ISSN 2277-3061

CLOUD COMPUTING SECURITY AND DATA PROTECTION: A REVIEW

Gurpreet Singh [1], Susmita Mishra[2]
[1] Research Scholar, Department of Electronics and Telecommunication, BMS College of Engineering, Punjab.
gurpreetjathol@gmail.com
[2] Assistant Professor, Department of Electronics and Telecommunication, BMS College of Engineering, Punjab.
susmita.mshr@gmail.com

ABSTRACT

Scientific computing in the 21st century has evolved from fixxed to distributed work environment. The current trend of Cloud Computing (CC) allows accessing business applications from anywhere just by connecting to the Internet. Evidence shows that, switching to CC organizations' annual expenditure and maintenance are being reduced to a greater extent. However, there are several challenges that come along with various benefits of cloud computing. Among these include security aspects. Our aim is to identify security challenges for adapting cloud computing and their solutions from real world for the challenge that do not have any proper mitigation strategies identified.This non-existence of global standards and guidelines could be help academics to know the state of practice and formulate better methods/standards to provide secure interoperability. The identified cloud computing security challenges and solutions, can be referred by practitioners to understand which areas of security need to be concentrated while adapting/migrating to a cloud computing environment.

Keywords

Cloud Computing, Cloud Security, Privacy, Challenges, Solutions, Cloud Zones, Grouping.

INTRODUCTION

Cloud Computing (CC)[1] is an emerging technology that has abstruse connection to Grid Computing (GC) paradigm and other relevant technologies such as utility computing, distributed computing and cluster computing. The aim of both GC and CC is to achieve resource virtualization. In spite of the aim being similar, GC and CC have significant differences. The main emphasis of GC is to achieve maximum computing, while that of CC is to optimize the overall computing capacity. CC also provides a way to handle wide range of organizational needs by providing dynamically scalable servers and application to work with. Leading CC service providers such as Amazon, IBM, `Dropbox', Apple's `iCloud',Google's applications, Microsoft's `Azure', etc., are able to attract normal users through out the world. CC have introduced a new paradigm, which helps its users to store or develop applications dynamically and access them from anywhere and anytime just by connecting to an application using Internet. Depending on customer's requirement CC provides easy and customizable services to access or work with cloud applications. Based on the user requirement CC can be used to provide platform for designing applications, infrastructure to store and work on company's data and also provide applications to do user's routine tasks. When a customer chooses to use cloud services, data stored in the local repositories will be sent to a remote data center. This data in remote locations can be accessed or managed with the help of services provided by cloud service providers. This makes clear that for a user to store or process a piece of data in cloud, he/she needs to transmit the data to a remote server over a channel (internet). This data processing and storage needs to be done with utmost care to avoid data breaches.

It is the model for convenient on-demand network access, with minimum management efforts for easy and fast network access to resources that are ready to use. It is an upcoming paradigm that offers tremendous advantages in economic aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power. Popularity of cloud computing is increasing day by day in distributed computing environment. There is a growing trend of using cloud environments for storage and data processing needs. To use the full potential of cloud computing, data is transferred, processed, retrieved and stored by external cloud providers. However, data owners are very skeptical to place their data outside their own control sphere.

BENFITS OF CLOUD COMPUTING

Some common benefits of cloud computing are:

• **Reduced Cost:** Since cloud technology is implemented incrementally (step-by-step), it saves organizations total expenditure.

• **Increased Storage:** When compared to private computer systems, huge amounts of data can be stored than usual.

• **Flexibility:** Compared to traditional computing methods, cloud computing allows an entire organizational segment or portion of it to be outsourced.

• **Greater mobility**: Accessing information, whenever and wherever needed unlike traditional systems (storing data in personal computers and accessing only when near it).

• **Shift of IT focus:** Organizations can focus on innovation (i.e., implementing new products strategies in organization) rather than worrying about maintenance issues such as software updates or computing issues. These benefits of cloud computing draw lot of attention from Information and Technology Community (ITC). A survey by ITC in the year 2008, 2009 shows that many companies and individuals are noticing that CC is proving to be helpful when compared to traditional computing methods.

