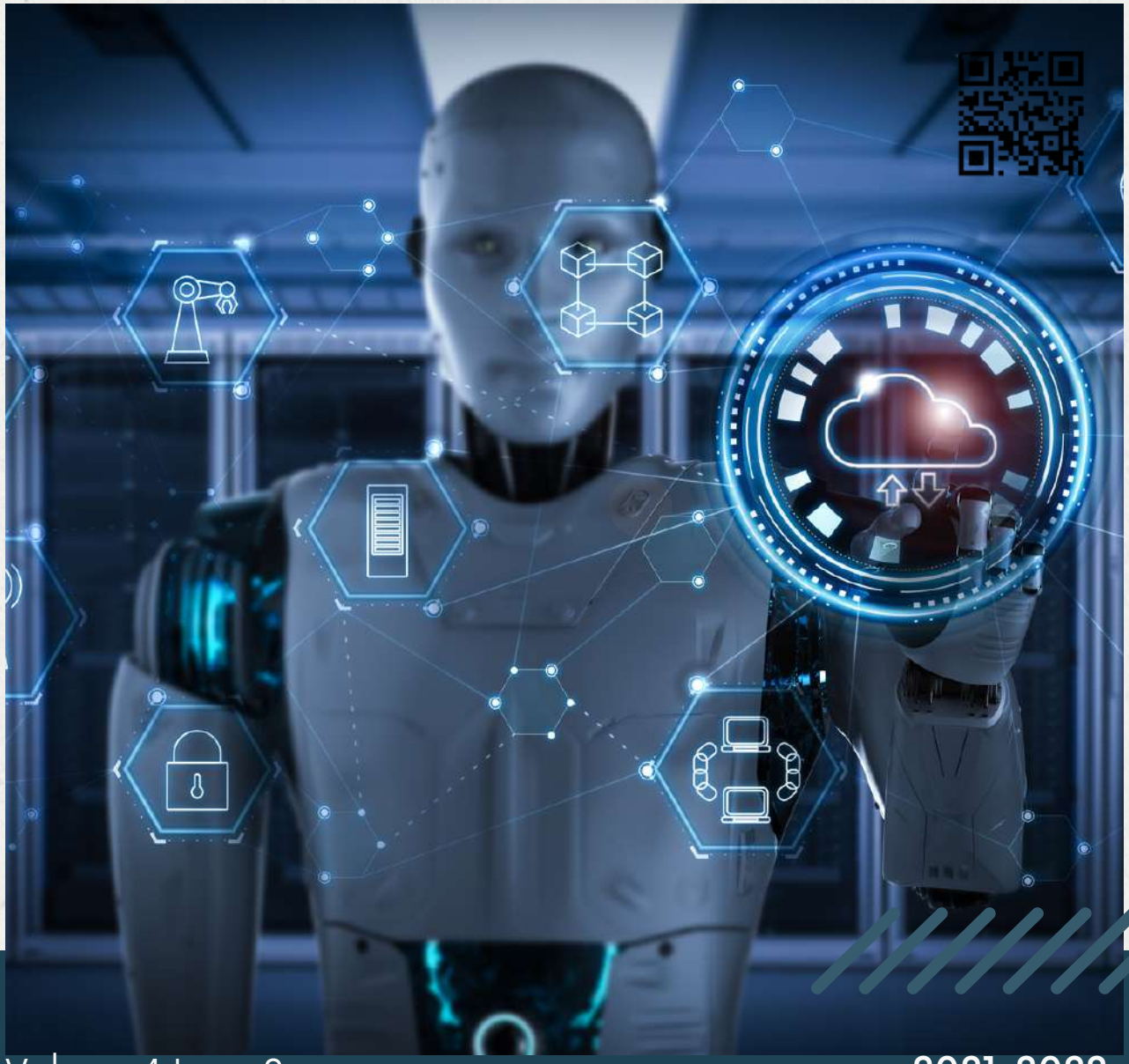
MARATHA VIDYA PRASARAK SAMAJ'S
Karmaveer Adv. Baburao Ganpatrao Thakare
College of Engineering, Nashik
Permanently Affiliated to Savitribai Phule Pune University Vide Letter No. : CA/1542 & Approved by AICTE New Delhi - Vide Letter No. : 740-89-32 (E) ET/98 AISHE Code - C-41622

COMPUTER DEPARTMENT

Presents

TECHNICAL MAGAZINE

KBT-DIGI



Volume 4 Issue 2

2021-2022

Computer Department

Vision

To be the center for excellence for training the world-class engineers to work with multi-disciplinary domain based on the state-of-the-art of technology enabled academic system blended with industrial and business practices.

