# Information Security Educational case study on the advanced network infrastructure security and technical aspects for large scale international organization

Chetan Sharma, 110893


Master's Thesis
Master of Science in Information Security
30 ECTS
Department of Computer Science and Media Technology
Gjøvik University College, 2013

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

# Information Security Educational case study on the advanced network infrastructure security and technical aspects for large scale international organization

Chetan Sharma, 110893

2013/11/27

# Abstract

Modern Organizations are highly depending on its network. It is because the communication process in the enterprises is impossible without a network. Networking and network security are the advanced terms for the modern enterprises. This thesis is related to describe advanced network related concepts for information security. This thesis work is a case study for the future students so that they can learn about the advanced networking and the importance of network security in the IT organizations. In the thesis work, the author described a multi subsidiary and international organization named CKTECK with the collaboration of a peer student. After that as an individual thesis work the author has concentrated mainly on the Technical concepts such as the CKTECK's whole Network Infrastructure design & plan which contained overall network infrastructure description, basic network security policy, network security related risk analysis, some tasks on risk analysis for network security in BYOD, Cloud , Social Media, some tasks related to network security policy and some list of potential projects on advanced networking concepts and so on. The author has concentrated on some challenges during the whole research which are:(1) To deliver overall network infrastructure plan, physical facilities and an overall concept (all discipline: authentication, accounting, authorization, encryption, physical security and backup procedures, disaster recovery planning, business continuity management, application security, web and email security, hot swap over to second site etc.) (2)To define Basic Network security Policy for CKTECK .(3)To process network related risk assessment for the network of CKTECK, tasks description and solutions of some tasks has been developed from the author side for the CKTECK. (4)To find the challenges and define what future students can learn with CKTECK? (5) Development of some solutions in some cases to hand out to the students.

For finding the solutions to these challenges, the author has used original research papers, white papers produced by experts, Organizational material produced for public used. Additionally, the interviews with experts helped the author a lot for the fulfillment of his goals.

# Acknowledgements

First of all, I am highly thankful to Professor Dr. Bernhard Hammerli, my supervisor. During the tough period of my master research, he always supported and motivated me. He gave me his precious time and guided me by showing a right path. It was impossible for me to complete this thesis work without him and his directions. I am feeling myself lucky to have a supervisor like him. He helped me with necessary documents whenever needed by me.

Moreover I also appreciate my colleague Ms. Khushbir Kaur Sharma, for the collaboration during the thesis work in defining an Organization. After that I am really thankful to my family who were always there for motivation. They every time supported me with full of motivations.

I am heartily thankful to Ms Jatinder Preet Kaur (Head of network security at Verizon , India) and Mr. Satish Das(CSO at Cognizant, India), who provided me valuable information by answering the interview questions. Software Developer at Nordea AS, Norway and Technical Support Engineer at Gallagher Group Ltd, New Zealand also provided information to the author to some extent by interviews. The author is also thankful to them.

I am glad that after completing this master thesis i will be able to complete my master degree in MIS, (Management) at HIG.

Thanks God for all
By Chetan Sharma

# Contents

# List of Figures

# List of Tables

# 1 Introduction

This thesis is initially combined with a peer student Khushbir Kaur Sharma in describing an international corporation named CKTECK. The combined jobs of Khushbir Kaur Sharma and the author of this thesis is to create history, to write job descriptions, to describe service areas, to describe products, to make organization's chart, to define 10 subsidiaries on different locations etc. After that this thesis is an individual job for the author of this thesis. The author is responsible for creating and describing overall network infrastructure of the CKTECK, for finding the advanced risks(BYOD, Cloud and Social media) in CKTECK's network infrastructure, for finding countermeasures to the risks, for describing basic network policy for CKTECK. Moreover to define task descriptions for the future students is also be a part of the research work.

This thesis will act as a case study for the future students on the networking related advanced concepts in modern network infrastructure of an international organization CKTECK. Networking concepts in any enterprise were common from previous time. But in now a these days, there are advanced networking schemes and concepts have been emerged in the enterprises. With the enhancement and advancement, new network security related problems have been come into place also. Several network securities related new and advanced threats have been introduced in the modern organizations. These are very harmful for the overall organization. It can harm the entire network of organization and can fail the overall working of the network system in any enterprise. The network has been changed from simple LAN, MAN, WAN to wireless LAN, Wireless MAN, Wireless WAN. Networking has been changed from wired to wireless. Everybody prefers wireless, smart, light weight technologies instead of Desktops. It is due to the drastic change in new technologies in the modern society. For instance smart phones have changed the way of doing job. Everybody wants to be connected always on these smart phones by using 3G, 4G technologies or by wireless networks. That has emerged BYOD networking in enterprises. With the emergence of BYOD, the usage of social networking has also been raised. Cloud computing networking has also been emerged as an advanced networking style in the organizations. Hence the BYOD, Cloud and Social media networking are the main trends in these days.

## 1.1 Topic Covered By The Project

This thesis work covers the topic of "Information Security Education case study on the advance network infrastructure and technical aspects for large scale international organization". Network security itself is part of information security. It is very important to have knowledge of new networking schemes and how to secure them. Network security is considered very important because of advanced and new network threats and risks in the modern society. New technologies

are smart as well as these are more risky. There are several problems in these technologies as technical aspect of view also. In the thesis work the author concentrates on to show the advanced problems in network graph of modern CKTECK. CKTECK is advanced and multi subsidiary enterprise with advanced networking frameworks. The author shows network security threats and countermeasures, CKTECK network policy etc. For future students author has made some tasks and will describe it with some solutions so that future students can take these tasks as a challenging job and can find creative solution on it. In overall the thesis is a case study framework on latest networking and technical aspects of network information security

## 1.2 Keywords

Network Infrastructure, network Security, Network security Risks, Corporation CKTECK, Information Security, Cloud Network, BYOD, Networking, Social Media Networking

## 1.3 Problem Description

In today's world, Society has become modern due to the use of several new and smart technologies. For instance, organizations are adapting several new technologies e.g. BYOD (Bringing your own device) at work, use of social networking, and use of modern cloud. The thesis work is based on the research under these technologies and some other related technological terms. In SOCOTEC AG, the case study from 2005, the company was national without subsidiaries. Furthermore, the threat and technology landscape has completely shifted. The challenge is to define multi country – multi subsidiary infrastructure allowing integrating new challenges for the development of innovative solutions and countermeasures of upcoming and/or advanced security threats related to network security of the overall organization. The CKTECK's network infrastructure, shown by the author in this thesis work, allows securing existing environment as well as integrates new technology with new network security challenges.

## 1.4 Choice Of Methods

The choice of methods behind this overall research is to use both qualitative and quantitative research techniques. For making a case study and an educational document for the future students, the author followed these methodologies. For making an educational tool it is very important to know that what is happening in the current time. What has happened in the past and what could be there in the future? .The methodology should cover all research questions and the author has tried his best to do this. The goal for the author was to make an educational platform on advance network security concepts in advance cloud, BYOD and social networking for the future students. In overall, the author has collected information from the literature study, scientific papers, white papers by organizations and the interviews sessions. The overall methodology is based on the two phases:

1. During the first phase of the research, the author collected and gathered the material from literature study and quantitative research.
2. In the second phase the qualitative research methodology was followed. In this the author conducted the interviews with several experts who are working in the modern IT organizations. The designations and organization names were Network Security Head at Verizon Communications India, CSO at Cognizant India, Software Developer at Nordea AS, Norway and Technical Support Engineer at Gallagher Ltd New Zealand. These interviews were taken for the purpose of finding several network security mechanisms and countermeasures for the network related risks. Moreover it gave the author a real research in the organizations. This can be very beneficial for the future students and they can learn what actually is done in the organizations. The author has also some basic experience in networking concepts as he already worked as Technical Support Engineer in TBSS(Tata Business Support Services, Chandigarh, India). There were some several sub parts for the overall research also.The overall process with two phases and its seven sub parts have been shown in Figure 1.

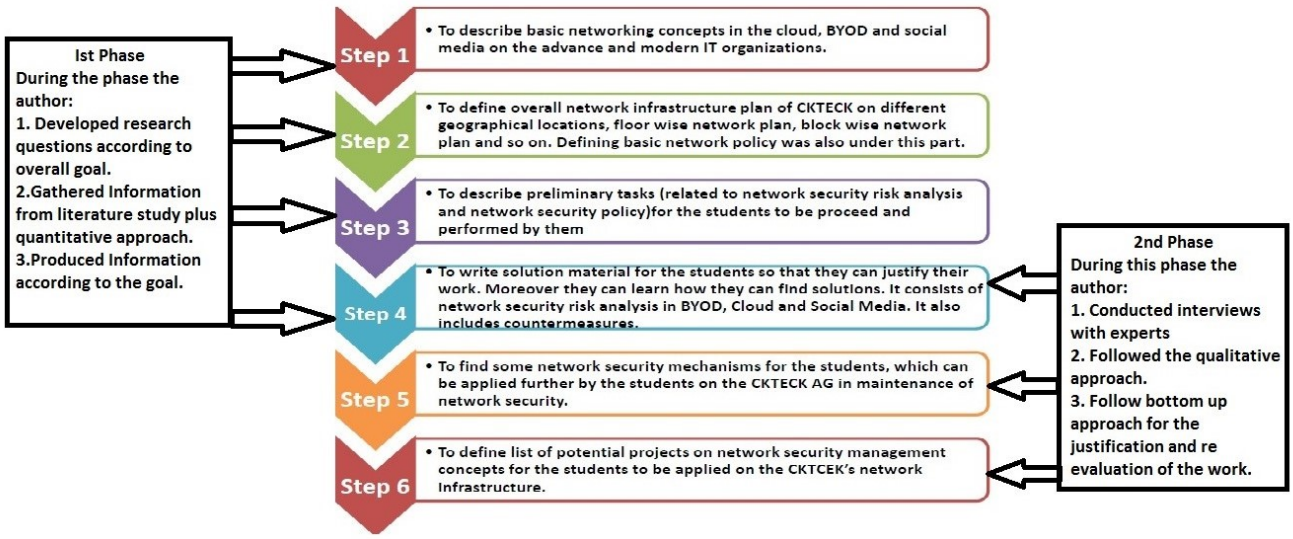


Figure 1: Choice of methods & Overall Methodology behind the research

The overall work was divided by the author into further parts.

1. ***To describe basic networking concepts in the cloud,BYOD and social media on the advance and modern IT organizations:*** It was done by following the quantitative research. It covered sources from the literature, organizational documents, original scientific papers etc. By using

such technique we found important information related to BYOD, Cloud and Social media networking concepts which will show the concept of advancement in the networking field in Modern IT organizations.

2. ***To define overall network infrastructure plan of CKTECK on different geographical locations, floor wise network plan, block wise network plan and so on. Defining basic network policy was also under this part:***It was done by applying the both qualitative and quantitative methods which includes the literature, organizational material on advance networking, interviews answers and some previous experience of author used in this. The author created a case study as a qualitative research method. Following this approach we knew how how develop overall network infrastructure for MNC and multi subsidiary organization. Moreover while using quantitative approach we found several material related to advance network from research papers and all.
3. ***To describe preliminary tasks (related to network security risk analysis and network security policy)for the students to be proceed and performed by them:*** It was done by both qualitative and quantitative approaches and some assumptions by the author. Some ideas were taken from interview answers and the literature. Assumptions and creativity of author was used for making those a different shape as tasks for students
4. ***To write solution material for the students so that they can justify their work:*** Moreover they can learn how they can find solutions. It consists of network security risk analysis in BYOD, Cloud and Social Media. It also includes countermeasures.It is also done by applying the mixture of qualitative and quantitative research. From interviews by experts author gor a lot of knowledge that how to protect network from its advance problems. Some solutions were also there in literature research
5. ***To find some network security mechanisms for the students, which can be applied further by the students on the CKTECK AG in maintenance of network security***It is also done by applying the mixture of qualitative and quantitative research. Experts helped the author a lot by giving recent example related to advanced network security mechanisms. Literature helped author some pre defined network security related mechanisms also.
6. ***To define list of potential projects on network security management concepts for the students to be applied on the CKTCEK's network infrastructure:*** It is done by applying the mixture of qualitative and quantitative research plus the assumptions by the author's point of view. Ideas were taken by studying the literature plus experts views. But the tasks are described by authors views and creativity.

These several subparts for the whole research work is based on two phases of the research period. These subtasks were considered very important for the author to make an effective educational tool with some basic tasks, some solutions for basic tasks, further advance tasks and then some hints for the solutions on it.

The overall methodology with its sub parts covers all the research questions. In the end, with the help of both quantitative research and qualitative research, the author got the output of the whole document as an educational tool for the students on advanced networking related concepts. The author's own experience was also useful for him in some cases. In author tried to gain the better results and outputs from these overall methods. Hence as a conclusion for this methodology, the author have used both qualitative and quantitative approaches for the evaluation of this overall project work.

## 1.5 Justification, Motivation And Benefits

As from the new networking frameworks like cloud networking framework, BYOD and Social media networking concepts, the demands for the more network security, have been taken place. It is very important for the future students so that they can learn about new networking trends by doing. Learning by doing is the best method of understanding any concept. Therefore when the case studies and some tasks related to it are given to the students as an challenge, then the students accept it as an challenge and go into deep for sort out the solutions. Hence students try to become more creative for solving tasks. It is the best method to teach them something in an interesting way. For instance a case study related to network infrastructure of modern, multi subsidiary, and international corporation CKTECK will help the future students to learn more about new networking concepts in BYOD, Cloud and Social Media Networking. Moreover it will help them to learn about advanced networking schemes, network security related advanced risks, their countermeasures and network policies.

## 1.6 Aim Of The Project

The aim of the project is to identify key challenges and define major existing security in order to train more realistically next generation students with CKTECK. Both – one and multistep task description – as well as proposal for security solutions have been elaborated. Moreover, the aim is to deliver overall all infrastructure plan, physical facilities and in depth framework of some discipline as e.g. authentication, accounting, authorization, encryption, physical security, disaster recovery planning, business continuity management, network security, application security, web security, BYOD, backup, hot swap over to second site etc. The network related risk assessment, related countermeasures, tasks description and solutions of some tasks have been developed for international multi Subsidiary Corporation. With this work it is possible to have a breakthrough in teaching and training processes towards realistic and in-depth applied security. Furthermore, studies on new security contents requiring corporate environment are feasible for the future students.

## 1.7 Research Questions

1. How to define international Multi-subsidiary corporation named CKTECK (along with peer student)? How to develop a model of network infrastructure for CKTECK organization?(network infrastructure and technical aspects are considered as individual job for the author)
2. What are typical CKTECK's network infrastructure security related risks in advanced BYOD, Cloud and Social Networking?
3. What are the corresponding preferred countermeasures that can be applied in CKTECK's network infrastructure information security? This leads to framework and task description for student training.
4. How to define a basic network security policiy and guidelines, strategies(Network Security Strategies & Mechanisms) to secure international corporation by today?
5. What are the task students should be able to perform? Which are the domains students should resolve in classroom together and where it is preferred to work in teams for developing prototypes?
6. How can the quality of the education tool be assessed?

## 1.8 Thesis Outline

The outline for the Master Thesis has been listed as following. The overall thesis structure is shown in Figure 2.

- Chapter 1 is about introductory part of the master thesis. In this author will provide information regarding topic of master thesis, keywords, research questions, choice of methods, justification motivation & benefits, and the outline of the thesis.
- Chapter 2 is about the related work for the master thesis. It will provide the information regarding basic networking related concepts for Cloud, BYOD and Social Media as a recent IT trends and technologies.
- Chapter 3 provides the description of MNC & multi subsidiary Corporation CKTECK, its overall network infrastructure plan, network related concepts, basic network security policy and Task Descriptions for the students.
- Chapter 4 is about solutions for the tasks which have been described in Section 3.4 previous chapter. Furthermore this chapter will provide solutions material for Network Security Risk Analysis and Network Security Policy related tasks.
- Chapter 5 provides the information on network security management plans for CKTECK like Application Security, Disaster Recovery, Business Continuity, Access Management, Authentication, Authorization and so on.

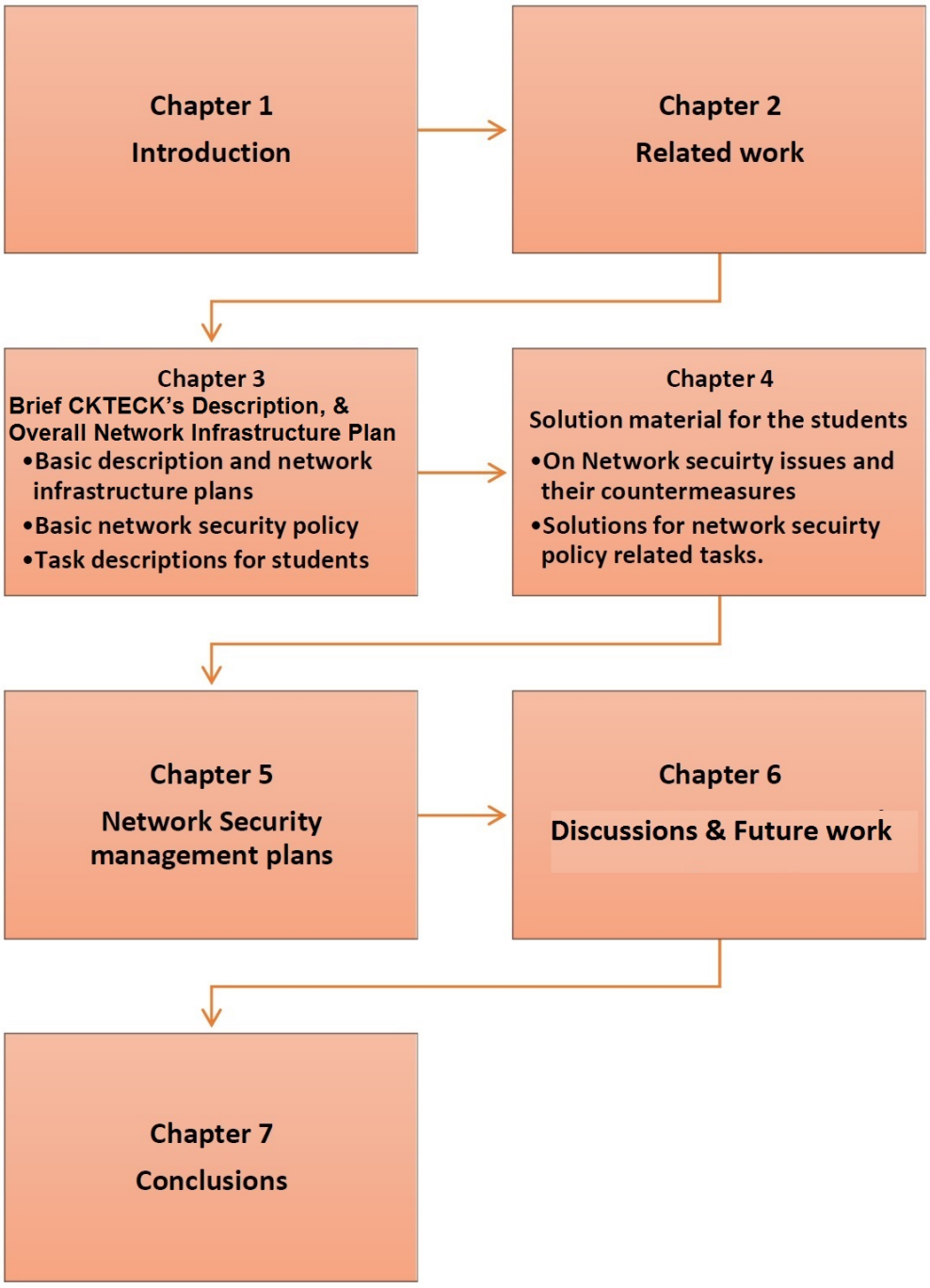


Figure 2: Thesis Outline Structure

- Chapter 6 is about interviews discussions. It also provides some further questions for the case and .Future directions has been described too in this chapter. The brief discussion on overall

research work has been written here also.

- Chapter 7 is about the conclusions what the author has concluded. It also contains Bibliography 7 where listed all references.
- Chapters A B C D are the several Appendices which are about all the ouestions and answers of interviews sessions which are conducted by the author. Chapter E of Appendix section is about Abbreviations.

# 2 Related Work

This section is all about the advanced networking related concepts in Cloud network, BYOD networking and Social Media Networking in modern enterprises. This has been considered as related work because these technologies are the latest technologies used by CKTECK's network infrastructure. Moreover the author has tried to show advanced networking risks in these three latest and new technologies further in Section 4.1. Moreover the related work provides the following information:

It describes the basic cloud network and different layers in the cloud networking. The layered cloud network has been described, the networking concepts of cloud in the organizations has been described. Moreover network virtualization concept has been also described here in the related work which is an important concept behind the Cloud networking..

It describes the facts about BYOD and its networking concepts that how a BYOD technology is related with cloud networking in the organizations like CKTECK AG.

It also describes the network graph for several people in the organizations at global level who are connected by using social networking sites over a cloud infrastructure.

It also provides the pre and basic knowledge for the modern technologies i.e( BYOD, Cloud and Social Media Networking). These technologies have the main role in the Corporation CKTECK AG. These are the recent technologies in the IT world and even though several advancements on these technologies are coming. To learn about the network infrastructure security related problems in these technologies in the modern organizations, it is very important to understand that how these technologies are related to the networking concepts in modern organizations.

All of this information is very important to understand the network infrastructure of CKTECK. CKTECK AG has its personal cloud VPN, which allows BYOD technology and Social media technology. Students have to found risks in the CKTECK network as the tasks described in Section 3.4. This knowledge will be helpful for the students to proceed on further. Without having basic knowledge in these networking concepts , it can be difficult for the students to understand the concepts of BYOD, Cloud & Social media behind the network infrastructure of CKTECK. Therefore, the author has explained this all in the related work.

Additionally the purpose of this related work is to make learn to the new students on BYOD, Cloud and Social Media Networking. The preliminary tasks which have been described in Sec-

tions 3.4.1 3.4.2 and the future tasks ( List of potential Projects on advance network management schemes) which have been described in 6.2 for the future students, is related to the concepts of BYOD Networking, Cloud Networking and Social Media Networking in the Modern Organizations.

## 2.1 Advance Networking Concepts In Cloud Network

**Basic Introduction**

Cloud computing has reached in the vast development with its several inventions. Cloud technologies [25] are emerging as a new way of provisioning virtualized computing and network infrastructure services on demand for collaborative projects and groups. Enterprises [13] are adapting cloud by launching their services by the cloud. Furthermore organizations have reduced their investment by changing their servers into the cloud [13]. Actually, cloud computing is very flexible because it is not only bound with PCs but it is also compatible with cell phones, android and so on. The emergence of new technology of smart phones had made cloud network very famous. By NIST in [13]

> "*Cloud computing is a computing model that enables the sharing of computer resources such as servers, platforms, and applications through a network anywhere, anytime, and on demand. This model consists of three service models with five basic characteristics [23] three service models" and four deployment models [28]*"

From [17] cloud computing services are growing as an important component of IT organizational infrastructure. Cloud computing is rapidly emerging and new development in Information Technology [39]. Cloud computing is one of the fastest [17] growing business opportunity for internet service providers and telecom operators. Author in [17] describes that, According to a recent forecast by 2014 the 80% of new software will be available as cloud services. Moreover there will be 30% of [17] annual growth in enterprises cloud services. Cloud computing is a novel paradigm [29] for sharing servers, storage devices, desktops and applications. Author in [12] explains that"*Cloud computing has evolved into a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)*" . Cloud computing is made upon advanced virtualization [20] and internet based computing. Cloud computing may have several type of users [24] like individual customers, individual business, startups, small and medium size business, enterprise business etc. Some good examples of big players [26] [27] of cloud are Amazon, Google, IBM etc. Cloud computing has become increasingly popular [32] with industries because it is reducing capital expenditure and transforming it into operational cost. Cloud computing have component based nature [27] like reliability, substitutability (alternative implementations and replacements), extensibility, customizability, scalability etc. A clear description of this can be defined as flexible nature of cloud from [33]. For instance cloud computing have abilities [33] like

- **(a) Significant scalability:** Cloud computing nature is very scalable for instance cloud provider Google has more than 100 billion servers. Amazon, Microsoft, IBM, Yahoo have hundreds of thousands of servers.
- **(b) Virtualization:** It means users can use cloud services at any location, by using a variety of terminal access to application services. Users need only a laptop or mobile for this.
- **(c) High Reliability:** Cloud computing nodes are interchangeable and more reliable than a local computer.
- **(d) Versatility:** Cloud is not made for only a particular application Applications in cloud support other different applications which are running simultaneously.
- **(e) High Scalability:** The size of cloud computing can be grown according to the need of users and size of applications.
- **(f) On demand Services:** Users of cloud can demand a service in cloud and get good response.
- **(g) Very Cheap:** This technology is not costly because it has low cost fault tolerance nodes.

Cloud computing can enable their users [41] to get what the users need. In recent years [44] a large number of cloud computing publications can be seen like books, white papers, articles, technical reports and so on.

### 2.1.1 Five Characteristics, Four deployment Models and Three Service Models of Cloud

**Five characteristics of cloud computing are [23] [37] [34]**

**1. On demand self service**

Consumer can one time demand of computing capabilities like server time and network storage

**2. Broad network access**

Consumer can get networked and accessed capabilities by using standard mechanisms like thin or thick platform usage.

**3. Resource pooling**

In cloud computing, the resources are pooled into a multitenant model. Consumers can use different physical and virtual resources. Resources examples are storage, memory, network bandwidth, processing and virtual machines.

**4. Rapid elasticity**

In cloud computing consumer can provision several capabilities very rapidly and elastically. For instance in some cases if required automatically scale in and scale out. It is because of flexibility of the cloud network.

**5. Measured service**

The usage of resources in the cloud can be controlled and optimized automatically. It is because that the cloud have capability of leveraging metering at some levels of abstraction, which are appropriate to the type of particular service.

**Three service models of cloud [13][14][15][16][20][21][24][28][29][30][45][46][37][34]**

- (a)Saas (Software as a service)
- (b)Paas (Platform as a service)
- (c)Iaas (Infrastructure as a service)

Figure 3 is about three layer networking architecture of cloud network. According to author in [46], In Iaas (the lowest layer of cloud networking architecture), there is a particular CSP (cloud service provider). The consumers can run, deploy and use software which is provided by CSP and CSP is responsible for controlling the whole cloud infrastructure. From [14] the main objective of Iaas is to reduce the capital expenditure and the overall maintenance of computer resources like hardware, servers, storage unit, networking capabilities, electric power etc. From author's point of view in [24] Iaas provides virtual machines and other abstracted hardware and operating systems which are controlled by API (Application programming Interface).