CLOUD COMPUTING: SERVICE MODELS

Cloud computing can be accessed through a set of services models. These services are designed to exhibit certain characteristics and to satisfy the organizational requirements. From this, a best suited service can be selected and customized for an organization's use. Some of the common distinctions in cloud computing services are Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), Infrastructureas-a-Service (IaaS), Hardware-as-a-Service (HaaS) and Data storage-as-a-Service (DaaS). Service model details are as follows:

• **Software as a Service (SaaS)[4]**: The service provider in this context provides capability to use one or more applications running on a cloud infrastructure. These applications can be accessed from various thin client interfaces such as web browsers. A user for this service need not maintain, manage or control the underlying cloud infrastructure (i.e. network, operating systems, storage etc.). Examples for SaaS cloud's are Salesforce, NetSuite.

• **Platform as a Service (PaaS)[5]**: The service provider in this context provides user resources to deploy onto cloud infrastructure, supported applications that are designed or acquired by user. A user using this service has control over deployed applications and application hosting environment, but has no control over infrastructure such as network, storage, servers, operating systems etc. Examples for PaaS cloud's are Google App Engine, Microsoft Azure, Heroku.

• **Infrastructure as a Service (IaaS)**: The consumer is provided with power to control process, manage storage, network and other fundamental computing resources which are helpful to manage arbitrary software and this can include operating system and applications. By using this kind of service, user has control over operating system, storage, deployed applications and possible limited control over selected networking components. Examples for IaaS cloud's are Eucalyptus (The Eucalyptus Opensource Cloud-computing System), Amazon EC2, Rackspace, Nimbus.

CLOUD COMPUTING: DEPLOYMENT MODELS

Among the service models explained above, SaaS, PaaS and IaaS are popular among providers and users. These services can be deployed on one or more deployment models such as, public cloud, private cloud, community cloud and hybrid cloud to use features of cloud computing. Each of these deployment models are explained as follows:

• **Public cloud:** This type of infrastructure is made available to large industrial groups or public. These are maintained and owned by organization selling cloud services.

• **Private cloud:** This type of cloud deployment is just kept accessible to the organization that designs it. Private clouds can be managed by third party or the organization itself. In this scenario, cloud servers may or may not exist in the same place where the organization is located.

• **Hybrid cloud:** With in this deployment model there can be two or more clouds like private, public or a community. These constituting clouds (combinations of clouds used, such as `private and public', `public and community', etc.) remain different but yet bound together by standardized or preparatory technology that enables application and data portability.

• **Community cloud:** This type of cloud infrastructure is shared by several organizations and supports a specific community with shared concerns. This can be managed by an organization or third party and can be deployed off or in the organizational premise.

Usage of deployments models and services modeled provided by CC changes how systems are connected and work is done in an organization. It adds up dynamically expandable nature to the applications, platforms, infrastructure or any other resource that is ordered and used in CC.

IMPORTANCE OF SECURITY IN CLOUD COMPUTING

The power, exibility and ease of use of CC comes with lot of security challenges. Even though CC is a new intuitive way to access applications and make work simple, there are a number of challenges/issues that can effect its adoption. A non-exhaustive search in this field reveals some issues. They are: Service Level Agreements (SLA), what to migrate, security, etc. Cloud Computing has a feature of automatic updates, which means a single change by an administrator to an application would reect on all its users. This advertently also leads to the conclusion that any faults in the software are visible to a large number of users immediately, which is a major risk for any organization with little security.

It is also agreed up on by many researchers that security is a huge concern for adoption of cloud computing. A survey by IDC on 263 executives also shows that security is ranked first among challenges in CC. Even though a company boasts to have top class security and does not update its security policies from time to time, it will be prone to security breaches in near future.

SECURITY CONCERNS IN CLOUD COMPUTING

a. Users authentication: User authentication process must be improvised to ensure that malicious users do not get access to powerful computing systems in cloud computing.

b. Leakage of data or Data loss: Data can be at risk if an unauthorized person gains access to shared pool of resources and deletes or modifies data. This risk can increase further if there exists no backup for that data.

c. Clients trust: There must be strong authentication practices implemented to ensure that the clients data is being protected from unauthorized access.

d. Malicious users handling: Malicious users can be attackers using cloud services with a malicious intent or an insider who has gained the trust of company but works to gain access to sensitive information stored in cloud [1].

e. Hijacking of sessions: These kind of attacks happen when a legitimate user is prone to phishing or insecure application interfaces that can be exploited by attackers. Through this kind of attacks, attackers gain user credentials and hijack legitimate users sessions [3].

f. Wrong usage of CC and its services: Cloud computing service providers give access to try their cloud services for a limited period of time for free. Some users utilize this trial period to misuse the resources obtained through CC service provider [2].

