July - September 2015

TRINITY TECH REVIEW

Innovations for a Smarter Planet

TRINITY INSTITUTE OF PROFESSIONAL STUDIES

Certified as "A" Grade Institution of GGSIPU by SFRC, Govt. of NCT of Delhi

ISO – 9001:2008 Certified

TRINITY TECH REVIEW

Trinity Tech Review (TTR) is a quarterly online magazine brought up by the IT department of Trinity Institute of Professional Studies. The articles, case studies, research papers and other contributions are made by academicians, consultants and engineers covering various areas of technology.

Disclaimer: The views and opinions presented in the articles, case studies, research work and other contributions published in Trinity Tech Review (TTR) are solely attributable to the authors of respective contributions. If these are contradictory to any particular person or entity, TTR shall not be liable for the present opinions, inadequacy of the information, any mistakes or inaccuracies.

Trinity Institute of Professional Studies
An ISO 9001:2008 Certified Institution
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)

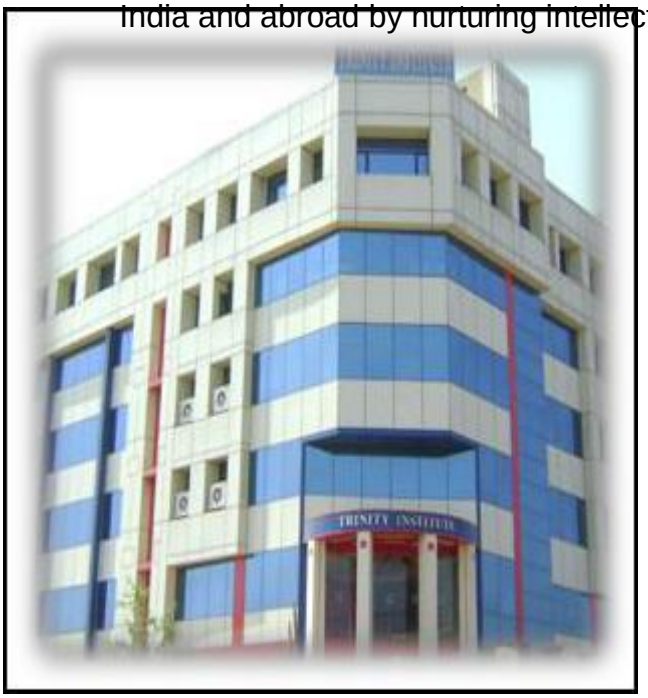
Sector-9, Dwarka, New Delhi-110075

Ph: 45636921/22/23/24, Telefax : 45636925 www.tips.edu.in, tips@tips.edu.in

ABOUT US

The Trinity Institute of Professional Studies (TIPS), Sector-9, Dwarka, an ISO 9001:2008 certified institute, is affiliated to Guru Gobind Singh Indraprastha University.

It was founded in 2007 under the aegis of Kamal Educational and Welfare Society (KEWS) with the objective of overcoming the critical demand for skilled professionals in India and abroad by nurturing intellectual capital by adopting best practices in quality education.



TIPS is offering courses / programs across various disciplines, such as Management, Commerce, Banking & Insurance, Information Technology and Journalism & Mass Communication. Today, the Institute has over 1500 students and more than 60 faculty members. The faculty at the Institute has proper experience both from the industry and academics as a result of which it brings the right mix of research and industry experience to education and consultancy offered by the Institute.