In Paas, (the middle layer of cloud networking infrastructure) consumers deploy those applications which are created by using some programming tools that are supported by provider [46]. These applications are run by a cloud service provider. From [14]the basic objective of Paas is

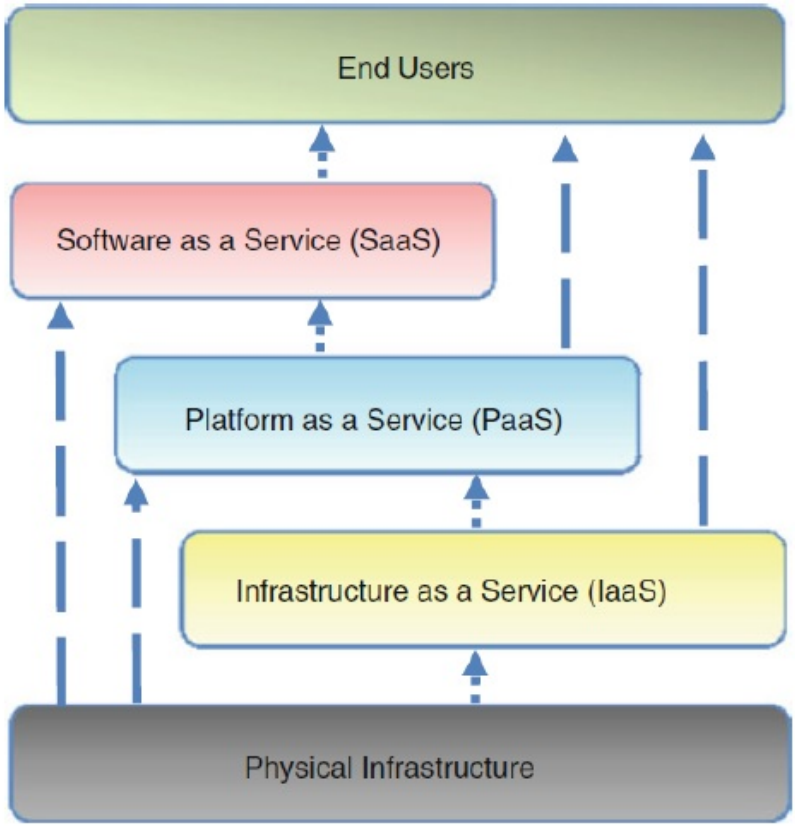


Figure 3: Three layered networking architecture of cloud

to reduce the overall cost of platform like operating systems and other development frameworks where applications and services are developed. In Paas users have main responsibility on applications and services. According to the author in [24] Paas allows customers so that they can develop new applications by using API which are implemented and operated remotely.

In Saas, (the top layer in cloud networking infrastructure) consumers use the applications of CSP's on a cloud infrastructure which is provided [46] by another. In all cloud services are included in all three layers of the architecture. Each layer has its own functions and capabilities. From [14] in Saas the whole responsibility of infrastructure, platform and maintainability of services are assigned to the provider. Users have limited access to the settings of applications. From [24], Saas is software which is offered by a third party provider. It is available on demand by Web browser. Examples are online word processor, spreadsheet tools, CRM (Customer relationship management) services and web content delivering services.

**Four deployment models of cloud [37][14][28][24][30] [47] [44] [48]**

**(a) Private Cloud**

Private cloud is the cloud which is operated by the private network of the organization. It is managed and controlled by the organization and may be the third party. Third party could be a part according to the organization's requirements. Private cloud is operated for a single organization. It may be managed by third party.

**(b) Public Cloud**

It is a cloud which is accessible to the public. It is not private and available in general public. Basically public cloud is for general public or large enterprise.

**(c) Community Cloud**

Community cloud is the cloud which is shared by several organizations for several purposes. Community cloud is shared by several organizations and supports a community. It is managed by organization or third party.

**(d) Hybrid Cloud**

Hybrid cloud is the combination of two or more clouds which are separate actually. But there could be chances of portability of data and applications between them. It could be the combination of public and private clouds. Hybrid cloud is combination of two or more clouds (Private, Public or Community). These are bound together by a standardized technology.

### 2.1.2 Cloud Networking Architecture And Basic Networking Concepts In Cloud

According to Figure 4, it is a cloud network scenario. The overall description can be defined as: The users in the Figure 4are in separate access networks, which are connected by internet via AP's (Access Points)

Several servers in the Figure 4 are used to combine and compose the overall cloud infrastructure. Several servers are like media server, storage server, application server, etc. These all servers are interconnected by internet. Cloud services are for the end users. There are several types of cloud connectivity i.e. Point to Point, Point to Multipoint, Multipoint to Multipoint and so on. Examples for these connectivity types are shown above. If any user A wants to do store something in the storage server then it is called point to point. If any Television on demand service is involved in users B and C then it is called point to multipoint. If the service is like video conferencing

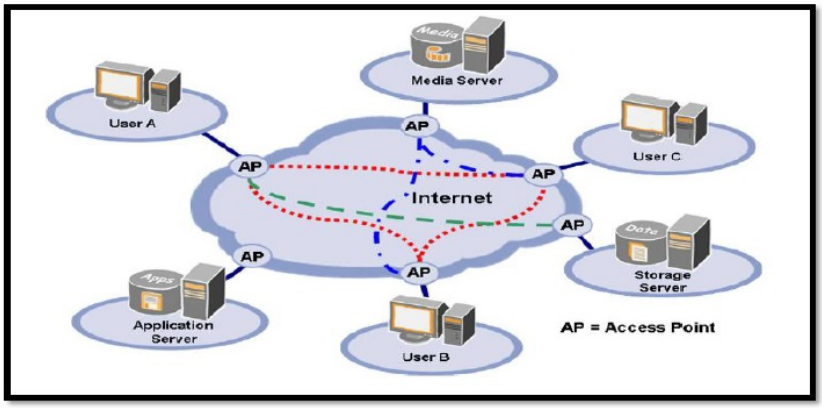


Figure 4: Cloud network Scenario, adapted from [29]

between several users then it is called multipoint to multipoint. For several connectivity types in the cloud NVP is required. NVP is network virtualization platform [43]. The Figure 5 from [29] is about NVP and its related services. Figure 6 is also related to several further services of Naas (Network as a service). NVP is a part of cloud virtualization platform as shown in Figure 6.

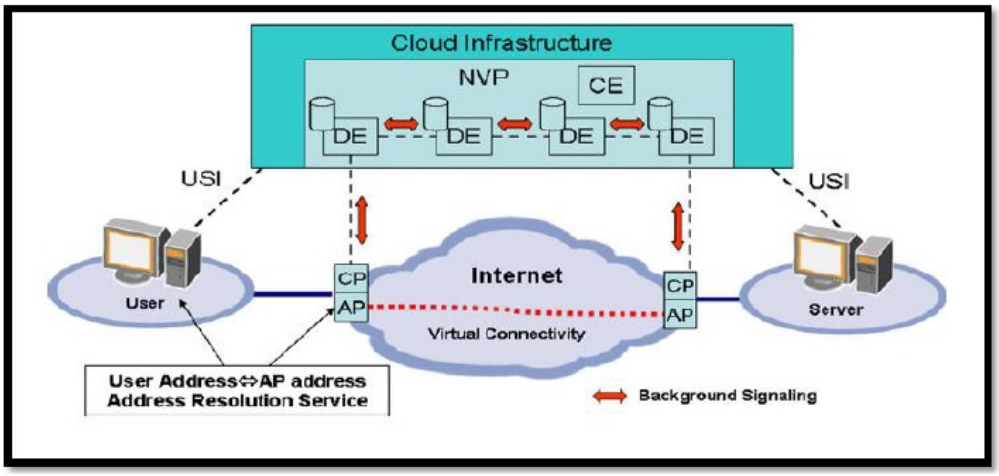


Figure 5: NVP (Network Virtualization Platform) in cloud network, adapted from [29]

From [29], the main purposes of NVC is described as follows

- To hide implementation details of the network infrastructure.
- To provide safety to the whole hardware or software of the end systems in case of any

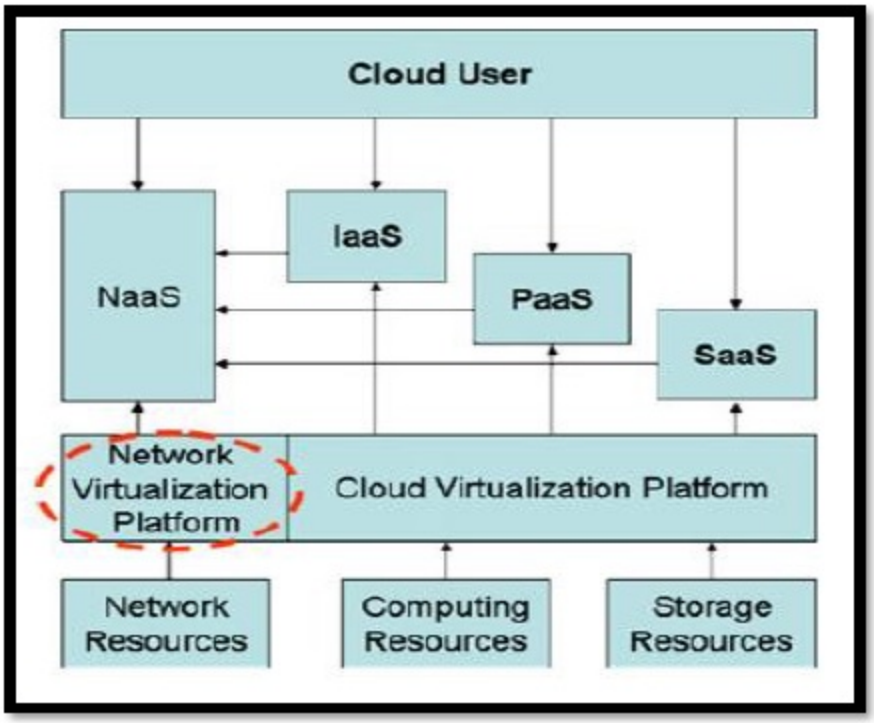


Figure 6: Cloud Architecture extension with Naas, adapted from [29]

changes.

- To minimize the networking nodes which are used in Naas (Network as a service)
- To provide connectivity to the quality of service within several provider domains.

As shown in the Figure 5 the NVP is collection of DE's and CE's (Distributed entities and Central entities). CE basically implements the database of profiles of the cuatomers. It also implements associated SLA's (Service Level Agreements) for the purpose of providing authentication and necessary required authorization to network related services. NVP shown in Figure 5 is basically based on the process of background signaling. The basic purpose of this is to collect information related to the network topologies. DE distributes the information to other DE's in the nwteork. DE also perform network resources virtualization. Moreover DE stores the status information in the local resource database. Basically DE is used by cloud users when they want to send request to Naas (Network as a service) via a VPN (Virtual Private Network)

In Figure 5, USI is called User to Service Interface. In this cloud users request to the network as a service (Naas) by sending messages to NVP. USI signaling is implemented is XML (Extensible

Markup Language). Messages are exchanged over TCP(Transmission Control Protocol) sockets. Furthermore XML allows to perform easily processing of the data in mappings of services and checking of structure. DE is collection of CP and AP. CP is used to integrate and extends the different layers of the network. Several applications in the layers request to CP for several services. Cloud networking architecture uses Naas (network as a service) concept. Naas is shown in Figure!7. Naas is a class of services for cloud computing which provides virtualized connectivity to end users at various levels of reliability, traffic quality of service, flexible and scalable transparency etc. Naas can be classified into two categories

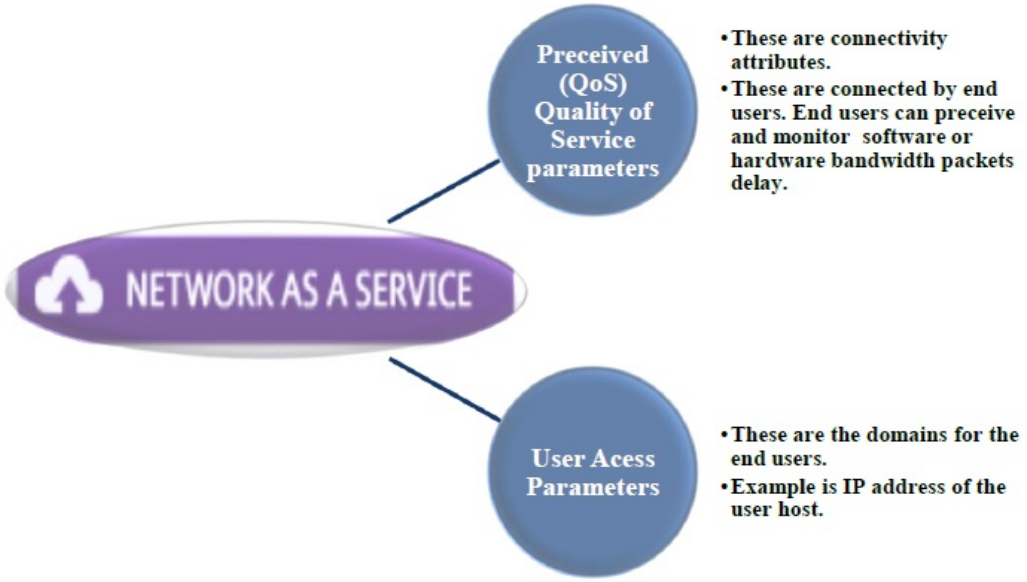


Figure 7: Classification of Naas parameters, idea taken from [29]

Naas can be also classified into several service units like network access service, virtual connectivity service, virtual topologly service, virtual node service, network cost estimation service etc. Several service units of Naas are described below.

***Network Access Service:*** It is used for Authentication and authorization. It provides user Identification for accessing grant. It is a kind of service acknowledgement.

***Virtual Connectivity service:*** It is responsible for monitoring and management of virtual connections which are created among several users. For example connection creation service provides create of any connection, connection deletion service provides delete of any connection and so

on. It also provides current status of certain connection parameters.

***Virtual Topology service:*** It is combination of management and monitoring of network topologies. Specially for virtually connected information like available bandwidth, packet delay, restoration etc.

***Virtual Node Service:*** It is responsible for monitoring and managing of virtual nodes. In this the information which is provided, is related to the type of virtual connectivity like VPN, or Private LAN.

***Network Cost Estimation Service:*** It is a grid functionality service. It provides information on the status and the behavior of transmission of the network to the grid services.

## 2.2 BYOD Networking Concepts

BYOD means that [61] personal devices used for both business and private purposes. Hence the usage of business is mixed with personal. BYOD (Bringing your own devices) [67] [68]at workplace has been become very popular in recent days. BYOD is common in several services and businesses [59]. Employees [53] want network access anytime and anywhere. In [64] author explains that *"BYOD can let an employer not only make use of free-cost IT resources which are contributed by employees, but also attract smarter employees who consider their mobile computers being their always available"*. The overview of BYOD in organizations has been shown in Figure 8.

As from [53] a survey by CISCO Internet Business Solutions Group (IBSG) in 2012 shows that 89 % of Information Technology Corporations support BYOD. From [55] 84 % of organizations are planning to implement Mobile Device Management by 2014. By 2017 [63], the BYOD has been forecasted as to spawn a $181.39 billion industry. From [52] BYOD is a technology in IT organizations which is used to support a variety of devices and their operating systems, and maintaining an expected level of service. Author of [56] describes his views about BYOD that "*Bring Your Own Device (BYOD) incorporates new devices into the enterprise outside of the process that IT normally follows for vetting, monitoring and auditing equipment for proper use. Instead of IT pushing down mandates to its employees' population, BYOD allows employees to express and dictate the technology they want to use back to IT.*"

IT Corporations are adapting because of several reasons. Some of the reasons from [53] are listed below:

- To improve the productivity

Figure 8: Modern BYOD Overview in enterprises, from google images

- To enable new ways of doing business
- To reduce desktop cost
- To mitigate risks
- To give freedom of work to the employees of the organization
- To improve satisfaction of employees
- To design a best class technology
- To integrate with third party
- To enable professional services
- To provide end to end support
- To provide consumerization of IT

Behind BYOD technology the name of the concept used is “Consumerization”. From [58], consumerization can be defined as cloud computing services with 3G/4G and smart devices. Furthermore from [62], consumerization is the IT innovations from the consumers market which acts as a challenge for the Corporate IT.

Organizations are allowing their employees to choose their [54] laptops, smart phones, tablets, macbooks etc. for supporting BYOD. The elements of BYOD technology is shown in figure 6 which

have taken from Google images. Employees in organizations are connected to the network interchangeably by using laptop, smart phone and tablets. Hence a number of devices per employee are also increasing [54]. BYOD has become a new business culture [60] of the smart work.

BYOD is also a part of cloud computing. From all above it could be concluded that Many organizations are adapting cloud computing and employees use their own devices at workplace for instance mobile devices as smart phones and many more. Cloud computing has a great role in emergence of the BYOD technology in the organizations. BYOD with cloud computing in enterprises is shown below in Figure 9.


Figure 9: BYOD with cloud computing in enterprises, adapted from [69]

With the Cloud computing and BYOD, the mobile computing has been become a recent trend also. Mobile Cloud Computing [66] [65] is also a related concept with the cloud computing and BYOD both. With the enhancement of mobile and smart phones ,cloud and BYOD the concept of mobile cloud computing has been grown and introduced. From [66], Mobile cloud computing can be explained as when someone is running any application (for instance facebook or gmail or any other application) on smart phone with the usage of its remote server correspondence. From [57]

> *"Because employees have become accustomed to self-service environments for applications and support, thanks to innovations such as Software as a Service (SaaS), cloud computing, and, of course, mobile devices, they are also much more comfortable with the concept of a BYOD program*

> *that allows them to use their own device(s) for work. BYOD programs should reflect best practices that recognize and embrace the inevitability of consumerization, yet offer "built-in" flexibility and adaptability because those best practices are emerging and changing as quickly as the mobile environment*"

This can be said as mobile cloud computing. Here mobile phone or smart phone works as a client which connects with a remote server via any 3G or 4G technologies. Mobile cloud computing architehture in enterprises has been shown below in Figure 10.

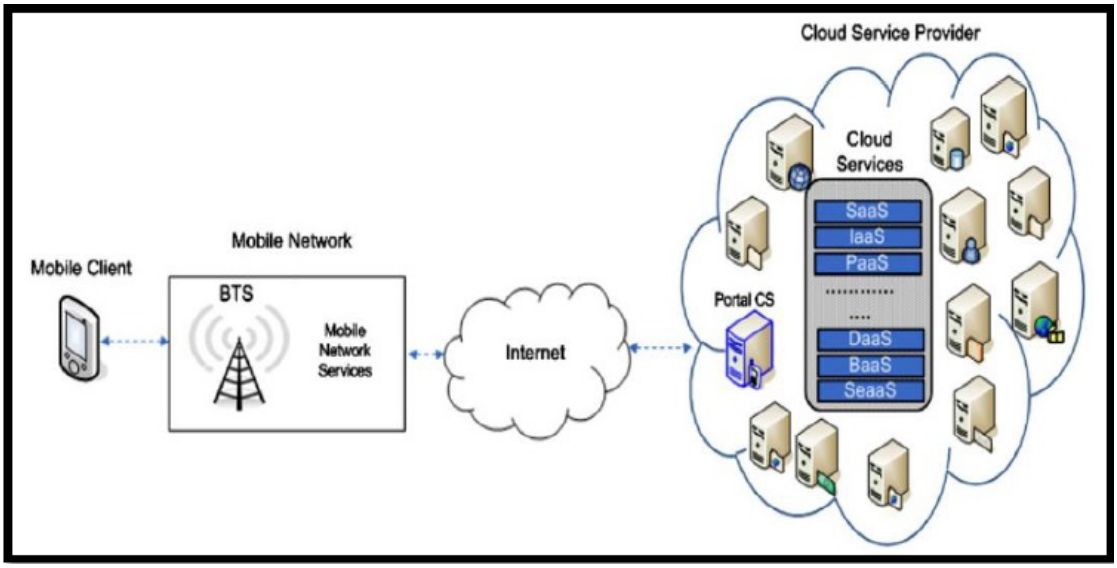


Figure 10: Mobile Cloud Computing Architecture from [65]

## 2.3 Social Media Networking Concepts

Social Networking from SANS institute [95] can be defined as

> "Social Media is the internet and the mobile technology based on the channels of communication in which people share contents with each other"

According to the author in [87],

> "Social networking sites have attracted millions of users. Through these sites, the users share their information (text messages, photos, and videos, etc) with their friends"

Social media or social networking are comes from the *"consumer oriented services"* [82]. These technologies are responsible for transforming [82] the way so that the people can communicate

and accelerate the spread of the information. As in recent and current time period, so many people are familiarized and attached with the usage of social media networking. Running examples are using face book, twitter, and linked in etc. As the time is going forward, the changes and advancements are also coming in the smart technologies.


Figure 11: Social Media Networking, from [96]

Figure 11 shows several social networking examples and its various features. Face book and Twitter had approximate 800 billion and 300 billion users [83] correspondently by 2011 and 2012. Author in [84] explains that with the advancement in social media recently, organizations are increasing interest in more usage of social networking. Organizations want to learn, understand and use of the social media and its interesting and flexible applications. Moreover in now a these days social media [85] has become the most popular in IT industries. It could be said that social media has taken its place as a recent trend for several organizations, From [85], statistics show that social media adaptation had been doubled in USA in small businesses in 2009. Social media has made the life easy of people. That's why the people are interested in use of these

advanced trends. Recently the social network service has become an increasingly popular web service which can provide knowledge sharing and user interaction based on Web 2.0 concepts [82]. The concept of social media connectivity in enterprises is shown below in Figure 12.

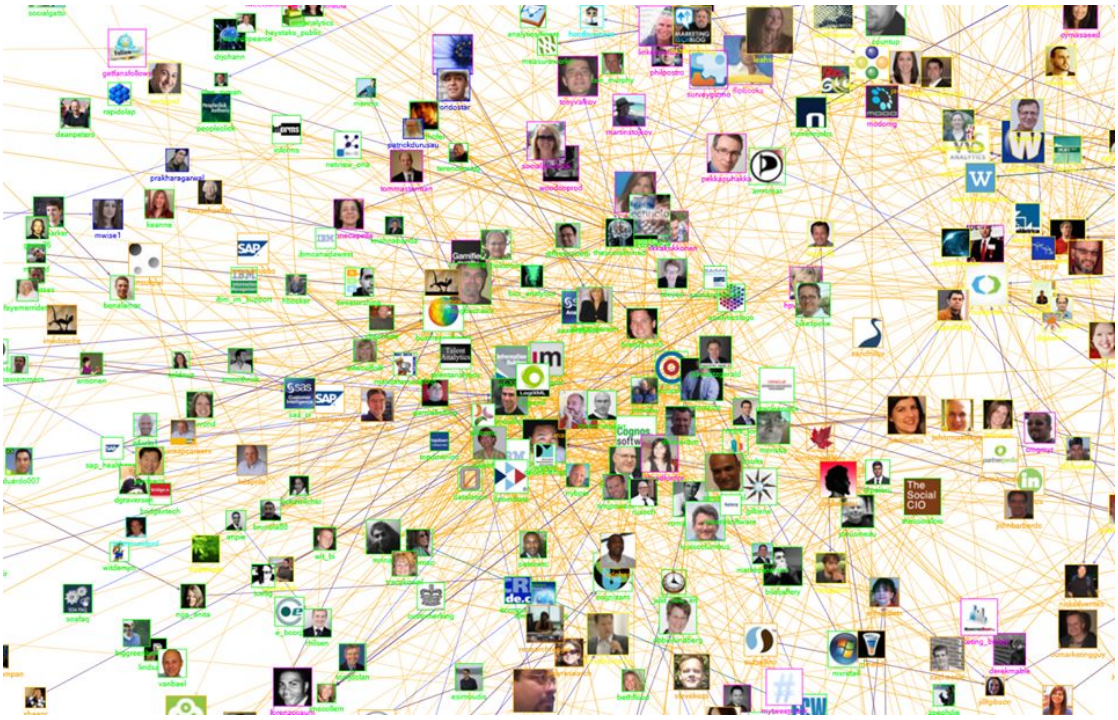

Figure 12: Social Media Networking Connectivity graph in enterprises, from Google images

Social media has several features for instance it provides us several demands like easy chatting, video conferencing, internet shopping, finding jobs, multimedia sharing, online games and many more. Author of [85] describes that many of the organizations hire their consultants and employees by using facebook, linked in, twitter or youtube. Linkedin is very good example of professional social networking site. Anyone can share his/her professional career and an make network with other several related professionals. It also helps to find jobs related to our career, study area, field and experience.

In case of face book, it has been become the most accessed [88] website in the cyber world. Is has been shown in [88] according to statistics that *"From one billion active users , 552 million users are the daily active users of facebook in year 2012"* With BYOD and cloud, the trend of mobile social networking [89] has been increased. Millions of users [89] are continuouslyusing "always on" and "always carried" mobile devices to access the internet and social networking applications. Author in [90] shows that Social networking has made the web friendly and more connected but

also more complexed. According to the SANS Institute [95], social media offers several advantages to the organizations. The competition has been raised among several organizations. Therefore it has been become the need of of organizations to adapt these smart technologies to move forward. Otherwise enterprises can't move forward and can't come in competition with other organizations. Social Media and technology is also known as Web 2.0 user generated contents. From [96] social media applications can be categorized into several categories. 15 categories of social media from [96] has been listed below and shown clearly with examples in Figure 11.

- Micro Blogging
- Publishing
- Photo Sharing
- Aggregators
- Audio
- Video
- Live Casting
- RSS
- Mobile
- Crowd sourcing
- Virtual worlds
- Gaming
- Search
- Conversation applications
- Social Networking

Social media is also related to cloud computing [96]. Furthermore it could be said that BYOD, Cloud Computing and Social Networking are related with each other and connected with each other in some manner.

# 3 Brief CKTECK's Description, & Overall Network Infrastructure Plan

## 3.1 Basic Description Of CKTECK AG

Section 3.1 has been taken from [77]. The Organization CKTECK was described by Khushbir Kaur Sharma in her Master Thesis. The author of this thesis is responsible for making overall network infrastructure plan, for finding network security related threats and risks, for finding solutions, for describing basic network policy for CKTECK Corporation, for describing several tasks to the future students and so on. Therefore for all this the author needed a basic information for a multidiary and multinational Corporation. Hence the information of Section 3.1 has been taken from [77].

CKTECK is a modern Information Technology related organization.CKTECK is multi international and multi subsidiary organization. CKTECK has been come from the SOKOTCEK AG, 2005. SOCOTECK AG case study was related to the problems and technologies in year 2005. But in these days the technologies are modern and there have been emergence of smart devices. CKTECK Corporation is related to the modern technologies, smart devices according to the environment in now these days.

CKTECK Corporation is related to three main recent technologies i.e. Cloud Networking, BYOD and Social Media networking. CKTECK's customers are from several locations which are listed below

- Bank of America (on different locations) bank
- AT & T wireless (Cellular company)
- US cellular
- Comeats
- Cable Connect Inc., Tel Aviv (Israel), Cable manufacturer
- Trossen AG, Honau (Germany) Engineering works
- Weiss & Partners, Goldau (Swiss) Arm manufacturer
- Lotti, Zurich (Swiss) Private bank

- Barmherziges Herz Charity organizations
- Kant. Psychiatrischer Dienst, Zurich (Swiss)
- Vardhman Limited Wool Manufacturer (India)

CKTECK is with Ten modern subsidiaries. The four countries are Switzerland, India, Poland, and Norway. The following are the locations of CKTECK Corporation. The description has been shown below.

### 3.1.1 CKTECK's Three Subsidiaries In Switzerland

There are three buildings in Switzerland.Figure 13 shows CKTECK's three subsidiaries at Switzerland Area. Two of them, Altodorf Ost & West, are located at the outskirts of Altdorf at the one side of the Reuss river, while the third building is located on the other side of the river in Attinghausen. The bee-line between these locations is approximately 800 m. The hardware department resists exclusively in Attinghausen, while 95% of the informatics department resist at the two buildings in Altdorf (see site plan also). Some collaborators of the automation department, who are responsible for system integration work at the hardware site.

The main gate at the Attinghausen area is attended around the clock by a gate keeper. The side is also accessible for trucks, in order to deliver and pick up goods. The employees parking ground is also located inside the area, which is surrounded by a fence and monitored by four video cameras. Robots ready for delivery, large amounts of electronic components, and raw materials are stored in that area.

Both buildings in Altdorf have air conditioning, located at the roof of the respective building. The side entrances in both buildings are locked, and are basically emergency exits, though the department chiefs have keys for them. At the main entrance of Altdorf Ost is the secretariat that also functions as a reception. The computer centre is located at Altdorf West. The building is secured via badge and a personnel code.

### 3.1.2 CKTECK's Five Subsidiaries In India

There are five subsidiaries of CKTECK in India. The organization contains advanced technologies with newly discovered infrastructure. The locations are situated in both North and south India. In south India the buildings are located in Banglore and Pune. The other three subsidiaries are in the north India i.e. Chandigarh (IT Park), New Delhi and Gurgaon.


