



Computer Networks for Medical Data and its Consequences – Medical Devices Literature Survey

Rastogi

*Asst. Prof. Dept. of Computer Science Engineering,
MIET, Engineering College, Meerut, U.P, India*

Article details:

Published: 30th January 2023



This paper describes about the computing environment and types of network used and various others existed possible networks available for certain purpose and can be used in the computer network environment. As everyone knows about the computer network, basically it is a collection of computer machine, servers, network devices, mainframes or any devices which has the capacity or features of connecting to each other and can form a network.

Minimum two machines or device can be connected and can be said as a computer network. Now this network is capable to share information or data within the connected devices or networks only. Its best suited example can be internet where many more than the million peoples are confined within the networks and exchange data or information worldwide in fractions of seconds on a single click of computer keyboard. Often we see and use widely in the applications of cloud computing and cyber crimes and security concern.

Keywords: Computer, network, cloud computing network, machine, device, server, internet, mainframes, ad-hoc networks, cyber security, wireless networks, mobile networks, LAN, MAN, WAN, PAN, WMAN

To cite this article:

Rastogi, U. (2019). Computer Network And Its Consequences –A Literature Survey. *The International Journal of Health, Education and Social (IJHES)*, 2(11), 12–26.



1. INTRODUCTION

1.1 Computer Networks fall into three classes regarding the size, distance and the structure namely: LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network). Before we, discussing about type of network we can discuss about what is a network. Computer networks are all around us. For example, they are essential for effective communication, sharing knowledge, research and development, modern education, entertainment and, of course, e-commerce.

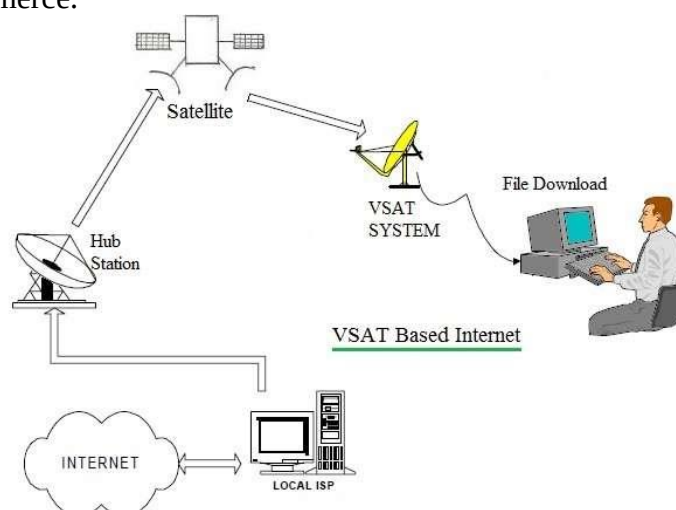


Figure 1 Example of Computer networks

In the today world, two devices are in network if a process in one device is able to exchange information with a process in another device. Networks are known as a medium of connections between nodes (set of devices) or computers. A network is consist of group of computer systems, servers, networking devices are linked together to share resources, including a printer or a file server. There are three types of Networks:

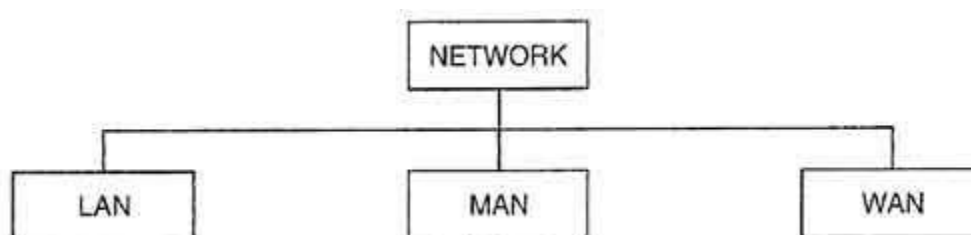


Figure 2 Network types Block structure



1. **LAN (Local Area Network):** A Local Area Network is a privately owned computer network covering a small Networks geographical area, like a home, office, or groups of buildings e.g. a school Network. A LAN is used to connect the computers and other network devices so that the devices can communicate with each other to share the resources. The resources to be shared can be a hardware device like printer, software like an application program or data. The size of LAN is usually small. The various devices in LAN are connected to central devices called Hub or Switch using a cable.
2. **MAN (Metropolitan Area Networks):** MAN stands for Metropolitan Area Networks is one of a number of types of networks. A MAN is a relatively new class of network. MAN is larger than a local area network and as its name implies, covers the area of a single city. MANs rarely extend beyond 100 KM and frequently comprise a combination of different hardware and transmission media. It can be single network such as a cable TV network, or it is a means of connecting a number of LANs into a larger network so that resources can be shared LAN to LAN as well as device to device.
3. **WAN (Wide Area Networks):** A wide area network (WAN) is a telecommunication network. A wide area network is simply a LAN of LANs or Network of Networks. WANs connect LANs that may be on opposite sides of a building, across the country or around the world. WANS are characterized by the slowest data communication rates and the largest distances. WANs can be of two types: an enterprise WAN and Global WAN. Computers connected to a Wide Area Networks are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites. The largest WAN in existence is the Internet. Some segments of the Internet, like VPN based extranets, are also WANs in themselves. Finally, many WANs are corporate or research networks that utilize leased lines.

1.2 Cloud computing network

Cloud computing is increasingly being adapted by a wide range of users starting from commercial entities to consumers. A survey by Right Scale¹ found that an average user runs at least four cloud-based applications and at any point in time is evaluating another four. The survey also found that 41% of commercial entities run significant workload on public clouds. With so much of our workload moving to cloud, security in cloud computing is under increased scrutiny. This assessment is also supported by the 2017 report by Forbes², which says that in 15 months, while 80% of all IT budgets will be committed to cloud solution, 49% of the businesses are delaying cloud deployment due to security skills gap and concerns. The problem appears to be multi-dimensional, with lack of skilled resources, lack of maturity, conflicting best practices, and complex commercial structures to name a few. Adaption of cloud has reached a tipping point and it is expected that more workloads will move from traditional local storage to cloud from not just average Internet users, but also from most if not all commercial entities. While there are many problems that need identifying, analyzing, and addressing, this document attempts to survey the security in cloud computing and reports



on various aspects of security vulnerabilities and solutions. Some questions that need urgent answers are: (a) Privileged User Access Management, (b) Regulatory Compliance, (c) Data Location, (d) Data Segregation, (e) Data Protection and Recovery Support, (f) Investigative Support, and (g) Long-term Viability.

1.3 Cyber crimes: A variety of activities can be considered cybercrimes. It is sufficient that they are facilitated by or involve the use of electronic communications or information systems. This includes any electronic device or computer or the Internet.

1.4 Cyber Security: The practice of cyber security is detrimental when it comes to confidentiality, integrity, and availability of a technological infrastructure. Every IT security expert understands that a lack of security can cause problems in any system or network. When computer systems become vulnerable, hackers can exploit their targets to steal credit card information, read and sell sensitive files, and block services. Vulnerabilities for computing networks and architectures can cause headaches for IT departments, but usually administrators and developers can create patches and updates that help combat against the upcoming attacks that may surface at any moment. If a Denial of Service (DoS) attack occurs, network admins will work to mitigate the attack and relocate services that had been taken offline or bogged down.

1.4 Various types of LAN

There are basically two types namely: **ARCnet** and **Ethernet**.

ARCNET (Attached Resource Computer NETWORK): ARCNET is one of the oldest, simplest, and least expensive types of Local-Area **Network protocol**, similar in purpose to Ethernet or Token Ring. ARCNET was the first widely available networking system for microcomputers and became popular in the 1980s for office automation tasks. ARCnet was introduced by Datapoint Corporation in 1977. A special advantage of ARCNET is that it permits various types of transmission media - twisted-pair wire, coaxial cable, and fiber optic cable - to be mixed on the same network. The specification is ANSI 878.1. It can have up to 255 nodes per **network**.

- a)** A new specification, called ARCnet Plus, will support data rates of 20 Mbps **Ethernet** is a family of computer networking technologies for local area networks commercially introduced in 1980. Standardized in IEEE 802.3, Ethernet has largely replaced competing wired local area network technologies. Ethernet uses a bus or star topology Network and supports data transfer rates of 10 Mbps.

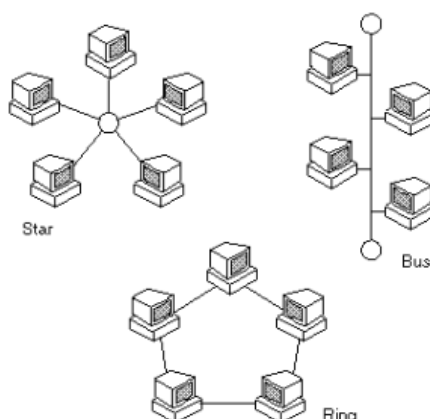


Figure 3 Network Topology

And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second. Ethernet is a physical and data link layer technology for local area networks (LANs). Ethernet Network was invented by engineer Robert Metcalfe.

