Security Aspects and Implementation of Secure Methods in a Data Center

Syed Rahil Faiz
MSc Cloud Computing,
National College of Ireland,
Dublin, Ireland.
faiz.zx4@gmail.com

Salman Hadi
MSc Cloud Computing,
National College of Ireland,
Dublin, Ireland.
salmanhadi1993@gmail.com

***Abstract*—Data center security is the most important factor in the cloud environment. The most important reason a client would choose cloud over on premise is the trust itself. Hence, making the data center secure at every level is extremely significant in establishing the integrity of the company. This paper proposes various requirements and tools that are needed to secure a data center from any intentional or unintentional malicious activity. Unauthorized access, biometric authentication, surveillance systems and other security measures are integral in securing the infrastructure.**

Keywords—cloud environment; Unauthorized access; unintentional malicious activity; biometric authentication; surveillance systems, infrastructure; integrity

I. INTRODUCTION

Cloud based architecture is hugely embraced in today's world, this is where Data centers come in picture. They are also known as the server farm, where in there is dedicated space where the most of the organizational servers or storage areas are located. It is composed of 4 main components as follows: white space, support infrastructure, IT equipment and operations. White spaces are referred to raised floors areas which are typically measured in square feet. Support infrastructure is referred to the space and components required to support the operations that are supposed to run in the Data Centers, components like power transformers, Uninterrupted power supply sources, air conditioners, chillers, air distribution channels and similar such equipment. IT equipment are referred to equipment like racks cabling, servers, management systems, routers and other networking components which are form the heart of Data centers for organizational services. Operations are referred to the maintaining of all components like for their proper functioning which include both IT equipment and support infrastructure. These operations are divided among respective staff like technical and non-technical members.

Data center can be unique in their designs based on their priorities, architectures and requirements can differ in many ways. An example for this is, data centers built by organizations like Amazon or Microsoft satisfies factors location chosen, infrastructure and other security requirements that can drastically be different for private Data centers such as the one built for Pentagon which requires a high security for its classified data.

Data center is an important operational area for businesses which is used to store, manage and distribute the data. They play a vital role in managing critical system's data and carrying operations needed for everyday basis. Therefore safe guarding Data centers stands one among the top priorities for all organizations.

As organizations and other users take advantage of cloud based approaches for their operational and economic benefits, it becomes really important to secure these virtualized Data centers which include cloud deployments and other hybrid environments effectively. Because if the security factor is compromised in any way then it creates a gate way is exposed to the vulnerable world of threats and Data breaches which can cause a huge impact. Thus security for data centers has to meet some security compliance standards, which even organizations enquired for before accepting the cloud services regardless the computing environment.

The complexity in providing the secure environment for access the critical data by sealing it from others, following end-user privacy agreement and assuring the seamless continuity in business in today's world is challenging and demands for hyper-dynamic, high-performance, data management infrastructure and new approaches in network and data security every now and then.

Below mentioned terms are some commonly used terms when it is concerned with security aspects:-

• **Threat** - An event that has the potential to harm any resource and disturb its normal functioning.
Example: Threat can be loss of important information or any application.
• **Vulnerability** - It can be referred to an insecure channel which when discovered can lead to threat.
Example: Vulnerability can be a server software running on an older or unknown version which could be dangerous to new attacks.
• **Attack** - Exploitation of a vulnerability and favoring unauthorized access to misuse the resources.
Example: Attack would be an event where in a person exploits a vulnerability to reduce the performance or even stop the normal functioning of server.

II. NEED FOR SECURE DATA CENTER

Data centers play a key role in business's success of organizations. The Data centers are the houses for storing and retrieving the data as and when desired, thus maintaining a proper security is mandatory task. The loss of data and applications can hugely impact the growth and functioning of any organization's business.

Huge usage of Data centers for storing confidential information and data makes it more critical for becoming targets for attacks and the number of data centers increase so are the number of attackers keep increasing year by year. There have been attacks with new techniques and more sophisticated tools [2].

Continuous expansion of internet and its applications with protocols used, is one of the cause for creating more vulnerabilities. For example: consider a complex application, this while installation can have more chances of improper installation when compared to smaller applications hence making ways to vulnerabilities. Data center management requires 3 main approaches in which first will to monitor and analyze the whole system and the situated area, secondly inspecting how can a data center can be made more efficient in energy and space, thirdly automating the synchronization among the facilities which include hardware , network and other related applications.