Figure 13: Three Subsidiaries In Switzerland

**Subsidiaries In South India, i.e. Pune And Banglore**

Figure 14 shows two South Indian Subsidiaries of CKTECK. Furthermore Figure 15 shows three North Indian subsidiaries of CKTECK


Figure 14: South Indian Subsidiaries in Pune And Banglore

***In Pune,*** there is an office of CKTECK, which is situated in Pune IT park. This building is responsible for making hardware for instance, android smart phone development, development of security alarm systems, development using micro controllers, development of RFID sensors and so on. For the security of this office biometrics system is available. The delivery systems for products are available by using robots. The robots are responsible for carrying the products into the vehicles. Other hardware and software security aspects are also available inside the organization.

***In Bangalore,*** the main area of development is Visual effect computing services. There is a small office situated in Bangalore IT Park. The main activities of the office are Development of visual effects, Animation development and Development of games.


Figure 15: North Indian Subsidiaries in Chandigarh, New Delhi And Gurgaon

**Subsidiaries In North India, i.e.Chandigarh, New Delhi And Gurgaon**

***In Chandigarh,*** the BPO has been established for customer's supports. Customer support services are available for 24*7. For the security point of view they use access card for entering in the office. The employees are allowed to bring their personal devices but they can use them only within the visitor areas. There is an entry system for any unknown person. Moreover the security surveillances are available to monitor each and every activity.

***In New Delhi,*** the building is situated in Information Technology Park. It is a software development area, where so many organizations are situated. There is one office of CKTECK AG situated in that area. In this building, the software are developed and maintained. This building is responsible for Relational Database development, SAP and ERP Development, PHP and Java Development, VC++ and automation. Python software solutions, CRM Software development, CAD, CAME software developments. This is a small subsidiary of the organization. In this office, there is also an access card system security for each employee.

***In Gurgaon,*** the office is situated in IT Park. This office is responsible for the testing of the softwares, which are made in New Delhi and handling of communication services. The software are checked and verified here at this location for the performance measurement. All communication

services are also handled in this building for instance LAN, MAN WAN, WLAN, VDI and cloud etc.

### 3.1.3 CKTECK's One Subsidiary In Poland

The office in Poland is in Warsaw is responsible for providing engineering and industrial design services. The main services are Product detailing, Solid surface modeling, Finite element analysis, Infrastructural management, Digital design virtualization development, Technical surface development, Reverse engineering etc. Figure 16 shows its picture.

**(Warsaw)**

Figure 16: CKTECK's One Subsidiary In Warsaw, Poland

### 3.1.4 CKTECK's One Subsidiary In Norway

**(Oslo)**

Figure 17: CKTECK's One Subsidiary In Oslo, Norway

The main office situated in Oslo. This is responsible for Information security training services such as General awareness services, IT and user training, Technical training, End user education. The main purpose for the building is providing IT security consultancy related services to the customers. Figure 17 shows the Oslo Subsidiary of CKTECK in Norway.

## 3.2 The CKTECK's Overall Network Infrastructure Plan

The important thing need to be considered that CKTECK's network infrastructure allows BYOD, cloud and Social Media Networking. There is basically VPN network where CKTECK AG employee can access the organizational network and perform their work on it. with the help of such type of flexible infrastructure the employee can perform their job in a effective manner.

### 3.2.1 Preparing network infrastructure for the modern organization like CKTECK AG

*"The network is the computer"*

[John Burdette Gage [11] ] [38] When Sun Microsystems popularized this phrase several years ago. And it's impossible to connect information systems, systems, stakeholders and staff, a great deal of productivity would cease at many organizations today.[38] With the help of such type of technology the Network manager of CKTECK AG also rethinks to establish the network infrastructure of CKTECK AG. For upgrading the network infrastructure of the CKTECK AG the manager has upgraded the speed of the internet and changes in switch from 10/100 for the changer and 10/100/1000 for such kind of the advanced organization. It is very important in today's world that if we want to make changes for the network infrastructure we have to take some decisions for technology and design in such a way so that they can accommodate the virtualization, cloud computing and BYOD services and also take over consideration over the upcoming risks with such technologies with the help of CKTECK AG network design students and the author too learn about techniques and guideline in the establishment of the network infrastructure for a particular organization.

There some basic principal which has been using now in these days for the establishment of the network for organization . The same way CKTECK AG has also been adapted the fundamental such a PC LAN's and the internet is still apply and other techniques has been changed. For the network infrastructure of CKTECK AG the five major trends and reasons which has been deploying for the network infrastructure at CKTECK, are mentioned below. From[38]

- The raise in expectations of the users is so high towards the CKTECK AG. Due to advancement in the network field the network infrastructure need more flexibility and should be more user friendly so that it can fulfill the expectation of the users. CKTECK AG is totally depends upon the mobile services and internet for increasing productivity the CKTECK AG need to

regenerate their network security policy or strategy.

- Due to advanced security related concerns and the ubiquitous nature of the network it make vulnerable all the assets of CKTECK AG. Because the network of any organization connects overall infrastructure of the organisation which includes servers, desktops workstations and so on which contains all impotent and confidential data which needs protection .

- The change has been drastically comes in the information security organization . And it also comes in CKTECK AG organization which is totally based on the virtualization.Therefore it needs the change in the tools and theirs relative advanced mechanisms for the successful working environment of the CKTECK AG.

- *Reliability requirements* in the network downtime is very much important for the CKTECK point of view. If there is technological downtime for instance then its very difficult to accommodate. So that, CKTECK has their own backup recovery and disaster recovery policy to overcome to such disaster scenario . With such techniques the network is available and reliable in nature.

- *Mobility, cloud technology, Virtualization and wireless WAN's* in the network infrastructure of CKTECK AG is totally based on the advanced technological platforms for the networking . Because for People working far away from the organization premises can easily connect to the organizational network through some of these schemes. So that they can perform their work being a part of the organization from the different geographical location. "*using cloud-based services, supporting work- anywhere mobility tools such as smart phones and notebooks, and upgrading WANs to handle latency- sensitive and bandwidth-sensitive applications.*"[38]

FROM [38] Table 1 has shown the design changes and technology changes for the advanced information security organization.

### 3.2.2 Concept behind the improved network of CKTECK AG

Networks always needs changes according to the technological changes , because it needs to fulfill the needs of the organization and its users. According to the network infrastructure of CKTECK from 2005 it has been drastically change in all manners (technology, geographical structure, risks scenario, and so on factors.)These needs often change as technology evolves and improves. A good IT manager always thinks sensible and critical while developing the advanced network infrastructure and same has been done in case of CKTECK AG. during the research of CKTECK network infrastructure the author mainly learn some core concept which needs to be

Table1

| Trend | Design Changes | Technology Changes |
|---|---|---|
| 1. User expectations | · Scaling up via multiple data centers, content distribution networks and geographic load balancing<br>· Tighter integration of old green-screen apps with self-service web apps<br>· Rethinking operations to move to 24x7 availability | · Federated identity management that links to other web service providers<br>· Tunnels to e-commerce and fulfillment partners<br>· Secure Sockets Layer (SSL) accelerators<br>· SSL decryption appliances<br>· Quality of Service (QoS) management for traffic |
| 2. Security concerns | · Increased use of defense-in-depth with built-in layers of apparently redundant security<br>· More internal access control points within all Layer 3 devices<br>· More traffic inspection points designed in | · High-speed, high-density firewalls with many interfaces<br>· Gigabit-speed intrusion prevention system (IPS)<br>· Data loss prevention, both for outbound and inbound traffic<br>· Application-layer firewalls for servers<br>· Network access control (NAC) and application-control tools for users |
| 3. Data center changes | · Completely redundant design everywhere<br>· Collapsed backbone into chassis-type products to reduce Layer 3 routing decisions<br>· Higher density in-cabinet switches<br>· Green power and HVAC-aware design | · Link aggregation at switches to scale up speeds<br>· 10Gbps interfaces to top-of-rack or end-of-row<br>· 10Gbps directly to blade servers<br>· Application delivery controllers placed in front of server farms<br>· Converged data/storage networks |
| 4. Reliability requirements | · Application designs that make use of multiple redundant systems and redundant storage elements distributed across data centers<br>· Active-active device design<br>· Change in design to permit rolling upgrades of infrastructure without downtime | · High-speed inter-data center links<br>· Data deduplication<br>· Continuous data protection backup<br>· Use of redundant 10Gbps interfaces<br>· Rapid speed spanning tree protocol (RSTP) |
| 5. Mobility, the cloud and more efficient WANs | · Rethink apps to reduce traffic for WAN and mobile users<br>· Push apps to cloud<br>· Unified communications, linking voice, video, presence and apps<br>· Threat mitigation at the perimeter for VPN users | · Wireless LAN 802.11n deployments<br>· WAN acceleration for branches<br>· UTM security devices<br>· Mobile device management tools<br>· Service level agreement (SLA) monitoring systems |

Table 1: Design and technology changes for the advanced information security organization CKTECK AG

study and for future protection of CKTECK network infrastructure. It needs to be take under consideration that what is at horizon and what need to be added in the CKTECK AG. There are four technologies in particular that IT managers should start to learn more about because they will more than likely affect their network in the near future.

**Virtualization:**
Virtualization is the one of the main concept behind the network infrastructure of the CKTECK AG. The presence of virtualization is everywhere in the network. There are so many benefits [43] behind such kind of technology that's why CKTECK AG adopted virtualization as a part of network infrastructure. Some benefits from [43] [42] shown below:

- Easy and user friendly with GUI end user and administrators at CKTECK.
- CKTECK have opportunity of single control plane which can manage multiple devices.
- Providing flexibility and compatibility is a benefit for CKTECK's network and other devices.
- Due to flexible in nature, it can be easily customized by end users at CKTECK.
- It also provides security from protocol level to application level.

**10-Gigabit networking:**
from [79] the network infrastructure and virtualized server of CKTECK AG has been established on the 10Gigabit Ethernet. Its because of it provides very high bandwidth for communication at very long distance over different geographical location at lower cost. The level of scalability of the 10 gigabits networking is 10Mbps to 10000 Mbps. It also provides the link between switches and servers. The reason for adapting the 10Gbps is that at the edge of the of the network where it puts all burden. "*Large-scale server virtualization needs that level of bandwidth to operate. And 10Gbps Ethernet switches also support large databases and backup-to-disk initiatives*" [38]

**Wireless:**
In CKTECK AG the advanced level of wireless is 802.11n now in these days CKTECK AG wireless network is not for guests only the employee of the CKTECK also using the same network for the their organizational use so that they can reduce the paperwork and time as well. [38] with such facilities the video surveillance services are also available on the network for the larger geographical area of CKTECK AG.

**Multilevel security :**
From [38] In past few decades the firewall security was only limited to the perimeter. But these types of network security features are outdated now. In advanced organization like CKTECK AG the firewall are installed throughout the network infrastructure on the basis of some new network related requirement like speed, reliability and manageability. for Higher level protection for the

network infrastructure of the organization is too expensive CKTECK AG security related tools has been established inside the core so that the protection of the system is most important at CKTECK AG.

### 3.2.3 How CKTECK AG planned for the virtualization in the organization

When we have a look at the network Infrastructure of CKTECK AG there are so many changes made from 2005 to 2013. The overall picture of the network of CKTECK AG has been change . Now in these days the organization adopted the new technologies such as Cloud, BYOD and Social media and so on. In many ways, some changes are like in Ethernet ports, more focus on TCP/IP, cloud services, BYOD (bring your own devices), wireless. Behind all these advancement in the network infrastructure of CKTECK AG organization requires the faster security devices. from all above it clears that there is too much difference in today's network and the LAN based network decades ago.[38]

When the CKTECK start up with the virtualization within the network infrastructure of CKTECK the first question was in mind of IT administrator that from[38] " How Virtualization Changes Data Centres Virtualization and server consolidation have resulted in three priority requirements for data centre networks: high density, high speeds and very high reliability and redundancy. Virtualization also has shifted the emphasis in data centre networking to reduce reliance on Layer 3 routing in favour of Layer 2 switching. This is because Layer 2 switching gives the virtualization manager greater flexibility to move VMs between hosts and — most important — between different data centres in the same or different buildings and campuses" [38].

**High Availability and Redundancy:**

The high availability and redundancy the network infrastructure of CKTECK AG, that most of the network manger didn't much about the redundancy because it was depending upon a single point. But now in these days the CKTECK AG suing virtualization services a part of network infrastructure. It requires redundancy in every connection for more flexibility of the network and with such the availability also improves. With this techniques it can identify the failure within the network easily.[38][80]. Server- to-network redundancy, done correctly, helps to increase the performance of the network of CKTECK AG .

**Rapid Spanning Tree Protocol:**

For the faster recovery from the failure in the network infrastructure, CKTECK AG is adopting the technique like RSTP (Rapid Spanning Tree Protocol) basically it is used to remove the loops from the loop bridged environment.[38]IT manger should follow the right procedure to apply the loop free operation with the help of RSTP. The RSTP is very fast to detect the common loops and later on place one into BLOCKING mode to avoid broadcasting storm. [78]

But behind such advanced technology there are so many loop holes from where an attacker or intruder can take advantage and disturb the normal working condition of the CKTECK AG. The advanced connectivity style which has been used behind the CKTECK'S network connectivity is MPLS VPN Technology for connectivity over the long distance . While at the local level every data centre are fully equipped with the Advanced security mechanisms. But No system is full proof. This section provides the information regarding the whole network infrastructure plan and networking concepts for CKTECK's three subsidiaries at Switzerland.

### 3.2.4 Overall Geographical network view of CKTECK's ten subsidiaries

Figure 18 shows a geographical view of the ten subsidiaries of CKTECK. The subsidiaries have been shown at different locations on the different maps of the different four countries.

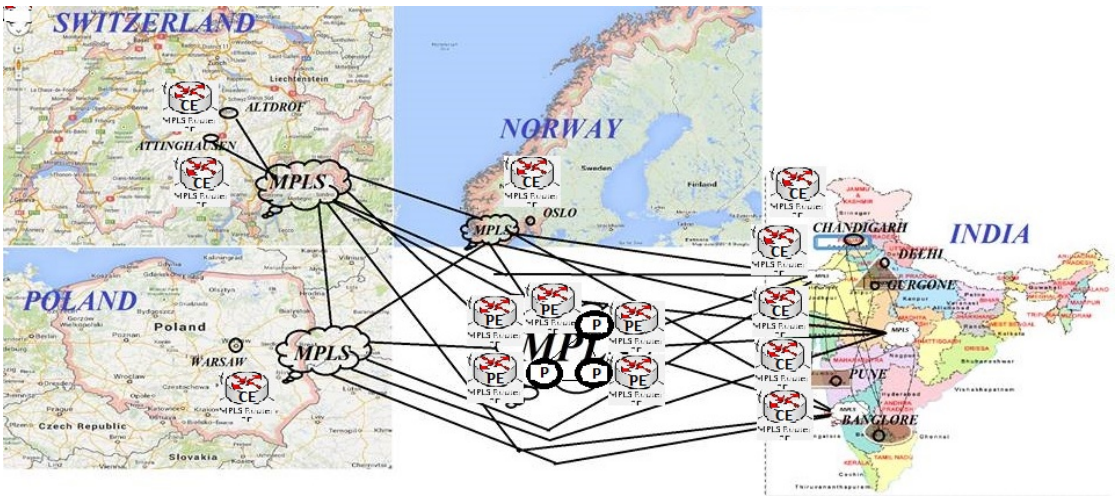


Figure 18: Geographical View of CKTECK's ten subsidiaries in different four countries

CKTECK AG adapted the MPLS VPN technology for connecting their subsidiaries over the different geographical location because the MPLS VPN provides the flexible communication channel to the subsidiaries. In MPLS contains P and PE routers and CE router at customer premises so that it can provide the connectivity between all subsidiaries at different location. P routers are in the core of the network infrastructure of MPLS VPN of CKTECK AG. whereas the PE router works as a Edge based router to provide connectivity with the other subsidiaries over the different geographical location. where CE router has been established for make connectivity with the PE router which are located in PE of the MPLS VPN edge.The main VPN protocols which can be used behind the connectivity of overall CKTECK AG's network are PPTP[107], L2TP[108],

IPSec[107], SSL[107]

### 3.2.5 CKTECK's Blockwise Network Infrastructure Plan

The network design of CKTECK based organization for the Switzerland subsidiaries which connects the others subsidiaries through the MPLS VPN network. This is advanced network infrastructure of CKTECK with advanced features of sharing the data between different geographical location with Multi protocol label switching technique. The ideas behind using MPLS technology in CKTECK AG, has been adapted from [10] [81] [101] [102].This section will describe Network connectivity and the block wise network infrastructure of CKTECK which is related to the Switzerland's Branch of the Organization.

This section describes the Network Infrastructure Design for Switzerland based subsidiary. The description of network infrastructure and the network design diagrams are shown as follows. Figure 19 is about the Network diagram for the Altdorf ost subsidiary of the CKTECK at Switzerland. Figure 20is related to Network infrastructure of the Altdorf west subsidiary of CKTECK at Switzerland. Figure 21 shows the Network infrastructure of CKTECK's Attinghausen Subsidiary at Switzerland. Figure 22 shows the MPLS network connectivity between three subsidiaries of CKTECK at Switzerland Area at local level.

- The network infrastructure of the CKTECK AG is based on MPLS VPN network [10] [81] [101] [102] with advanced features of cloud, BYOD and SOCIAL media.
- The advanced versions of windows server patches are installed in the organization.
- Over 95% of staff work with the PC and are dependent on the availability of the network and other advanced features of the network in the CKTECK AG. With some Advanced features of network like Cloud ,BYOD, Social media, VDI etc. the employees rely on the network for overall work.
- The data centres are located in every location for better communication services. With advancement in network the employee can access the data anywhere anytime but under the security policy guideline of the CKTECK AG.
- For safety reasons, all servers are in a Fire proof cabinet of the data canter , from which ventilation reasons is tight.
- In addition to the 10 Gbps Ethernet and fiber optic connection, Wireless connectivity for MPLS VPN and the central server's attitude were exclusively used Ethernet and Fast Ethernet. The speed of the network is good. The three are each router in the basement of the three buildings. You are trapped in closets.

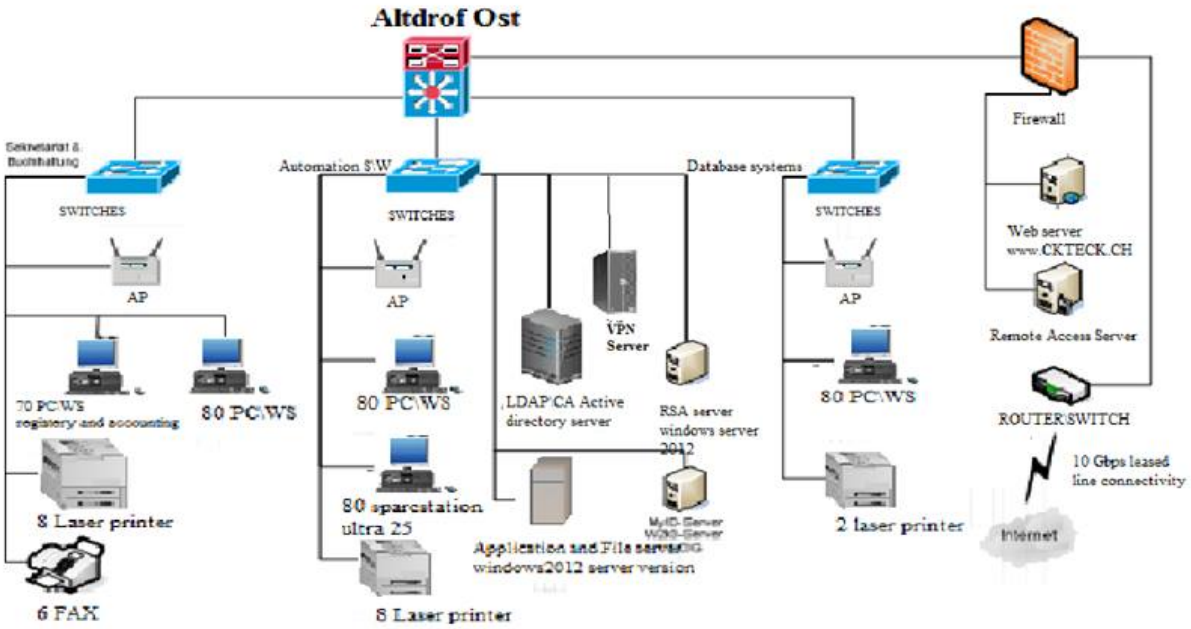


Figure 19: Network diagram for the Altdorf ost subsidiary of the CKTECK network infrastructure

- All servers are connected via a UPS , and other power backups systems because currently Fluctuations have been observed. All backup devices are at place because the information stored over the servers is accessed by the all employees who have access to the server data
- For the safety of the data are made a backup of all servers every week and included in a Fire proof cabinet, the server located the ground Floor of the computer centre are the terminal server and are usable only by authorized persons.
- Access to the building is possible only with a badge and a personal code . Some advanced access systems are also applied over the entry systems e.g. Access card system, biometric systems and RFID technology etc.
- In the each of the building CKTECK infrastructure there are several Ethernet and wireless for laptops desktop and other resources are available.
- The company CKTECK AG has installed its own web server in the DMZ. The server acts as a pool of information to interested parties to present the company and the new products. The CKTECK network infrastructure is separated from Internet by a Firewall.
- The Firewall has been administered only by Mr. Sharma . This is a task for the network administrator to be set.
- For all employees which are part of the organization have their account on the Firewall for the security point of view . This allows access to the network server via the Internet. Such

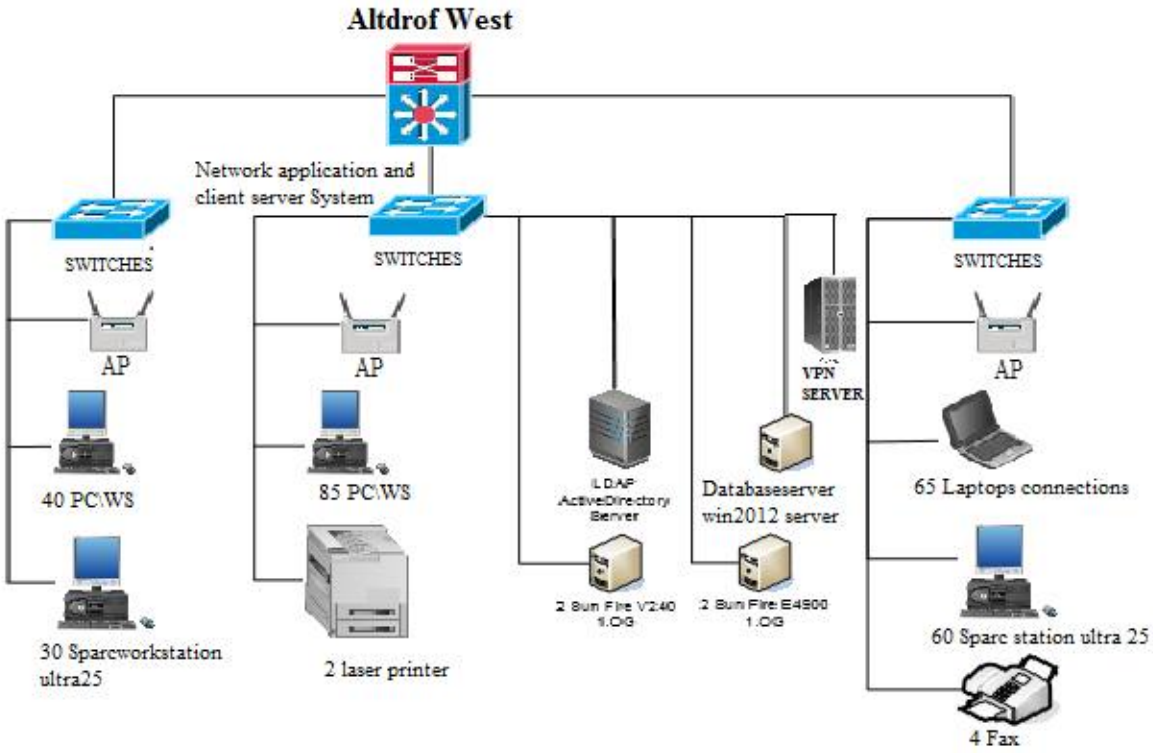


Figure 20: Network infrastructure of the Altdorf west subsidiary of CKTECK network infrastructure

requests are authenticated using login and password through the Firewall. There will be sending sensitive data. that how they are accessing the sensitive data

- The network management tools were served almost exclusively by Mr. Sharma . Two employees are in this direction, and expertise in all aspects while dealing with such tools.
- The hardware infrastructure was inventoried recently in this year. A new software was introduced for this purpose, however, is frequently also recorded everything on paper and stored.
- Advanced Encryption standards are set for the passwords. There is an instruction in the use of passwords and number codes Badge. These include the password structure, the length and the cyclic change of passwords and codes .The badges must be worn visibly.
- The Field staff can also access the infrastructure over ISDN and PSTN . While using the Remote Access they are cover the same security policy which are apply during the access inside the organization. During the abroad travel they are staying connect with the organizational network with the help of MPLS VPN. Tele workers use various client devices, such as desktop and laptop computers, smart phones, and personal digital assistants (PDA), tablets , to read and send email, access Web sites, review and edit documents, and perform many other tasks. Most Tele worker use remote access, which is the ability for an organization's users to ac-

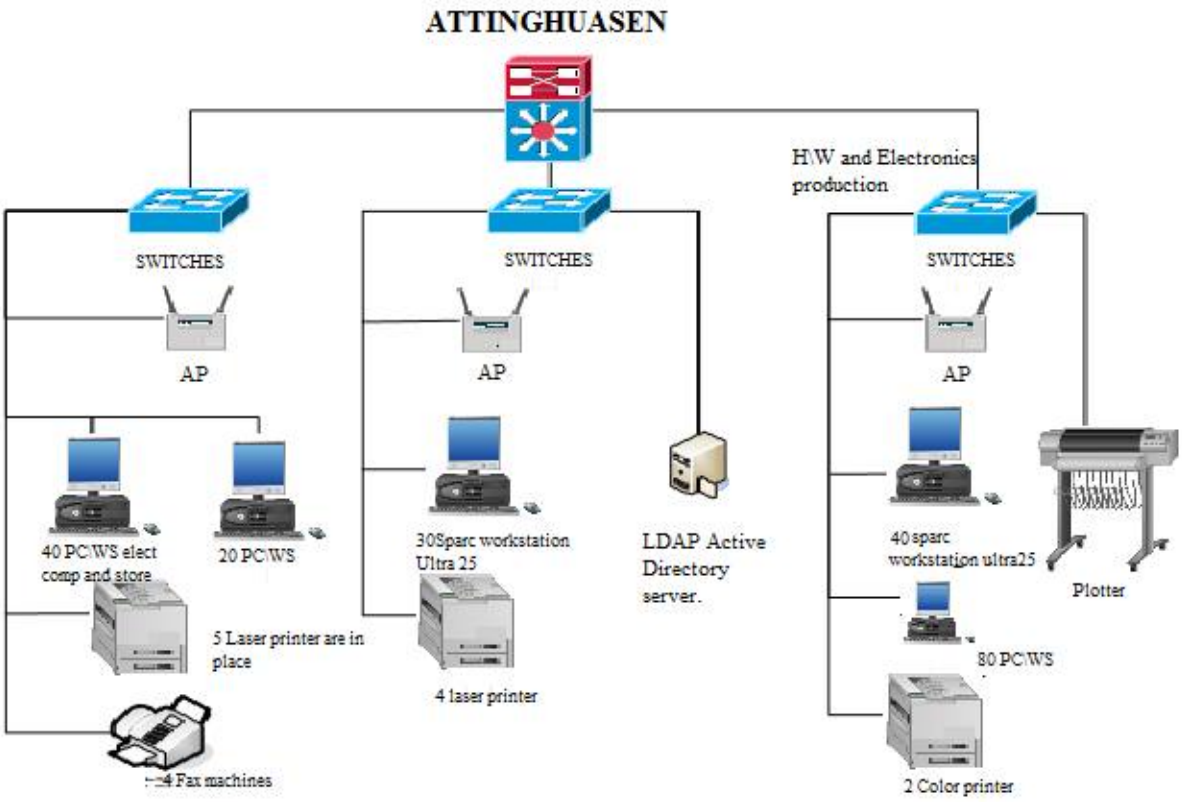


Figure 21: Network infrastructure of CKTECK's Attinghausen Subsidiary at Switzerland

cess its non-public computing resources from external locations other than the organization's facilities[113]

- Server takes over the task of the access check. Remote authentication is performed using normal login and password.
- In section two hardware development staff have set up on their own initiative, several switches . Hence, have the ability to control their workstations remotely from home to access the personal data and to control any intense, prolonged calculation processes.
- In the production department, a separate connection has been installed to react more quickly to customer inquiries.