Himeldev, Tanmoysen [12] has proposed the concept of privacy of the cloud data from data mining and attacks on the cloud data. We first identify the data mining based privacy risks on cloud data and propose a distributed architecture to eliminate the risks. Cloud data distributor is an entity that receives data from single client, where data is partitioned into multiple parts. These parts are distributed among several cloud providing companies.

Vishal Jain and Mahesh Kumar[13] develops a practically implemented research model for the information retrieval using Multi-Agent System with Data Mining technique in a Cloud Computing environment. The paper will undertake a Cloud computing is a model for enabling service user’s ubiquitous, convenient and on-demand network access to a shared pool of configurable comput ing resources (e.g., networks, servers, storage, applications, and services), that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing enables cloud services. The security architecture and functions highly depend on the reference architecture.

Alawode A. olaide [11] has proposed the concept of securityin the cloud. This paper discusses effort directed to which degree this skepticism is justified, by proposing to model Cloud Computing Confidentiality Archetype and Data Mining 3CADM. The 3CADM [10] is a step-by-step framework that creates mapping from data sensitivity onto the most suitable cloud computing architecture and process very large datasets over commodity clusters with the use of right programming model. To achieve this, the 3CADM determines the security mechanisms required for each data sensitivity level, which of these security controls may not be supported in certain computing environments, which solutions can be used to cope with the identified security limitations of cloud Computing.

Neha Tirthani [14] has contemplated a design for cloud architecture which ensures secured movement of data at client and server end. We have used the non breakability of Elliptic curve cryptography for data encryption and Diffie Hellman Key Exchange mechanism for connection establishment. The proposed encryption mechanism uses the combination of linear and elliptical cryptography methods. It has three security checkpoints: authentication, key generation and encryption of data.

Amar Gondaliya [15] identifies security concerns arising in cloud computing environments and outlines methods to maintain compliance integrity and preserve security protection as virtual resources move from on-premise to public cloud environments. Many organizations that are providing security software that provides security control for cloud computing, but this paper provides the checklist of key questions for enterprise and service provider for cloud computing deployment.

R. Kalaichelvi Chandrahasan [17] specifies Cloud computing is a promising computing standard where computing resources in large data center are made available as services over Internet. Cloud computing has become prominent IT by offering the businessenvironment data storage capacity. This new profitable paradigm for computing is an attractive, massive, largescale investment that includes any subscription-based or pay-per-use service over the Internet. It is on-demand access to virtualized IT services and products.

Anthony Bisong [16] discussed security risks and concerns in cloud computing and enlightened steps that an enterprise can take to reduce security risks and protect their resources. We have also explained cloud computing strengths/benefits, weaknesses, and applicable areas in information risk management.

MANDEEP KAUR [19] specifies Cloud computing is the internet based development and used in computer technology. The prevalent problemassociated with cloud computing is data privacy,security, anonymity and reliability etc. But the most important between them is security and how cloudprovider assures it. In this research paper, the proposedwork plan is to eliminate the concerns regarding dataprivacy using encryption algorithms to enhance thesecurity in cloud as per different perspective of cloudcustomers.

Mr.Tejas P.Bhatt [20] concern is to provide the security to end user to protect files or datafrom unauthorized user. Difference is that the research isdone in cloud, but security related issue can’t be resolved yet.Security is the main intention of any technology throughwhich unauthorized intruder can't access your file or data incloud. Thus, we can give maximum effort to avoid the issuesof security occurs. We have designed one proposed designand architecture that can help to encrypt the file and decrypt it. In this research paper, we have used the AES Algorithm for the encryption.

Eng. Anwar J. Alzaid and Eng. Jassim M. Albazzaz [21] has proposed the concept of cloud computing in detail. Cloud computing is a relatively new term, it refers to a new way of processing and storing information this new style of processing promises to offer a huge amount of computing power to its users without requiring them to invest in expensive hardware.

Vahid Ashktorab [18] has cast light over the major security threats of cloud computing systems, while introducing the most suitable countermeasures for them. He also cited the aspect to be focused on when talking about cloud security. He has categorized these threats according to different viewpoints, providing a useful and little-known list of threats. After that some effective countermeasures are listed and explained.