III. TOOLS AND METHODOLOGIES

In general a data center security can be divided into 3 segments as follows,

a. Physical segment
b. Data segment
c. Network segment

a. Physical segment:

Physical segment consist of all the hardware components which are available for the seamless working of data center. This includes components like servers, racks, doors, cabling and such components, which act as the part of data center physically.

b. Data segment:

Data segment refers to the confidential data and other important information stored in the servers. This can be data or information related to any privately owned data center or a cloud provider's data center.

c. Network Segment:

Network segment refers to the connections required in connecting all the servers internally as well as to the outer environment. This out environment refers to organizations or users who are involved in accessing the data center.

In depth analysis of each layer,

a. Physical layer:

Designing a physical security for data center needs more and more use of innovative architectural and engineering approaches [3]. Physical access should strictly be controlled and monitored on both points, the perimeter and at the entry point of the buildings by professional security members using modern techniques like video surveillance, intrusion detection systems and other electronic means. Physical security should have some readily accessible rules like,

- No badge sharing or entries using piggy back
- All visitors should have a record at the reception and should be escorted with an authorized staff till the end.
- A statement in written when an individual has signed in for work.
- At least two-factor authentication should be required to access data center floor.

Tools used:

1. *Physical barrier:*

These are the barrier used to prevent individuals to communicate with other side of environment. In this paper, we make use of anti-ram gates which act as the first level of barrier by covering the area which are used to enter. Secondly, bollards are short and thick post which are commonly used to block the area from entering any vehicle. Thirdly vehicle barriers are the equipment that are used to stop the vehicle from entering which are usually placed in vehicle entrances, these barriers can expanded when needed or closed when not in use.

2. *Biometric scanner:*

These are the instruments that are used to authenticate a person's authorization by scanning any unique feature such as thumb print, retina scan, body fluid levels, and heart rate. Similar such features can be used as unique identity of a person, where in the mentioned ones are some of the commonly used.

3. *Key Cards:*

They are thin, rigid, rectangular cards which usually has a magnetic strip containing some data with respect to authentication of an individual. There are many different types of key cards like cards with microchips, bar codes magnetic scanner and so on.

4. *Cameras:*

There are special cameras called the surveillance cameras that are used particularly used to monitoring the activities and other changing aspects, here mainly used for managing and directing people to avoid any undesired behavior.

5. *Access control vestibule:*

These are typically door type frames which are placed in the entrances of buildings or any rooms where in it has capability to detect the items which are not supposed to be carried. These vestibules can include features like ID card scanning and so on.

6. *Motion detectors or sensors:*

These are the equipment that are used to detect any movements of objects, most commonly used to detect people. For example:

Automatic switching on and off of lights when human movements are detected.

7. *Alarms:*

All exterior doors and sensitive areas within the facility must be hard wired with alarms.

Below mentioned are some of the security designs with some brief explanation that needs to be incorporated in the infrastructure.

1. *Outer perimeter:*

Outer most perimeter of data center acts as a basic and critical part in avoiding intruders from outside world. This perimeter include equipment like 24/7 video surveillance, fences, limited entry points and access control near to entry points. Physical security barrier include tall strong walls, anti-ram gates with bollards by the sides, vehicle barriers and guard stations whose duty is to enquire to confirm the authorization and then let to enter the premises. Inner premises should have sensors to monitor intrusion detection or to check any suspicious activities on the premise and these inner premise will also be monitored using cameras which will be connected to security room.

2. *Entering the building:*

Just after entering the building premises which is the exterior portion hidden inside are the IT equipment where all the servers and other operational services are placed.
Below mentioned are few things that are to be adhered when securing the entrance of the building,

- Video surveillance is generic factor.
- There should be least number of entrances in a building which complies with fire ordinance policies.
- All employees or visitors should enter through access control vestibule.
- Include security checks like key cards scanners, biometrics.
- There should be strict security policies with regards to persons for all facility entrances.
- Security guards should be available all time onsite.
- Systematic logging procedure for any visitor who enters the premises.
- ID cards system should be must for all employees and visitors and badges should be worn all time when on premises.