### 3.2.6 MPLS Connectivity in CKTECK's subsidiaries

When the communication between different subsidiaries is required then the MPLS VPN technology is used. At local level the subsidiary is connected to its remote and regional office in

such manner.The network infrastructure of CKTECK is based on MPLS [10] (Multiprotocol Label switching ) technology.

With the help of such technology the multi-subsidiaries of CKTECK has been connected with each other over the different geographical locations. It supports up to 10000 users over different locations. The reason for choosing such kind of network is as following [10] [81] [101] [102]:

- IT is too flexible in nature.
- Scalability level is so high.
- Resiliency and security.
- Easily manageable.
- Advanced technological structure with advanced features.

In this Advanced CKTECK network infrastructure the support staff can design and implement the services in such a way, so that these services would be used in beneficial or effective manner.

**Overview of Architecture MPLS VPN Design [10] [81] [101] [102] for All Subsidiaries connectivity**

This section provides the information regarding basic MPLS connectivity at Switzerland Area in three buildings. Moreover it also provides the information behind the concept of MPLS connectivity for CKTECK's subsidiaries and its features, benefits and many more about MPLS technology.

The Figure 22 shows the basic local MPLS connectivity at Switzerland Based Subsidiaries. The MPLS connectivity has been shown in three subsidiaries of CKTECK at Switzerland area.

The CKTECK's network infrastructure with MPLS provides highly availability, security and optimization connection between the different remote site LAN's. When it comes over the subsidiary at different geographical location IP based connectivity comes in existence. These IP based technique provide a risk free environment between different locations.

In Figure 23 shows the remote connectivity by the use of MPLS technique with following features:

- It provides the MPLS WAN connections more than 500 remote sites.
- It also provides the primary and secondary resiliency.
- A wired LAN technology at remote site and IP based connectivity over the Geographical

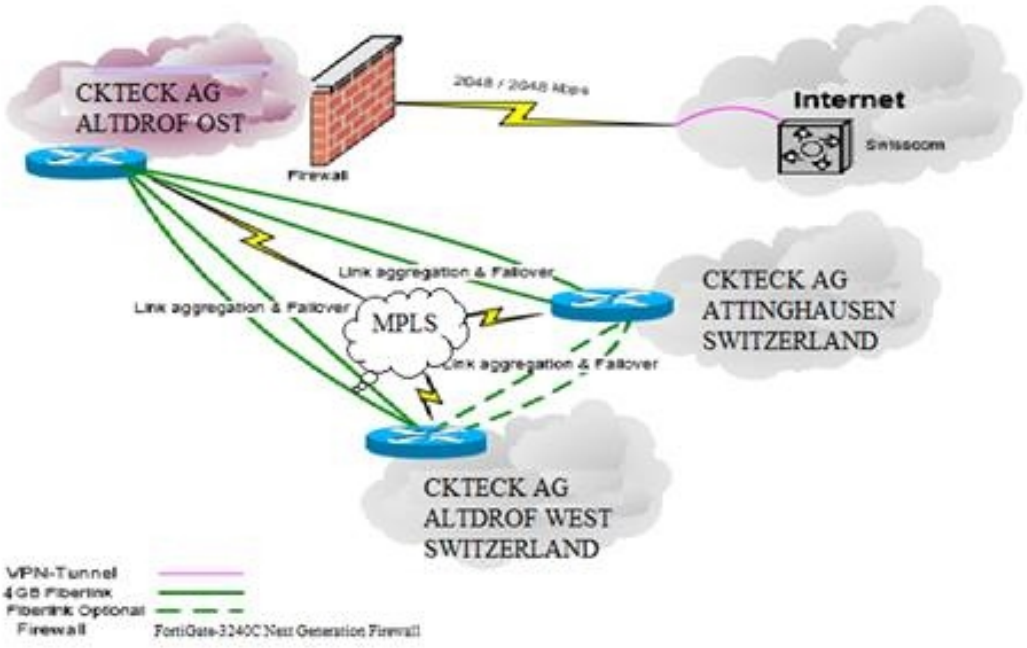


Figure 22: MPLS network connectivity between three subsidiaries of CKTECK at Switzerland Area at local level

location.

The one of the foremost Focused part of the CKTECK MPLS [10] [81] [101] [102] design is to allow usage of the commonly deployed WAN transport.

- MPLS VPN layer 3 (Primary)
- MPLS VPN layer 3 (Secondary)
- Internet VPN (Secondary)

The primary site uses network equipment for measurement of high performance and redundancy. In this design the primary WAN aggregation site is co resident to the data centre and same with main campus or LAN .The MPLS design of CKTECK network is a next generation network infrastructure which provide wide variety of advanced and VAS(value added services). The network infrastructure is provides cost effectiveness over the different geographical location with IP, frame relay, ATM or Ethernet. At layer 3 of CKTECK MPLS infrastructure the main use of a peer to peer VPN model that provides the BGP (Border gateway protocol) to explore VPN re-

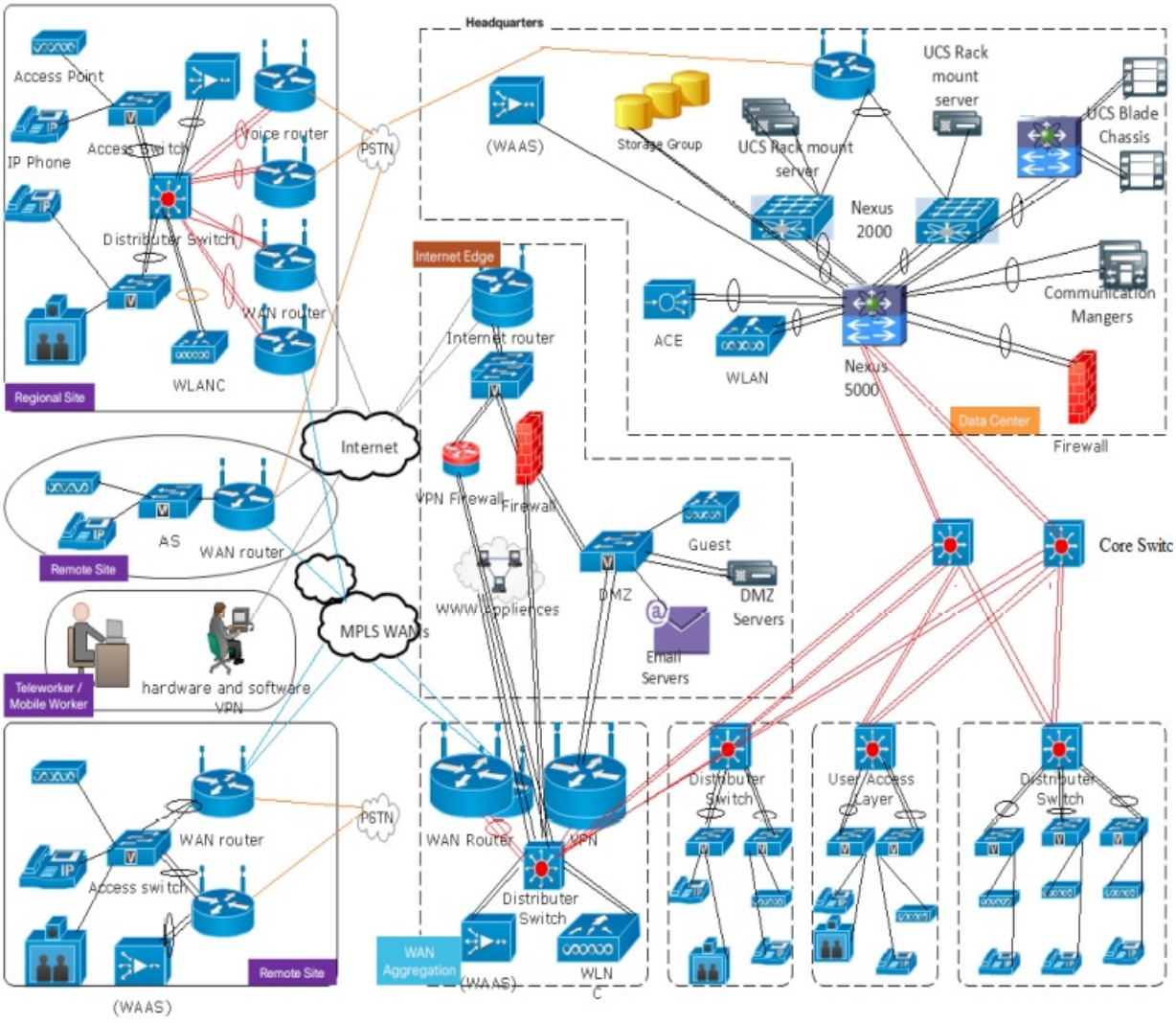


Figure 23: The MPLS VPN connectivity behind the CKTECK's Network Infrastructure, Adapted from [10]

lated information. With the help of such model CKTECK outsource routing information to service providers. Which is very cost saving and less operational complexity for CKTECK.

The subscribers who need to transport the IP multicast are using MVPN's. In such case of MPLS CKTECK network architecture leverages MPLS VPN as a primary or backup WAN transport. The architecture design of CKTECK is statically or dynamically routed with either single or multiple MPLS carrier. The main difference between the subsidiaries is the overall size of the network architecture. The other concept is based on the routing protocol .In these network architecture there is no difference between the distribution layer and dedicated WAN distribution layer. At distribution layer IP route summarization is performed. In infrastructure dual WAN edge tech-

nology has been introduced because of regional office and remote campus location are with more user population. Because it provide the redundancy to the single point failure.

There are some characteristics of CKTECK design model [10] [81] [101] [102].

- IP routing
- LAN access.
- High availability.
- Path selection performance.
- QoS
- Design parameters.

CKTECK MPLS Infrastructure is far better and effective over multinational locations. For emerging organization like CKTECK the WAN architecture requires flexibility that's why CKTECK using MPLS. Following are some facts mentioned below [10] [81] [101] [102]:

- MPLS VPNs are an IP Routing Service—the Implications
- MPLS WAN Explorer—Visibility through the MPLS VPN Cloud
- MPLS VPN Reach ability Monitoring, Alerting and Visualization
- Fast Detection of MPLS VPN Routing Outages and Instabilities
- End-to-End Path Tracing and Detailed Routing Analyses
- Powerful BGP Troubleshooting Tools for VPN Peering Problems
- Monitoring and Alerting on Breaches in MPLS VPN Privacy
- Monitoring of Remote Site IGP Routing Issues
- Scalable Monitoring of Satellite Sites
- Integrated Routing and Traffic Analysis across MPLS VPNs

Some features and benefits of MPLS WAN Explorer for MPLS VPN Network design for the CKTECK has been shown below [10] [81] [101] [102]:

- Connectivity all over the country on fiber as well as RF
- Three-tier network i.e. core, aggregation& access layers built to ensure "no single point of

failure"

- High level of scalability to handle both geographic expansions and bandwidth growth
- End-to-end assured network security
- Convergent network i.e. capable of running voice, video & data
- Supports layer 2 & layer 3 VPNs
- Support full/partial- mesh, hub & spoke topology
- Bandwidth availability from 64 Kbps to multiple STMs customizable as per the customer requirement
- 24/7 monitoring via multiple network operation centres MPLS WAN Explorer offers enterprise IT managers a number of benefits when deployed to help manage MPLS VPN services and ensure application delivery across the WAN.

### 3.2.7 Floor Wise Network Infrastructure For CKTECK AG in Switzerland's three subsidiaries

This subsection is about the network structure of different Floors of each subsidiary at Switzerland. In Switzerland, there are three subsidiaries as already described. Hence the Floor wise network infrastructure of three CKTECK's subsidiaries at Switzerland has been shown in this section. All devices are placed in the right place with advanced technologies and advanced features. This s diagram for the Switzerland subsidiaries which are located in different geographical location in Switzerland (Altdorf ost, Altdorf west, Attinghausen). The organization contains video surveillance for the sake of physical security and all building and floors are secured with access card system so that nobody can enter without permission .there are basically three floors in each of the subsidiaries of the CKTECK AG Switzerland branches. In all three subsidiaries some common devices are placed on the each floor like Advanced laser printer, Fax machine , workstation/ PCs and switches, but some of devices are special which needs description to understand the overall infrastructure of the CKTECK AG. At local level connectivity the CKTECK AG again using the MPLS VPN for domestic communication. The firewall is placed in between the connection which comes from the outside of the network and the company's internal environment . So that it can protect the internal environment of CKTECK AG from the Malicious outsider or other dangerous attacks. There are server and Virtual servers are location inside the CKTECK AG to provide the network flexibilities and reliability and availability for the employee working inside and outside the network. the use of Novell filr, remote access server, file server and directory server, database server, application server, virtual server and other devices which are placed inside the networked environment to make the CKTECK AG more strong at International level. Figure 24 is about floor wise network infrastructure of CKTECK's three subsidiaries at Switzerland.

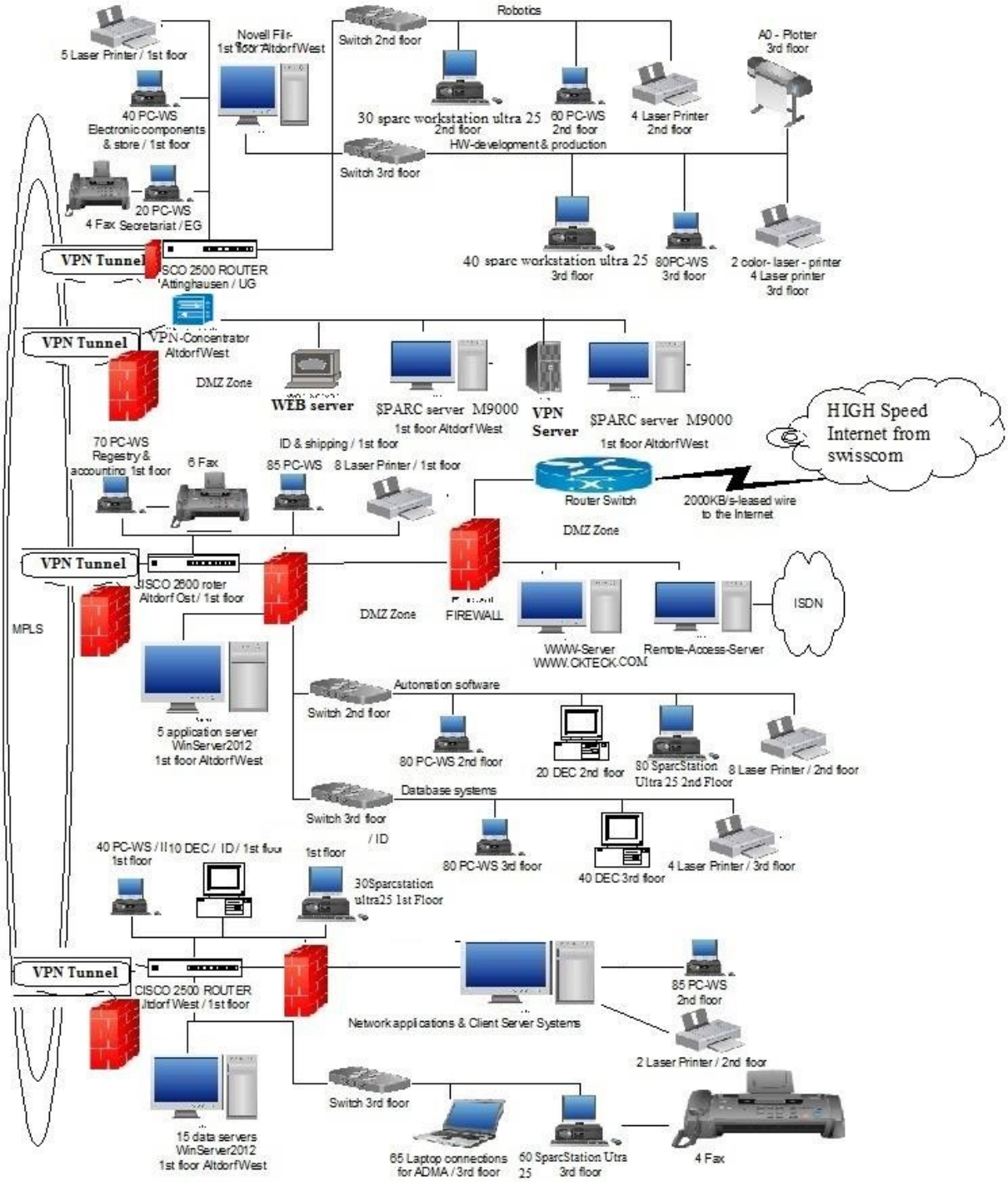


Figure 24: Floor Wise Network Infrastructure of CKTECK's three subsidiaries at Switzerland.

In this section we are going take a look on the network details Novell Filr [104] is now combine with the new technology which is very much suitable for the BYOD in the network infrastructure of CKTECK AG . It is integrated with MobileIron with the help of which the staff of CKTECK can access the file through the Mobile devices and That will possible in secure manner . The Employees can access the file from the servers which is resides inside the corporation . the every access which is performed under the flir that only provides to the authorized persons of the CKTECK AG. While Mobile Iron App Connect keeps managed and personal data separate creating another level of security for IT.[104]"Novell Filr provides file access and sharing, and lets users access their home directories and network folders from mobile devices. Users can also synchronize their files to their PC and Mac computers. They can also share files internally and externally, and comment on files."[105]

In CKTECK AG tunnelling based protocol techniques has been used for transmission control over the data. The Different tunnelling techniques has been followed by the CKTECK network infrastructure. Based on the tunnelling protocol it provides services to the client machines. It also provides protocol based services to mobile devices for communication purpose with security. From author in [**?**] "*This method performs the virtual calling to the virtual port of the VPN server. Because the smart phone VPN client application tries to connect to the AP by connecting the virtual points and to secure the data by 3-way handshaking method, the basic security vulnerability can be removed.*"

## 3.3 Basic Network Security Policy For CKTECK's Network Infrastructure

Network Security Policy is a general document which provides the main rules for any computer network access. The Network Security policy of any Corporation describes the basic architecture of the corporation's network environment. The Network Security policy document provides some specific rules for individuals or groups of individuals throughout the company. The policies can be explained as a set of instructions that could be understood by special purpose network hardware dedicated for securing the network. For writing network security policy for CKTECK, ideas have been taken from [1],[2],[3], [4], [5] [6], A

From[2]

> "*An acceptable use policy is a set of established guidelines for the appropriate use of computer networks within an organization. The policy is a written agreement, read and signed by employees, that outlines the terms, conditions, and rules of the Internet and internal network use for the company. An acceptable use policy helps educate employees about the kinds of tools they will use on the network and what they can expect from those tools. The policy also helps to define boundaries of behavior and, more critically, specify the consequences of violating those boundaries. The policy also specifies the actions that management and the System Administrators may take to*

*maintain and monitor the network for unacceptable use, and they include the general worst-case consequences or responses to specific policy violation situations*"

**PURPOSE:**

The purpose of the network security policy is to prevent the network client workstations at CKTECK could be prevented from the accessing and using services which are outside from those they are authorized to use by implementing controls.

**SCOPE:**

This policy is applied to everyone who is using the systems at CKTECK, information technology resources, and the facilities at CKTECK. This policy is not limited to employees, customers, visitors, contractors, consultants, temporary employees, contractors etc. This policy applies to all information technology facilities, systems and network which are owned, used and controlled by CKTECK Corporation. It is also applied to all third party equipment connections to such facilities, networks and systems at CKTECK.

**STATEMENT OF THE POLICY:**

The network design of CKTECK and all process related to it, should be utilized to restrict the path between network client workstations and CKTECK's computer systems and computing resources. It is just because to reduce the chances for unauthorized access and use.

**DEFINITIONS**

1. *Network Infrastructure:* Network infrastructure is related to the hardware and software resources of an entire network which can be used to create the network connectivity, communication, operations and management of an enterprise network. Network infrastructure of any Corporation provides the communication path and services between users, processes, applications, services and external networks and the Internet. Network infrastructure basically a part of IT Infrastructure .The entire network infrastructure of any Corporation and relate subsidiaries is interconnected, and can be used for internal communications, external communications or both. Any network infrastructure includes:
2. *Networking Hardware:* Routers, switches, LAN cards, wireless routers, cables, etc.
3. *Networking Software:* Network operations and management, operating systems, a firewall and network security applications
4. *Network Services:* T-1 Line, DSL, satellite, wireless, protocols, IP addressing, etc.

5. *Network Computing Resources:* It is any kind of any physical or any virtual component, which has limited availability within any computer system and any network. The internal and external devices which are connected to any computer systems could be memory areas, resources including files or network connections.

**GENERAL RESPONSIBILITIES OF NETWORK ADMINISTRATOR AT CKTECK**

- A network administrator will be responsible for manage and configure network systems.
- He is responsible to monitor logs and events on systems to monitor any security concern.
- He is responsible to monitor & ensure that all systems are backup and running at all times.
- He is responsible to monitor & ensure backup of vital systems and network components.
- He is responsible to monitor the per formance of network and manage bandwidth of network.
- He is responsible to monitor & ensure that internet services are taken from at least two service providers for maximum redundancy specially during disasters.

**GENERAL RESPONSIBILITIES OF THE CISO (Chief Information Security Officer) FOR THE MANAGEMENT OF NETWORK SECURITY AT CKTECK**

The CISO at CKTECK should oversee the internal policies, standards, guidelines, processes, and procedures regarding network security management at the Corporation network. Some of the general responsibilities of CISO at CKTECK in maintaining the network security are listed as following

- CISO should be responsible for Monitor and oversee that scheduled network security testing and controls are in place or not? It is because to alert management of unauthorized attempts
- He should responsible for monitor and work with network managers to implement controls. It is because to ensure the security of information in networks and the protection of connected services from unauthorized access
- CISO should be responsible for monitor and ensure that appropriate logging and monitoring controls are in place to enable recording of relevant events and alerts.

**REFERENCES:**


- CKTECKNP1 Network Security Standards
- CKTECKNP2 Wireless Security Standards

- CKTECKNP3 Firewall Standards
- CKTECKNP4 Remote Access Standards
- CKTECKNP5 Authentication and Authorization Standards
- CKTECKNP6 Role Based Access Control Standards
- CKTECKNP7 Encryption Mechanisms (WEP, WPA1 WPA2, End to End Encryption)

## 3.4 Task Descriptions For Future Students On (1)Network Security Risks Analysis (2)Network Security Policy

This section covers the information related to the tasks descriptions for the students. The students can read overall case study description and then they can accept tasks as challenges. Students can find solutions on the network security related tasks for the MNC and multi subsidiary Corporation CKTECK and similar Organizations. Students have to do two basic tasks.

1. To do Network security risk analysis in advanced technologies(Cloud Networking, BYOD Networking & Social Media Networking) on the network infrastructure at CKTECK Corporation.
2. To find solutions on tasks related to basic network security of CKTECK Corporation.

### 3.4.1 Tasks on Network Security related risks, vulnerabilities and threats in CKTECK's Advanced Network Infrastructure

In the first task, the students must find the overall network security related threats, vulnerabilities and risks in the network infrastructure of Corporation CKTECK. CKTECK provides Wireless network access too for its several employees. After finding minimum 20 risks in each technology (MPLS Networking connectivity, BYOD Networking, Cloud Networking and Social Media Networking), the next task is to find at least 3 countermeasures for each risk.

Task 1 Guidelines have been listed below.

- It must be clear that the risks should be related to the network security only.
- It is clearly shown that CKTECK's network infrastructure consists of BYOD networking, Cloud Networking and Social Media Networking.
- The Network Infrastructure of CKTECK is connected behind the MPLS (Multi Protocol Label Switching) connectivity style, which itself is a kind of advanced and modern style of network connectivity. In MPLS ,in the case of a static route that points to an interface, the CE(Customer Edge) router doesn't need to know any IP addresses of the core network or even of the

PE(Provider Edge) router. This has the disadvantage of needing a more extensive (static) configuration, but is the most secure option. In this case, it is also possible to configure packet filters on the PE interface to deny any packet to the PE interface. This protects the router and the whole core from attack. In all other cases, each CE router needs to know at least the router ID (RID, i.e., peer IP address) of the PE router in the core, and thus has a potential destination for an attack. One could imagine various attacks on various services running on a router. In practice, access to the PE router over the CE-PE interface can be limited to the required routing protocol by using access control lists (ACLs). This limits the point of attack to one routing protocol, for example, BGP(Border Gateway Protocol). A potential attack could be to send an extensive number of routes, or to flood the PE router with routing updates. Both could lead to a DoS (Denial Of Service), however not to unauthorised access.

- Bringing your own devices at job is very common and provides flexible features but can anyone imagine how can this technology can harm the overall network?
- Cloud VPN is also using by several organizations but if not used carefully, it could harm the network of any Corporation.
- Social media is an attractive technology but we need to know that how can it destroy the network devices and can provide loss for the organizations?
- What technique should be followed by the network or system administrator to avoid or protect the overall network architecture from the risk of Misconfigurations?
- What technique should be followed to minimize the risk of "internal" attacks and What type of standard mechanism followed by the organization to face such risks?
- What you will do if we give 12 days to you for network security at CKTECK? For instance you can
  1. Focus on real threats rather than theoretical threats
  2. Focus on finding recently happened network security related incidents
  3. What have been applied after occurring those network security incidents and so on
- Natural Disasters and Physical Security breaches are also big problems itself on the network infrastructure of CKTECK. Students can also find how can it be? What are risks of these problems on the network infrastructure at CKTECK?
- The threats, vulnerabilities and risks picturization is very clear. We are living in modern networked society. In these days, several advanced problems and security related issues have been faced by several Corporations. It is must that the students need to find advanced risks and problems by 2012 and 2013 related to network security only. The students can find advanced security related concerns and issues in for instance related to botnets, advanced malwares, advanced network attacks, network worms, Advance forms of Trojans and rootkits, bluetooth and wifi attacks and so on.
- Students need to find countermeasures for the maintenance of network security at CKTECK. Some of the protection schemes are encryption, network access controls, authentication, and

authorization etc. Students can find advanced forms and versions of theses security preventions which are used in these days.

- Students can work in group of 3. Students can define their work on individual what they have contributed in the whole report. Students can find real examples of risks from organizational surveys. They can make report of 10 to 12 pages maximum with the following sections.
  1. Abstract
  2. Introduction
  3. Goal and Scope of Report
  4. Network Security Risk Analysis and To Find network security related countermeasures for each risk
  5. Conclusions and Findings
  6. References
- Students can take help from SANS, ISO 27001, ISACA, IEEE Xplore, ACM, Springer Link, Science Direct, CISCO and many more.
- Do your job as a designation of Network Analyst for an international multi subsidiary Organization CKTECK. You are hired and the Organization needs your best efforts and approaches.