Mission

To educate and train undergraduate students in Computer Engineering by instilling excellence to fulfill professional and social requirements in business and industry on the platform of scientifically designed academic processes.

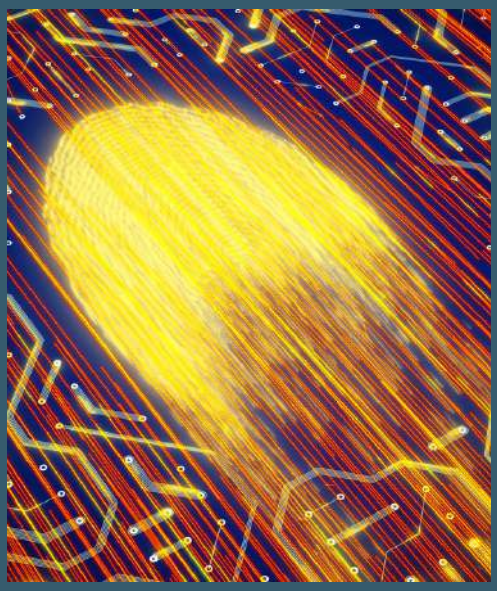
Editorial Team

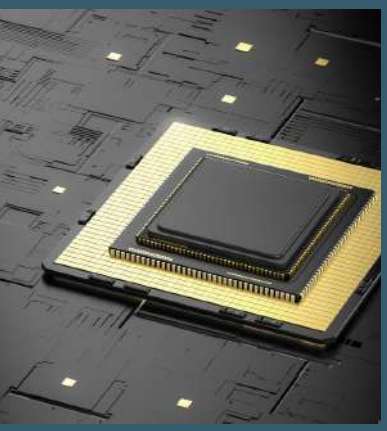
Program Educational Objectives

1.To inculcate computational and programming skills in the field of Computer Engineering.
2.To prepare the graduates to fulfill professional requirements in industry.
3.To motivate students to solve problems related to society.

TECH MAGAZINE

CONTENTS





Reliability Issue in Cloud Computing Solved By Blockchain

Author: Abin Biju (SE)

Cloud computing has become a trend and everyone even the nontech person is aware of this technology. Cloud computing has become the foundation for development, artificial intelligence, and in emerging smart cities. Due to the increased number of users, the need for reliability and security also increases. Companies are working on the reliability of the cloud.

In recent years the research has moved from reliability to security and other dimensions and like mobile computing, fog computing, and edge computing. Due to the heavy user, we are facing challenges regarding reliability, the requirements for reliability are different for different so the SLA(Service License Agreement) can't achieve it. Also, the cost and provider for the security are some of the other issues.

The issue of privacy and reliability is only with the public cloud. To solve this problem blockchain technology has paved the way into it. Blockchain provides a decentralized without the interaction of the third party in distributed computing. Each block is combined in the form of a chain. Nodes participate in the blockchain based on the value exchange protocol.

Similar to distributed consensus, the idea of service computing is to find select specific service nodes in the distributed to join in the service.

Quality of Service is the basic principle of the cloud computing system. QoS and SLA are important factors for the reliability of cloud computing. In cloud computing in order to maintain the indicators of the QoS, reliability, and trust the user will sign the agreement and a penalty will be made if the user violates it, this is known as SLA(Service License Agreement).

Blockchain is operated and maintained by all the nodes present in the chain. Similarly, the serviced distributed service is dynamically scheduled and combined according to resource strategy. Both blockchain and cloud have consensus mechanisms. The main advantage of the blockchain is that it provides encapsulation of various consensus algorithms. It has a very strong decentralized decision-making power. The consensus in the cloud is that if the QoS fails in some of the services it will update or reconstruct in a self-organizing manner. Cloud contains hardware devices like data center operating systems and servers. It also contains the market module and app verification to verify whether the changes are done according to the specification

The transaction framework uses blockchain which increases security, and trust allowing to register and make payments through it. In this scenario. SLA is eliminated as there is no one-time agreement between the user and the providers. As the open market is on a blockchain network consumers get rewarded for it .