A. Raja Rajeswari and R.Sakkaravarthi [22] has proposed the concept of data based privacy attacks in the cloud. As an alternative of maintaining personal data on the own hard drive or updating important applications for user needs, user can use a service over the network, to a different location, to store user information and / or use its applications. This also provides flexibility so it is very useful in a new generation of services and products. One of the main security[6] problems in cloud is data mining based privacy attacks that involve analyzing data over a long period to extract valuable information. It gives the outside attackers and providers having unconstitutional access to the cloud and a prospect of analyze the client information over an extensive period of time to extract the sensitive information that causes privacy violation of clients.

T.V. Mahendra [23] discussed an algorithm to mine the data from the cloud using sector/sphere framework with association rules. Data mining is the process of analyzing data from different perspectives and summarizing it into useful information. Mining association rules is one of the most important aspects in data mining. Association rules are dependency rules which predict occurrence of an item based on occurrences of other items. Apriori is the best-known algorithm to mine association rules.

Bhagyashree Ambulkar[24] has specified mining applications can derive much demographic information concerning customers that was previously not known or hidden in the data. By and large, data mining systems that have been developed to data for clusters, distributed clusters and grids have assumed that the processors are the scarce resource, and hence shared. When processors become available, the data is moved to the processors.

Eng. Anwar J. Alzaid[25] has discussed the concepts, definitions , architecture and outline of the cloud environment.

A.Raja Rajeswari [26] has identified the data mining based privacy risks on cloud data and propose a distributed architecture to remove the privacy risks.This also provides flexibility so it is very useful in a new generation of services and products. One of the main security problems in cloud is data mining based privacy attacks that involve analyzing data over a long period to extract valuable information. It gives the outside attackers and providers having unconstitutional access to the cloud and a prospect of analyze the client information over a extensive period of time to extract the sensitive information that causes privacy violation of clients. This is a big problem in many clients of cloud.

Cloud computing[4] involves distributed computing over a network, where a program or application may run on many connected computers at the same time. The cloud makes it possible for you to access your information from anywhere at any time. While a traditional computer setup requires you to be in the same location as your data storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data.

MOTIVATION FOR RESEARCH

As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through the adoption of this new model. The effectiveness and efficiency of traditional protection mechanisms are being reconsidered as the characteristics of this innovative deployment model differ widely from those of traditional architecture [6] as more and more information on individuals and companies is placed in the cloud, concerns are beginning to grow about just how safe an environment it is.

Cloud based systems saves data off multiple organizations on shared hardware systems. Data segregation is done by encrypting data of users, but encryption is not complete solution. We can do segregate data by creating virtual partitions of data for saving and allowing user to access data in his partition only. Malicious activity monitoring is a tough task in cloud system as logging data might be spread over multiple hosts and data centres. Restricting user to his own virtual partition only will not allow logs to be dispersed allowing access to logs for monitoring easily.

User access is another major concern in restricting user access is a major challenge in cloud based storage system. Use of virtual partition and enhanced user access control in cloud system will allow us to improve data security.

Enhanced Cloud system will be compared with existing secure cloud systems. We will compare enhanced system against security, performance & ease of use.

Three cloud service models (SaaS, PaaS and IaaS) not only provide different types of services to end users but also disclose information security issues and risks of cloud computing systems [9].

- The hackers might abuse the forceful computing capability provided by clouds by conducting illegal activities. IaaS is located in the bottom layer, which directly provides the most powerful functionality of an entire cloud.

- Data loss is an important security risk of cloud models. In SaaS cloud models, companies use applications to process business data and store customer's data in the data centers.

- Traditional network attack strategies can be applied to harass three layers of cloud systems. For example, web browser attacks are used to exploit the authentication, authorization, and accounting vulnerabilities of cloud systems.

OBJECTIVES

Various data analysis techniques are available now a day that are successfully extract valuable information from a large volume of data. These analysis techniques are being used by cloud service providers. Attackers can use these techniques to extract valuable information from the cloud.

By distributing data on different clouds it introduces performance overhead when client needs to access all data frequently, e.g. client needs to perform a global data analysis on all data. The analysis may have to access data from multiple locations, with a degraded performance. By simply using in single cloud provider can having the following main issues: Less Security. Loss of data; No privacy; Cost of maintenance is high.