### 3.4.2 Tasks on Network Security Policy

Having Network Security Policy is important for Organizations but the most important thing is to implement and follow that policy in a right and an appropriate manner. It is responsibility of related persons in any organization to take care of such kind of policy. The basic network policy has been shown in Section 3.3. In 2nd Task the students need to find some solutions for the following questions. The questions are listed below:

1. As a job designation of Network Security Administrator in CKTECK, you need to define your efforts in following areas:
   - How can you establish and enforce policy for transmission of confidential information over the network ?
   - What kind of different techniques you will follow and how? List any three of them.
   - Describe at what level your protection mechanisms are secure?

2. As a network Administrator how will you setup secure servers, routers, switches and other network related devices under the network security policy of CKTECK Corporation. You can also develop password security policy mechanisms for the more security. List some password

management schemes in case of BYOD, Cloud and Social Media network connectivity and explain them.

3. What kind of Network Security related education and training is important for employees in CKTECK? Are these kind of trainings are really important, explain How? What important things should be covered in such type of trainings?
4. As a network Administrator, How will you provide different kind of access control mechanisms for CKTECK's network. You can tell that how will CKTECK's network could be saved from third party access? Describe at which level third parties are allowed to access the CKTECK's network and for which services and purposes?
5. If there is any case of Natural Disasters, what is your role for CKTECK to recover the whole network? What are your pre, during and post plans for network incidents at CKTECK? Describe those plans in following areas:

   - CKTECK's Business Continuity plans in case of network failures
   - CKTECK's Disaster Recovery plans in case of natural disasters
   - CKTECK's Data Backup plans in case of any failure in network

Task 2 Guidelines

You can describe what best efforts you will do for all this. What are your plans and recommendations in such cases described above? Try to describe how will you be responsible for handling such kind of problems.

Students can perform these tasks at individual level. They need to answer at least 2 questions. They need to list what will they do? How will they do? Students should list their findings in a smart report of 8 top 15 pages as a main document. The report can describe:

1. Abstract
2. The Questions which have chosen by students
3. The solutions for the Questions and how they find it?
4. What the students had learned from all this as a conclusion?
5. References used for finding solutions

# 4 Solutions Material for the Students

This chapter will work as providing the solutions material for the task descriptions described in Section 3.4 for the students. It will provide information on the (1)Solution Material For Network Security Related Threats, Vulnerabilities, Risks and Possible Countermeasures in BYOD, CLOUD & Social Media Networking at CKTECK's Network Infrastructure (2) Solution Material For Network Security Policy related tasks. This Chapter is divided into three subsections which have shown below. Section 4.1 & Section 4.2 is related to solution material for the tasks related to Network Security Risk Analysis & its possible countermeasures. Section 4.3 will provide some solutions or training material for the tasks which are related to network security policy in CKTECK.

1. Section 4.1 is about Network Security Related Risks, Vulnerabilities and Threats in CKTECK Network Infrastructure (In Advanced Cloud, BYOD and Social Media Networking).
2. Section 4.2 is about the Possible Countermeasures for maintain the Network Security Related Risks, Vulnerabilities and Threats in CKTECK Network Infrastructure.
3. Section 4.3 is about some hints for finding solutions material related to the Network Security Policy related tasks.

## 4.1 Network Security Related Issues In Advanced BYOD, Cloud and Social Media Networking at CKTECK's Network Infrastructure

This section is about advanced network security related problems (In advanced BYOD, Cloud and Social Media Networking) that concerns with the network security at CKTECK's network Infrastructure.

### 4.1.1 BYOD Network Security Related Issues In CKTECK Network Infrastructure

CKTECK is an advanced corporation with advance network services and their appropriate technologies. The risks related to BYOD networking security in CKTECK has been listed and explained and shown below. Figure 25 is related to the BYOD Network Security related risks, vulnerabilities and threats in CKTECK.

**1. Risks related to Malware[93]:**

Malware are the malicious programs and these can be categorized in different forms as described in[49]. First malware type is Trojan horse, and by this the malicious program the attacker can gain control on the mobile phone. The attacker can also gather secret, sensitive and important

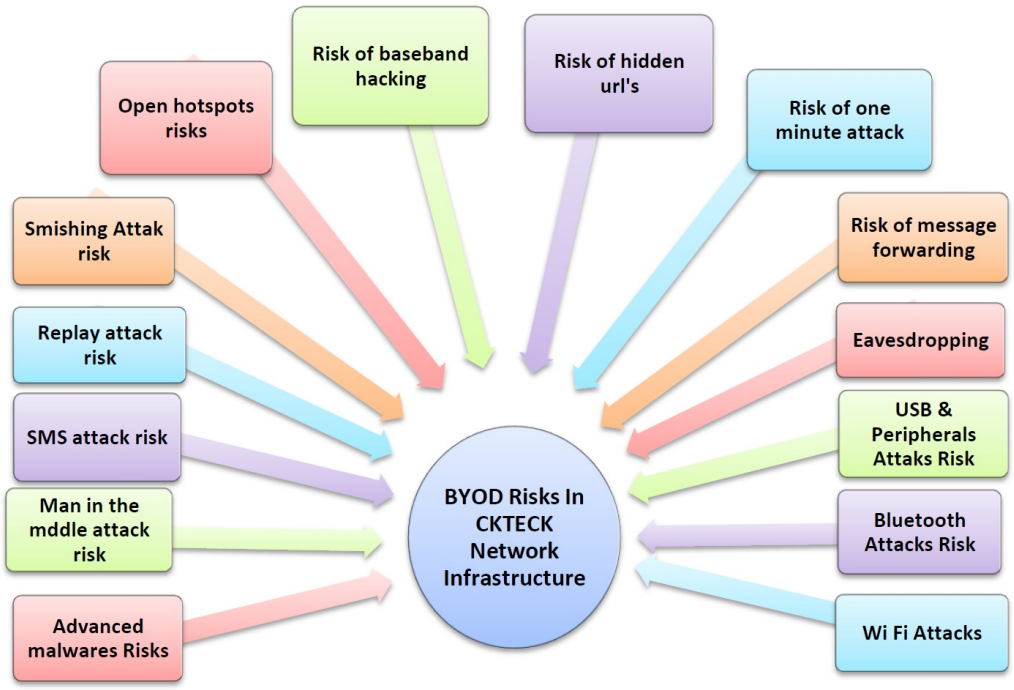


Figure 25: Network Security related issues in BYOD Networking in CKTECK's Network Infrastructure

information. Malware can spread worms, viruses [50] into the whole network of CKTECK. Trojan is very harmful and can be used for phishing activity. For instance "any false banking transaction can gather information. For example, a recent attack that clearly targets end-users is to deploy malware that encrypts their data, and then use this as a basis for extorting money from them" [49]

- **(a) Botnet:**It is a new type of attack. These type of attacks can do bad activities like spamming or denial of service attacks. The example of botnet for mobile devices is waledac [49]. "Waledac uses SMS and MMS messages to exchange the data between nodes, therefore enabling the botnet to remain active even if the nodes are not connected to internet"[49]. Another recent Bot in smart phones are Zeus Bot [71]. Zeus Bot is specially designed for financial crime. It could affect the CKTECK's financial department. It is a network related risk and can collect the configurations and can collect transactions and personal information [71]. Zeus in the mobiles can steal financial data of CKTECK from personal accounts. It can affect the CKTECK's network performance and can destroy the networking functions at CKTECK.
- **(b) Worm:** It is a malicious code which is self-replicating for mobiles, Cabir is the one of the best example of worm types. Another example is Ikee.B which is used to steal financial

sensitive data from the IPhones. Ikee worm [71] on iphones can steal ssh by default. It is a type of password vulnerability which can be distributed on the whole CKTECK's network. Another latest and advanced worm which can be propagated into CKTECK's network is SQL slammer [70]. It is traditional worm which can destroy network servers of the corporation by using internet

- **(c) Rootkit:** Rootkits are the malicious activities which can gain rights in the privileged mode. It is an emerging threat to the mobile users.[49] . CKTECK's network security can be compromised by this.
- **(d) Virus:**Viruses continue to spring up from untrusted market place applications [98]. Viruses are common in mobile phones due to internet over the mobiles phones. Even viruses are attached with emails and can spread in software by opening it. Trojan Genimi [71] ia a recent threat in mobile phones. It can intercept inbound SMS, send SMS, restart packages, Access GPS locations, access browsers history and so on.
- **(e) Spyware:**This is also an dangerous threat to the smart phones. As from [97] spyware collects personal information likes location text message history over a period of time. With this, the attacker has gain physical access to the device. He/she can install software without user's knowledge. "Spyware has risen to become one of the most prominent threats of recent years [50], with IDC analysts predicting the market for anti-spyware products will grow from $12 million in 2003 to $305 million by 2008" [50]. It can infect the whole network of CKTECK and can make ham to the overall corporation's security. Recent example is Mac Spyware, described in [94]

**2. Risk of Man in the middle attack:**

Such type of attacks are common threats to the smart phones. For instance, when we use internet in café bars, airport, and other public areas in which we don't need to use username and password. So in that condition anyone can hack the device and can access or steal our important information [99]. Because CKTECK's employees are allowed to use mobile s at their jobs therefore if the device is defected then it can destroy and make harm the corporation's data.

**3. Risk of SMS Attacks:**

It means if we click on the special crafted message, the malware can spread on phone and gain full control. It is very easy method to infect the phone.[99]. CKTECK's employees can be victim of this attack. It can harm the networking processes in CKTECK too.

**4. Risk of Replay Attacks:**

It is the type of network attack in which transmission of data is repeated by the fraud[100].

**5. Risk of Smishing:**

It means short text messaging on phishing attacks. Smishing use text messages to impress victims a fake bank or credit card company. When the customer calls the texted number then it records customers account number and password by cheating. [99]

**6. Risk of Open Hotspots:**

Many owners of smart phones create instant hot spot so that their smart phones get online but by this hacker may be get gain to our connection and further communications.[99] . Wi fi Hijacking [99] is a related threat, when the employee of any company enters into open hotspot then by the attackers it is possible to steal secret information on the device. Information could be personal or CKTECK's emails credit card information etc. Smart devices can be compromised with malwares or viruses infection. When again these devices will enter and connect to CKTECK's personal network then it can affect the whole network.

**7. Risk of Baseband Hacking:**

It is a method by which an attacker can easily intercept the cellular calls at CKTECK, basically in this technique in which vulnerabilities exploits is in the chips and firmware which are used in the iPhones and Android-based smart phones. By the help of such kind of attacks, the attacker can easily eavesdrop on the conversations at CKTECK. They can use the phone's baseband processor to turn it into a listening device. The attacker should have can create a false or artificial network towers [99]. It can breach the CKTECK's network and can compromise network security at CKTECK.

**8. Risk of Hidden URLs:**

Whenever we are discussing about the hidden URL's first of all need to more concentrate over the text messages, there is a service such as Bit.ly. Which make Face book and tweeter URL's shorter. By taking the advantage from shortened URL's are being used to hide malicious sites and software, leading surfers astray to porn sites, spam pages and worse[99]. These malicious sites can infect the network of CKTECK and can result in financial and reputation loss too.

**9. Risk of The One-Minute Attack:**

The meaning of this type of attack is simple. In this the attacker gains advantage from the smart phones always on nature. In this the attacker attack quickly and then easily get out from it without the knowledge of user of CKTECK. It can work If the user at CKTECK hasn't awareness about the attack. "That's the idea behind Android.Spyware.GoneSixty.Gen , recently discovered by Bit defender. When once it is installed on a phone, then it sends all messages, recent calls, browsing history and other information to a remote location and then uninstalls itself. All this takes place in less than 60 seconds."[99] . It can spread infections into CKTECK network and can steal data. Hence network security of CKTECK can be compromised.

**10. Risk of Message Forwarding**

In this type of technique the attacker can easily get access by guessing the weak passwords such as childhood address, pets name, wife first name, elder son name and so on. There was an Example ,Florida man got hold of those compromising pictures of Scarlett Johansson . A weak password based on some personal information can make possibility for a hacker to hac into the Hollywood star's email account and then set it to automatically forward all incoming and outgoing emails to him. Researchers say hackers are now focusing on using the same technique to hack into smart phones in order to extract important corporate data and industrial secrets" [99]. This could be occurred in CKTECK too.

**11. Risk of Eavesdropping**

This is threat in which someone listens into the conversation or data steal secret information by using CKTECK's network. A 3G call can also be eavesdropped as described in [72] "if connected to a GSM base station and an encrypted 3G call can be recorded and decrypted later after intercepting a 2G call on the same handset, because of a known key vulnerability"

**12. USB and other peripherals risks to Corporation CKTECK's network [49]**

Mobile devices or other personal devices could be compromised by using other connections, like widely spread USB. When the software used to synchronize the mobile device or any other personal device is compromised, then the attacker can access private information and install malicious applications on the devices. When these devices will connect to CKTECK's network and other devices at CKTECK Network, then it can destroy other device's data at CKTECK's network. Moreover it can affect the network security of CKTECK Corporation.

**13. Bluetooth attacks:**

[49] Bluetooth can spread malware from one device to another device of different employees. It can inject CKTECK's networks by spreading malicious codes and applications. It will result in slow network processing, network infection, bad network performance and bandwidth, network crash, stop network's function and so on. When two devices are in range, the compromised device pairs with its target by using default Bluetooth passwords. Bluetooth snooping attack comes under Bluetooth attacks. Bluetooth device-pairing default passcodes for smartphones are usually "0000" or "1234." Many users never change the defaults. By this an attacker can crash the devices by using Bluetooth signaling. It can also affect the CKTECK's network infrastructure. [99]

**14. Wi Fi Attacks:**

These are emerged due to the wireless network. There are several wi fi related attacks which can harm the CKTECK Corporation's wireless network for example [7] Identity theft attacks, Man in the middle Attacks, Caffe Latte Attacks, Denial of Service attacks, network injection attacks and

so on.

### 4.1.2 Cloud Network Security Related Issues In CKTECK Network Infrastructure

Cloud technology is a part of whole CKTECK Corporation. Advanced technology cloud is also susceptible to several network related risks in the whole organization. Hence the risks related to network security of CKTECK in cloud has been listed and explained below. Ideas have taken from [23], [24], [30], [35], [36]. The risks are under the three layers in the cloud network. Table 2 shows the cloud networking Problems and issues in CKTECK's network Infrastructure. According to the author in [31], there are several security and availability issues as recent incidents at the major public cloud provider AmazonWeb Services.

**1. Risk of insufficient networking environment for unauthorized changes**

If the employees are unknown or careless or not able to do design and maintain the proper sufficient networking environment in cloud network then there is always a risk to the whole network of CKTECK.

**2. Risk of insufficient implementation of best security policies for the installation and configuring the cloud network**

CKTECK's network infrastructure and its services are under risk in this condition too.

**3. Risk of ensuring the CIA**

(Confidentiality, Integrity, and Availability) of CKTECK's cloud network and the data in the transits to and from a public cloud provider

**4. Risk of ensuring proper access control**

like AAA (Authentication, Authorization, and Auditing) to the resources which are used at the CKTECK's public cloud provider

**5. Risk of the availability of the internet related resources in a public cloud which is used by CKTECK**

which can lead in making harm to the entire CKTECK's network infrastructure by leaking company's information.

**6. Risk of replacing the established model of the CKTECK network zones and tiers with domains of the whole CKTECK Corporation**

is itself a big risk. It is because when technology changes.

Table2

| Risks in several layers in Cloud network in CKTECK | | | | |
|---|---|---|---|---|
| Sr. no | Service level cloud network | Layers of cloud network system | Users at different layers | Risks related to Network Security In Separate layers of CKTECK's Cloud Network |
| 1 | Application Level | Saas (Software as a service) | End Users | • Risk of impersonation attack in CKTECK's network<br>• Risk of session hijacking attack in CKTECK's network.<br>• Risk of interruption of CIA and AAA services related to CKTECK network<br>• Risk of unavailability of internet resources in CKTECK network<br>• Risk of breaches in privacy of data in the CKTECK network<br>• Risk of phishing attack in CKTECK's network<br>• Risk of Zeus Trojan botnet attack in CKTECK's network.<br>• CKTECK's Virtualization vulnerabilities risk<br>• Dos and DDos risk in CKTECK's network<br>• IP spoofing in CKTECK's network<br>• ARP spoofing in CKTECK's network<br>• DNS positioning in CKTECK's network<br>• Session riding attack in CKTECK's network<br>• Risk of SQL and OS injection at CKTECK's network<br>• CKTECK's SSL certificates spoofing<br>• CKTEK's Browser cache attacks<br>• Zombie attacks at CKTECK's network due to insecure browsers and API's vulnerabilities<br>• Metadata spoofing attack at CKTECK's network<br>• Backdoor channel attacks risk at CKTECK's network<br>• Side channel attack risks at CKTECK's network<br>• CKTECK's network's Port scanning attacks |
| 2 | Virtual Level | Paas(Platform as a service) | Developers | • Risk of Impersonation at CKTECK<br>• Risk of Dos attack at CKTECK's network<br>• Risk of DDos attack at CKTECK's network<br>• Risk of programming bugs at CKTECK's CLOUD network<br>• CKTECK's Connection flooding risk<br>• Communicational errors risks at CKTECK's network<br>• Side channel attacks at CKTECK's network<br>• Backdoor channel attacks at CKTECK's network<br>• Risk of software modification at CKTECK's network |
| 3 | Physical Level | Iaas and centre of data (Infrastructure as a service) | CKTECK infrastructure users | • Risk of theft of cloud hardware in CKTECK.<br>• Risk of all networking attacks at CKTECK's network<br>• Risk of interruption of CKTECK's hardware<br>• Risk of CKTECK'S hardware malfunctioning<br>• Risk of theft of hardware by insiders of CKTECK<br>• Risk of modification of cloud networking hardware by malicious CKTECK's insiders<br>• Risk of natural disasters at CKTECK's network<br>• DDos attack at CKTECK's network<br>• Risk of poorly configured virtual machines at CKTECK's network<br>• Risk of poorly designed and configured CKTECK cloud network design<br>• Risk of insecure implementation in CKTECK network infrastructure |

Table 2: CKTECK's Cloud Network Security related risks in different layers of cloud

**7. Risk of phishing attack by hackers**
which can steal the secret credentials of the organization CKTECK.

**8. Risk of improperly configured Virtual Machines**
which can give chance to the attackers to get access to the host machines of the CKTECK.

**9. Risk of Zeus botnet Trojan**
can affect the availability of network related services in CKTECK.

**10. Risk of Denial of service attack**
can also affect the entire network. It could make the CKTECK's network unavailable. Denial of service attack is when attacker can cause unavailability of network service by attacking to a single server. It can also affect other related network related services. With this attack the servers are not able to perform its tasks.

**11. Risk of getting control on the guest operating system of CKTECK by an attacker**
because operating system virtualization has multiple guests running according to the configuration criteria of the cloud network.

**12. Risk of cloud computing virtualization vulnerabilities**
It can compromise the entire control of guest operating system of CKTECK. An attacker can perform cross VM side channel attacks and denial of service attacks.

**13. Risk in virtual layer in cloud**
can be very harmful for the CKTECK because the attacker can modify the installed hypervisor and can gain the control on the hosts of CKTECK.

**14. Risk of man in the middle attack**
in cloud network could be harmful for the entire organization's network. Man in the middle means when the attacker is able to access the data communication of CKTECK's network among the data centers. It could be performed by using internet protocols. Some other similar related risks are

- IP spoofing
- ARP spoofing
- DNS positioning

**15. Risk of HTTP weakness of cloud network**

can be victim of “session hijacking” and “session riding” attacks at CKTECK.

**16. Risk of unauthorized access to CKTECK’s data**

because of there is higher number of administrators and users available in cloud network.

**17. Risk of cloud network vulnerabilities**

like SQL injection, Operating System injection. Attackers can disclose application components of CKTECK by using this. It could be happen due to the reason of defective design and architecture of the applications of network infrastructure.

**18. Risk of cloud vulnerabilities in browser and APIs**

It can result in SSL certificates spoofing, browser cache attacks on the mail accounts of the CKTECK Corporation. Insecure APIs can also affect the availability and the security of the CKTECK’s network and its services.

**19. Risk of Zombie attack can be very harmful for the overall network and service of CKTECK**

It can flood the network by sending requests from the innocent hosts in the network. These hosts are called “Zombies”. An attacker can flood large number of zombies. It can affect the behavior and availability of the cloud services in CKTECK network infrastructure. Cloud network could be overloaded by denial of service (Dos) and distributed denial of service (DDos) to the servers of CKTECK. Distributed denial of service attack is when the whole cloud network system got full loss and is not able to handle any service request. DDos is an advanced form of Dos attack.

**20. Risk of metadata spoofing attack**

It is when the attacker is able to change the WSDL. WSDL is the web services description language in any organization. By this the attacker is able to interrupt the service innovation code from WSDL file at the delivering time.

**21. Risk of phishing attack**

is very harmful for the entire CKTECK. It can redirect a user into a false link for getting sensitive data. It can hijack accounts and other services of cloud network of CKTECK.

**22. Risk of backdoor channel attacks**

can compromise the virtual machines can affect the availability of the private data of the CKTECK.

**23. Risk of Ports Scanning is very dangerous risk for entire cloud network of CKTECK**

Port scans are continuously used by both worms and human attackers to probe for vulnerabilities in Internet facing systems [73]. Attackers perform port scan attacks because they want to enter in the system [74]. To understand the systems, to steal secret information, to do malicious activities with the systems and so on can be the main goals of the attackers.

> *"A port scan is an attempt by the attacker to find out open (possibly vulnerable) ports on a victim machine. The attacker decides to invade the victim, through a vulnerable port, on the basis of the response to a port scan. These port scans are usually very fast and hence an attacker can take control of a major proportion of the vulnerable machines on the Internet in a small amount of time[75]"*

**24. Risk of impersonation attack**

(By this attack the integrity can be compromised. It can be done by obtaining unauthorized access to a wireless network and its devices [8]) on CKTECK'S network.

**25. Risk of Theft of cloud hardware**

It could be possible in CKTECK by employees or others.

**26. Risk of misuse of cloud hardware and modification of cloud hardware by harmful CKTECK's insiders**

can also happen in the CKTECK Corporation.

**27. Risk of natural disasters to the cloud hardware and entire cloud network system at CKTECK**

can destroy the whole network of CKTECK

**28. Risk of interruption of cloud hardware in the CKTECK organization**

can lead problems for CKTECK's network.

### 4.1.3 Social Media Network Security Related Issues In CKTECK Network Infrastructure

Social media networking services are considered as advanced technologies in CKTECK network system. Facebook, Linkedin, Twittter ate three commonly used networking sites by the employees of CKTECK organization. Therefore risks in social media networking on entire CKTECK's network and platform have been listed and described as following [86] [90] [91] [92] [95]. These risks have been shown clearly in Figure 26.


Figure 26: Network Security related issues in Social Media Networking in CKTECK's Network Infrastructure

**1. Risk of impersonation attack on CKTECK organization**

can create false user profile by compromising the network communication. It could be in the form of falsifying username, personality, gender, age. Social networking sites are susceptible for this type of attack.

**2. Risk of message manipulation attack in CKTECK**

Social networking sites like face book and twitter can cause this attack on CKTECK enterprise by compromising its network communication. It can result in spreading malicious rumors, false propaganda.

**3. XSS (Cross site scripting attack) on CKTECK**

It can cause by using face book in the enterprise. It can result in launching of self propagating spams and worms in the entire network. CKTECK employees are using mobile face book which have vulnerability of insecure API by insufficient javascript validation. XSS is also possible when the web browsers of systems in CKTECK execute malicious codes. After that it can steal personal information of users, it can also launch attack against third party by the employees side without their knowledge.

**4. Risk of Spreading viruses and worms to the whole network of CKTECK**

is always present in case of using face book and twitter social networking sites. Malware affected systems make malicious to other connected systems. And as an advanced organization CKTECK is using internet related services in entire network. Malware can also steal money. It can send expensive messages and can turn CKTECK's devices into mini botnets.

**5. Risk of Facebot and related attacks**

can affect the network performance of CKTECK. It can target the servers of the entire CKTECK network by flooding it.

**6. Risk of Dos and DDos attacks**

is very harmful. It can harm the working process of the network of CKTECK by flooding the network. It can degrade the network performance.

**7. Risk of CSRF Attack**

Cross site request forgery attacks can force users of CKTECK to install malicious applications on the network and it can result in network exploits. It can cause the authenticated browsers too. It can compromise the users data, entire network communication and the servers of CKTECK.

**8. Risk of Phishing attack**

is also there in CKTECK while using face book. It can send phishing messages on the organization's network. It can obtain login details, accounts and then send malicious messages to other devices on the network.

**9. Linejacking attack risk**

is always possible while using social networking sites. When the user or any employee of CKTECK click on invisible malicious link then the attacker can spread and identify malware mechanism. It can propagate harmful worms in organization's network and can exploit in network communications and integrity of data.

**10. Risk of diminishing CKTECK network's bandwidth**

could be possible by using social networking sites. It is because social networking sites consume more bandwidth by video conferencing, videos watching on you tube for example. Hence it can degrade the overall network performance.

**11. Risk of spreading flashback Trojan**

while using smart phone with social networking sites is possible in the CKTECK. Flashback Trojan is designed for operating system platform of mobile devices. It can affect the OS platform and other network devices which are connected via a common network in the enterprise CKTECK.

**12. MAC Spyware Risk**

This spyware comes from java file and can operate at kernel level. Social networking sites are capable of producing this type of risk in the CKTECK. It can intercept mouse movements, instant messages communications, compromise video calls, open webcam, open backdoors in the CKTECK enterprise.

**13. Risk of Spear Phishing Attack**

is also possible on the CKTECK network while using social networking sites. This attack is victim of spreading RAT's (Remote Access Trojans) over the entire network of CKTECK. It can penetrate the cryptographic procedures.

**14 Risk of Brute Force Attack**

By using social networking sites the employees of CKTECK are in under this risk. It can gain insufficient control on the authentication control. It can also compromise the systems of the entire organization.

**15. Risk of information leakage**

is possible with the use of social media. It can inject the CKTECK network and network devices with injection attacks like XML attacks. Hence the secret information can be leaked to attackers.

**16. Risk of Automation attacks**

can be there in place by the use of social networking sites in CKTECK It can run the automated generated queries can retrieve large amount of data on the CKTECK's network.

## 4.2 Possible Countermeasures for Network Security Related Issues In Advanced BYOD, Cloud and Social Media Networking at CKTECK's Network Infrastructure

This section is about countermeasures for network security related problems (In advanced BYOD, Cloud and Social Media Networking) that concerns with the network security at CKTECK's network Infrastructure, which have been described in the previous Section 4.1 .

### 4.2.1 Possible Countermeasures against BYOD Network Security Related Issues In CKTECK Network Infrastructure

For CKTECK's BYOD Networking Related Risks, some of the countermeasures have been listed below. Ideas Have been taken from [69],[71],[55],[56],[53],[54],[9],[98], [8]. The ideas for several countermeasures are found from A B C D also to some extent.

**1 Advanced Malwares**

- Use of NAC(Network Access Control) mechanisms which provides automatic intrusion detection and prevention, anti viruses, anti malware, anti spyware protection etc to the smart devices at CKTECK.
- Use of updated antivirus in CKTECK's devices.
- Use of smart security software solutions for automatic blocking of infectious applications from outside network.
- Strong encryption mechanisms on CKTECK's email system.
- Hardening the CKTECK's devices firewalls, ports, services, users and groups.
- To do Centralized management system of CKTECK's smart device firewalls so that it can't be visible to the internet and the attacker.

**2 Man In The Middle**

- Use of wireless IDS and IPS.
- Use of strong encryption mechanisms on CKTECK's network.
- Use of Hashing MAC(Message Authentication Codes), to secure CKTECK's network
- Secure Guest network access of CKTCEK's network.

**3 SMS Attacks**

- Apply encryption mechanisms on CKTECK's smart devices memory and storage.
- Use of smart security software solutions which automatically can detect and block the bad applications.
- Apply encryption on CKTECK's email system.
- Restrict employees of CKTECK for applications downloading.