COURSES OFFERED:

Programme	Annual Student Intake	First Shift	Second Shift
BJMC	120	60	60
BCA	120	60	60
BBA (G)	120	60	60
B.COM (H)	160	100	60

TRINITY INSTITUTE OF PROFESSIONAL STUDIES

Sector-9, Dwarka Institutional Area, New Delhi-110075, Tel: 011-45636921/22/23/24

Certified as "A" Grade Institution by SFRC, Govt. of NCT of Delhi

ISO – 9001:2008 Certified
Affiliated to GGSIP University

INTRODUCTION

Trinity Tech Review is a quarterly online journal published by Trinity Institute of Professional Studies, Dwarka. The journal aims to bring to the fore latest trends and inventions in IT industry, in India and Abroad. The Theme for this edition of TTR is "**Innovations for a Smarter Planet**". The edition brings to the readers an overview of recently emerged technologies in the field of IT that are making lives easier. The article – "Emergence of Smart Cities and the Need for Big Data Analytics", brings to light a raging area of research in today"s time. Quoted by Tech Giants as "the next big invention after the internet", it was a compelling area to cover. The article "Ubiquitous Computing – Emerging Invisible and Everywhere Technology", introduces the readers to a new "breed" of computing that is seamless and pervasive. The edition also contains an article on sensors, titled – "A Formal Approach on Sensors". It gives a brief about various kinds of sensors that are being used around the world in everyday life, making possible things that were previously believed impossible. An article on cloud computing titled – "Cloud Computing Security Issues" familiarizes the users with serious security threats faced while using cloud computing solutions like Google Drive and Amazon EC. The edition could not have been completed without an article on another commonly utilized technology especially in business applications, i.e. data mining and warehousing. The article – "OLAP, A Solution to Data Warehousing" covers it very well, doing justice to the significance of accessibility to data.

We express gratitude towards the writers and a special thanks to Dr. L. D. Mago, for his valuable guidance.

EMERGENCE OF SMART CITIES AND NEED FOR BIG DATA ANALYTICS

Himja Sethi

In the near future the cities of the world will be better connected through high speed network, communicating, exchanging, using and generating information at a very high speed. In India too, the Narendra Modi Govt. has been paying rightfully deserved attention to the technology sector. The smart city mission is one of the four flagship schemes announced by the Govt. in the past year which has brought IT at the forefront of the nation‟s development agenda and established itself as the prime means of welfare of the rich as well as the poor. As the country looks towards a new horizon, IT, ITES, ICT and its peripheral sectors are relishing a boom in research initiatives as well as job opportunities. At the centre of this success story of twenty first century, lies Big Data.

Smart city and Big Data are two leading areas of research in IT today. It would not be wrong to state that the two are inseparable. The inter twining of Internet of Things, RFID and Big Data Generation and Analysis creates the fabric of a smart city. One may wonder, ***what makes a City Smart***?The

Answer is, when a city‟s infrastructure is so "dynamic" that it stays few steps ahead of the constantly changing needs of its citizens, it is termed as smart. Let‟s consider a few examples…

Smart Transportation System: The driver of a bus receives real time and predictive information of number of passengers waiting at bus stops along the route in the form of a density map, on a small LCD screen. It enables reduction in fuel consumption, better traffic management and improved efficiency of public transport system.

Smart Metering: Water and Electricity meters automatically collect and transmit information of consumption using sensors, advanced communication networks and digital signals in regular intervals or on demand enabling remote manipulation like power cut off.

Smart Healthcare: Implantable transmitters and sensors detect an emergency situation in real time and send signals wirelessly to nearest medical facility and loved ones enabling early intervention and immediate medical attention.

One may notice certain common factors in all these revolutionary innovations (which have been or are being implemented in developed nations) like, embedded RFID chips, miniature processors that make sense of audio or visual input, wireless communication through radio frequency, remote sensors and an effective and responsive support infrastructure. A smart city has all this and a lot more. With the help

of Information Technology, lightning fast computing capabilities and fast wireless communication network, a smart city can be powered up!

