto currency exchanges](https://en.wikipedia.org/wiki/Cryptocurrency_exchange) are increasingly required by law to address the source of funds for crypto traders. [Singapore](https://en.wikipedia.org/wiki/Singapore), [Japan](https://en.wikipedia.org/wiki/Japan), the [USA](https://en.wikipedia.org/wiki/United_States) are examples of countries that have passed laws that now require the exchanges to track the source of the crypto funds.

**ARTIFICIAL INTELLIGENCE**

**Overview**

Artificial Intelligence (AI) is the simulation of human intelligence process by machines, especially computer systems. These processes include the acquisition of information and rules for using the information, using rules to reach approximate or definite conclusions and self-correction.

Artificial Intelligence has the capability to find patterns in big data to learn and reveal hidden information or deliver solutions to deliver complex problems. It is an automated processes.



**Types of Artificial Intelligence**

Artificial Intelligence categorized into four types are :

**Reactive Machines :**

This means they cannot form memories or past experiences to influence present made decisions they can only react to currently existing situations.

**Limited Memory :**

Thisis comprised of machine learning models that derive knowledge from previously-learned information, stored data, or events.

**Theory of Mind :**

It refers to the understanding that others have their own beliefs, desires and intentions that impact the decisions they make.

**Self-Awareness :**

It is also called as consciousness. Machines with self-awareness understand their current state and can use the information to infer what others are feeling.

**COMPONENTS OF ARTIFICIAL INTELLIGENCE**

**Types of Models**

* Deep Learning
* Machine Learning
* Neural networks

**Deep Learning**

Deep learning is a subset of machine learning in artificial intelligence (AI) that has networks capable of learning unsupervised from data that is unstructured or unlabeled. Also known as deep neural learning or deep neural network.

**Machine Learning**

Machine learning is an application of artificial intelligence (AI) that provides systems the ability to automatically learn and improve from experience without being explicitly programmed. Machine learning focuses on the development of computer programs that can access data and use it learn for themselves.

**Neural Networks**

A neural network is a series of algorithms that endeavors to recognize underlying relationships in a set of data through a process that mimics the way the human brain operates. In this sense, neural networks refer to systems of neurons, either organic or artificial in nature.

**Theoritical Types of Artificial Intelligence :**

* Artificial Narrow Intelligence(ANI)
* Artificial general Intelligence(AGI)
* Artificial Super Intelligence(ASI)

**Artificial Narrow Intelligence(ANI)**

Artificial narrow intelligence refers to a computer's ability to perform a single task extremely well such as crawling a webpage or playing chess.

**Artificial General Intelligence(AGI)**

Artificial general intelligence (AGI) is the intelligence of a machine that can understand or learn any intellectual task than a human being.

**Artificial Super Intelligence(ASI)**

Artificial super intelligence is a hypothetical agent that possesses intelligence far surpassing that of the brightest and most gifted human minds.

**Applications of Artificial Intelligence**

* Image recognition
* Speech recognition
* Natural language generation
* Sentiment Analysis
* Chatbots

## DATA MINING

### Overview

Data Mining is the analysis step of the “Knowledge discovery in Database” (KDD). Data Mining is the extraction of hidden predictive information from large databases, is a powerful new technology with great potential to help companies focus on the most important information in their Data Warehouses. Data Mining is discovering the hidden values in your Data Warehouse. It uses the mathematical algorithms to segregate the data. Here is the list of steps involved in the knowledge discovery process:

* + - **Data Cleaning** - In this step the noise and inconsistent data are removed.
    - **Data Integration** - In this step multiple data sources are combined.
    - **Data Selection** - In this step relevant to the analysis task are retrieved from the database.
    - **Data Transformation** - In this step data are transformed or consolidated into forms appropriate for mining by performing summary or aggregation operations.
    - **Data Mining** - In this step intelligent methods are applied in order to extract data patterns.
    - **Pattern Evaluation** - In this step, data patterns are evaluated.
    - **Knowledge Presentation** - In this step, knowledge is represented.