1.3 MAN Structures and standards: A MAN can be created as a single network such as Cable TV Network, covering the entire city or a group of several Local Area Networks (LANs). In this way resource can be shared from LAN to LAN and from computer to computer also. MANs are usually owned by large organizations to interconnect its various branches across a city.

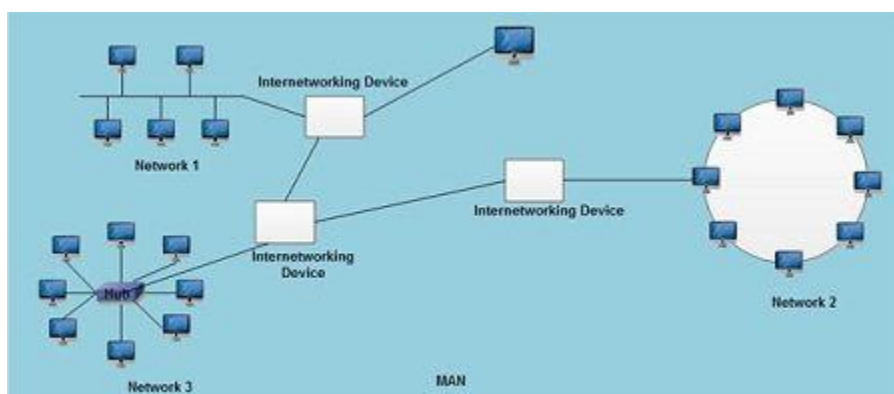


Figure 4 MAN Structure Layouts

1.4 WAN and its Global standards

Numerous WANs have been constructed, including public packet networks, large corporate networks, military networks, banking networks, stock brokerage networks, and airline reservation networks. Organizations supporting WANs using the Internet Protocol are known as Network Service Providers (NSPs). These form the core of the Internet. Clarify Global WANs and WLANs.



- a) **Global WANs** (wide area networks) also span the world but they do not have to connect LANS (Local Area Networks) within a single organization. The Internet is an example of a global WAN. It connects diverse locations, organizations and institutions throughout the world. Global WANS (wide area networks) can be public or private. Private WANs (wide area networks) are called Intranet which belongs to an organization. Public WANs (wide area networks) are open to everybody so that anybody can connect and use the resources and services available.
- b) **WLANs - Wireless Local Area Networks:** A WLAN typically extends an existing wired local area network. WLANs (Wireless Local Area Networks) are built by attaching a device called the access point (AP) to the edge of the wired network. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter. Network security remains an important issue for WLANs (Wireless Local Area Networks). Random wireless clients must usually be prohibited from joining the WLAN. Technologies like WEP raise the level of security on wireless networks to rival that of traditional wired networks.

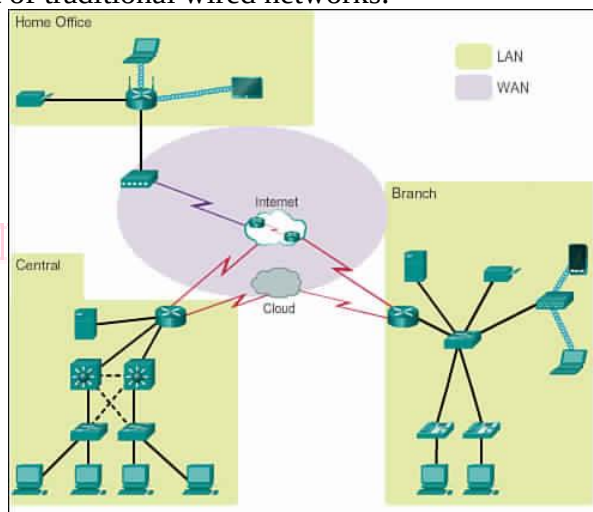


Figure 5 LANs, WANs, and Internet exploration

All components that can connect into a wireless medium in a network are referred to as stations. Wireless stations fall into one of two categories: access points, and clients. Access points (APs), normally routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones and other smart phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