But when everyday things like buildings, medical equipment, homes and even people are embedded with chips that generate signals or "information", it leads to generation of vast amounts of data at a very high speed. According to a report published in a leading IT journal in 2014, the amount of data generated by IoT devices will be massive, with the total amount of data generated estimated to hit 40,000 exabytes (1 exabyte = 1 trillion gigabytes) as opposed to the current 10,000 exabytes. But ***what is Big Data? Or what makes a data Big?***

Wikipedia explains Big Data as "**a** broad term for data sets so large or complex that traditional data processing applications are inadequate. Challenges include analysis, capture, data curation, search, sharing, storage, transfer, visualization, and information privacy. The term often refers simply to the use of predictive analytics or other certain advanced methods to extract value from data, and seldom to a particular size of data set**."**

In other words, large amounts of seemingly unrelated data, produced at high speed when analyzed help establish correlation between factors that were previously considered independent. This enables us to "prevent crime, spot business trends and prolong life expectancy" among other things. The applications are truly boundless.

To get a perspective on Big Data, consider the fact that by analyzing the content of comments on social media websites, governments can put tab on the citizens of their country and familiarize with what they "think", promoting responsiveness and efficient policy making as well as preventing anti-social activities.

Tech giants like IBM, Adobe, Tech Mahindra, Wipro and others are leading big data research initiatives. As Big Data has placed itself as the next big thing after the invention of internet, technology scientists have enthusiastically immersed themselves in finding out solutions to problems of handling, processing, storage and utilizing it.

Conclusion

A Smart city model is unimaginable without big data analytics. A city needs Big Data to function and fulfill the needs and expectations of its citizens. With the help of IoT, Artificial Intelligence, Data Mining, Advanced computer Networks and cyber security mechanism, a Smart city can come to life in near future. The issues and obstacles that are faced in maintenance of such an infrastructure needs to be seen, but till then the future for technology driven cities looks bright.

UBIQUITOUS COMPUTING

EMERGING INVISIBLE AND EVERYWHERE TECHNOLOGY

Charanpreet Kaur

Today the physical world environment is being increasingly digitally instrumented and strewn with the embedded sensor-based and control devices. These can sense our location and can automatically adapt to it, easing access to localised services, e.g., doors open and lights switch on as we approach them. Positioning systems can determine our current location as we move. They can be linked to other information services, i.e., to propose a map of a route to our destination.

This is a new and booming concept in software engineering and computer science where computing is made to appear everywhere and anywhere. This is what we call **Ubiquitous Computing or Pervasive Computing**. Pervasive computing is an area of computing that aims at pervading all aspects of human life that may benefit from the intervention of computing services. It is also known as Invisible Computing or Everywhere Computing. Pervasive Computing Infrastructure comprises of computing elements, communicating elements, sensors, actuators, and interface devices. The infrastructure offers seamless connectivity to the devices / entities / services.

Mark Weiser, the Father of Ubiquitous Computing, researcher in the Computer

Science Lab at Xerox‟s PARC (Palo Alto Research Centre) first articulated the idea of ubiquitous computing in 1988. He has called

UC "…highest ideal is to make a computer so embedded, so fitting, so natural, that we use it without even thinking about it."

During one of his talks, Weiser outlined a set of principles describing ubiquitous computing:

– The purpose of a computer is to help you do something else.

– The best computer is a quiet, invisible servant.

– The more you can do by intuition the smarter you are; the computer should extend your unconscious.

– Technology should create calm.

Principles of Pervasive Computing System Design

Simplicity: Low complexity allows elegant designs and maintainable systems

Versatility: Ability to provide a range of services with due customization

Pleasurability / Usability: If users do not find it convenient or pleasurable for their purpose, it would be of limited use, if any.

User Safety: Nothing should compromise on safety of the users.

Fitness for the purpose but at reasonable cost.