3. *Equipment location:*

This is the core area where in all the IT equipment needed to help the business run seamlessly, are placed. Below mentioned are some of the rules that has to be adhered for maintaining more secure environment:

- There should be video surveillance and motion detectors installed for all entrances and interior doors, other important equipment location.
- Equipment should be placed in a secure room.
- Cabinets should be locked and sealed when not physically accessed.
- Firewall services with 24x7 monitoring should be managed.
- Backup services like lighting systems and cable vaults should be available.

b. Data Layer:

Data protection of a company aims to improve the integrity of the business by reducing the lack of data verification while improving the data availability of the data center. There are 5 basic strategies for data protection.

1. Backup and recovery
2. Remote data movement
3. Storage System Security
4. Data Lifecycle Management
5. Information Lifecycle Management

Most of the organizations tend to believe that having a backup of data or storing it to another location is sufficient to protect the data. Downtimes in a data center are mainly caused by hardware failures, power outages, security breaches etc. [1]

The strategy that needs to be implemented for the proposed data center is as follows:-

a. File Fragmentation

File Fragmentation needs to be implemented in order to strengthen the security. Data of a particular file are fragmented and stored in random slots in order to protect the confidentiality of the data. File fragmentation may lower the performance speed but it ensures security [8].

b. Replication

Apart from storing data in different locations, replication is another strategy for securing the clients data. Creating a replication of original data on other machines and servers and at a location away from the original one is important. This strategy will help in reducing the downtime during disaster recovery planning [8].

c. *File Naming*

The next strategy in protecting the data is file naming. The files stored in the data center needs to be given random generated names that are not in clear text and are unreadable by humans [8].

d. Data Formatting

When a hard disk drive is corrupted in the system, it needs to be destroyed completely. To ensure that there is no trace of existing data and it unrecoverable, a destruction process needs to be followed. The HDD will be first crushed with the help of a crushing device and then shredded to pieces. The shredded pieces will then be sent for recycle.

e. RPO and RTO

RPO stands for recovery point Recovery Point Objective and RTO stands for Recovery Time Objective. RPO and RTO are one of the most crucial parameters for disaster recovery. These assist enterprises to choose an efficient backup plan.

RPO or Recovery Point Objective is basically an estimation about the amount of data that can be lost. On the other hand, RTO or Recovery Time Objective implies after how much time it will take to recover after a downtime in the server. [9]

f. *Encryption*

The best encryption tool that can be used enhancing security measures is AES, which is short for Advanced Encryption Standard. It is a symmetric encryption algorithm, which comprises of fixed block size of 128 bits, and a key size of 128, 192 or 256 bits. The number of cycles of repetitions depends on the key size used for an AES cipher. It uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key. Below is an example of the working of the AES encryption.

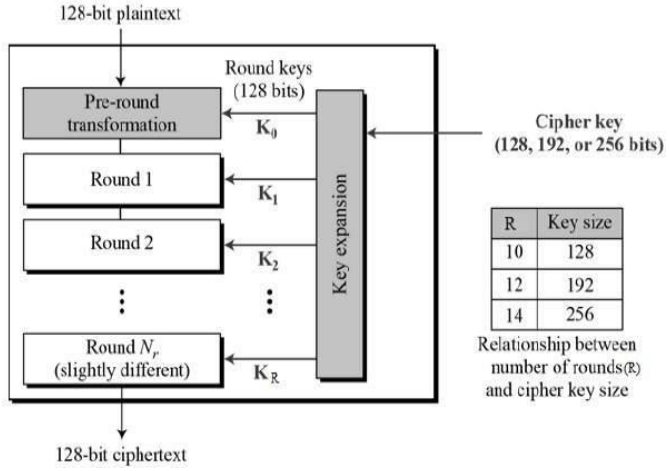

Fig 1: Advanced Encryption standard

Due to the encryption key size used by the algorithm being in the order 128, 192 or 256 bits, it results in billions of permutations and combinations. This is why AES will be a useful algorithm. Furthermore, it performs faster with low RAM requirements compared to other encryption tools. It also works well. [10][11]

c. Network and Operations Layer

Network security in data center can be defined as the security measures taken to avoid any interruption in the operational environment of the whole networked infrastructure. Network security of data center is a very important factor which concerns the clients, where in clients include their critical information regarding their organization, need of data theft protection, 24/7 monitoring networks to prevent any intrusions, taking regular actions and mitigate if any threats[6]. Thus meeting all demands by regularly updating to compliance standards.