Reference: Reliability Service Assurance in Public Clouds based on Blockchain Sa Meng, Liang Luo, Peng Sun, Yuan Gao School of Computer Science and Engineering University of Electronic Science and Technology of China Chengdu, China .

FOG COMPUTING

Author:
Onkar Arun Kulkarni (TE)

What is fog computing?

Fog computing is a service started by networking giant, CISCO. It would be very difficult to define fog computing without first defining cloud computing, since fog computing is basically an extension of the cloud. Cloud computing is the process of running ICT tasks and services and storing computer resources over the Internet.
This makes it possible for people and businesses to make use of third-party hardware and software hosted online.

Cloud computing makes it quite easy to access information and computer resources from anywhere so far as internet connection is available. With the all-round availability of shared/pooled computing resources, cloud computing offers advantages over traditional on-site hosted services in terms of speed, cost, and efficiency. Fog computing can be implemented using a basic communication system as opposed to being implemented using a heavy backbone network. As a result, it has a denser coverage. This advantage makes it easier to run a real-time, big-data operation with the ability to support billions of nodes in highly dynamic, diverse environments.

Hierarchical Fog Computing Architecture:

The proposed architecture must either be application agnostic or application specific. The architecture can be broadly classified into three main layers:

1. Things layers.
2. Fog layer.
3. Cloud layer

1. Things layer :- It is also referred to as the perception layer and can be regarded as a point where the IoT structure starts with the generation and collection of data. It has network Things like Sensors objects and devices which have communication protocols allowing transmission of the generated data through nodes to the fog.
2. Fog layer :- It is supposed to have several decentralized nodes present in each location. This layer has the task of handling all the networks and the data received. The primary refining computation and processing of data is done here and after that, the IoT applications are enhanced by controlling the data transmission to the cloud layer and reducing the request-response time taken for an IoT application.
3. Cloud layer: - The cloud layer or the data center's layer is regarded as IoT architecture's topmost layer. This layer has the function of allowing network access, conveniently and properly across all the shared resources in the IoT network. The storage and services areas of the IoT network requires heavy duty and is performed by the cloud layer.

Layered Fog Computing Architecture:

1. Physical and Virtualization Layer:- This layer comprises nodes (Physical and virtual). The nodes perform the primary task of capturing data and are located at different locations. Nodes usually involve sensing technology to capture their surroundings.Sensors used at this node collect data from the surroundings and collect data which is then sent to upper layers via gateways for further processing.

A node can be a stand-alone device like a mobile phone or it can be a part of a large device like a temperature sensor fitted inside a vehicle
2. Monitoring Layer:- In this layer, we perform node monitoring related to various tasks. Nodes can be monitored for the amount of time they work, the temperature and other physical properties they are possessing, the maximum battery life of the device, etc. The performance of applications as well as their present state is also monitored. The fog nodes are checked for their energy consumption, the amount of battery power they consume while performing their tasks.
3. Pre-processing Layer :- This layer performs various data operations mainly related to analysis. Data is cleaned and checked for any unwanted data present. Data impurity is removed and only useful data is collected. Data analysis at this layer can involve mining meaningful and relevant information from a vast amount of data collected by the end devices. Data analysis is one of the essential features that should be taken into consideration before data is used for a specific purpose.
4. Temporary Storage :-This layer is associated with non-permanent distribution and replication of data. Storage virtualization like VSAN is used in this layer. Data is removed from the temporary layer once data is moved to the cloud, from this layer.

5. Security Layer:- This layer is involved with the privacy of data, the integrity of data, encryption, and decryption of data. Privacy in the case of fog computing data can include use-based privacy, data-based privacy, and location-based privacy. The security layer ensures secure and preservation of privacy for the data which is outsourced to the fog nodes. 6. Transport Layer:- The primary function of this layer is to upload partly-processed and fine-grained secure data to the cloud layer for permanent storage. For efficiency purposes, the portion of data is collected and uploaded. The data is passed through smart-gateways before uploading onto the cloud. The communication protocols used are chosen to be lightweight, and efficient, because of the limited resources of fog computing.