Elements of Pervasive Computing Systems

- **Device / Hardware elements**
  - Computing elements
  - Sensory elements connected to compute elements or Sensor-compute elements
- **Networking elements**
- **I/O Elements**
  - Power-provisioning elements
- **Software elements**
  - OS
  - Other system software
  - Application software
- **HCI elements**

Core Properties of UbiCom Systems

1. Computers need to be networked, distributed and transparently accessible.
2. Human–computer interaction needs to be hidden more.
3. Computers need to be context-aware in order to optimize their operation in their environment.
4. Computers can operate autonomously, without human intervention, be self-governed, in contrast to pure human–computer interaction.
5. Computers can handle a multiplicity of dynamic actions and interactions, governed by intelligent decision-making and intelligent organizational interaction.

Architectural Design for Ubiquitous Computing Systems: Smart DEI Model

Three basic architectural design patterns for UbiCom System are: **smart devices, smart environment and smart interaction.**

Here the concept smart simply means that the entity is active, digital, networked, can operate to some extent autonomously, is reconfigurable and has local control of the resources it needs such as energy, data storage, etc.

Smart Devices

Smart devices, e.g., personal computer, mobile phone, tend to be multi-purpose ICT devices, operating as a single portal to access sets of popular multiple application services that may reside locally on the device or remotely on servers.

Smart devices tend to be personal devices, having a specified owner or user. In the smart device model, the locus of control and user interface resides in the smart device.

Figure 1

Smart Environments

Cook and Das refer to a smart environment as „one that is able to acquire and apply knowledge about the environment and its inhabitants in order to improve their experience in that environment".

A smart environment consists of a set of networked devices that have some connection to the physical world.

“

e.g., motion or body heat sensors coupled to a door release and lock control.

Figure 2

Smart Interaction

“

Smart interaction is needed to promote a unified and continuous interaction model between UbiCom applications and their UbiCom infrastructure, physical world and human environments.

“

In the smart interaction design model, system components dynamically organize and interact to achieve shared goals.

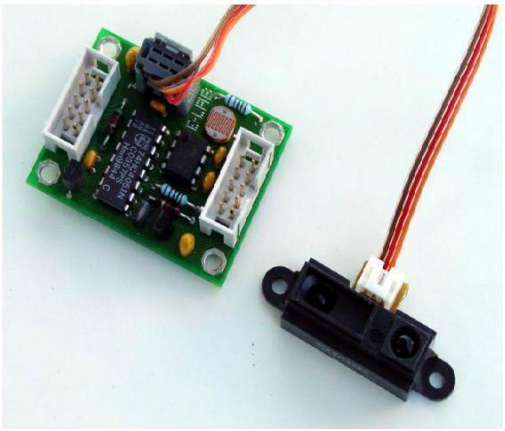


Figure 3

A FORMAL APPROACH ON SENSORS

Priyanka Rattan

As we all know that the sensors are the most important part of the embedded system and the robotics world. By using different types of sensors we can minimize the logic circuits and also make the system more efficient to get output by taking less input. Therefore, here is detailed view of different types of sensors.

INTRODUCTION

Sensors are sophisticated devices that are frequently used to detect and respond to electrical or optical signals. A **Sensor** converts the physical parameter (for example: temperature, blood pressure, humidity, speed, etc.) into a signal which can be measured electrically. Let‟s explain the example of temperature. The mercury in the glass thermometer expands and contracts the liquid to convert the measured temperature which can be read by a viewer on the calibrated glass tube.

CRITERIATOCHOOSETHE SENSORS

There are certain features which have to be considered when we choose a sensor. They are as given below:

1. Accuracy
2. Environmental condition - usually has limits for temperature/ humidity
3. Range - Measurement limit of sensor
4. Calibration - Essential for most of the measuring devices as the readings changes with time
5. Resolution - Smallest increment detected by the sensor
6. Cost
7. Repeatability - The reading that varies is repeatedly measured under the same environment.