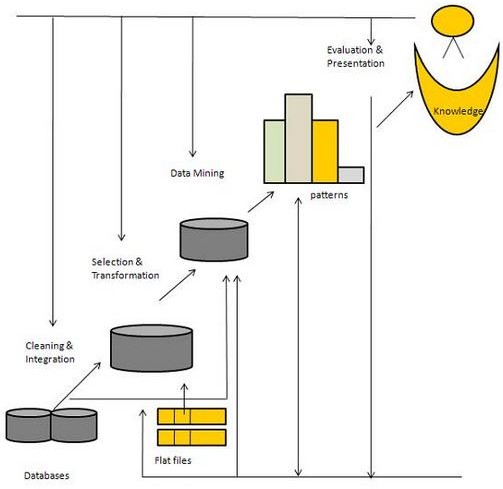


Fig.1 steps in knowledge discovery in database

### KEY PROPERTIES IN DATA MINING

* + - Automatic discovery of patterns.
    - Prediction of likely outcomes.
    - Creation of actionable information.
    - Focus on large data sets and databases.

### DATA MINING TECHNOLOGIES

Data mining supports by three technologies that are now sufficiently mature:

* + - Massive data collection
    - Powerful multiprocessor computers
    - Data mining algorithms

### DATA MINING TECHNIQUES

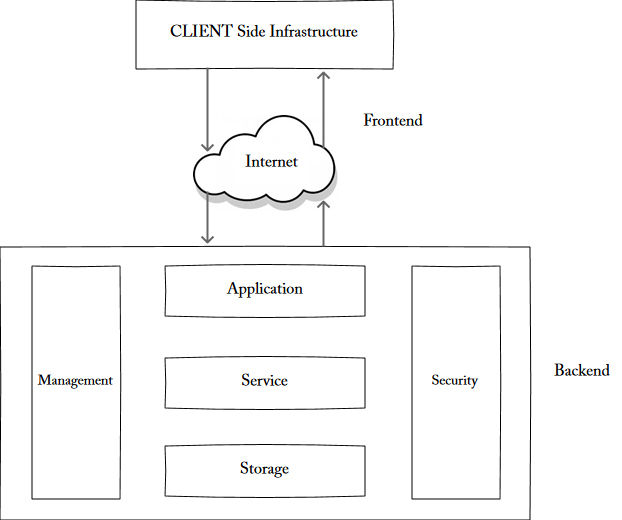
The most commonly used techniques in data mining are:

* + - **Artificial neural networks**: Non-linear predictive models that learn through training and resemble biological neural networks in structure.
    - **Decision trees**: Tree-shaped structures that represent sets of decisions. These decisions generate rules for the classification of a dataset. A Specific decision tree method includes Classification and Regression Trees (CART) and Chi Square Automatic Interaction Detection (CHAID).
    - **Genetic algorithms**: Optimization techniques that use processes such as genetic combination, mutation, and natural selection in a design based on the concepts of evolution.
    - **Nearest neighbor method**: A technique that classifies each record in a dataset based on a combination of the classes of the k record(s) most similar to it in a historical dataset (where k ³ 1). Sometimes called the k-nearest neighbor technique.
    - **Rule induction**: The extraction of useful if-then rules from data based on statistical significance.

**CLOUD COMPUTING**

Cloud computing is a general term for anything that involves delivering hosted services over the Internet These resources include tools and applications like data storage, servers, databases, networking, and software.

Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security.



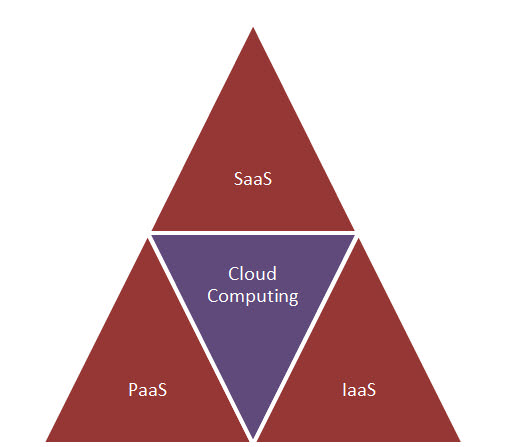
**THREE TYPES OF CLOUDS**

Cloud computing is a way of delivering technology resources to users from remote hubs. There are three main models of cloud computing, based on the type of resources being delivered. Software as a service (SaaS) is the delivery of fully functional products to end users. Infrastructure as a service (IaaS) provides secure network and storage capacity to system administrators. Platform as a service (PaaS) is somewhere in between, giving developers the building blocks to create apps while freeing them from tedious back-end concerns.