Future Research Direction:

Fog computing may be the next big thing for the Internet of things. The fog computing market, valued at S22.3 million in 2017, will expand at an explosive rate and grow to S203.5 million over the next five years, according to projections by Markets and Markets. IoT interconnectivity, machine to machine communication, real-time computing demand and demand for connected devices are driving the fog market's growth. Businesses impacted by these trends are turning to fog computing for greater efficiency, faster decision-making processes and lowered operating costs. Here's a closer look at what fog computing is, why it will play a key role in the future of IoT technology and how it will help with cybersecurity.

Fog computing is a recent evolution in the computing world and has extended the scope of services like Cloud Computing further. This new age technology eliminates the limitations being faced by the Cloud technologies. In spite of large-scale usage of cloud computing in providing day-to-day services, some applications/services could not benefit much.

Conclusion: Fog computing provides a convenient way to use data near to IOT locations for better control over actuators as well as solve the problem of exploding the data volume. Complete IOT network can work smoothly by using FOG as there is no extra overhead of external traffic or computing. Fog computing accelerates awareness and response to events by eliminating a round trip to the cloud for analysis. It avoids the need for costly bandwidth of network traffic from the core network. It also protects sensitive IoT data by analyzing it inside company jurisdiction. Ultimately, organizations that adopt fog computing gain deeper and faster insights, leading to increased business agility, higher service levels, and improved safety. Fog Computing aims to reduce the processing burden of cloud computing. Fog computing is bringing data processing, networking, storage and analytics closer to devices and applications that are working at the network's edge. That's why Fog Computing is today's trending technology mostly for IoT Devices.

References:
https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00372-z
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8026115
www.ieeexplore.ieee.or

Touching Virtual Reality

Author: Yash Ringe (TE)

As a result, a haptic glove has to be able to conform to the user in order to be successful. It must be small and light, supply a lot of power, and have a very low latency. Numerous research projects have suggested using traditional DC motors, synthetic muscles, shape memory alloys, or dielectric elastomers.

The haptic glove is both the most requested and most difficult to create of all VR engagement devices. In fact, each person has a set of hands that are not similar and are not even symmetrical, in addition to having a hand that is different in size and shape. The hand is also one of the body's most perceptive organs. It can detect minute details at extremely high frequencies, but it can also create and detect very strong forces.

Classification of haptic gloves:
To simplify the analysis, the following classification of haptic gloves is adhered to in this work:
1. traditional gloves,
2. thimbles and
3. exoskeletons.

Despite the fact that all of the classes have the same goals and limitations, the three categories approach achieving these goals and limitations using quite diverse technological strategies.

The three categories are described in the sections that follow, along with more in-depth analyses of illustrative commercial product examples.
The term "traditional glove" refers to a piece of clothing made of a flexible material that fits the curve of the hand and allows the fingers to move independently. These gloves either include actuators mounted to the exterior or stitched into the fabric to measure the bending of the fingers and provide feedback to the skin or skeleton.
There are various difficulties for the haptic glove designers. The sensors and actuators first need to be small enough to fit inside the cloth or to be positioned extremely close to the fingers. Second, the entire piece of equipment (including the wire) needs to be exceedingly flexible, or else the user would feel like their movements are limited. The glove must be able to withstand significant deformations, including stretching that occurs during fitting and unfitting. Repeatedly undergoing these deformations shouldn't harm the glove's structure or compromise its usefulness.
1)T**raditional gloves:**
Such haptic gloves are now being developed by the Spanish company Neurodigital Technologies in two iterations, the GloveoneTM and the AvatarVRTM. With 10 vibrotactile actuators distributed as follows: one under each fingertip, three under the palm, and two on the back of the hand, both products enable interaction with the user's five fingers. It's unknown what kind of actuator was used.

In both products, the hand pose is determined using an IMU; the Gloveone employs flex sensors to determine the position of each finger, whilst the AvatarVR uses individual IMUs. As of March 2018, it is possible to order the products on the company website, although delivery issues have been raised in forum discussions.
Since 2015, the USA-based startup Senso has been developing the "Senso GloveTM." Five fingers can be used for interaction, and each finger has a vibration motor under the last phalange. Inertial sensors are used to measure hand and finger movements. This assures a high refresh rate and makes the device inexpensive and simple to calibrate, albeit at the expense of precision. The grip pressure is measured by integrated pressure sensors. For men, the Senso Glove is available in sizes S, M, ML, L, and XL; for women, sizes S, M, and L. Software developers can now access the second edition of the product as of March 2018.