CLASSIFICATION OF SENSORS

The sensors are classified into the following criteria:

1. Primary Input quantity (Measured)
2. Transduction principles (Using physical and chemical effects)
3. Material and Technology
4. Property
5. Application

TYPES OF SENSORS:

1. Temperature Sensors

This device collects information about temperature from a source and converts into a form that is understandable by other device or person. The best illustration of a temperature sensor is mercury in glass thermometer. The mercury in the glass expands and contracts depending on the alterations in temperature. The outside temperature is the source element for the temperature measurement. The position of the mercury is observed by the viewer to measure the temperature. There are two basic types of temperature sensors:

Contact Sensors – This type of sensor requires direct physical contact with the object or media that is being sensed. They supervise the temperature of solids, liquids and gases over a wide range of temperatures

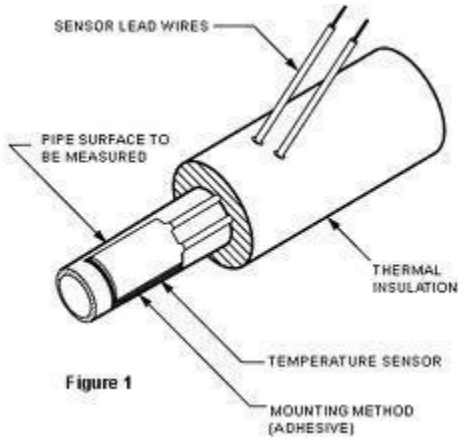


Figure 1

Non contact Sensors – This type of sensor does not require any physical contact with the object or media that is being sensed. They supervise non-reflective solids and liquids but are not useful for gases due to natural transparency. These sensors use Plank‟s Law to measure temperature. This law deals with the heat radiated from the source of heat to measure the temperature.

2. IR Sensor

This device emits and/or detects infrared radiation to sense a particular phase in the environment. Generally, thermal radiation is emitted by all the objects in the infrared spectrum. The infrared sensor detects this type of radiation which is not visible to human eye.

Advantages

Easy for interfacing Readily available in market

Disadvantages

Disturbed by noises in the surrounding such as radiations, ambient light etc.

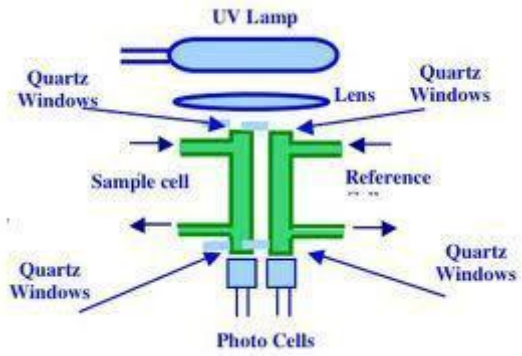
3. UV Sensor

These sensors measure the intensity or power of the incident ultraviolet radiation. This form of electromagnetic radiation has wavelengths longer than x-rays but is still shorter than visible radiation. An active material known as polycrystalline diamond is being used for reliable ultraviolet sensing. UV sensors can discover the exposure of environment to ultraviolet radiation.

Examples include:

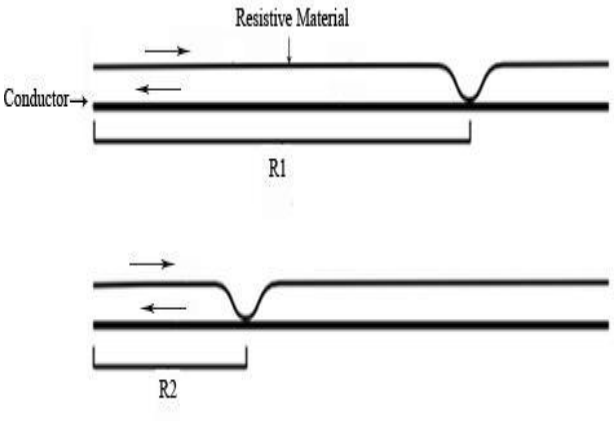
- UV phototubes are radiation-sensitive sensors supervise UV air treatments, UV water treatments, and solar irradiance.
- Light sensors measure the intensity of incident light.
- UV spectrum sensors are charged coupled devices (CCD) utilized in scientific photography.
- Ultraviolet light detectors.
- Germicidal UV detectors.