Uploading data on distributed cloud providers: - Although this scenario will protect the client's data as the data will be distributed to the different cloud providers. But it will increase the cost to the client as purchasing different cloud will increase the cost. But using only single cloud also has the issues. So by using single cloud and then dividing the single cloud into multiple zones overcomes the problem of cost and privacy.

Here, user will create his/her own account at the cloud Provider. Cloud Provider will assign the different privileges to the user depending upon the role of the user. Different access policies for different zones will be implemented over here. If the user has been assigned a role as a Read, then he/she can only read the data from the server. If the policy allows writing the data, then only user can write the data into the server. The file sent by the user is stored into the multiple zones available at the server. If the company tries to perform the mining at the user's data, then proper results will not be available.

RESEARCH METHODOLOGY

To enhance the security in cloud systems by creating user access policies:-

- We will be enhancing the security by using single cloud provider and dividing single cloud into different zones thereby saving a cost of the client and also enhancing the security.

- We will segregate data by creating virtual partitions of data for saving and allowing user to access data in his partitions only. Each user will have the rights according to the role of the client i.e. role based access policies.

- Use of virtual partitions and enhanced user access control in cloud system will improve data privacy and thereby fixing the threats in data mining to personal / private data in the cloud systems.

- Cloud is divided into multiple zones.

- The zones chosen by the user are grouped together and the data of the user is stored inside the grouped zone.

User will create his/her own account at the cloud Provider.

- Cloud Provider will assign the different privileges to the user depending upon the role of the user.

- Different access policies for different zones will be implemented over here.

- If the user has been assigned a role as a Read, then he/she can only read the data from the server.

- If the policy allows writing the data, then only user can write the data into the server.

- If the company tries to perform the mining at the user’s data, then proper results will not be available.

The file is sent by the user is stored into multiple zones available at the server.

CLOUD SIM

Cloud service providers charge users depending upon the space or service provided. In R&D [16], it is not always possible to have the actual cloud infrastructure for performing experiments. For any research scholar, academician or scientist, it is not feasible to hire cloud services every time and then execute their algorithms or implementations. For the purpose of research, development and testing, open source libraries are available, which give the feel of cloud services. Nowadays, in the research market, cloud simulators are widely used by research scholars and practitioners, without the need to pay any amount to a cloud service provider.

Tasks performed by cloud simulators :

The following tasks can be performed with the help of cloud simulators:

- Modelling and simulation of large scale cloud computing data centres.
- Modelling and simulation of virtualised server hosts, with customisable policies for provisioning host resources to VMs.
- Modelling and simulation of energy-aware computational resources.
- Modelling and simulation of data centre [18] network topologies and message-passing applications.
- Modelling and simulation of federated clouds.
- Dynamic insertion of simulation elements, stopping and resuming simulation.
- User-defned policies for allocation of hosts to VMs, and policies for allotting host resources to VMs.

The scope and features of cloud simulations include:

- Data centres
- Load balancing
- Creation and execution of cloudlets
- Resource provisioning
- Scheduling of tasks
- Storage and cost factors

CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks, as well as the destruction of infrastructure and services. There is no doubt that the cloud computing is the development trend in the future. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues and so on. But to solving the existing issues becomes utmost urgency. To protect against the compromise of the compliance integrity and security of their applications and data, firewall, Intrusion detection and prevention, integrity monitoring, log inspection, and malware protection. Proactive enterprises and service providers should apply this protection on their cloud infrastructure, to achieve security so that they could take advantage of cloud computing ahead of thei r competitors. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. To advance cloud computing, the community must take proactive measures to ensure security.

REFERENCES

[1] Bhagyashree Ambulkar and Vaishali Borkar,“Data Security in Cloud Computing”, MPGI National Multi Conference 2012 (MPGINMC-2012), 7-8 April 2012.

[2] Peter Mell, and Timothy Grance,“The NIST Definition of Cloud Computing”, the National Institute of Standards and Technology, USA, 2011.

[3] ORACLE, “Cloud Security Techniques and Algorithms”

[4] M.Kantardzic, “Data Mining: Concepts, Models, Methods and Algorithms”, John Wiley & Sons Inc., 2002.

[5] “Introduction to Cloud Computing Architecture”, Sun Microsystems, 2009.

[6] “Top 10 Algorithms in Data Security”, Springer-Verlag London Ltd., 2007.

[7] Jianzong Wang,Zhuo Liu, Peng Wang,”Data Mining of Mass Storage Based on Cloud Computing”.