**SOFTWARE AS A SERVICE(Saas)**

SaaS is the most common type of cloud computing. It delivers complete, user-ready applications over the internet. These typically do not have to be downloaded and installed on each individual user’s computer, saving technical staff lots of time. Maintenance and troubleshooting are handled entirely by the vendor

Software programs perform specific functions and are generally intuitive to use. Examples include Salesforce’s suite of customer relationship management tools, Microsoft Office 365 products, Google Apps, QuickBooks, Dropbox, Zendesk, and Slack. These are fully functional productivity tools that can be customized to the users’ needs without coding or programming. SaaS provides the greatest amount of customer support.



**INFRASTRUCTURE AS A SERVICE (Iaas)**

IaaS is the most open-ended type of cloud service for organizations that want to do a lot of customization themselves. The greatest benefit of IaaS is extra capacity, which can be accessed on demand for long-term or short-term needs. IaaS makes it possible for tech-savvy businesses to rent enterprise-grade IT resources and infrastructure to keep pace with growth, without requiring large capital investments .

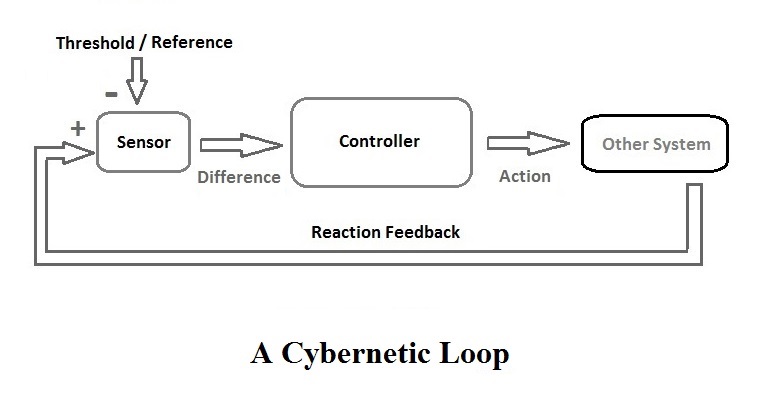
With IaaS, a third party hosts elements of infrastructure, such as hardware, servers, firewalls, and storage capacity. However, users typically bring their own operating systems and middleware. A business that is developing a new software product might choose to use an IaaS provider to create a testing environment before deploying the program in-house. Clients typically access cloud servers through a dashboard or an API. IaaS is fully self-service.

**PLATFORM AS A SERVICE(Paas)**

PaaS provides the building blocks for software creation, including development tools, code libraries, servers, programming environments, and preconfigured app . components. With PaaS, the vendor takes care of back-end concerns such as security, infrastructure, and data integration so users can focus on building, hosting, and testing apps faster and at lower cost With a platform like Salesforce, resources are standardized and consolidated so you don’t have to reinvent the wheel each time you build a new app. Multiple developers can work on the same project simultaneously. In many cases, people without coding skills can create problem-solving business applications with drag-and-drop page layouts, point-and-click field creation , and customizable reporting dashboards.