. Photo stability sensors.



4. Touch Sensor

A touch sensor acts as a variable resistor as per the location where it is touched. The figure is as shown below.

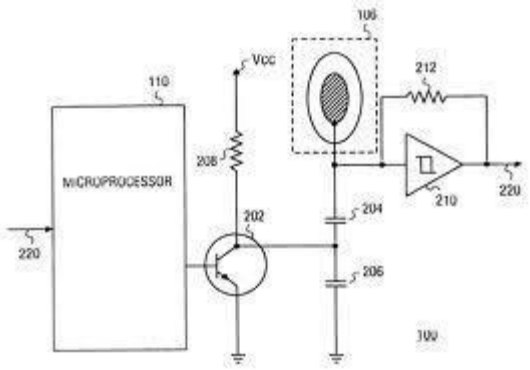


A touch sensor is made of:

- Fully conductive substance such as copper

· Insulated spacing material such as foam or plastic

Partially conductive material



5. Proximity Sensor

A proximity sensor detects the presence of objects that are nearly placed without any point of contact. Since there is no contact between the sensors and sensed object and lack of mechanical parts, these sensors have long functional life and high reliability. The different types of proximity sensors are Inductive Proximity sensors, Capacitive Proximity sensors, Ultrasonic proximity sensors, photoelectric sensors, Hall-effect sensors, etc.

CONCLUSION

By knowing these types of sensors and their application we can be able to use them in a much specified manner. And also we can them in the various fields according to their principles and applications.The flexibility, fault tolerance, high sensing fidelity; low-cost and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the future, this wide range of application areas will make sensor networks an integral part of our lives. However, realization of sensor networks needs to satisfy the constraints introduced by factors such as fault tolerance, scalability, cost, hardware, topology change, environment and power consumption. Since these constraints are highly stringent and specific for sensor networks, new wireless ad hoc networking techniques are required. We encourage more insight into the problems and more development in solutions to the open research issues as described in this article.

CLOUD COMPUTING SECURITY ISSUES

Ruchika Bajaj **Bharti Dewani**

Cloud word is used to denote the network. With the help of cloud computing, user can get access to the software for a given time period without license from the concerned company. User can also store data on cloud like in gmail. However, security of cloud is the main problem which limits its adoption.

In this article various security issues of cloud like XML Signature Element wrapping, Browser security, Cloud malware injection attack and flooding attacks are discussed along with its solution.

THE CLOUD COMPUTING SECURITY ISSUES

1. **XML Signature Element Wrapping**

In this issue, attacker changes an element in SOAP message, thus breaching the security .An attacker can also intercepts the SOAP message and changes the receiver‟s e-mail address to the attacker‟s e-mail address, the web service will forward the e-mail to the attacker.

The possible solution would be using a combination of WS (Web Service)Security with XML signature to sign particular element and digital certificated such as X.509 issued by trusted Certificate Authorities (CAs). Furthermore, the web service server side should create a list of elements that is used in the system and reject any message which contains unexpected messages from clients.

2. **Browser Security**

For the security of web browser, SSL/TLS is used to encrypt the credential and 4-way handshake process is used to authenticate the client. SSL/TLS only supports point-to-point communications, if there is a middle tier between the client and the cloud server, such as a proxy server or firewall, the data has to be decrypted on the intermediary host. If there is an attacker sniffing packages on that host, the attacker may gain the credentials and use the credentials in order to log in to the cloud system as a valid user. So, SSL/TLS is still limited in its capacities as an authentication for cloud computing.

The potential solution for this is that the vendors that create web browsers apply WS-Security concept within their web browsers. The reason why WS-Security appears to be more suitable than SSL/TLS is WS-Security works in message level. As a result of this, web browsers are able to use XML Encryption in order to provide end-to-end encryption in SOAP messages. Unlike point-to-point encryption, end-to-end encryption does not have to be decrypted at intermediary hosts. Consequently, attackers are unable to sniff and gain plain text of SOAP messages at the intermediary hosts illustrated.