**4 Replay Attacks**

- Use of device authentication mechanisms.
- VOIP traffic at CKTECK must be encrypted.
- Wi Fi Traffic at CKTECK must be encrypted.
- User can't bypass VPN, it should be secure enough.

**5 Smishing Attack**

- Provide Education and training to CKTECK's employees
- Train them by giving awareness programs regarding network related threats and harm effects of these threats.
- Encryption mechanism on CKTECK's email system.

**6 Open Hotspots**

- Network Security training, education and awareness.
- Disabling Wi Fi options when devices are outside from CKTECK.
- Device encryption mechanisms.
- Strong Passwords mechanisms.
- Smart solutions for automatic detection of malwares and other harmful applications from outside.

**7 Baseband Hacking**

Use of BYOD NAC(Network Access Control) solutions, which provides

- Limited Access Zones.
- Support wired and wireless LAN.
- Limit Access according to user's role.
- Provides SSL VPN
- Restricts Access to unknown applications and data.
- VOIP and Wi Fi traffic encryption.

**8 Hidden URL's**

- Awareness, Training and Education to CKTECK's employees
- Security related guidance to CKTECK's Employees.
- Instruct and teach strictly not to click on any links while using social media.
- Use of mobile device management tools.
- Restriction on Applications downloading.

**9 One Minute Attack**

- Mobile Device Management Tools.
- NAC Mechanisms Tools.
- SSL VPN.
- Two way Authentication.
- Restriction on application downloading.

**10 Message Forwarding**

- Device Level Encryption Protection to protect data at OS level.
- Restriction of residing sensitive data at rest on the mobile devices.
- Treat mobile device as GUI dump terminal and then traffic encryption.

- Encryption on CKTECK's email system.

### 11 Eavesdropping

- VOIP Encryption
- Role Based Access Control Mechanisms
- Wi Fi Encryption Mechanisms

### 12 USB and Peripherals

- Data Permission and Access is aligned within the data classification.
- Two Way authentication Factor.
- Strong password and should be expires in a limited time.
- Data accessibility and permissions should be within job functions and data classification.

### 13 Bluetooth Attacks

- Strong Encryption Techniques.
- Strong bluetooth passwords.
- Disabling bluetooth options to anyone.
- Devices bluetooth should be off. It should be on according to employee's request.

### 14 Wi Fi Attacks

- Hide and Change CKTECK's Network SSID
- Strong end to end Encryption WPA1 and WPA2.
- There should be strong password for CKTECK's Wi Fi Router Admin.
- To Enable CKTECK'S router Firewall.
- Use of SSID (Service Set Identifier) hiding process.
- Use of Static IP Addressing
- Use of WEP(Wired Equivalence Privacy)

- Use of MAC ID Filtering, Means to only allow access from known pre-approved MAC addresses
- Disable auto connect option.
- To give instructions to CKTECK's employees not to use open hotspots.
- For remote access at CKTECK, there should be use of VPN or IPSEC.
- There should be WPA2 protection scheme or better for CKTECK'S network to maintain network security.
- Use of Network Access Control rules for maintaining better network security at CKTECK.
- Use of Smart cards, USB tokens, and software tokens
- Use of WIPS and WIDS(Wireless Intrusion Detection and Prevention Systems)
- Use of Access Control Policies like Role Based Access Control policies at CKTECK network infrastructure which includes Allow some applications to users for instance emails, calendar, contracts etc. It also includes to block access to CKTECK's intellectual property and data.

### 4.2.2 Possible Countermeasures against CLOUD Network Security Related Issues In CKTECK Network Infrastructure

For CKTECK's CLOUD's Networking Related Risks, some of the countermeasures have been listed below. Ideas have been taken from [18][14][20][22][23][24][28][35][36][37][76] [40]. Moreover interview questions answers A B C D also helped in finding countermeasures.

**1 Risk of Insufficient Networking Environment of cloud in CKTECK**

- CKTECK should implement best practices for network installation and configuration.

**2 Risk regarding insufficient implementation of best security policies**

- Best practices and network security policies for the security of CKTECK network security should be implemented, configured and installed.
- Vulnerability Scanning and configuration audits
- Service level agreements should be there for patching and vulnerability remediation.

**3 Risk of ensuring proper CIA**

- Internet availability should be essential for cloud network's availability.
- There should Role based Access Control Mechanisms
- Authentication and Authorization Mechanisms
- Two factor Authentication Mechanisms
- Encryption Mechanisms at several branches of CKTECK

**4 Risk of improper Access Control**

- There should be use of network level access controls

**5 Risk of the availability of the internet related resources in a public cloud which is used by CKTECK**

- There should be use of Network Intrusion detection systems and intrusion prevention systems.

**6 Risk of replacing CKTECK's established Network**

- Updation of patches should be in proper and regular basis at CKTECK
- There should be security audit reviews
- Updations of network Level gateways, firewalls, NIDS, NIPS
- Updated antivirus should be used

**7 Phishing**

- Spam emails should be identified

**8 Improper Configured VMs**

- Virtual machines should be designed and configured in a proper way.

- Use of NIDS and NIPS
- An agent based business aware incident detection system for cloud environments can be used.

**9 Zeus Botnet**

- Use of latest antivirus and patches
- Use of NIDS, NIPS
- An agent based business aware incident detection system for cloud environments.

**10 Denial of Service attack**

- Use of network level access control mechanisms
- Use of NIDS, NIPS etc.
- An agent based business aware incident detection system for cloud environments.

**11 Operating System Access by an attacker**

- Role based Access Control Mechanisms should be used.
- Effective data classification schemes should be there.

**12 Virtualization Vulnerability**

- Use of Network level intrusion detection systems
- Use of cloud based IDS and IPS
- Use of secure hyper vision
- Activities at Hyper vision should be monitored properly
- Virtual Machine Isolation should required

**13 Virtual Layer risks**

- Use of Network Access Control Mechanisms

- Use of NIDS and NIPS
- Use of proper SSL configuration schemes
- Data communication testing should be there between authorized parties

**14 Man in the middle**

- Use of IDS and IPS
- There should be strong two factor Authentication
- There should be prohibitation of account sharing credentials between users and services
- There should be strong security policy and activity monitoring shemes

**15 HTTP weakness**

- Use of NIDS and NIPS
- Use of cloud based IDS and IPS
- VM images should be kept up to date with security patches

**16 Unauthorized access**

- Use of NAC mechanisms
- There should be proper strong authentication, authorization, accounting, control mechanisms for administrative access and operations

**17 Cloud network Vulnerabilities**

- For API , there should be followed of strong authentication mechanism with encryption.

**18 API and browser's vulnerabilities**

- Integrity checking modules should be updated and implemented
- There should be strong isolation between Virtual Machines
- Proper use of hashing mechanisms

- Web browsers and API's should be secured by using network security control mechanisms

**19 Zombie attack**

- Use of NIDS, NIPS
- Better Authentication
- Better Authorization

**20 Metadata spoofing**

- Strong authentication and authorization
- Applications should be kept in encrypted form

**21 Phishing**

- There should be proper identification of spam emails

**22 Backdoor Channel Attack**

- Better Authentication and authorization
- Strong isolation between Virtual Machine Images

**23 Port Scanning**

- Port Scan Mechanisms
- Network IDS and IPS
- Application Based, Host Based and Network based IPS and IDS
- Use of firewalls and gateways

**24 Impersonation**

- For identity security, there should use of strong authentication and authorization
- There should be strong passwords

**25,26,28 Theft and misuse of cloud hardware**

- Role based Access control Mechanisms
- Classification of information according to level of authority
- There should be proper job description, roles and responsibilities of each employee
- Restriction of security areas in CKTECK
- Strong Authentication
- End to End encryption

**29 Natural Disasters**

- Recovery can be done by backing procedures in virtual machines
- Recovery can be done by backing the templates on Virtual machines in cloud storage. It can be proceed by on demand during disaster recovery from the templates.
- Data storage on multiple locations
- Recovery and backup plans in advance
- Business continuity plans for cloud failure like redundancy and automation

### 4.2.3 Possible Countermeasures against Social Media Networking Security Related Issues In CKTECK Network Infrastructure

For CKTECK's SOCIAL MEDIA NETWORKING Related Risks, some of the countermeasures have been listed below. Ideas have been taken from [89] [95] [92][52]. Interviews A B C D were also helpful for finding countermeasures.

There are some common countermeasures and schemes which can help in maintaining the security from Social Media Networking threats, risks and vulnerabilities to some extent. The countermeasures for social media networking related threats and vulnerabilities have been shown in

the following Figure 27 and have explained further too.

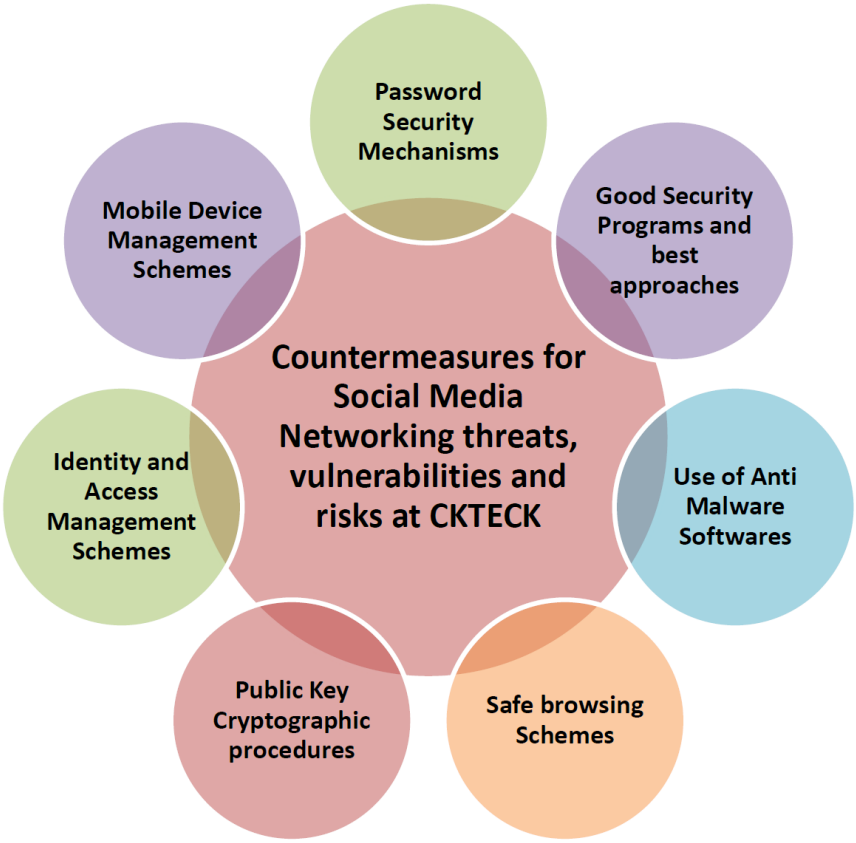


Figure 27: Security Mechanisms against Social Media Networking Problems and issues for CKTECK network Infrastructure

**1. Password Security Schemes**

- Use of strong passwords
- Use of different passwords at different sites
- Use of different passwords for different accounts
- Not write down password on a sheet near ur PC
- Use of encrypted database for passwords storage
- Change old passwords regularly

**2. Good Security Programs Schemes**

- Safe message handling technologies should be used
- Safe message handling technologies can mitigate phishing, XSS and CSRF attacks
- There should be good security practices and programs. For instance not to click on suspicious links, don't answering the unknown emails, not to respond infectious messages, infectious messages should be disgarded, not to click on sites via a third party, visiting to sites directly which helps in mitigation of XSS attack.

**3. Anti Malware Softwares Schemes**

- It mitigates the phishing attack on network
- It mitigates the risk of damaging network and its bandwidth from viruses, spywares, botnets, facebots, malwares etc.
- It provides safety and security to users machines which may be compromised from the future attacks.
- It can mitigates the threats which are related to the integrity of the information
- Antivirus software should be updated time to time
- Use of firewalls, application gateways, IDS, IPS to protect the network from outside attacks.
- Use of content aware firewalls

**4. Safe Browsing Schemes**

- It protects the network from CSRF and XSS attacks related to network.
- It protects the network from automated attacks
- There should be installation of desktop firewalls
- There should use of Application firewalls, NIPS, Web content filters, Application Layer proxies
- There should be use of automated vulnerability scans mechanisms
- There should be proper review of manual codes
- There should be use of secure web gateways

**5. Public Key Cryptography procedures**

- It provides secure network connection and communication.
- It can be used with MAC(Message Authentication Codes)
- There should be used device level encryption mechanisms

**6. Identity and Access Management Schemes**

- Use of Identity Servers which can confirm the authorized identity
- Use of anonymous identifiers with cryptographic hashing procedures.
- While using bluetooth or Wi Fi, there should be use of anonymous identifiers in between two devices.

**7. Mobile device and other device management Mechanisms**

- Individual Virtual Servers should be used for long term availability.
- Use of strong authentication and authorization schemes for mobiles
- Biometrics with mobile devices can be used

## 4.3 Solution Material For Network Security Policy related tasks

This section provides the hints for the solutions on tasks related to network security policy which have been described in Section 3.4.2. This is the solution hints for Task No. 4.

**Task 4:**
As a network Administrator, How will you provide different kind of access control mechanisms for CKTECK's network. You can tell that how will CKTECK's network could be saved from third party access? Describe at which level third parties are allowed to access the CKTECK's network and for which services and purposes?

**Solution Hints For Task 4:**

1. Access Control Mechanisms are Several Authorization Mechanisms on the CKTECK network. Students can write about several authorization methods for instance role based, device au-

thorization, physical access control and so on. Student can divide the several areas according to public, private and sensitive zones. Students can implement plan for different roles for different authorities at CKTECK. Moreover they can apply mobile device management schemes on CKTECK's network. Students can also implement proxy based internet and its services.

2. For the security of third party access students can apply role based access controls, physical access based controls. Bluetooth access controls, Network Access controls to the logs. Students can define their own structure and plan with the use of these techniques.
3. These are the hints for the solution, students can find solutions according to their wish and their own thoughts. Students are free to find and approach other related methods.
4. For making the report, students should make half page of abstract showing the overall job.
5. Introduction part of the report should explain the brief introduction for the overall process. It can include which questions students have chosen, why they have chosen the questions? Moreover they approached to solve these questions? It could be from 1 to 3 pages
6. Main part should include solutions for the questions and the methods used for it. It can include 5 to 8 pages.
7. Conclusions by the students should be mentioned after this including half page.
8. In the end, all the references should be listed used for the whole research.

# 5 CKTECK's Network Security Management Concepts and Plans

This section is about, the network security related mechanisms. Network Security mechanisms [109] are the secure network designs. These are the network security related mechanisms, have been shown below:

- Authentication
- Authorization
- Accounting
- Encryption
- Application Security
- Web Security& Email Security
- Disaster Recovery & Business Continuity Planning
- Physical Security, Hot Swap to second site and Backup Procedure

The author have described these networking management concepts in such a way that the students can learn that what actually these are and then the students can proceed further on it in finding the solutions for List of Potential Projects 6.2. In the chapter, there are some hints described by the author for the students, so that the students can take help from these hints to apply these mechanisms on CKTECK AG. This chapter will work as a hints and ideas for the solutions of List of Potential Projects 6.2. The solution hints are followed from [109] A B C D.

The students can apply these mechanisms on the several subsidiaries at CKTECK AG. In this way the students will be able to learn that how actually these network security mechanisms can be applied to design a secure network. Moreover this educational tool will help the students to learn from it and to proceed further projects in the future too.

## 5.1 Authentication

Authentication is the process in CKTECK AG is of claiming who is requesting network services at CKTECK. Authentication can be referred to authenticate the users, devices or the other services of the software at CKTECK. Authentication process at CKTECK can be achieved by using several

schemes:

- By implementing some routing protocols that support route authentication ( a router must pass some criteria before another router accepts its routing updates)
- By using a valid login ID and password, that should be authenticated by a security server.
- By applying one time passwords schemes, authentication could be applied on the CKTECK's Network. (Example for this is smart cards which is combination of pin and one time password)
- By applying two-factor authentication, which needs a user to have two proofs of identity. For instance access control system that needs a security card and a password. It is a better scheme. With the one proof only, the system can't be compromised. The malicious persons need to compromise both proofs. We can say if any bad person find security card, he can't compromise the system with the use of this card because he needs passwords too. In the same manner if the bad guy have only password, then he can't do anything without the security card. Hence the security is depending on two proofs.
- By using digital certificates and the biometrics.
- By using strong firewalls
- By applying VPN authentication
- By applying ESA(Enhanced Subscriber Authentication) on BYOD
- By applying Packet Filtering Mechanisms

## 5.2 Authorization

The authentication is about who is accessing the network. The authorization is to grant privileges to processes and users at CKTECK. Authorization is the process of providing several access controls according to the designation and requirement of the employee. Authorization is applied so that a network security administrator can control several parts of a network (for example, directories and files on servers). Authorization can be different to several users. For instance Network Administrators at CKTECK should have different permissions and access controls. But a normal employee at CKTECK should not have permissions on all files. Authorization can be implemented at CKTECK's network by implementing following concepts:

- Device-specific authorization should be implemented, in case of BYOD. Only approved devices should be allowed for office work. Private devices should be used in personal matters only.
- By providing different role based access controls to different positions of employees at CKTECK.
- Enabling of proxy based internet to normal employee at CKTECK in order to restrict from the use of social networking.
- Users at CKTECK should not have admin access on their machines.

- Wi-Fi and Bluetooth access should be disabled to many systems at CKTECK.
- VPN client should be allowed on BYOD, only allowed on authorized devices.
- It BYOD is allowed to managers then at some level for instance only in non sensitive environments.
- By applying packet filtering.

## 5.3 Accounting

The main purpose of the term accounting at CKTECK AG is to analyze the security of CKTECK's network and to respond to security incidents at CKTECK network. To maintain and establish the accounting procedures at CKTECK, some following questions should be answered

- How to collect the information about network related activities?
- How Network at CKTECK can be designed with strict security policies?
- How to get information regarding audit data? that should be achieved by attempting the authentication and authorization by any person at CKTECK's network.
- How to log the data of guest access to public servers and all attempts by users to change their access rights?
- How to collect the data regarding user and hostnames for login and logout attempts, and in case of changing in access rights?
- How to do monitoring of security incidents which network monitoring tools can be applied?

## 5.4 Encryption

Encryption is a security mechanism which have both encryption and decryption process. An encryption device can be used to encrypt the data at CKTECK's network before placing it on a network. The data can be decrypted by device, which can decrypt the data at CKTECK's network before passing it to any application. Data that is encrypted is called ciphered data (or simply encrypted data). Data that is not encrypted is called plain text or clear text. For implementing encryption mechanism on CKTECK's network some following directions can be used:

- A router, server, end system, or dedicated device can be used as an encryption or decryption device.
- Encryption protocols can be implemented on CKTECK's network for instance
  - PPTP[107]
  - L2TP[108]
  - IPSec[107]

  - SSL[107]
- Device level encryption can be applied on CKTECK's network
- All systems and office sites of CKTECK should be connected to the leased , secured and encrypted network lines.

The description of these protocols [106] [107][108] has been shown as:

**PPTP (Point-to-Point Tunneling Protocol):**

It supports CKTECK's VPN between Windows users. There is a disadvantage of it that it can't support encryption. In case of implementation of security measures it needs PPP(Point To Point Protocol).Moreover, PPTP is very fast and compatible with Linux and Mac users. It was developed by Microsoft.

**L2TP (Layer 2 Tunneling Protocol):**

it's also a tunneling protocol .It supports VPNs. It provides data confidentiality and data integrity. L2TP was developed by Microsoft and Cisco .

**IPsec protocol:**

It can be used for encryption with L2TP tunneling protocol. It provides security to the communications of Internet Protocol (IP). It can provide authentication and encryption to each IP packet of a data stream". Disadvantage is that it is expensive and having time consuming client installations.

**SSL (Secure Socket Layer) :**

It can support VPN via https over web browser. SSL VPN doesn't need any software installed because it uses the web browser as the client application. SSL VPNs can provide the user's access. It can be restricted to specific applications instead of allowing access to the whole network. It can be considered important in VPN.

## 5.5 Application Security

Application Security [110] , [111] can be referred as to find several vulnerabilities in the several applications which are running at CKTECK's network. After that, to apply security schemes on it. For maintaining the CKTECK's application security some schemes to be applied on CKTECK are listed as following

- By finding several network threats, vulnerabilities and countermeasures at CKTECK network according to advanced technologies BYOD, Cloud and Social Media.
- By doing Overall Risk Management on CKTECK's network according to ISO27001 Standards.
- By doing several security tests on CKTECK AG applications.

## 5.6 Web Security & Email Security

Web security at CKTECK is that how to maintain the security of CKTECK's network infrastructure against web related cyber threats. Email security is to apply protection on the emails (incoming and outgoing) at CKTECK network from viruses and other malwares. For maintaining it, following ideas can be helpful:

- How to implement firewalls on CKTECK's network behind DMZ and in place?
- How to apply antivirus? Which antivirus software is good and which could be harmful at CKTECK network?
- How to apply security against email spams and scams?
- In which ways the CKTECK's emails and the network traffic can be monitored?
- How to disallow the CKTECK users for using unapproved software?
- How to provide necessary security related training and user awareness regarding this?

### 5.6.1 Disaster Recovery and Business Continuity Planning

Disaster recovery is how to recover the network after any disaster. Author in [52] says that

> *Disaster recovery mechanism (abbreviated to DRM) is one of the focuses in replication research fields. It helps us restore data after a disaster. Designing a right disaster recovery mechanism is an important and complex task. Although some A Fast Disaster Recovery Mechanism for Volume Replication Systems 733 mechanisms have been presented, e.g. full or difference disaster recovery mechanism, we still need to improve the recovery efficiency and to afford the trade-off between data loss and the efficiency. It is ideal to implement a fast disaster recovery mechanism with the minimal data loss.*

.

Business continuity is to continue the all processes at CKTECK if any case of incidents. According to the author in [19]

> *The Business Continuity maintenance process is to ensure the restoration of the company's functioning in the event of any unexpected or undesirable incident that could negatively affect the continuity of the critical business functions and their supporting elements, with a threat of losing the entire business.*

Some schemes that can be applied for disaster recovery and business continuity planning are shown as follows:

- How the Remote access can granted to critical users to work from home during disaster.
- How to maintain alternate sites for the business continuity in case of any security incident?
- How to access the third party with CKTECK's network for providing emergency help in case of any failures?
- How to develop pre during and post incidents plans for CKTECK?

## 5.7 Physical Security, Hot Swap to second site and Backup Procedures

To limit the access to key network resources by keeping the resources behind a locked door and protected from natural and human-made disasters is the physical security for CKTECK AG's hardware resources. It protects a network so that nobody can misuse it. It can also protect the CKTECK's network from hackers, competitors, and terrorists walking in off the street and changing equipment configurations. In CKTECK, physical security can be implemented on core routers, demorcation points, cabling, modems, servers, hosts, backup storages etc. Backup plans are how to back the information if it is lost due to any reasons. Hot Swap [112] is to do replacement of any network device in case of failure of device, failure of storage device, and to substitute other data. For the maintenance of physical security, backup plans, hot swap etc. at CKTECK's network, the following guidelines can be helpful.

**In case of physical security:**

- How to make well guarded network?
- How to provide hardware access control methods in case of cloud hardware, other hardware at CKTECK and BYOD?
- Are CCTV cameras helpful? How to maintain it for CKTECK's physical security?
- How to segregate sensitive, public, private and semi public areas? How to install RFIDs for the track moments of unauthorized device and person too? How to maintain security alarms in the CKTECK's buildings?
- How to provide Cleaning and checking of incoming hardware and dispatching of outgoing hardware at CKTECK?
- Which persons and which machines are allowed to bring at CKTECK?
- How to monitor CKTECK's network 24 * 7? How to make possible CKTECK's network in such way so that it can show the details of device which is connected it with in radius of 10 meters?
- How to close external ports of CKTECK network with BIOS level passwords?
- How to lock systems and how to install security for the doors at CKTECK?

**In case of hot swap to second site:**

- In which way the backup procedure for CKTECK can be maintained by additional hot seats at the each site?
- How to cater the data recovery and backup plans for CKTECK when need to move people from one to another site?
- How to create additional alternate sites of multiple offices at CKTCEK?

**In case of backup plans:**

- How to ensure backup of CKTECK's vital systems and other network components at CKTECK?
- How to ensure that internet services at CKTECK are taken from at least two service providers for the maximum redundancy?
- How to make backup of CKTECK's data from the failure of BYOD devices, Cloud Hardware etc? If data is lost from any kind of trojan which have come from social networking site then how we can get it back?
- What could be several data loss prevention measures for the CKTECK's network, including backup plans?
- How the data systems at CKTECK can be maintained for online backup 24 * 7 with all required redundancy?

# 6 Discussions And Future Work

## 6.1 About Interviews Discussions

### 6.1.1 First Interview's Discussion

**Type OF Interview : Skype Session, Video Conferencing**
Name Of Interviewee : JatinderPreet Kaur, Head of Network Security at Verizon Communications, India
Name Of Interviewer : Mr Chetan Sharma, The Author of this thesis

During the interview session, the interviewer asked the questions related to advanced concepts of network security in the organizations. The author found the related information and gained some important knowledge related to advance networking concepts. Verizon Communication is a leading telecommunications based organization. Verizon Communications are using their VPN personal cloud network and the organization has several benefits of having personal VPN for example.

1. It Provides privacy to information being sent.
2. It Provides Safety of customer information.
3. It provides information of active employees
4. It provides productivity work trends of resources,
5. Only Authorized persons can connect to the network

Moreover they are personal VPN cloud network for the security purpose. If the cloud technology has positive results, then it also has some negative aspects and risks. For instance

1. Unstable internet connectivity which will cause frequent drop in VPN connectivity,
2. High latency will make connection too slow making it difficult for employees to work
3. No internet connectivity would result in no VPN connectivity

In case of BYOD, Verizon allow this only in case of non sensitive environments, which is good from the security point of view. Hence there are no bad effects of BYOD on network security at Verizon. With the use of BYOD, the VPN enabled network has no effect because the machines at Verizon, where VPN has installed, are secured. For the security purpose

1. All the external ports are disabled
2. There is no local storage
3. Bluetooth and Wi-Fi is also disabled

While discussion on network security policy, the main concepts are: authentication, monitoring & control of systems in network, dedicated network connectivity lines etc. In case of protection from advance malwares, viruses, worms and botnets, Verizon are using certified software, updated anti-viruses etc. According to their policy they are not allowing un authorized and un approved software in the organization. Moreover they are doing routine checkups for such kind of software. They filter their emails too from viruses.

For maintain the physical security, they have BIOS level passwords, which are known to only LAN team. Furthermore systems are locked and strapped for the security of system components. They have access control mechanisms. Verizon's network is secure against any attack from outside environment. They have their own generated white list for the approved devices. If the device is not in the white list of the network they there is an alarm system to concerned person for the mitigation.

### 6.1.2 Second Interview's Discussion

**Type OF Interview : An Email Interview**

Name Of Interviewee : Satish Das, CSO Chief Security Officer at Cognizant Technology Solutions, India

Name Of Interviewer : Mr Chetan Sharma, The Author of this thesis

While in an interview session with the CSO (Chief Security Officer at Cognizant) Mr. S. Das, the author found some real facts related to network infrastructure of the organisation. They are using public cloud by a third party which has some advantages and disadvantages. For instance.

1. It allows authorized resources to connect to company network from anywhere.
2. Resources can be allowed to work during travel.
3. Resources can be allowed to work from home minimizing company expenses towards office space fitments, furnishing, and electricity in other expenses.
4. It saves productive hours by minimizing travel to office.
5. It Provides secured connection.

By the use of public cloud they are facing some problems also which are slow internet, corruption of VPN clients, disruption of internet connection, some remote areas has no internet connection.