Attacks can be of many different types where in the commonly known are as below [4]:

- Packet sniffing
- IP spoofing
- Denial-of-service (DoS) attack
- Password attack
- Man-in-the-middle attack
- Application attack
- Port redirection attack

Network security is a critical for any organization's business point. Hence some of the security options which can be included as must are as follows [4]:

- Firewall protection services
- Intrusion Detection and Prevention services (IDPs)
- Virtual Private Network (VPN) services
- Payment Card Industry (PCI) Compliance services

Types of attacks and their solution:

a. Packet sniffing:

Aside from refraining from using public networks, encryption is your best bet to protect yourself from potential packet sniffers [5] [6]. Using HTTPS, the secure version of HTTP, will prevent packet sniffers from seeing the traffic on the websites you are visiting.

Solution:

- Encryption makes the channel more secure for data access because even if there is the data is captured, without the secret key combination the data cannot be retrieved. This encryption is used in secure version of HTTP. i.e., HTTPS. Combination of both Network based encryption and application-layer encryption can be more effective [5][6].
- Virtual Private Network (VPN) is another way of protecting the data by creating a secure tunnel of encrypted data which is being used on websites, services and applications.

b. IP Spoofing:

IP spoofing attack is a situation where in the attacker uses the same IP as the user to stay hidden while accessing the data at same time. There 2 types of spoofing attacks which are Address Resolution protocol (ARP) and Domain Network Service (DNS). In ARP, the attacker uses the MAC address for accessing the data across the network. In DNS, the attacker uses the domain names to reroute the user from the original website to attacker's information trapping location.

Solution:

- Packet Filtering: they help in filtering and blocking packets which are conflicting source address information.
- Avoiding trust relationships, this makes attackers more difficult to access data.
- Use of cryptographic network protocols like Transport Layer Protocol (TLS), Secure Shell (SSH), Secure HTTP (HTTPS).

c. Denial-of-service (DoS) attack or application DoS:

This is a situation where in the attacker prevents the users from accessing any site by shutting down the functioning

of any particular site. A study reported (2015) that an average of $1.5 million in costs over the period of 12 months and on average, companies had 4 DoS attacks annually. Below in Fig. 2 is the breakdown of the financial consequences of a DoS attack.

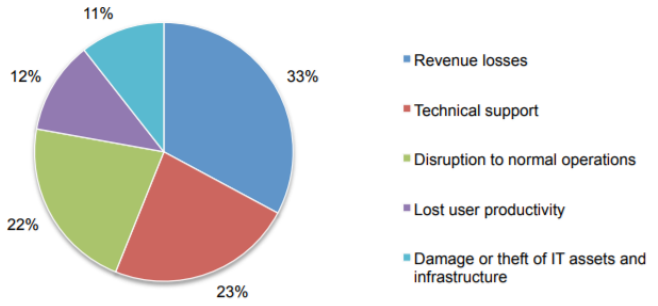

Fig. 2 Breakdown of the financial consequences of a DoS attack

Solution:

- Use of Intrusion Detection and Prevention systems (IDPs) offer the ability to defend DDoS attacks.
- Providers should "scrub" incoming traffic against the known vectors which will help in scanning suspicious traffic from untrusted resources and route the legit traffic from the bots.

d. Man-in-the-middle attack:

Man in the Middle (MITM) Attack is a situation where in the attacker keeps an active eave dropping between 2 communication points.

Solution:

- Intrusion Detection System (IDS) can help in monitor the network activities and immediately alert if any unauthorized access has been attempted. Tools like Advance Address resolution Protocol (XARP or ARPOn) and Dynamic Host Configuration Protocol (DHCP) methods can help reduce of MITM attacks.
- Use of VPN avoids confidential data to be protected even if the attacker accesses the data, the data will be encrypted.

e. Port redirection attack:

Port redirection is a trust based exploitation, here the attacker if is able to compromise the host will easily gain access to firewall and would otherwise will be blocked. This attack is illustrated in Fig.3 which shows how a hacker can misuse a host.