[8] M. Bramer. “Principles of Data Security”. Springer, 2007.

[9] M. Brantner, D. Florescu, D. A. Graf, D. Kossmann, and T. Kraska. “Building a database on s3. In J. T.-L. Wang”, editor, ACM, pages 251–264, 2008.

[10] S. H. Brown. “Multiple linear regression analysis: A matrix approach with matlab”. Alabama Journal of Mathematics, 2009.

[11] Alawode A. olaide, “On Modeling Confidentiality Archetype and Data Mining in Cloud Computing”, IEEE, African Journal of Computing and ICT, March 2013.

[12] Himeldev, Tanmoysen, “An Approach to Protect the Privacy of Cloud Data from Data Mining Based Attacks”, IEEE.

[13] Vishal Jain, “Information Retrieval through Multi-Agent System with Data Mining in Cloud Computing”, IJCTA, January 2012.

[14] Neha Tirthani: “Hellman and elliptical curve cryptography, Proceedings of TCC”, volume 3378 of LNCS, pages 325-341. Springer-Verlag (2005)

[15] Amar Gondaliya : “Security in Cloud Computing”, Technical Paper Contest 2011.

[16] Anthony Bisong, “An Overview of the Security Concerns in enterprise Cloud computing”, International Journal of the Security Concerns in Enterprise Cloud Computing, 2011.

[17] R. Kalaichelvi Chandrahasan, “Research Challenges and Security Issues in Cloud Computing”, International Journal of Computational Intelligence and Information Security, March 2012 Vol. 3, No. 3.

[18] Vahid Ashktorab, “Security Threats and Countermeasures in Cloud Computing”, International Journal of Application or Innovation in Engineering and Management, Vol 1, Issue 2, October 2012.

[19] Mandeep Kaur, “Using encryption algorithms to enhance the data security in Cloud computing”, International journal of communication and computer technologies, Vol 1, No 12, 2013.

[20] Mr. Tejas P. Bhatt, “Security in Cloud Computing using File Encryption”, International Journal of Engineering Research and Technology , Vol. 1 Issue 9, November 2012.

[21] Eng. Anwar J. Alzaid and Eng. Jassim M. Albazzaz, ”Cloud Computing Challenges and related Security Issues”, 2009 A sur vey Paper http://www.cse.wustl.edu/~jain/cse571- 09/ftp/cloud/index.html

[22] A. Raja Rajeswari and R.Sakkaravarthi , “Top Threats to Cloud Computing V1.0” , March 2010

[23] T.V. Mahendra, “Data Mining for High Performance Data Cloud using Association Rule Mining”, International Journal of Advanced Research in Computer Science and Software Engineering, January 2012.

[24]. Bhagyashree Ambulkar, “Data Mining in Cloud Computing”, MPGI National Multi Conference 2012.

[25] Eng. Anwar J. Alzaid, “Cloud Computing : An Overview”, International Journal of Advanced Research in Computer and Communication Engineering, September 2013.

[26] A.Raja Rajeswari, “Mitigating Data Mining Attack in Cloud”, International Journal of Innovative Research in Computer and Communication Engineering, April 2014.

Er. Gurpreet singh is currently pursuing his M.Tech in Micro Electronics from BMS College of Engineering, Sri, Mukatsar Sahib, Punjab and has received his B.Tech degree in Electonics and communication from GGSCMT kharar, Mohali, Punjab.

Er. Susmita Mishra, received her B.Tech. degree in Electonics and Telecommunication from Orissa engineering College, bhubaneswar, Under Biju patnaik University of Technology, Rourkela, Odisha in 2009, the M.Tech. degree in VLSI and embedded system design from Synergy institute of engineering and technology, Dhenkanal, Under Biju patnaik University of Technology, Rourkela, Odisha, in 2011, She was a lecturer with Department of Electonics and Telecommunication, Govt College of Engineeing Kaladandi, Odisha, in 2010 . She was an assistant professor, with Department of Electonics and Telecommunication , synegy institute of engineering and technology,dhenkanal, odisha in 2011 She was an assistant professor, with Department of Electonics and Telecommunication,lovly professional university in 2012. And Currently, She is working as an assistant professor, with Department of Electonics and Telecommunication, Bhai Maha Singh College of engineering, Sri Muktsar Sahib, Punjab.