3. **Cloud Malware Injection Attack**

Cloud malware injection is the attack that attempts to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IssA) [4]. In order to perform this attack, an intruder is required to create his own malicious application, service or virtual machine instance and then the intruder have to add it to the cloud system. Once the malicious software has been added to the cloud system, the attacker had to trick the cloud system to treat the malicious software as a valid instance. If it is successful, normal users are able to request the malicious service instance, and then the malicious is executed.

Another scenario of this attack might be an attacker try to upload a virus or Trojan program to the cloud system. Once the cloud system treats it as a valid service, the virus program is automatically executed and the cloud system infects the virus which can cause damage to the cloud system. In the case of the virus damages the hardware of the cloud system, other cloud instances running on the same hardware may affect to the virus program because they share the same hardware.

In addition, the attacker may aim to use a virus program to attack other users on the cloud system. Once a client requests the

malicious program instance, the cloud system sends the virus over to the internet to the client and then executes on the client‟s machine. The client‟s computer then is infected by the virus.

The possible countermeasure for this type of attack could be performing a service instance integrity check for incoming requests. A hash value can be used to store on the original service instance‟s image file and compare this value with the hash values of all new service instance images. As a result of using the hash values, an attacker is required to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance into the cloud system.

4. Flooding Attacks

Although data transmission between a client and the server may secure, attackers might choose to attack the cloud environment directly. One of the common characteristics of the cloud system is to provide dynamically scalable resources. It offers a benefit for variability in usage. Once there are more requests from clients, cloud system automatically scale up by starting up new service instances in order to support the clients‟ requirements. On the other hand, this also can be a severe vulnerability of flooding attack such as DoS, which, basically, is an action of sending a large number of nonsense requests to a certain service. When an attacker performs a DoS (Denial of service) attack to a particular service in a cloud system, cloud computing operating system realizes the extra requests. It begins to provide more service instances in order to deal with the workload. If the attacker sends more requests, the cloud system will try to work against the requests by providing more computational resources. Eventually, the system might consume all of the resources on the cloud system and be not able to provide services to normal requests from users. Indirectly, the other service instances running on the same cloud hardware server of the target service instance may also suffer from the workload caused by the DoS attack. Once the resources of the server are almost or Completely depleted, there are no resources available for other services on the same server. As a consequence, the other services also might not be able to provide their services to normal users. In terms of accounting point of view, DoS attack costs extra fees to the consumers.

Even though it is difficult to completely prevent DoS attacks, installing a firewall or intrusion detection system (IDS) is able to filter malicious requests from attacking the server. Nonetheless, sometimes, anIDS (Intrusion Detection System) can mislead the administrator because it gives false alerts. It may consider normal requests as intrusive requests.

OLAP
A SOLUTION TO DATA WAREHOUSING

Ritika Kapoor

Corporate data has grown consistently and rapidly during the last decade. During the 1980‟s, businesses and governments worked with data in the megabytes and gigabyte

range. Contemporary enterprises have to manipulate data in the range of terabytes and petabytes. Concurrently, the need for more sophisticated analysis and faster synthesis of better quality information has grown. The numbers of individuals within an enterprise who have a need to perform more sophisticated analysis is growing.Therefore, we need something more than the relational databases i.e. Data Warehouse. A Data Warehouse is a relational database that is designed for query and analysis rather than for transaction processing. It usually contains historical data derived from transaction data, but it can include data from other sources. Data warehouses are targeted for decision making.