1.5 WLAN (Wireless Local Area Networks) types

a) Private home or small business WLAN



Commonly, a home or business WLAN employs one or two access points to broadcast a signal around a 100- to 200-foot radius. You can find equipment for installing a home WLAN in many retail stores. With few exceptions, hardware in this category subscribes to the 802.11a, b, or g standards (also known as Wi-Fi); some home and office WLANs now adhere to the new 802.11n standard. Also, because of security concerns, many home and office WLANs adhere to the Wi-Fi Protected Access 2 (WPA2) standard.

b) Enterprise class WLAN

An enterprise class WLAN employs a large number of individual access points to broadcast the signal to a wide area. The access points have more features than home or small office WLAN equipment, such as better security, authentication, remote management, and tools to help integrate with existing networks. These access points have a larger coverage area than home or small office equipment, and are designed to work together to cover a much larger area. This equipment can adhere to the 802.11a, b, g, or n standard, or to security-refining standards, such as 802.1x and WPA2.

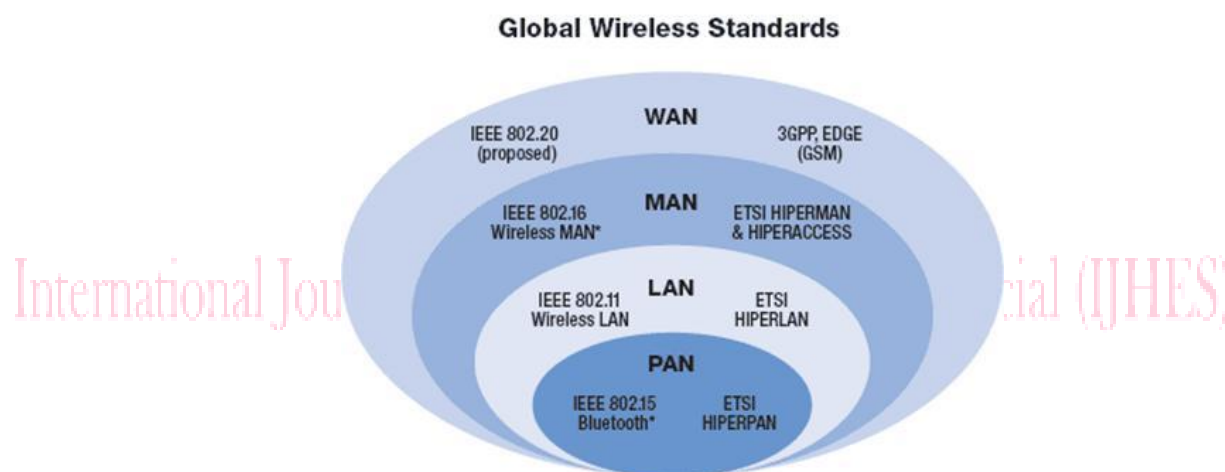


Figure 6 Global Wireless Standards

c) Storage Area Network (SAN)

A storage area network (SAN) is a type of local area network (LAN) is a high-speed special-purpose network. A SAN typically supports data storage, retrieval and replication on business networks using high-end servers, multiple disk arrays and Fibre Channel interconnection technology. Storage Area Networks (SANs) technology is similar but distinct from network attached storage (NAS) technology. While SANs traditionally employ low-level network protocols for transferring disk blocks, a NAS device typically works over TCP/IP and can be integrated fairly easily into home computer networks.

d) Campus Area Network (CAN)

A campus area networks (CANs) is a computer network interconnecting a few local area networks (LANs) within a university campus or corporate campus Network. Campus area network may link a variety of campus buildings. A campus area network is larger than a local



area network but smaller than a metropolitan area network (MAN) or wide area network (WAN). CAN can also stand for corporate area network.

e) Personal Area Network (PAN)

A personal area network is a computer network organized around an individual person. Personal area networks typically involve a mobile computer, Personal area networks can be constructed with cables or wirelessly. Personal area networks generally cover a Network range of less than 10 meters (about 30 feet). PAN (Personal Area Network) first was developed by Thomas Zimmerman and other researchers at M.I.T.'s Media Lab and later supported by IBM's Almaden research lab.

f) Wireless Personal Area Network (WPAN)

It is virtually a synonym since almost any personal area network would need to function wirelessly. Conceptually, the difference between a PAN (personal area network) and a wireless LAN (Local Area Network) is that the former tends to be centered around one person Network while the latter is a local area network (LAN) that is connected without wires Network and serving multiple users.