To maintain the security with third party they have some security controls which help for maintaining the network infrastructure security

1. Dual authentication on the network.
2. Dedicated servers.
3. Segregation of network with firewalls.
4. Adequate security controls on server.
5. secure databases

They are allowing BYOD but only for mangers and their network is secured to detect, prevent any connection to unauthorized devices. For the security of BYOD they are not allowing VPN client on BYOD devices. VPN client is secured and installed only on the authorized devices. VPN client can't be copied from the authorized device to another unauthorized device. Because all points of data leakage in the networks and systems are plugged. All network related risks are mitigated for VPN cloud environment.

They are maintaining the security policy as per ISO 27001. The network is secured by using.

1. Strong firewalls and Domains
2. VPN authentication.
3. ESA token based authentication
4. Antivirus control.
5. Monitoring of Email and network traffic from virus attack
6. Necessary education for the user for not forwarding chain emails within the organization.
7. Entire network is behind the DMZ.

Physical security in Cognizant is maintained in the following manner.

1. Well guarded 24*7
2. Access controlled systems.
3. CCTV cameras.
4. Segregation of public semipublic and private Zones.
5. Checking of incoming hardware for viruses.
6. Outgoing hardware is cleaned of any data on it before dispatch
7. Only authorized persons are allowed to bring in or out companies material.

8. Proper access control to highly sensitive areas and systems limited to a few individual for instance the use of RIFD sensors with Laptops for tracking the movement.

The most of the Smartphone's to senior management at cognizant are official. For maintenance the security of Smartphone's they have some security related solution shown below:

1. Using good software for the protection of smart phones.
2. Using good software for the segregation of office communication and personal communication.
3. Users at cognizant don't have facility to copy any official data and send out for personal use
4. Network is monitored 24*7
5. Any device which is connected to network shows details of the device , location with in 10 meters of radius

### 6.1.3 Third Interview's Discussion

**Type Of Interview : A Face to Face Interview**
Interviewee : Software Developer at Nordea AS, Norway
Name Of Interviewer : Mr Chetan Sharma, The Author of this thesis

It was an small interview with the employee of Nordea AS Oslo Norway. During the interview session author gets small amount of information from the interviewee related to network infrastructure. It was because the interviewee was not able to provide that much knowledge to the author. To some extent that information helps author to understand related topics. Form the interviewees point of view they are not using VPN cloud With BYOD in their organisation. Regarding the network security policy, Nordea AS has their own security policy control on the place for the security point of view. Which are as following:

1. Login and password (Authentication)
2. Using only that devices which are provided by the organization for organizational purpose.
3. Firewalls
4. They are providing user awareness training to the employees

For maintaining the physical security there are some security controls in the organisation

1. Access control mechanisms on the organizational hardware
2. Only the users have knowledge about the login details.

### 6.1.4 Fourth Interview's Discussion

**Type Of Interview : An Email Interview**
Interviewee : Technical Support Engineer at Gallagher Group Limited, New Zealand
Name Of Interviewer : Mr Chetan Sharma, The Author of this thesis

It was an email interview with the concerning person. In this interview the author send the questionnaire to the technical support engineer at Ghallagher Group Ltd. At New Zealand. The interviewee provided some important information which was helpful for the author. According to the interviewee, they have network security policies in their organization. They are using webmarshal and mailmarshal, concepts for the purpose of maintain the network security policy. Webmarshal is used for internet security in their organization and it provides network security from web attacks. Mailmarshal is also used for maintain network security, which provides protection to incoming and outgoing emails in the organization.

By using "Trend" They are protecting their network from malwares, botnets, spywares, advance viruses etc. Trend is an antivirus protection system which provides security regarding viruses , online threats, hackers, attackers, intruders, malicious inks, spams, scams and many more.

For maintenance of the physical security in their organization they are using security lock enabled doors and access cards systems.

For maintenance the security of BYOD devices, they are using Mobile Device Management Schemes. This ia a security mechanism for maintaining the network security related to BYOD.

## 6.2 Potential Projects related to Advanced Network Security Concepts, for The Future Students

The list of potential projects on this case study can be given to the students for further tasks .Students can choose one project individually from these and can find solutions on it then can write a report of maximum 20 pages. The several hints for finding the solutions of these potential projects has been described in Chapter 5. The students have chance to learn sub tasks on the advance network security mechanisms, which they can apply for CKTECK's network infrastructure. The list of some potential projects for the students has been shown below:

1. Data Leakage Prevention Schemes for CKTECK's Network Infrastructure.
2. Several Authentication techniques for smart phones, to improve the security of BYOD for CKTECK's network security.
3. Encryption mechanisms as a security tokens for the CKTECK's network security purpose. Dis-

cuss challenges and countermeasures.

4. Several port scanning mechanisms for the CKTECK's network security.
5. Maintenance of Physical security and backup plans for CKTECK AG.
6. Several web related threats and their prevention schemes for secure CKTECK's network.
7. BYOD network policy for CKTECK's network security.
8. Social Media networking problems and prevention schemes for CKTECK.
9. A secure VPN cloud private/public cloud for CKTECK.
10. Overall process for Consolidation for CKTECK's data centers. Describe advantages and disadvantages. Consolidation can be defined as to reduce the IT assets.
11. Produce policies like Remote Access control policy, Laptop security policy for CKTECK. Describe other related policy examples.
12. Design of one of the other subsidiaries of CKTECK. Explain overall network infrastructure plan.
13. A secure and scalable BYOD strategy related to networking concepts for the CKTECK's network.
14. Networking and Internet secuirty plans for CKTECK.
15. Analysis of Identity theft. How it can be done and can be secured in CKTECK's network?

## 6.3 Overall Thesis Discussions

As an overall discussion on whole research, the author can say that it was a good experience for him in learning several advance networking related aspects in modern organizations. The author has decided to make a study tool for the future students on the basis of an Organization's network infrastructure. And the author achieved his goal as a result of this document. According to the good qualities to any case study: it should be easily understandable by students, it should provide necessary related information, it should describe basic and challenging tasks for the students, it should describe some solutions for their help, it should provide innovative ideas to develop new projects, it should encourage the students to make a better case study on it and future work and so on.

From this whole research, the author has tried to fulfill all the good qualities of a case study as mentioned above. This case study has following qualities:

- It contains necessary information regarding the advance networking concepts
- It contains the network infrastructure plan to be proceed further also by the students

- It contains advance and basic networking related tasks for the students to be followed as individual and common projects in the classroom
- It contains some solutions as innovative ideas for the students to take help
- It contains the real life experience from the experts in the Real Organizations
- This case study also have some loopholes in the network infrastructure, so that the students can apply network security mechanisms on it and can proceed further. Hence it is reproduce able and can be researched further.

As a conclusion for accessing quality, this case study completes the requirements of a good study tool and platform. The author has put his best efforts on making this educational tool. Hence the author tried to achieve maximum output. On the resulting document by the author's research of this thesis, the students can find innovative and the creative solutions on the pre described tasks on advance networking concepts in BYOD, cloud and social media. Moreover the students can develop a better case study in the future by finding several loopholes in the network infrastructure of CKTECK. Additionally they can apply several networking management mechanisms by extending the pre defined network infrastructure of CKTECK. In overall, they can learn from this, they can reproduce it for the new future work, they can accept challenges of the case study and can prepare themselves for the organizations like advance problems and so on.

# 7 Conclusions

In nutshell, the author has learned and gained experience regarding the security of network infrastructure in the organizations. The case study has been developed for the coming students. They can learn about advance networking and network security related concepts from the case. While making such kind of case study the author have described CKTECK's Network infrastructure with its necessary details in such a way so that the students can find advanced network security related issues, problems, risks, threats and vulnerabilities in the organizational like conditions. Furthermore some network security related tasks has been described for the students by the author. These tasks are the challenges for the students so that they can solve those tasks. Additionally the author has provided example solutions for the tasks, which can be handed in to the students later on. A sample of network security policy has been also described. From all above, the students can learn about the advancement in the networking field in Modern IT organizations. Interviews discussions have been described so that the students can learn that what is actually happening in the organizations in these days related to the advance networking concepts. Interviews discussions will help the students to learn more about several network security mechanisms used by the organizations in these days. Some potential projects have been listed as further tasks for the students to proceed further. This research work is an educational tool on advanced networking concepts which can be modified according to the technological changes and changes in the demands. At last for the author, this research work played an important role for the educational point of view, because the author have learned too on advanced networking problems & solutions and concepts. Networking is an essential part of an organization, and in the future more advancement will be there in this field because organizations will more rely on the upcoming advance network.

# Bibliography

[1] *MICROS Systems Inc, Version 7.2, November 2011, Enterprise Information Security Policy for public use* http://www.micros.com/NR/rdonlyres/72E62768-5BD3-471B-B190-60169E42B977/0/MICROSSystemsIncEnterpriseInformationSecurityPolicyRevision72November2011.pdf

[2] *Organizational Security and Compliance* http://www.mhprofessional.com/downloads/products/0071770380/01-chapter-1_0071770380.pdf

[3] *Network Security Policy Definition* http://en.wikipedia.org/wiki/Network_security_policy

[4] *Whitepaper of WatchGuard Technologies Inc. Corporation on " Producing your Network Security Policy", July 2007, Frederick M. Avolio, Steve Fallin, D. Scott Pinzon, CISSP, NSA-IAM Watchguard Technologies, Inc.* http://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf

[5] *Network Infrastructure Definition* http://www.techopedia.com/definition/16955/network-infrastructure

[6] *Roles And Responsibilities of CISO, California Office of Information Security and Privacy Protection*, Guide for the Roles and Responsibilities of an Information Security Officer Within State Government April 2008, http://www.cio.ca.gov/OIS/Government/documents/pdf/ISO_Roles_Respon_Guide.pdf

[7] *Wireless Security Definition* http://en.wikipedia.org/wiki/Wireless_security

[8] *Author: Slobodan Petrovic, Lecture 1 notes, Wireless Communication Security, IMT masters in HIG, November 2012*

[9] *Improving Web Application: Security Threats and countermeasures, Microsoft Corporation,* J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan, Chapter 2, 2003 http://msdn.microsoft.com/en-us/library/aa302418.aspx

[10] *MPLS Technology , Newer Design Guide, February 2013 series by CISCO* http://www.cisco.com/en/US/docs/solutions/SBA/February2013/Cisco_SBA_BN_MPLSWANDeploymentGuide-Feb2013.pdf

[11] *The network is a computer* By John Burdette Gage , http://en.wikipedia.org/wiki/John_Gage

[12] "*Infrastructure as a service (IaaS) for NASA's mission directorate NASA's Nebula pioneers a new frontier for cloud computing,*" *Computing, Networking and Communications (ICNC),*Shackelford, K.; Williams, J., 2012 International Conference on , vol., no., pp.29,33, Jan. 30 2012-Feb. 2 2012, http://dx.doi.org/10.1109/ICCNC.2012.6167432

[13] "*PaaS on IaaS,*" *Advanced Information Networking and Applications (AINA),* Kibe, S.; Watanabe, S.; Kunishima, K.; Adachi, R.; Yamagiwa, M.; Uehara, M., 2013 IEEE 27th International Conference on , vol., no., pp.362,367, 25-28 March 2013 http://dx.doi.org/10.1109/AINA.2013.73

[14] "*Proxy Network Intrusion Detection System for cloud computing*" , Ucman; Sahingoz, Ozgur Koray, " Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), Oktay, 2013 International Conference on , vol., no., pp.98,104, 9-11 May 2013, http://dx.doi.org/10.1109/TAEECE.2013.6557203

[15] "*Cloud networking: An infrastructure service architecture for the wide area,*" *Future Network & Mobile Summit (FutureNetw)*, Murray, P.; Sefidcon, A.; Steinert, R.; Fusenig, V.; Carapinha, J., 2012 , vol., no., pp.1,8, 4-6 July 2012, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6294196&isnumber=6294166

[16] "*Identity management framework for cloud networking infrastructure*", Dhungana, R.D.; Mohammad, A.; Sharma, A.; Schoen, I., Innovations in Information Technology (IIT), 2013 9th International Conference on , vol., no., pp.13,17, 17-19 March 2013 doi: 10.1109/Innovations.2013.6544386, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6544386&isnumber=6544378

[17] "*Role of optical network infrastructure virtualization in data center connectivity and cloud computing*" ,Publications of ieeexplore, Nejabati, R.; Peng, S.; Simeonidou, D., Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), 2013 , vol., no., pp.1,3, Publication Date:17-21 March 2013, ISBN:978-1-4799-0457-0, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6532801&isnumber=6532492

[18] "*Network-Level Access Control Management for the Cloud*", *Cloud Engineering (IC2E)*Beaty, K.; Kundu, A.; Naik, V.; Acharya, A.„ 2013 IEEE International Conference on , vol., no., pp.98,107, 25-27 March 2013 doi: http://dx.doi.org/10.1109/IC2E.2013.18, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6529273&isnumber=6529250

[19] "*Business Continuity and Information Security Maintenance*" *Masters' Training Program*, Information Assurance and Security Education and Training, IFIP Advances in Information and Communication Technology, Volume 406, 2013, pp 95-102 ,By Natalia, DOI:http://dx.doi.org/10.1007/978-3-642-39377-8_10, Print ISBN: 978-3-642-39376-1, Online ISBN: 978-3-642-39377-8, Miloslavskaya, Mikhail Senatorov, Alexandr Tolstoy, Sergei Zapechnikov, http://download.springer.com/static/pdf/189/chp%253A10.1007%252F978-3-642-39377-8_10.pdf?auth66=1385704914_8368ff1c94d68daad81b118827a17239&ext=.pdf

[20] "*A Cloud-based Intrusion Detection Service framework,*" Yassin, W.; Udzir, N.I.; Muda, Z.; Abdullah, A.; Abdullah, M. T., Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on , vol., no., pp.213,218, 26-28 June 2012 http://dx.doi.org/10.1109/CyberSec.2012.6246098

[21] "*Rethinking cloud platforms: Network-aware flexible resource allocation in IaaS clouds,*"Wickboldt, Juliano Araujo; Granville, Lisandro Zambenedetti; Schneider, Fabian; Dudkowski, Dominique; Brunner, Marcus, Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on , vol., no., pp.450,456, 27-31 May 2013 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6573017&isnumber=6572961

[22] "*Engineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor,*" *Service Oriented System Engineering (SOSE),* Laniepce, S.; Lacoste, M.; Kassi-Lahlou, M.; Bignon, F.; Lazri, K.; Wailly, A., 2013 IEEE 7th International Symposium on , vol., no., pp.25,36, 25-28 March 2013 doi: 10.1109/SOSE.2013.27, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6525501&isnumber=6525477

[23] "*Cloud security: Analysis and risk management of VM images,*" *Information and Automation (ICIA),*Bindra, G.S.; Singh, P.K.; Kandwal, K.K.; Khanna, S., 2012 International Conference on , vol., no., pp.646,651, 6-8 June 2012 doi: 10.1109/ICInfA.2012.6246757, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6246757&isnumber=6246755

[24] *Cloud Infrastructure Security,* By Dimiter Velev, Plamena Zlateva in Open Research Problems in Network Security (2011), Open Research Problems in Network Security, Lecture Notes in Computer Science Volume 6555, 2011, pp 140-148, ISBN: 978-3-642-19227-2

[25] *Privacy and Security for Cloud Computing,Security Infrastructure for Dynamically Provisioned Cloud Infrastructure Services,* Computer Communications and Networks 2013, pp 167-210, Yuri Demchenko, Canh Ngo, Cees de Laat, Diego R. Lopez, Antonio Morales, Joan A. García-Espín, http://staff.science.uva.nl/~delaat/pubs/2013-b-1.pdf

[26] *Management Infrastructures for Power-Efficient Cloud Computing Architectures*, Cloud Computing, Computer Communications and Networks 2013, pp 133-152 Antonio Corradi, Mario Fanelli, Luca Foschini, http://dx.doi.org/10.1007/978-1-4471-5107-4_7, Print ISBN:978-1-4471-5106-7, Online ISBN: 978-1-4471-5107-4

[27] *Cloud Infrastructure & Applications – CloudIA* Cloud Computing Lecture Notes in Computer Science Volume 5931, 2009, pp 583-588 , Anthony Sulistio, Christoph Reich, Frank Doelitzscher, http://dx.doi.org/10.1007/978-3-642-10665-1_56, ISBN:978-3-642-10664-4, Online ISBN 978-3-642-10665-1

[28] *Cloud Computing Solution Patterns: Infrastructural Solutions* Cloud Computing Computer Communications and Networks 2013, pp 197-219 Shyam Kumar Doddavula, Ira Agrawal, Vikas Saxena, http://dx.doi.org/10.1007/978-1-4471-5107-4_10, Print ISBN 978-1-4471-5106-7, Online ISBN 978-1-4471-5107-4

[29] *Network virtualization for cloud computing* annals of telecommunications - annales des télécommunications December 2010, Volume 65, Issue 11-12, pp 713-721 Fabio Baroncelli, Barbara Martini, Piero Castoldi, http://dx.doi.org/10.1007/s12243-010-0194-y, Print ISSN 0003-4347, Online ISSN 1958-9395

[30] *Understanding Cloud Audits* Privacy and Security for Cloud Computing, Computer Communications and Networks 2013, pp 125-163, Frank Doelitzscher, Christoph Reich, Martin Knahl, Nathan Clarkes, http://dx.doi.org/10.1007/978-1-4471-4189-1_4, Print ISBN 978-1-4471-4188-4, Online ISBN 978-1-4471-4189-1

[31] *An agent based business aware incident detection system for cloud environments* This article is part of Security in Cloud Computing, Journal of Cloud Computing July 2012, http://dx.doi.org/10.1186/2192-113X-1-9, Online ISSN 2192-113X

[32] *How to adapt applications for the Cloud environment* , June 2013, Volume 95, Issue 6, pp 493-535, Vasilios Andrikopoulos, Tobias Binz, Frank Leymann, Steve Strauch, http://dx.doi.org/10.1007/s00607-012-0248-2, Print ISSN 0010-485X, Online ISSN 1436-5057

[33] *Cloud Computing Infrastructure and Application Study* Information Computing and Applications, Lecture Notes in Computer Science Volume 7473, 2012, pp 358-364, Ming Ye, ZeHui Qu, Print ISBN 978-3-642-34061-1, Online ISBN 978-3-642-34062-8, http://dx.doi.org/10.1007/978-3-642-34062-8_47

[34] *Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach* Journal of Grid Computing March 2011, Volume 9, Issue 1, pp 3-26, Bhaskar Prasad Rimal, Admela Jukan, Dimitrios Katsaros, Yves Goeleven, http://dx.doi.org/10.1007/s10723-010-9171-y

[35] *A survey on security issues and solutions at different layers of Cloud computing* The Journal of Supercomputing February 2013, Volume 63, Issue 2, pp 561-592 Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel, Muttukrishnan Rajarajan, http://dx.doi.org/10.1007/s11227-012-0831-5

[36] "*Cloud implementation security challenges,*" *Cloud Computing Technologies, Applications and Management (ICCCTAM),* Bamiah, M.; Brohi, S.; Chuprat, S.; Brohi, M.N., 2012 International Conference on , vol., no., pp.174,178, 8-10 Dec. 2012 doi: 10.1109/ICCCTAM.2012.6488093, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6488093&isnumber=6488050

[37] *Cloud Computing and Related Security Issues* Guide to Computer Network Security Computer Communications and Networks 2013, pp 465-489

Joseph Migga Kizza, http://dx.doi.org/10.1007/978-1-4471-4543-1_22

[38] *Design and Technology changes, Network Infrastructure Building a more efficient network with greater capabilities, capacity and security*,Published in May 2011, http://www.edtechmagazine.com/higher/sites/edtechmagazine.com.higher/files/rg_nw_optim_042011.pdf

[39] *A Study on Scalability of Services and Privacy Issues in Cloud Computing*

Distributed Computing and Internet Technology, Lecture Notes in Computer Science Volume 7154, 2012, pp 212-230, R. S. M. Lakshmi Patibandla, Santhi Sri Kurra, Nirupama Bhat Mundukur, http://dx.doi.org/10.1007/978-3-642-28073-3_19

[40] *Cloud Security and Governance* Guide to Cloud Computing, Computer Communications and Networks 2013, pp 223-239, Richard Hill, Laurie Hirsch, Peter Lake, Siavash Moshiri, http://dx.doi.org/10.1007/978-1-4471-4603-2_10

[41] " *Cloud Computing Technology and Science (CloudCom),* , Bo Peng; Hammad, A.; Nejabati, R.; Azodolmolky, S.; Simeonidou, D.; Reijs, V., "A Network Virtualization Framework for IP Infrastructure Provisioning,2011 IEEE Third International Conference on , vol., no., pp.679,684, Nov. 29 2011-Dec. 1 2011, doi: 10.1109/CloudCom.2011.105, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6133214&isnumber=6133119

[42] *Network Infrastruture Adapting networking strategies and techniques for today's challenges*, MAY 2013 | 800.808.4239 | CDWG.COM/NETWORKGUIDE, http://webobjects.cdw.com/webobjects/media/pdf/Solutions/Data-Center/050713_RG_G_Networking_121835.pdf

[43] "*Enabling infrastructure as a service (IaaS) on IP networks: from distributed to virtualized control plane,*", Kim-Khoa Nguyen; Cheriet, M.; Lemay, M., Communications Magazine, IEEE , vol.51, no.1, pp.136,144, January 2013, doi: 10.1109/MCOM.2013.6400450, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6400450&isnumber=6400427

[44] *Enterprise cloud service architecture* , Information Technology and Management, December 2012, Volume 13, Issue 4, pp 445-454, Heyong Wang, Wu He, Feng-Kwei Wang, http://dx.doi.org/10.1007/s10799-012-0139-4

[45] *Cloud Computing Solution Patterns: Application and Platform Solutions* Cloud Computing Computer Communications and Networks 2013, pp 221-239, Shyam Kumar Doddavula, Ira Agrawal, Vikas Saxena, http://dx.doi.org/10.1007/978-1-4471-5107-4_11

[46] *Privacy, Security and Trust in Cloud Computing, Privacy and Security for Cloud Computing,* Computer Communications and Networks 2013, pp 3-42 By Siani Pearson, http://dx.doi.org/10.1007/978-1-4471-4189-1_1

[47] *Guide to Cloud Computing Business Adoption Models and Legal Aspects of the Cloud*, Computer Communications and Networks 2013, pp 21-42, Richard Hill, Laurie Hirsch, Peter Lake, Siavash Moshiri, http://dx.doi.org/10.1007/978-1-4471-4603-2_2

[48] "*Identity management framework for cloud networking infrastructure,*" Dhungana, R.D.; Mohammad, A.; Sharma, A.; Schoen, I., Innovations in Information Technology (IIT), 2013 9th International Conference on , vol., no., pp.13,17, 17-19 March 2013 doi: 10.1109/Innovations.2013.6544386, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6544386&isnumber=6544378

[49] "*Emerging security threats for mobile platforms,*" Delac, G.; Silic, M.; Krolo, J., MIPRO, 2011 Proceedings of the 34th International Convention , vol., no., pp.1468,1473, 23-27 May 2011 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5967292&isnumber=5967009

[50] *Internet threats to end-users: Hunting easy prey*, Steven Furnell [Author Vitae], Network Research Group, University of Plymouth, Available online 19 July 2005, http://dx.doi.org/10.1016/S1353-4858(05)70258-0 Network Security, Volume 2005, issue 7, july 2005, pages 5-9

[51] *A Fast Disaster Recovery Mechanism for Volume Replication Systems*, Yanlong Wang, Zhanhuai Li, Wei Lin, DOI: http://dx.doi.org/10.1007/978-3-540-75444-2_68, Print ISBN:978-3-540-75443-5,Third International Conference, HPCC 2007, Houston, USA, September 26-28, 2007. Proceedings, http://download.springer.com/static/pdf/330/chp%253A10.1007%252F978-3-540-75444-2_68.pdf?auth66=1385705481_db0a17cf08980150f1b61e841ca1642e&ext=.pdf

[52] *Conquering today's bring-your-own-device challenges,Corporation Aruba Whitepaper* A framework for successful BYOD initiatives, Copyright © 2012 Aruba Networks, http://www.wit.co.th/pdf/Aruba/WP_BYOD.pdf

[53] *Cisco BYOD Smart Solution*, Copyright © 2013, Cisco corporation, http://www.cisco.com/web/solutions/trends/byod_smart_solution/docs/byod_smart_solution_aag.pdf

[54] *Aruba Inc Whitepaper for BYOD challenges*Copyright © 2012 Aruba Networks, http://uct.com.do/wp-content/uploads/2012/03/Bring-Your-Own-Device_BYOD.pdf

[55] *Networking for the BYOD Enterprise* , By Philip Clarke, Research Analyst,Nemertes Research, Copyright ©Nemertes,Research 2013, www.nemertes.com, 888-241-2685, DN2504, http://h20195.www2.hp.com/V2/GetPDF.aspx/c03660924.pdf

[56] *The security implications of BYOD* , Original Research Article, Network Security, Volume 2013, Issue 4, April 2013, Pages 12-13, Brian Tokuyoshi, http://dx.doi.org/10.1016/S1353-4858(13)70050-3

[57] *Bring Your Own Devices Best Practices Guide, A Practical Guide for Implementing BYOD Programs at Your Organization*, Whitepaper By DELL Corporation @All rights reserved, 2012 http://i.dell.com/sites/doccontent/business/smb/sb360/en/Documents/good-byod-best-practices-guide.pdf

[58] "*New Security Perspectives around BYOD,*" *Broadband, Wireless Computing, Communication and Applications (BWCCA),* Scarfo, A., 2012 Seventh International Conference on , vol., no., pp.446,451, 12-14 Nov. 2012 doi: 10.1109/BWCCA.2012.79, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6363095&isnumber=6363025

[59] "*BYOD: Security and Privacy Considerations,*" *IT Professional ,* , Miller, K.W.; Voas, J.; Hurlburt, G.F.,vol.14, no.5, pp.53,55, Sept.-Oct. 2012, doi: 10.1109/MITP.2012.93, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6320585&isnumber=6320581

[60] *A White-List Based Security Architecture (WLSA) for the Safe Mobile Office in the BYOD Era*, Grid and Pervasive Computing, Lecture Notes in Computer Science Volume 7861, 2013, pp 860-865, Jaeho Lee, Yongjin Lee, Seung-Cheon Kim, http://dx.doi.org/10.1007/978-3-642-38027-3_98

[61] *Selecting Access Network for BYOD Enterprises with Business Context (eBC) and Enterprise-Centric ANDSF*, Mobile Wireless Middleware, Operating Systems, and Applications, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Volume 65, 2013, pp 221-235, Rebecca Copeland, Noel Crespi, http://dx.doi.org/10.1007/978-3-642-36660-4_16

[62] *Consumerization*, Business & Information Systems Engineering,December 2012, Volume 4, Issue 6, pp 363-366, Dipl. Wirtsch.-Inf. Frank Weiß, Prof. Dr. Jan Marco Leimeister, http://dx.doi.org/10.1007/s12599-012-0234-4

[63] *Android forensics: Automated data collection and reporting from a mobile device Original Research Article*, Digital Investigation, Volume 10, Supplement, August 2013, Pages S12-S20, Justin Grover, http://dx.doi.org/10.1016/j.diin.2013.06.002

[64] *The role and effectiveness of cryptography in network virtualization: a position paper*, Author:Wenbo Mao,DaoliCloud Company, Beijing, China, Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, Pages 179-182 , ACM New York, NY, USA ©2013,ISBN: 978-1-4503-1767-2, http://dx.doi.org/10.1145/2484313.2484337

[65] *Towards secure mobile cloud computing: A survey Original Research Article*, Future Generation Computer Systems, Volume 29, Issue 5, July 2013, Pages 1278-1299, Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani, http://dx.doi.org/10.1016/j.future.2012.08.003