The solution to this is **OLAP** in the Data Warehouse. Data Warehouse is for **On Line Analytical Processing (OLAP)**.The key indicator of a successful OLAP application is its ability to provide information as needed, i.e., its ability to provide "just-in-time" information for effective decision-making. A truly flexible data model ensures that OLAP systems can respond to changing business requirements as needed for effective decision making. On Line Analytical Processing (OLAP) systems can respond to changing business requirements as needed for effective decision making. It supports complex queries that access millions of records.

A data warehouse is a relational database that is designed for query and analysis rather than for transaction processing. It usually contains historical data derived from transaction data, but it can include data from other sources. It separates analysis workload from transaction workload and enables an organization to consolidate data from several sources. In addition to a relational database, a data warehouse environment includes an extraction, transportation, transformation, and loading (ETL) solution, an online analytical processing (OLAP) engine, client analysis tools, and other applications that manage the process of gathering data and delivering it to business users. The data warehouse is maintained separately from the organization‟s operational databases. There are many reasons for doing this. The data warehouse supports on-line analytical processing (OLAP), the functional and performance requirements of which are quite different from those of the on-line transaction processing (OLTP) applications traditionally supported by the operational databases.

Operational databases are for On Line Transaction Processing

- Automate day-to-day operations (purchasing, banking etc.)
- Transactions access (and modify!) a few records at a time
- Database design is application oriented
- Metric: transactions/sec

Users need the ability to perform multidimensional analysis with complex calculations, but we find that traditional tools of report writing, query products, spreadsheets, and language interfaces are distressfully inadequate. Then what is the ANSWER?

Clearly, the tools used in OLTP and basic data warehouse environments do not match up to the task. We need different set of tools and products that are specifically meant for serious analysis. **That is we need OLAP in the data warehouse.**

SOLUTION TO THE PROBLEM

Data Warehouse is for On Line Analytical Processing (OLAP)

– Complex queries that access millions of records

– Need historical data for trend analysis

– Long scans would interfere with normal operations

– Synchronizing data-intensive queries among physically separated databases would be a nightmare!

– Metric: query response time

The key indicator of a successful OLAP application is its ability to provide information as needed, i.e., its ability to provide "just-in-time" information for effective decision-making. This requires more than a base level of detailed data.

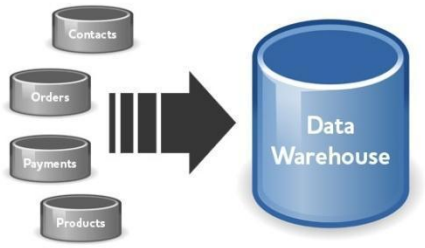


Figure 1

Features of OLAP

Although OLAP applications are found in widely divergent functional areas, they all require the following key features:

- **Multidimensional views of data**
- **Calculation-intensive capabilities**
- **Time intelligence**

Multidimensional Views

Multidimensional views are inherently representative of an actual business model. Rarely is a business model limited to fewer than three dimensions. Managers typically look at financial data by scenario (for example, actual vs. budget), organization, line items, and time; and at sales data by product, geography, channel, and time.

Time Intelligence

Time is an integral component of almost any analytical application. Time is a unique dimension because it is sequential in character (January always comes before February). True OLAP systems understand the sequential nature of time.

Complex Calculations

The real test of an OLAP database is its ability to perform complex calculations. OLAP databases must be able to do more than simple aggregation. While aggregation along a hierarchy is important, there is more to analysis than simple data roll-ups.

OTHER ALTERNATIVES

Using spreadsheets

A spread sheet such as that is a useful tool for analysing sales data such as product sold, number of purchases, and city of sale. A pivot table is a two-dimensional spread sheet with associated subtotals and totals that supports viewing more complex data by nesting several dimensions on the x- or y-axis and displaying data on multiple pages.

Using sql

Using a Structured Query Language database management system offers considerable flexibility in structuring data.

However, formulating many desirable computations such as cumulative aggregates (sales in year to date), combining totals and subtotals, or determining rankings such as the top 10 selling products is difficult if not impossible in standard SQL.

Figure 2