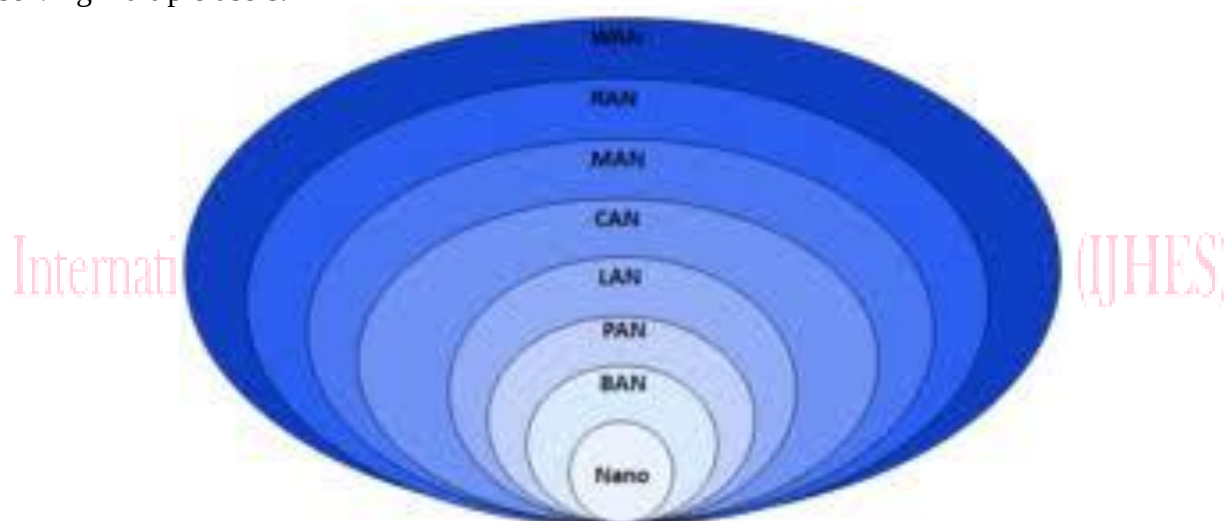


Figure 7 Types of various network generations

2. LITERATURE SURVEY

To arrive at well-defined plan and methods to carry out the study, the next step the researcher undertook was review of literature. Literature and review is one of the fundamental tasks of any researcher, it helps, guides the researcher.

[2] Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices, (Reed 2003). This review addresses how highly sophisticated intruders are penetrating internet networks despite high levels of security. As per study of Internet of Things



Wake-Up Call for Enterprises its —Organizations need to plan for the new generation of Internet-enabled devices that may be located anywhere in the world.

[3] According to Anil Lamba, 2016, forbes' report published in 2015, cloud-based security spending is expected to increase by 42%. According to another research, the IT security expenditure had increased to 79.1% by 2015, showing an increase of more than 10% each year. International Data Corporation (IDC) in 2011 showed that 74.6% of enterprise customers ranked security as a major challenge. This paper summarizes a number of peer -reviewed articles on security threats in cloud computing and the preventive methods. The objective of our research is to understand the cloud components, security issues, and risks, along with emerging solutions that may potentially mitigate the vulnerabilities in the cloud. It is a commonly accepted fact that since 2008, cloud is a viable hosting platform; however, the perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combatting threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting.

[6] Anil Lamba published one article in 2017, This research aims to investigate the current status and future direction of the use of information systems for supply chain management for companies with multicomponent production. Paper presents a qualitative research method for analyzing a supply chain processes and for identifying ways of its information support. Based on data collected from different enterprises, can be concluded that in order to identify the most effective strategies of information support of supply chain the attention should focus on the identification and management of the sources of uncertainties, risks and cyber security. To successfully integrate business processes between suppliers and customers, manufacturers must solve the complex problem of information security. The main practical results are: proposed a new approach to the identification and prediction of supply risk within uncertainties conditions; proposed a complex solution to secure data in information systems for supply chain management.

[7] Vehicular Network Security use for modern applications and threats can easily circumvent port-blocking firewalls, to render ineffective the usual cornerstones of enterprise network security. Most of the attempts to remedy such situations with cyber attacks are required to detect first and then it takes the preventive actions — helpers that bolt application awareness onto existing firewall products, or turn to Unified Threat management devices - have been unsuccessful. Enterprises can simplify their enterprise network security infrastructure with Palo Alto Networks' Next-Generation Firewall.

[8] Preventive and detective attacks, his paper concludes here it he believe that enterprise networks are different from the Internet at large and deserve special attention: Security is paramount, centralized control is the norm, and uniform, consistent policies are important. However, providing strong protection is difficult, and it requires some tradeoffs. There are clear advantages to having an open environment where connectivity is unconstrained and every end



host can talk to every other. Just as clearly, however, such openness is prone to attack by malicious users from inside or outside the network.