[66] *Mobile cloud computing: A survey Original Research Article*, Future Generation Computer Systems, Volume 29, Issue 1, January 2013, Pages 84-106, Niroshinie Fernando, Seng W. Loke, Wenny Rahayu, http://dx.doi.org/10.1016/j.future.2012.05.023

[67] John Thielens, Why APIs are central to a BYOD security strategy, Network Security, Volume 2013, Issue 8, August 2013, Pages 5-6, ISSN 1353-4858,http://dx.doi.org/10.1016/S1353-4858(13)70091-6 http://www.sciencedirect.com/science/article/pii/S1353485813700916

[68] *BYOD: enabling the chaos Original Research Article*, Network Security, Volume 2012, Issue 2, February 2012, Pages 5-8 Gordon Thomsonhttp://dx.doi.org/10.1016/S1353-4858(12)70013-2

[69] *Bringing IT out of the shadows Original Research Article*, Network Security, Volume 2013, Issue 4, April 2013, Pages 5-11, Richard Walters, http://dx.doi.org/10.1016/S1353-4858(13)70049-7

[70] *The state of information security Original Research Article*, http://dx.doi.org/10.1016/S1353-4858(12)70064-8, Network Security, Volume 2012, Issue 7, July 2012, Pages 9-11, Mike Potts

[71] *BYOD with secure*By TCS & ISACA,2-23-2013, http://www.theiiat.or.th/media/km/thumbnail/47/130226142847/BYOD%20-%20ISACA%20-%20Final%2020130223%20Vorapoj%20Lookmaipun.pdf

[72] *Mobile phone calls as a business risk*, Simon Bransfield-Garth [Author Vitae], Cellcrypt, Available online 1 October 2010, http://dx.doi.org/10.1016/S1353-4858(10)70114-8, Network Security, Volume 2010, Issue 9

[73] *A Practical Approach to Port scan Detection in Very High-Speed Links Port scans are continuously used by both worms and human attackers to probe*, JakubMikians, Pere Barlet-Ros, Josep Sanjuàs-Cuxart and JosepSolé-Pareta, Lecture Notes in Computer Science, Volume 6579, Passive and Active Measurement, Pages 112-121, 12th International Conference, PAM 2011, Atlanta, GA, USA, March 20-22, 2011. Proceedings , http://dx.doi.org/10.1007/978-3-642-19260-9_12

[74] *A Flow Based Slow and Fast Scan Detection System,* By .N. Muraleedharan and Arun Parmar, Communications in Computer and Information Science, 1, Volume 89, Recent Trends in Network Security and Applications, Part 1, Pages 191-200, http://dx.doi.org/10.1007/978-3-642-14478-3_20

[75] *A Comparative Study of Fuzzy Inference Systems*,M. Zubair Shafiq, Muddassar Farooq and Syed Ali Khayam, Lecture Notes in Computer Science, 2008, Volume 4974, Applications of Evolutionary Computing, Pages 52-61, http://dx.doi.org/10.1007/978-3-540-78761-7_6

[76] *How to ensure business continuty in cloud*, Michael Crandell , May 29, 2011, http://gigaom.com/2011/05/29/how-to-design-your-service-for-failures-in-the-cloud/

[77] Master Thesis of Author Khushbir Kaur Sharma, Student at HIG, Student Of Masters in Information Technology at HIG

[78] *Rapid Spanning Tree Protocol (RSTP) Deployment Guidelines for Converged Networks – Revision 01*, Extreme Networks Application Note http://www.extremenetworks.com/libraries/whitepapers/ANRSTDeployGuidelines_1779.pdf

[79] *By CISCO Corporation, networking concepts related knowledge* http://www.cisco.com/en/US/tech/tk389/tk214/tk771/tsd_technology_support_sub-protocol_home.html

[80] *Redundancy, Load Balancing, and High Availability*http://docs.oracle.com/cd/E14148_02/wlcp/ocsg41_otn/archoverview/alt-redundancy.html

[81] *White Paper on MPLS, MPLS WAN Explorer Enterprise Network Management Visibility through the MPLS VPN "Cloud"* http://www.packetdesign.com/resources/white-papers/MPLS%20WAN%20Explorer%20White%20Paper--Routing%20and%20Traffic%20Visibility%20for%20Outsourced%20MPLS%20VPN%20WANs.pdf

[82] "*A social collaboration platform for enterprise social networking,*" *Computer Supported Cooperative Work in Design (CSCWD),* , Minbo Li; Guangyu Chen; Zhe Zhang; Yi Fu, 2012 IEEE 16th International Conference on , vol., no., pp.671,677, 23-25 May 2012, doi: http://dx.doi.org/10.1109/CSCWD.2012.6221890

[83] *Understanding risks, benefits, and strategic alternatives of social media applications in the public sector Original Research Article*, http://dx.doi.org/10.1016/j.giq.2012.07.002, Government Information Quarterly, Volume 29, Issue 4, October 2012, Pages 504-511, Sergio Picazo-Vela, Isis Gutiérrez-Martínez, Luis Felipe Luna-Reyes

[84] "*Social Network Analysis in Enterprise,*", Ching-Yung Lin; Wu, L.; Zhen Wen; Hanghang Tong; Griffiths-Fisher, V.; Shi, L.; Lubensky, D., Proceedings of the IEEE , vol.100, no.9, pp.2759,2776, Sept. 2012, doi: 10.1109/JPROC.2012.2203090, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6249715&isnumber=6269941

[85] "*The Key to Social Media Implementation: Bridging Customer Relationship Management to Social Media,*" *System Sciences (HICSS),* , Mousavi, S.; Demirkan, H., 2013 46th Hawaii International Conference on , vol., no., pp.718,727, 7-10 Jan. 2013, doi:10.1109/HICSS.2013.531, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6479920&isnumber=6479821

[86] "*Emerging social media threats: Technology and policy perspectives,*" Chandramouli, R. Cybersecurity Summit (WCS), 2011 Second Worldwide ,Publication Year: 2011 , Page(s): 1-4, Print ISBN: 978-1-4577-1449-8, INSPEC Accession Number:12172678

[87] *A secret sharing based privacy enforcement mechanism for untrusted social networking operators*, Author:Pradeep K. Atrey, The University of Winnipeg, Winnipeg, MAN, Canada, Proceeding, MiFor '11 Proceedings of the 3rd international ACM workshop on Multimedia in forensics and intelligence, Pages 13-18 , ACM New York, NY, USA ©2011 , ISBN: 978-1-4503-0987-5 doi http://dx.doi.org/10.1145/2072521.2072525

[88] "*Impact of trust, security and privacy concerns in social networking: An exploratory study to understand the pattern of information revelation in Facebook,*" Dhami, A.; Agarwal, N.; Chakraborty, T.K.; Singh, B.P.; Minj, J., Advance Computing Conference (IACC), 2013 IEEE 3rd International , vol., no., pp.465,469, 22-23 Feb. 2013 doi: 10.1109/IAdCC.2013.6514270, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6514270&isnumber=6506800

[89] *Privacy Issues in Mobile Social Networks* , Original Research Article, Procedia Computer Science, Volume 10, 2012, Pages 672-679, Racha Ajami, Nabeel Al Qirim, Noha Ramadan, http://dx.doi.org/10.1016/j.procs.2012.06.086

[90] *Anti-social networking: exploiting the trusting environment of Web 2.0* , Original Research Article, Network Security, Volume 2008, Issue 11, November 2008, Pages 4-7, Steve Mansfield-Devinehttp://dx.doi.org/10.1016/S1353-4858(08)70127-2

[91] *The threats of social networking: Old wine in new bottles?* ,Original Research Article, Information Security Technical Report, Volume 16, Issue 2, May 2011, Pages 38-43 ,George R.S. Weir, Fergus Toolan, Duncan Smeed, http://dx.doi.org/10.1016/j.istr.2011.09.008

[92] *Social networking in the workplace*, Network Security, Volume 2011, Issue 10, October 2011, Page 20, http://dx.doi.org/10.1016/S1353-4858(11)70109-X

[93] *2013 Security threat report by Websenses*, http://www.websense.com/assets/reports/websense-2013-threat-report.pdf

[94] *Security review: the past year*, Original Research Article, Computer Fraud & Security, Volume 2013, Issue 1, January 2013, Pages 5-11, Steve Mansfield-Devine, http://dx.doi.org/10.1016/S1361-3723(13)70006-X

[95] *Whitepaper by SANS Institute on Information Security*, http://www.sans.org/reading-room/whitepapers/policyissues/reducing-risks-social-media-organization-33749

[96] *SANS institute Whitepater on Risk Assessment on Social Media*, http://www.sans.org/reading-room/whitepapers/privacy/risk-assessment-social-media-33940

[97] *A survey of mobile malware in the wild*, ACM New York, NY, USA ©2011, ISBN: 978-1-4503-1000-0 doi>http://dx.doi.org/10.1145/2046614.2046618, Authors Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, David Wagner.

[98] *10 best practice suggestions for common smartphone threats*, By Jeff R Fawcett & M Brandon Swain ,Security Practice Executives at Dell , http://i.dell.com/sites/content/business/solutions/whitepapers/en/Documents/smart-phone-threat-mitigation.pdf

[99] *The Top 10 Threats to Your Smartphone* By John R. Quain, Security NewsDaily Contributor, http://www.securitynewsdaily.com/1181-top-10-threats-smartphone.html

[100] *Replay Attack Definition*, http://en.wikipedia.org/wiki/Replay_attack

[101] *MPLS WAN Development Guide By Cisco Corporation*, August 2012 series ,http://www.cisco.com/en/US/docs/solutions/SBA/August2012/Cisco_SBA_BN_MPLSWANDeploymentGuide-Aug2012.pdf

[102] *Design Guide of MPLS WAN Development By Cisco Corporation, August 2013 series*, http://www.cisco.com/en/US/docs/solutions/CVD/Aug2013/CVD-MPLSWANDesignGuide-AUG13.pdf

[103] *Guide to Enterprise Telework and Remote Access Security Recommendations of the National Institute of Standards and Technology* , http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

[104] *About Novell Flir Server*, http://www.novell.com/products/filr/

[105] *What is Novell Flir*, http://www.novell.com/documentation/novell-filr1/filr1_overvw/data/what_is_filr.html

[106] *Types Of VPN Protocols*, POSTED ON 17/02/2010, https://www.ibvpn.com/2010/02/types-of-vpn-protocols/

[107] "*Network Performance Analysis of VPN Protocols: An Empirical Comparison on Different Operating Systems,*", Narayan, S.; Brooking, K.; de Vere, S., Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on , vol.1, no., pp.645,648, 25-26 April 2009, doi: http://dx.doi.org/10.1109/NSWCTC.2009.367

[108] "*A DoS-vulnerability analysis of L2TP-VPN,*" , Kara, A.; Suzuki, T.; Takahashi, K.; Yoshikawa, M.,Computer and Information Technology, 2004. CIT '04. The Fourth nternational Conference on , vol., no., pp.397,402, 14-16 Sept. 2004, doi: 10.1109/CIT.2004.1357228, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1357228&isnumber=29791

[109] " *Developing network security strategies by CISCO*", © 2013 Pearson Education, Cisco Press. All rights reserved. 800 East 96th Street, Indianapolis, Indiana 46240, By Priscilla Oppenheimer, Sample Chapter is provided courtesy of Cisco Press. Date: Oct 4, 2010. http://www.ciscopress.com/articles/article.asp?p=1626588&seqNum=2

[110] *A Paper on the Promotion of Application SecurityAwareness*,By Man-Sau Yi, August 2001, GSEC, Version1.2e ,ID: Man-Sau001 http://www.sans.org/reading-room/whitepapers/basics/paper-promotion-application-security-awareness-456

[111] *Application Security by Wiki*, http://en.wikipedia.org/wiki/Application_security

[112] *Definition of Hot Swap*, http://whatis.techtarget.com/definition/hot-swap

[113] *Security Enhancement of Smart Phones for Enterprises by Applying Mobile VPN Technologies*, Computational Science and Its Applications ICCSA 2011, volume:6784, Lecture Notes in Computer Science , editor: Murgante, Beniamino and Gervasi, Osvaldo and Iglesias, Andrés and Taniar, David and Apduhan, BernadyO , doi: 10.1007/978-3-642-21931-3_39, http://dx.doi.org/10.1007/978-3-642-21931-3_39,publisher:Springer, By: Berlin Heidelberg ,author : Hong, Young-Ran and Kim, Dongsoo , pages:506-517, 2011 , isbn:978-3-642-21930-6

# A Interview1: The interview was conducted by using Skype Video Conferencing

**By Jatinder preet Kaur, Head of Network Security, Verizon Communications, India**

***Question1:*** Do you have Virtual Private Network Cloud in your Organization? If yes then can you list five advantages of it? Just name those?

***Answer:***Yes, advantages are:

- Provides privacy to information being sent
- Provides Safety of customer information,
- It provides information of active employees
- Provides productivity work trends of resources,
- Only Authorized persons can connect to the network

***Question2:*** While using VPN cloud what kind of challenges networking related problems you are facing, just give some examples.

***Answer:*** One can face challenges if

- (a) unstable internet connectivity which will cause frequent drop in VPN connectivity,
- (b) high latency will make connection too slow making it difficult for employees to work
- (c) no internet connectivity would result in no VPN connectivity

***Question3:*** Are you using VPN Cloud by third party outsourcing or you have private cloud network? Can you please list some security mechanisms which is used by your organization for maintain the security by third party side?

***Answer:*** We are using own cloud services.

***Question 4:*** Is BYOD Bringing your own devices allowed in your organization? While using personal devices at job? If yes, then at which level?

***Answer:*** Yes, BYOD are allowed. These are allowed in only non sensitive environments.

***Question 5:*** Is BYOD have any bad effects on the network infrastructure of organization?

***Answer:*** No, BYOD has no bad effects on network infrastructure of organization.

***Question6:*** What kind of network related risks your organization feels while using your VPN cloud with BYOD technology? Just give some examples?

***Answer:*** BYOD has no affect on VPN cloud computing as the systems on which VPN client is installed are fully secured. VPN is allowed on thin client machines. All external ports are disabled. There is no local storage on disk, Bluetooth and Wi-Fi is disabled.

***Question7:*** Do you have any network security policy in your organization? If yes, what are the security mechanisms used for maintaining the network security? List names.

***Answer:*** Yes, we have network security policy. We have decided systems with proper authentication; In addition have monitoring controls in the network. Plus we use dedicated network lines for connectivity.

***Question8:*** How you protect your organization's network from viruses, worms, spywares, botnets and advanced malwares?

***Answer:*** We have antivirus systems in place to detect and kill viruses that make an entry to our systems. Users are not allowed to install unapproved software. Systems are monitored for viruses and use of un approved software. Emails are filtered for presence of any virus as well.

***Question9:*** How you protect your organization's hardware from physical security flaws? What physical security controls are in place in your organization?

***Answer:*** Every system is a branded system with genuine sw and tools. All external ports are closed at bios level password to which is known to LAN team only. The systems are locked and strapped so that HDDHard Disk Drives and other components are secured inside CPU. The facility is access controlled.

***Question10*** While using smart phones, what kind of restrictions you have when you work in our organization for your organization's network security purpose?

***Answer:*** Only approved devices are allowed for official purposes. Private devices are allowed for personal use only. Network is secured against any attack. Network maintains list of approved systems as white list. Any system which shows up on network and is not listed in white list is alarmed to concerned persons for mitigation. Bluetooth and Wi-Fi is disabled on most systems. Users don't have admin access to their machines.

***Question11:*** How you manage Access control, Application security, authentication, accounting, authorization, encryption, physical security, disaster recovery planning, business continuity management, network security, web security, backup, hot swap over to second site etc?

***Answer:*** We have multiple offices in same and alternate sites in India and abroad. All systems and office sites are connected over leased and secured and encrypted network lines. Data systems are backed up online and available 24x7 with all required redundancy. We take backup(additional) hot seats at each site to cater to disaster recovery and business continuity when we need to move people. All systems are on cloud which can be accessed from anywhere in the globe. Remote access is granted to critical users to work from home during disaster.

***Question12:*** Can you please list some examples of potential projects related to information security and network security?

***Answer:*** Cloud computing, Consolidation of project resources, Data consolidation System consolidation etc.

***Question13:*** What kind of different roles and responsibilities of Network Administrator in your organization?

***Answer:*** A network administrator will manage and configure network systems. He will monitor logs and events on systems to monitor any security concern. He will ensure that all systems are up and running at all times. He will ensure backup of vital systems and network components. He will monitor performance of network and manage bandwidth of network. He will ensure that internet services are taken from at least two service providers for maximum redundancy specially during disasters.

***Question14:*** What kind of security policies used in your organization?

***Answer:*** We use policies such as : info security policy, remote access policy, laptop security policy, bb security policy, data management policy, etc.

# B Interview2: The interview was an Email Interview and the answers were sent in Author's Gmail ID

**By Satish Das, CSO(Chief Security Officier) Cognizant Technology Solutions Corporation, India**

***Question1:*** Do you have Virtual Private Network Cloud in your Organization? If yes then can you list five advantages of it? Just name those?

***Answer:*** Yes we are using VPN connection over cloud computing. Advantages are

1. It allows authorized resources to connect to company network from anywhere.
2. Resources can be allowed to work during travel.
3. Resources can be allowed to work from home minimizing company expenses towards office space fitments, furnishing, and electricity in other expenses.
4. It saves productive hours by minimizing travel to office.
5. It Provides secured connection.

***Question2:*** While using VPN cloud what kind of challenges networking related problems you are facing, just give some examples.

***Answer:*** Slow internet, VPN client corrupted, internet connection disrupted, remote areas having no internet connection.

***Question3:***Are you using VPN Cloud by third party (outsourcing) or you have private cloud network? Can you please list some security mechanisms which is used by your organization for maintain the security by third party side?

***Answer:*** Yes using third party cloud. Security controls involve dual authentication on network, dedicated servers, segregation of network with firewall, adequate security controls on servers, secured databases.

***Question 4:*** Is BYOD Bringing your own devices allowed in your organization? While using personal devices at job? If yes, then at which level?

***Answer:*** Yes we allow BYOD for managers and above in nau environment

***Question 5:*** Is BYOD have any bad effects on the network infrastructure of organization?

***Answer:*** Our network is secured to detect, prevent any connection to unauthorized devices.

***Question 6:*** What kind of network related risks your organization feels while using your VPN cloud with BYOD technology? Just give some examples?

***Answer:*** VPN client is not allowed on BYOD devices. VPN client is secured and installed only on authorized devices. VPN client cannot be copied from auth devices to any unauthorized devices as all points for data leakage in the network and systems are plugged. All network related risks are mitigated for VPN cloud environment.

***Question7:*** Do you have any network security policy in your organization? If yes, what are the security mechanisms used for maintaining the network security? List names.

***Answer:***Yes we maintain security policy as per iso 27001 standards. Network is secured using strong firewall, domain, VPN authentication and ESA token based authentication. Antivirus control and network monitoring systems are established to secure network. We also use private ip addressing scheme. Above all individuals are given role based access to systems. Any violation to rules is monitored and alerted to concerned persons. Enhanced Subscriber Authentication for BYOD

***Question8:*** How you protect your organization's network from viruses, worms, spywares, botnets and advanced malwares?

***Answer:*** Email and network traffic is monitored to prevent any virus attacks. Users are educated to not to forward chain emails within org. Systems are secured such that users cannot copy any tool or application into the same via CD ROM or USB or Bluetooth etc. Firewalls are in place and entire network is behind DMZ.

***Question9:*** How you protect your organization's hardware from physical security flaws? What physical security controls are in place in your organization?

***Answer:***Our org is physically protected with following measures:

- (a) Well guarded 24x 7.
- (b) Access controlled using access control systems.
- (c) CCTV cameras.
- (d) Segregation of public, semi public and private zones.
- (e) Access to highly sensitive areas and systems limited to a few individuals, systems such as laptops etc have RFIDs installed to track movement which is mapped to respective owner (example any person carrying somebody else's laptop will be detected by system and alarm will go off to intimate guards on duty.

All systems are secured at respective place. Incoming hardware is checked for viruses and outgoing hardware is cleaned of any data on it before dispatch. Only authorized persons are allowed to bring in or take out company material.

***Question10:*** While using smart phones, what kind of restrictions you have when you work in our organization for your organization's network security purpose?

***Answer:*** most smart phones to senior management are official. GOOD software is used to protect and segregate office communication from personal communication. Users don't have the ability to copy any official data and send out for personal use. Network is monitored 24X7. Any device if connected to network shows up giving details of device, location within a radius of 10 meters.

# C Interview3: The interview was a face to face interview at Oslo, Norway

**By Software Developer at Corporation Nordea A/S, Norway**

***Question1:*** Do you have Virtual Private Network Cloud in your Organization? If yes then can you list five advantages of it? Just name those?

***Answer:*** I have not used it.

***Question2:*** While using VPN cloud what kind of challenges networking related problems you are facing, just give some examples.

***Answer:*** NA

***Question3:*** Are you using VPN Cloud by third party outsourcing or you have private cloud network? Can you please list some security mechanisms which is used by your organization for maintain the security by third party side?

***Answer:*** NA

***Question 4:*** Is BYOD Bringing your own devices allowed in your organization? While using personal devices at job? If yes, then at which level?

***Answer:*** Yes. We cannot use Wi-Fi or connect to organization network.

***Question 5:*** Is BYOD have any bad effects on the network infrastructure of organization?

***Answer:*** No, cannot connect to network in the organization.

***Question 6:*** What kind of network related risks your organization feels while using your VPN cloud with BYOD technology? Just give some examples?

***Answer:*** We don't use VPN cloud with BYOD.

***Question7:*** Do you have any network security policy in your organization? If yes, what are the security mechanisms used for maintaining the network security? List names.

***Answer:*** Login and password. Also, we can use only devices provided by the organization to access the organization network, Firewalls.

***Question8:*** How you protect your organization's network from viruses, worms, spywares, botnets and advanced malwares?

***Answer:*** Using above security policies by spreading user awareness.

***Question9:*** How you protect your organization's hardware from physical security flaws? What physical security controls are in place in your organization?

***Answer:*** Access control on hardware. Only users know the login information.

***Question10:*** While using smart phones, what kind of restrictions you have when you work in our organization for your organization's network security purpose?

***Answer:*** Cannot connect to network within the organization.

# D Interview4: The interview was an Email interview

**By An Employee of Corporation Gallagher Group Ltd,New Zealand**

***Question1:*** Do you have Virtual Private Network Cloud in your Organization? If yes then can you list five advantages of it? Just name those?

***Answer:*** NA

***Question2:*** While using VPN cloud what kind of challenges networking related problems you are facing, just give some examples.

***Answer:*** NA

***Question3:*** Are you using VPN Cloud by third party outsourcing or you have private cloud network? Can you please list some security mechanisms which is used by your organization for maintain the security by third party side?

***Answer:*** NA

***Question 4:*** Is BYOD Bringing your own devices allowed in your organization? While using personal devices at job? If yes, then at which level?

***Answer:*** NA

***Question 5:*** Is BYOD have any bad effects on the network infrastructure of organization?

***Answer:*** NA

***Question 6:*** What kind of network related risks your organization feels while using your VPN cloud with BYOD technology? Just give some examples?

***Answer:*** NA

***Question7:*** Do you have any network security policy in your organization? If yes, what are the security mechanisms used for maintaining the network security? List names.

***Answer:*** webmarshal and mailmarshal.

***Question8:*** How you protect your organization's network from viruses, worms, spywares, botnets and advanced malwares?

***Answer:*** Using Trend.

***Question9:*** How you protect your organization's hardware from physical security flaws? What physical security controls are in place in your organization?

***Answer:*** Security lock doors.

***Question10:*** While using smart phones, what kind of restrictions you have when you work in our organization for your organization's network security purpose?

***Answer:*** MDM to wipe out the device.

# E Abberivations

1. MPLS————————-Multiprotocol label switching.
2. NVP————————Network Virtualization Platform.
3. BYOD————————Bring your own device.
4. VPN————————Virtual private network.
5. UPS————————Uninterrupted power supply.
6. LAN————————-Local area network
7. MAN————————Metropolitan area network
8. WAN————————Wide area network
9. WLAN————————-Wireless local area network.
10. CEO————————-Chief executive officer.
11. 3G and 4G——— 3 Generation and 4 Generation.
12. TBSS————————Tata business support services.
13. MNC————————Multinational corporation.
14. PC's————————Personal computers.
15. NIST————————- National Institute of standards and technology.
16. Naas————————-Network as a service
17. Saas ————————-Software as a service.
18. Paas————————-Platform as a service.
19. Iaas ————————-Infrastructure as a service.
20. IBM————————International Business Machines
21. CSP———————— cloud service provider.
22. API————————Application programming Interface.
23. CRM ————————-Customer relationship management
24. AP's ————————Access Points
25. DE's———————— Distributed entities
26. CE's ————————-Central entities

27. SLA's————————Service Level Agreements
28. USI————————User to Service Interface
29. XML————————Extensible Mark-up Language
30. TCP————————Transmission Control Protocol .
31. IBSG———————— Internet Business Solutions Group
32. CISCO————————-Computer Information System Company
33. SANS———————— System Administration, Networking, and Security Institute
34. RSS————————Really Simple Syndication
35. RFID————- Radio frequency identifiers.
36. HDD———————— hard disk drive.
37. CIA————————- Confidentiality , Integrity, Availability.
38. AT & T——— American Telephone & Telegraph
39. BPO———————— Business process outsourcing.
40. RFID————- Radio Frequency Identification
41. SAP———————— System application programming.
42. ERP————- Enterprise resource planning.
43. PHP———————— Personal home pages.
44. VC++——— Visual C++
45. CAD————Computer aided design.
46. CAME——- Computer Aided Manufacturing Environment
47. GUI————————-Graphics user interface
48. TCP/IP———————— Transmission control protocol/ Internet protocol.
49. RSTP————Rapid Spanning Tree Protocol
50. CE————————Customer Edge
51. PE———————— Provider edge.
52. PPTP————Point to point tunnelling protocol
53. L2TP————Layer 2 tunnelling protocol
54. IPSec————internet protocol security
55. SSL————————Secure socket layer
56. DMZ——- Demilitarized Zone.
57. ISDN————-integrated switch digital network

58. PSTN———public switch telephony network
59. PDA———-personal digital assistant
60. BGP————border gateway protocol
61. VAS————Value added services.
62. ATM————-Asynchronous transfer mode
63. QoS————-Quality of services.
64. IGP———— Internet gate way protolcol.
65. RF————Radio frequency.
66. DSL————-Digital subscriber lines.
67. T1 line———— T-carrier 1 (digital transmission line, 1.544 Mbps, 24 voice channels)
68. WEP———— Wired Equivalent Privacy
69. WPA1———— Wi - Fi Protected Access
70. WPA2————Wi - Fi Protected Access
71. RID————————Router ID
72. ACL————————-Access control list.
73. DoS————————Denial of service.
74. GSM———————— Global System for Mobile Communications
75. USB———- universal serial bus
76. AAA——— Authorization, Authentication, Accounting
77. CIA———— Confidentiality, Integrity, Availability.
78. DNS———— Domain name server.
79. ARP————-Address resolution protocol.
80. SQL———— structured query language.
81. DDoS————Distributed denial of service..
82. IPS/IDS——Intrusion prevention systems/Intrusion detection systems.
83. MAC————Message authentication code.
84. SMS————————Short message servicing.
85. VoIP————————-Voice over internet protocol
86. NAC————————Network Access control.
87. MDM————————-Mobile device management
88. OS————————-Operating system.

89. SSID————————-Service set identifiers.
90. WIPS/WIPS———Wireless intrusion detection system/ prevention systems.
91. NIDS————————Network intrusion detection systems
92. XXS————————Cross site scripting.
93. CSRF————————-Cross-site request forgery
94. ESA————————-Enhanced subscriber authentication.
95. CCTV————Closed-circuit television
96. BIOS————Basic input output system.