2) Thimbles:
The term "thimble" refers to a setup in which a fingertip-mounted actuator is used. If many thimbles could be combined, input could be given to multiple fingers simultaneously. In this manner, a function resembling that of a haptic glove may develop. Designing thimbles presents a difficulty because it is necessary to incorporate sensors, actuators, a power supply, and a wireless transmission into a very small and light object. The thimble must also fit on fingers of various sizes without severely compressing them and without increasing the chance of slipping.
A straightforward thimble with just one electromagnetic actuator, the VRtouchTM device from the French startup GoTouchVR presses down on the fingertip.

The thimble is simply fastened to the finger using a magnetic clip. The attachment of numerous devices on various fingers (a maximum of three per hand) enables multi-finger contact. Similar to other thimble methods, collisions between modules stop motions made when fingers are too close together. The VRtouchTM can track the hand and finger using Leap Motion and a few other external tracking devices. Since November 2017, software developers have had access to the product.

3) **Exoskeletons**:
An articulated device known as an exoskeleton is worn over the hand by the user and sends forces to the fingers. Designers typically do not employ the same kinematics as the fingers since it would necessitate for each user a very exact modification of the segment lengths due to the necessity to adapt to a diversity of hand sizes and shapes. On the outside of the hand, the structure instead runs parallel to the fingers. The hand's many phalanges are then connected to the exoskeleton via a variety of intermediary links. The most well-known and original commercial exoskeleton is the CyberGraspTM. To deliver the force of a pulling wire to the fingertip without constricting the other joints is the function of the extremely intricate mechanical mechanism. A dataglove (CyberGlove) worn by the user underneath the exoskeleton instead of the exoskeleton itself measures the movement of the fingers.
The highest force (12 N) is sufficient to totally halt a finger's movement.

On the phalanges and palm, however, the result of having one's fingertips dragged rearward while nothing else happens is highly peculiar and not entirely believable. Nevertheless, the business has successfully sold the product for more than 20 years. The sales volume has been low (about 2–5 units per year) due to the expensive cost and the extremely limited range of applications accessible. Nevertheless, it is a noteworthy accomplishment for a gadget that was so much ahead of its time. The DexmoTM by Dexta Robotics (China) among the new generation of exoskeletons has been eagerly awaited due to its stunning design that resembles a sizable claw. The resistance of virtual objects was first simulated using mechanical brakes in the early prototypes; however, the final design incorporates servomotors for changeable force feedback. The exoskeleton monitors thumb rotation in addition to finger flexion and abduction. With a maximum force of 0.3 Nm, the force-feedback is restricted to one degree of freedom per finger. After abandoning its first attempt at crowdsourcing, the start-up Dexta Robotics has experienced a tumultuous year. As of March 2018, the only options are expensive developer kits.

Conclusion:
The actuation principles that haptic glove designers select for their commercial products tend to condense to a very small number of options. All other commercial systems use conventional electromagnetic motors, with the exception of HaptX, which relies on a smart textile with embedded air channels and hence indicates that it cannot be made wireless.
This contrasts with the vast array of drive mechanisms that have been and are now being investigated by research teams around the world. However, it seems that even with such tried-and-true technology, the designers have significant difficulties in delivering the promised products on schedule.

Refrences:
1)
https://www.neurodigital.es/gloveone
/, March 2018
2) https://senso.me/, March 2018

Digital Identity

Author:
Krutika Rawal (TE)

Introduction

A digital identity is information used by computer Systems to represent an external agent – a person, organization, application, or device. Digital identities allow access to services provided with computers be automated and make it possible for computers to mediate relationships.

How Digital Signature Works:
The use of digital identities is so widespread that many discussions refer to the entire collection of information generated by a person's online activity as a "digital identity". This includes usernames, passwords, search history, birthdates. An individual's digital identity is often linked to their civil or national identity and many countries have instituted national digital identity systems that provide digital identities to their citizenry.
Like its human counterpart, a digital identity is comprised of characteristics, or data attributes, such as the following:

- Username and password
- Online search activities, like electronic transactions
- Date of birth
- Social security number
- Medical history
- Purchasing history or behavior

A digital identity is linked to one or more digital identifiers, like an email address, URL or domain name. Because identity theft is rampant on the Web, digital identity authentication and validation measures are critical to ensuring Web and network infrastructure security in the public and private sectors.