[9] 2016, In the past decade, technologies in vehicles have been rapidly advancing creating both a new type of “on the road” entertainment and safer environment while driving. Technologies such as anti-lock brake systems, steering assist, and in some cases autonomous driving, manufactures nearly eliminated the dangers of driving. To maintain the advances in safe technologies, it is vital to establish a strong security system for automotive networks and is crucial to advance the state of the art in automobile security. Motivated by this, one of the main goals of this research paper is to define a threat environment for CAR networks by discussing the existing security vulnerabilities and threats/attacks that an automobile network is currently facing. To address these security challenges, we also present a distributed firewall system to protect a CAR network from both internal and external networks.

[10] Evaluating and Strengthening Enterprise Network Security Using Attack Graphs by R.P. Lippmann, K.W. Ingols, C. Scott, K. Piwowarski, K.J. Kratkiewicz, M. Artz, R.K. Cunningham, its recommends that need to ENSASE. Assessing the security of large enterprise networks is complex and labor intensive. We present a new approach that uses configuration information on firewalls and vulnerability information on all network devices to build attack graphs that show how far inside and outside attackers can progress through a network by successively compromising exposed and vulnerable hosts.

[12] 2018, One of the key advantages of additive manufacturing (AM) is its digital thread, which allows for rapid communication, iteration, and sharing of a design model and its corresponding physical representation. While this enables a more efficient design process, it also presents opportunities for cyber-attacks to impact the physical world. In this paper the authors examine potential attack vectors along the Additive Manufacturing process chain. Specifically, the effects of cyber-physical attacks, and potential means for detecting them, are explored. Based on the results of this study, recommendations are presented for preventing and detecting cyber-physical attacks on AM processes.

[15] 2018, Cyber-secure, resilient energy is paramount to the prosperity of the United States. As the experience and sophistication of cyber adversaries grow, so too must the US power system’s defenses, situational awareness, and response and recovery strategies. Traditionally, power systems were operated with dedicated communication channels to large generators and utility-owned assets but network connectivity in today’s industrial entities, including electrical utilities, has exposed many digital communication and control aspects to the threat of cyber attacks. When forward looking improvements including smart grid, smart meters and other advancements are considered, security is of foremost concern. In fact, governments around the world have recognized the existing vulnerability and need to protect the grid infrastructure. To solve the problem, regulations and standards are being developed to ensure that the proper security steps are taken. In addition, cyber attackers have targeted crude oil and natural gas (O&G) companies with attacks growing in frequency, sophistication, and impact as the industry



employs ever more connected technology. But the industry's cyber maturity is relatively low, and O&G boards show generally limited strategic appreciation of cyber issues.

[16] Industry-centric benchmarking of information technology benefits, costs and risks for small-to-medium sized enterprises in construction by Peter E.D Love, Zahir Iranib & David J Edwardsc, its recommends that need to ENSASE. The evaluation of information technology (IT) is a perennial problem for businesses as they seek to improve their performance and sustain a competitive advantage. While businesses are increasing their expenditure on technology to keep abreast of competitors, organizations in the construction industry have become _technological laggards. As per paper based upon the reported findings a series of benchmark metrics for benefits, costs and risks of IT were propagated. These metrics can serve as a reference point for initiating benchmarking, which should form an integral component of the IT evaluation and learning process.

[17] Industrial Control System architecture (ICS) identifies the main components of the organization, its information systems, the ways in which these components work together in order to achieve defined business objectives, and the way in which the information systems support the business processes of the organization. The components include staff, business processes, technology, information, financial and other resources, etc. Enterprise architecting is the set of processes, tools, and structures necessary to implement an enterprise-wide coherent and consistent IT architecture for supporting the enterprise's business operations. It takes a holistic view of the enterprise's IT resources rather than an application-by-application view.

[18] 2017, Modern Supervisory Control and Data Acquisition (SCADA) systems are essential for monitoring and managing electric power generation, transmission and distribution. In the age of the Internet of Things, SCADA has evolved into big, complex and distributed systems that are prone to be conventional in addition to new threats. Many security methods can be applied to such systems, having in mind that high efficiency, real time intrusion identification and low overhead are required. Keywords: SCADA systems; Security, Anomaly based algorithm; Classification algorithms; Data communication; Denial of service attack; Intrusion detection; Cyber Security; Cloud Security; Network ; Cyber; Cyber Threats; Threat Analysis ; Information Security; Data security.