**CYBERNETICS**

**Cybernetics** is a [trans disciplinary](https://en.wikipedia.org/wiki/Transdisciplinary)approach for exploring regulatory systems their [structures](https://en.wikipedia.org/wiki/Structure), constraints, and possibilities. The essential goal of the broad field of cybernetics is to understand and define the functions and processes of systems that have goals and that participate in circular, [causal chains](https://en.wikipedia.org/wiki/Causality) that move from action to sensing to comparison with desired goal, and again to action. Its focus is how anything (digital, mechanical or biological) processes information, reacts to information, and changes or can be changed to better accomplish the first two tasks. Cybernetics includes the study of [feedback](https://en.wikipedia.org/wiki/Feedback), [black boxes](https://en.wikipedia.org/wiki/Black_box) and derived concepts such as [communication](https://en.wikipedia.org/wiki/Communication) and [control](https://en.wikipedia.org/wiki/Control_theory) in [living organisms](https://en.wikipedia.org/wiki/Life), [machines](https://en.wikipedia.org/wiki/Machine) and [organizations](https://en.wikipedia.org/wiki/Organization) including [self-organization](https://en.wikipedia.org/wiki/Self-organization). Cybernetics has been defined in a variety of ways, by a variety of people, from a variety of disciplines. Science concerned with the study of systems of any nature which are capable of receiving, storing and processing information so as to use it for control. Studies in cybernetics provide a means for examining the design and function of any system, including social systems such as business management and organizational learning, including for the purpose of making them more [efficient](https://en.wikipedia.org/wiki/Efficiency) and [effective](https://en.wikipedia.org/wiki/Effective). Fields of study which have influenced or been influenced by cybernetics include [game theory](https://en.wikipedia.org/wiki/Game_theory), [system theory](https://en.wikipedia.org/wiki/System_theory) (a mathematical counterpart to cybernetics), [perceptual control theory](https://en.wikipedia.org/wiki/Perceptual_control_theory), [sociology](https://en.wikipedia.org/wiki/Sociology), psychology (especially [neuropsychology](https://en.wikipedia.org/wiki/Neuropsychology), [behavioral psychology](https://en.wikipedia.org/wiki/Behavioral_psychology" \o "Behavioral psychology), [cognitive psychology](https://en.wikipedia.org/wiki/Cognitive_psychology)), [philosophy](https://en.wikipedia.org/wiki/Philosophy), [architecture](https://en.wikipedia.org/wiki/Architecture), and [organizational theory](https://en.wikipedia.org/wiki/Organizational_theory). [System dynamics](https://en.wikipedia.org/wiki/System_dynamics), originated with applications of [electrical engineering](https://en.wikipedia.org/wiki/Electrical_engineering) [control theory](https://en.wikipedia.org/wiki/Control_theory) to other kinds of [simulation models](https://en.wikipedia.org/wiki/Simulation_modeling) (especially business systems)



Researchers in Artificial Intelligence (AI) use computer technology to build intelligent machines; they consider implementation (that is, working examples) as the most important result. Practitioners of cybernetics use models of organizations, feedback, goals, and conversation to understand the capacity and limits of any system (technological, biological, or social); they consider powerful descriptions as the most important result. Cybernetics as a process operating in nature has been around for a long time; actually, for as long as nature has been around.

Cybernetics as a concept in society has been around at least since [Plato](http://en.wikipedia.org/wiki/Plato) used it to refer to [government](http://en.wikipedia.org/wiki/Government).

Cybernetics has always been a hard field to pin down. Wiener presented it a synthesis of work in digital computing, information theory, and feedback control. As such, it represented a new kind of science, devoted to immaterial elements such as ‘bits’ of information rather than the material substances that define traditional sciences like physics, chemistry, and biology. Again, in contrast to the traditional organization of knowledge, cybernetics was strongly interdisciplinary. The Macy conferences brought anthropologists, sociologists, psychologists, and psychiatrists together with natural scientists, mathematicians, and engineers, and claims were made for cybernetics as a universal superscience capable of accommodating all of the disciplines.

Cybernetics is concerned with concepts at the core of understanding complex systems such as learning, cognition, adaptation, emergence, communication, and efficiency. Cybernetics has been influenced by and, in turn, has applications in fields as diverse as psychology and control theory, philosophy and mechanical engineering, architecture and evolutionary biology, or social sciences and electrical engineering.

There is little wonder that philosophers and scientists have different definition of cybernetics. Cybernetics is “the art of creating equilibrium in a world of constraints and possibilities,” according to the philosopher Ernst von Glasersfeld. The famous mathematician Andrey Nikolaevich Kolmogorov defines cybernetics as the “science concerned with the study of systems of any nature which are capable of receiving, storing, and processing information so as to use it for control.”