A digital identity is the body of information about an individual, organization or electronic device that exists online.

Unique identifiers and use patterns make it possible to detect individuals or their devices. This information is often used by website owners and advertisers to identify and track users for personalization and to serve them targeted content and advertising.

A digital identity arises organically from the use of personal information on the web and from the shadow data created by the individual's actions online. A digital identity may be a Pseudonymous profile linked to the device's IP address, for example, or a randomly-generated unique ID. Digital identities are seen as contextual in nature since a user gives selective information when providing authentication information.

with privacy and security risks, including identity theft. Pseudonymous profiles can also yield an individual's identity through cross-site data analysis. While passports and licenses identify users in real life, the inclusion of such personally identifying information (PII) online may pose more risks than benefits for the user.

Several authentication and authorization systems have been explored, but there is still no standardized and verified system to identify digital identities.

Trust, authentication and authorization:

In order to assign a digital representation to an entity, the attributing party must trust that the claim of an attribute (such as name, location, role as an employee, or age) is correct and associated with the person or thing presenting the attribute. Conversely, the individual claiming an attribute may only grant selective access to its information (e.g., proving identity in a bar or PayPal authentication for payment at a website). In this way, digital identity is better understood as a particular viewpoint within a mutually-agreed relationship than as an objective property.

Authentication

Authentication is the assurance of the identity of one entity to another. It is a key aspect of digital trust. In general, business-to-business authentication is designed for security, but user-to-business authentication is designed for simplicity.

Authentication techniques include the presentation of a unique object such as a bank credit card, the provision of confidential information such as a password or the answer to a pre-arranged question, the confirmation of ownership of an email address, and more robust but costly techniques using encryption. Physical authentication techniques include iris scanning, handprinting, and voiceprinting; those techniques are called biometrics. The use of both static identifiers (e.g., username and password) and personal unique attributes (e.g., biometrics) is called multi-factor authentication and is more secure than the use of one component alone.

Authorization

Authorization is the determination of any entity that controls resources that the authenticated can access those resources. Authorization depends on authentication, because authorization requires that the critical attribute (i.e., the attribute that determines the authorizer's decision) must be verifie. For example, authorization on a credit card gives access to the resources owned by Amazon, e.g., Amazon sends one a product. Authorization of an employee will provide that employee with access to network resources, such as printers, files, or software. For example, a database management system might be designed so as to provide certain specified individuals with the ability to retrieve information from a database but not the ability to change data stored in the database, while giving other individuals the ability to change data

Digital identifiers

Digital identity requires digital identifiers—strings or tokens that are unique within a given scope (globally or locally within a specific domain, community, directory, application, etc.). Identifiers may be classified as omnidirectional or unidirectional. Omnidirectional identifiers are be public and easily discoverable, whereas unidirectional identifiers are intended to be private and used only in the context of a specific identity relationship.

as a domain name or email address, may be easily dereferenced into the entity they represent, or some current state data providing relevant attributes of that entity. Non-resolvable identifiers, such as a person's real name, or the name of a subject or topic, can be compared for equivalence but are not otherwise machine-understandable.
There are many different schemes and formats for digital identifiers. Uniform Resource Identifier (URI) and the internationalized version Internationalized Resource Identifier (IRI) are the standard for identifiers for websites on the World Wide Web. OpenID and Light-weight Identity are two web authentication protocols that use standard HTTP URIs (often called URLs). A Uniform Resource Name is a persistent, location-independent identifier assigned within the defined namespace.

Digital Object Architecture

Digital Object Architecture is a means of managing digital information in a network environment. In Digital Object Architecture, a digital object has a machine and platform independent structure that allows it to be identified, accessed and protected, as appropriate. A digital object may incorporate not only informational elements, i.e., a digitized version of a paper, movie or sound recording, but also the unique identifier of the digital object and other metadata about the digital object. The metadata may include restrictions on access to digital objects, notices of ownership, and identifiers for licensing agreements, if appropriate.