[19] Enterprise Local Area Networks (ELANs) have been expanding following an increase in the number of staff which necessitates establishment of new offices. However, reliability and security of services provided by ELANs need to be ensured at all times to meet expectations of users. As per his paper, the network security holes existing within the ELANs were investigated. Vulnerabilities and threats were critically examined in one of the ELANs. It was observed that known vulnerabilities were still around within the network. The suggestions will ensure stability of the network during scaling out as the number of staff continues to grow.

[20] The security and trustworthiness of enterprise networks have been a major concern in the research and practice of Intranet security. The security of endpoints and their network access are inevitably two important factors regarding enterprise network security. As per paper shown that present a novel architecture to enforce controls on endpoint application execution and network



access, in which the policy decision point (PDP) and policy enforcement point (PEP) are introduced. Security analysis and performance evaluation prove that the proposed architecture maintains a balance between security and flexibility of enterprise network control.

[21] 2015, Cloud computing is becoming increasingly fashionable in distributed computing environment. Processing and Data storage use cloud environment is becoming a movement universal. Software as a Service (SaaS) has on many business applications as well as in our day to day life, we can simply say that this disruptive technology. Cloud computing can be seen since Internet based computing, in which shared resources, software, and information are made available to devices on demand. It allows resources towards leveraged on per-use basis. It diminishes cost and complexity of service providers by means of assets and operational costs. It allows users to access applications tenuously. On behalf of user, this construct directs cloud service provider to feel software updates and cost of servers etc. For both, cloud providers and consumers; availability, integrity, authenticity, confidentiality, and privacy are important concern. Infrastructure as a Service (IaaS) serves as base layer for many other release models and Platform-as-a-Service (PaaS) clouds. Security of PaaS clouds is considered from multiple perspective including access control, service continuity and privacy while protecting together the service provider and the user. Security problems of PaaS clouds are explored and classified.



3. INFERENCES/FINDINGS

Sr. No.	Authors	Outcomes
[2]	Nicholas Arconati	The intruders increase, the network experts are deriving many techniques in preventing attackers from accessing company networks.
[3]	Lamba A.	The perception with respect to security in the cloud is that it needs significant improvements to realise higher rates of adaption in the enterprise scale. As identified by another research, many of the issues confronting the cloud computing need to be resolved urgently. The industry has made significant advances in combatting threats to cloud computing, but there is more to be done to achieve a level of maturity that currently exists with traditional/on-premise hosting.
[6]	Lamba A.	Proposed a new approach to the identification and prediction of supply risk within uncertainties conditions; proposed a complex solution to secure data in information systems for supply chain management.
[14]	Victor-Valeriu	Current security analysis tools typically examine only individual firewalls, routers, or hosts separately and do not comprehensively analyze overall network security.



[9]	Lamba A.	It is vital to establish a strong security system for automotive networks and is crucial to advance the state of the art in automobile security.
[19]	Vinod Yegneswaran, Paul Barford , Dave Plonka	Based on the findings, the paper suggests that all software used in the networking devices need to be updated; unneeded open ports need to be closed; cache servers and security policy need to be implemented.
[20]	Kaisler, S.H	A hybrid mechanism is proposed such that the control of application and network access of endpoints are integrated.
[21]	Lamba A.	It diminishes cost and complexity of service providers by means of assets and operational costs. It allows users to access applications tenuously

4. PROBLEMS FORMULATION

Several approaches for securing private P2P networks have been presented by researchers. Some of these ideas have been implemented and some implementations have been based on the developers own ideas. The most striking feature of all of these is their diversity. A small network may find a simple solution where peers connect directly to a centralized server favorable. A single peer may have the responsibility of approving new peers, distributing keys, and evicting abusers. Larger networks may favor a more distributed approach where peers are allowed, at their own discretion, to invite new peers they trust to the network. In other networks it may be some other form of relation, such as location or presence that allows users into the network, one such system. This diverse selection of systems and the diversity of peers using them offer and demands different aspects security. Before we are able to identify the complete scope of the problem, we must look at the different levels of security that may be implemented and desirable in such systems.

5. CONCLUSION

In this paper literature study can be concluded and how we help form computer network through in real education. Such networks help in Information technology security. For instance, it can be used for securing the higher education environment without disrupting the openness, accessibility, academic and intellectual freedom which is at the very heart of the higher education environment. It is one of the fundamental process towards the broader security because the further processing steps depends of what types of security breaches has been occurred and what strategies are in place to cope up with these. Despite the numerous functionality of security, IT security in Higher education is still a subject of on-going investment and it cannot be conclusively stated that education field is highly secured because of the application, technological and intrusion's diversity.



REFERENCES

- [1] Frederick M. Avolio by Best Practices in Network Security by Frederick M. Avolio March 20, 2000
- [2] Nicholas Arconati, 'One Approach to Enterprise Security Architecture-SANS Institute InfoSec Reading'.
- [3] Lamba, A., Singh, S., Dutta, N., Sai, S., & Muni, R. (2016). A COMPREHENSIVE SURVEY ON SECURITY IN CLOUD COMPUTING. In International Journal For Technological Research In Engineering ISSN. Retrieved from www.ijtre.com
- [4] Jeff Bertolucci, "Internet of Things Wake-Up Call For Enterprises", 2013,
- [5] According Jericho, Shaul Efraim, Vice President of products, "Marketing and Business Development at Tufin Technologies",
- [6] Lamba, A., Singh, S., Singh, B., Dutta, N., ... Islands, C. (2017). ANALYZING AND FIXING CYBER SECURITY THREATS FOR SUPPLY CHAIN MANAGEMENT. 4(5), 5678–5681.
- [7] Hulus onder, "A security management system design", July 2007, 99 pages
- [8] Plamen Nedeltchev, Principal Architect of IT, Borderless Networks, "The new opportunities of enterprise networking", 2010,
- [9] Lamba, A., Singh, S., Dutta, N., Sai, S., Islands, C. (2016). IDENTIFYING & MITIGATING CYBER SECURITY THREATS IN VEHICULAR TECHNOLOGIES. 3(7), 5703–5706.
- [10] Victor-Valeriu PATRICIU, Iustin PRIESCU and Sebastian NICOLAESCU, "Interdisciplinarity New Approaches and Perspectives in the Use of Quantitative Methods",
- [11] Homer, J. Kansas State Univ., Manhattan, KS ; Xinming Ou, "SAT-solving approaches to context-aware enterprise network security management",
- [12] Lamba, A., Singh, S., Singh, B., Dutta, N., Sai, S., & Muni, R. (2018). PREVENTING AND DETECTING CYBER ATTACKS (STL & AMF) ON ADDITIVE MANUFACTURING (AM) PROCESS CHAIN. 5(9), 5752–5759.
- [13] Shawon m. Rahman, "An overview of the security concerns in enterprise cloud computing".
- [14] Martin Casado, Tal Garfinkel, Aditya Akella, Michael J. Freedman Dan Boneh, Nick McKeown, Scott Shenker, "SANE: A Protection Architecture for Enterprise Networks",
- [15] Lamba A. (2018). RESEARCH ARTICLE PROTECTING " CYBERSECURITY & RESILIENCY " OF NATION ' S CRITICAL INFRASTRUCTURE- International Journal of Current Research, 10, (12), 76865-76876.
- [16] R.P. Lippmann, K.W. Ingols, C. Scott, K. Piwowarski, K.J. Kratkiewicz, M. Artz & R.K. Cunningham "Evaluating and Strengthening Enterprise Network Security Using Attack Graphs"
- [17] Scott A. Bernard, "An Introduction to Enterprise Architecture: Third Edition"



- [18] Anil Lamba, Satinderjeet Singh, Balvinder Singh, Natasha Dutta, & Sivakumar Sai Rela Muni. (2016). MITIGATING CYBER SECURITY THREATS OF INDUSTRIAL CONTROL SYSTEMS (SCADA & DCS). Retrieved from <http://arxiv.org/abs/1611.07722>.
- [19] On the Design and Use of Internet Sinks for Network Abuse Monitoring by Vinod Yegneswaran, Paul Barford, Dave Plonka, Volume 3224 of the series Lecture Notes in Computer Science pp 146-165
- [20] Lamba A. (2019). SR-MLC: Machine Learning Classifiers in Cyber Security-An Optimal Approach. In International Journal of Research in Informative Science Application & Techniques (IJRISAT) (Vol. 3). Retrieved from www.ijrisat.com.
- [21] Lamba,A 2015." A Study Paper on Security Related Issue before Adopting Cloud Computing Service Model", International Journal for Technological Research in Engineering, Volume 3 Issue 4, pp.5837-5840, 2347-4718.



International Journal of Health, Education and Social (IJHES)