Solution:

Port redirection can be controlled primarily through the use of proper trust models. Antivirus software or a host-based intrusion detection system (IDS) can help avoid attackers to succeed in changing the configurations of the firewalls and compromise them.

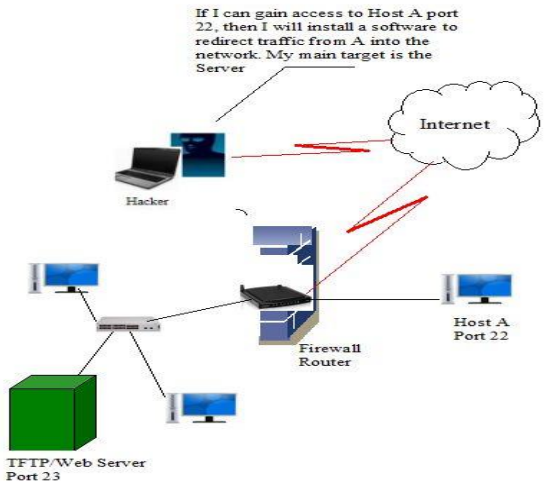

Fig 3. Block diagram on how port redirection will work

IV. Certification Compliance

ISO 27001 is the international standard which is used globally for managing risks and possible threats to the information that the company holds. It facilitates the management of the security of the client's and stakeholder's information that the cloud holds. It basically sets a series of requirements that needs to be met for Information Security Management System (ISMS). The ISO 27001 certification is accredited by both INAB and UKAS. This means that the ISO 27001 and ISMS lays out a framework and best practice that will help the organization to meet the following factors:

a. Protect client and employee information
b. Manage risks to information security
c. Achieve compliance with various regulations including European Union General Data Protection Regulation (EU GDPR) [12]

Some of the advantages apart from managing and monitoring the information are:

a. Keeping confidentiality
b. Providing clients details on how to manage risk
c. Secure exchange of information
d. Competitive advantage
e. Minimizing risk exposure [12]

V. Testing

a. Physical layer penetration testing:

The main intention of doing penetration testing is to check how well is the infrastructure of data center is organized to handle intruders and to make sure there are no vulnerable points. The basic step by step approach as shown in Fig.4 for identifying the information about security vulnerabilities is as follows [7]:

1. Gathering required information

2. Threat modelling
3. Vulnerability Analysis
4. Exploitation
5. Post-Exploitation
6. Reporting [7]

Fig. 4: Physical penetration testing approaches.

Below are the step by step methods which are shown in the Fig. 5 and briefly explained,

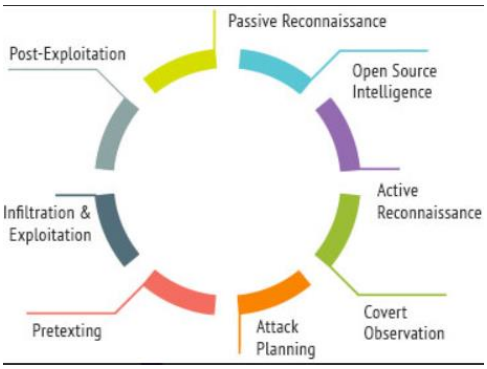

Fig. 5: Physical penetration testing Methodologies.

- Passive Reconnaissance is the initial stage where in the intention is to gather as much as information possible about the particular area.
- Open Source Intelligence is a process of collecting information which is freely available and conveys more about the tools used, its people and the environment it is in.
- Active Reconnaissance is a process where in information gathering is done via phone calls, emails and other such medium directly to the particular member in case of information not being found from open sources.
- Covert Observation is a step where in control and monitoring staff are observed to identify any pattern which might be useful for further proceeding.
- Attack Planning is a phase where all the information gathered from above steps makes things easier in analyzing the security well and can be prepared for the next part of plan.
- Pretexting is a step where in the planned steps for executing are set and are ready for implementation purpose.
- Infiltration, Exploitation & Post-Exploitation are phases where in the planned things from the early stages are implemented accordingly. After the implementation, Post-Exploitation is done where in not only flaws are eliminated but also care is taken no other vulnerable points can be found [7].

b. Data and Network layer testing:

Intrusion Detection System

In cloud computing systems, data is prone to a number of attacks. Denial of service, (DOS) or Distributed Denial of Service (DDOS) is one of the most common attacks. It affects data availability of the system and can have serious implications on the integrity of the company. To avoid such attacks, intrusion detection systems are needed. The IDS are of three types:

a. Host-based IDS
b. Network-based IDS
c. Distributed IDS

Host based IDS are responsible for monitoring host machines, network based IDS detects intrusions on the network system and distributed IDS tries to detect intrusions on both host and network systems. There are two types of IDS, namely, Anomaly detection that detects any irregular or suspicious occurrences from the user's behavior. Another type is misuse detection that tracks the existing patterns of an attack and tries to detect a similar pattern in the system. Once detected, it alerts the system to take necessary steps. [13]

Alien Vault-

The intrusion detection system software that can be used for the data center is Alien Vault. It meets all the security assurances for an efficient IDS. Alien Vault is capable of collecting security events, review log data and perform analysis without having to deploy and manage multiple security point products. Threat detection, incident response and compliance management are all included in one easy to use solution software. It collects security data from on premise and cloud applications and monitors it to detect any probable threats or attacks. It includes behavioral monitoring, asset discovery and vulnerability assessment apart from intrusion detection. The software consists of automated jobs that makes it more convenient to use and manage the security aspect of the data center [14].

Penetration Detection Testing:-

Penetration test is used to evaluate the vulnerability of the security system in the IT infrastructure. The vulnerabilities can be present anywhere in the system, be it the operating system or even the end-user behavior. Therefore, a series of assessment is done in order to detect any possible flaws that may be present in the architecture. Penetration tests can either be manual or automated, depending on what domain of the system is being tested systematically. Some of the benefits of penetration testing are:-

a. Intelligently managing vulnerabilities.
b. Reducing cost of network downtime.

c. Meet regulatory requirements.
d. Improve industry image.
e. Clients and stakeholders loyalty [15].

Metasploit:-

Metasploit is a penetration testing tool that provides multiple ready-to-use exploits and a range of customizable testing tools for the user. It consists of a Java GUI and builds web-based support. Metasploit consists of built in sniffer, DNS server and access point to provide with test attacks. Following steps are some steps in Metasploit that is taken while facilitating an attack:

1. Choice for exploits.
2. Configuration of an exploit using remote IP address and remote port number.
3. Choose a Payload.
4. Configuration of payload using local IP address and local port number.
5. Execution.

Metasploit will definitely make the security system more secure and the efficiency will further bring out more vulnerabilities that can be solved and hence making the infrastructure safe from attacks. [16]

Network Layer Testing:-

Testing in Network layer for data centers follows the PASS methodology. PASS stands for *Performance, Availability, Security and Scalability.* Network layer can come across various attacks like Man in the Middle, Packet Sniffing, IP spoofing, Denial of service, Port redirection attack. To counter such attacks, system vulnerabilities needs to be addressed by performing efficient testing methods. Following are some of the best practices:

a. Vendor Performance Testing:

Making sure that the network devices perform according to what the vendors have claimed the performance to be through testing tools.

b. Network Failure Threshold Testing

Detecting points in the network where failure occurs within the applications and user bandwidth beforehand.

c. Configuration Detect Testing

Configuration testing is essential in a network system that is complex and unifies the entire architecture of the data center.

d. PASS Methodology Testing

PASS stands for performance, availability, security and scalability. It improves network uptime, eliminates vulnerabilities and validates maximum number of users at one time. [18]

VI. FINDINGS AND RISK RATINGS

1. **Physical security** involves placing the data center equipment securely from unauthorized access because physical security includes direct physical contact with the equipment. Since exposure by placing to public buildings can increase the risk of unauthorized access, it is very important to have strong control over the access [26].
   Risk rating: High

2. **Periodic Review of visitor Access** is crucial in maintaining the security levels high and a key card has to be issued to make easily track able. Since observing these activities shows if there any suspicious activities.
   Risk Rating: medium

3. **Key card logs** are important for securing access to doors, since it shows both passed and failed attempts. For example, if any contractor or employee has many failed attempts to access can be taken for account and the reason for that cause.
   Risk Rating: medium

4. **Background check of employees** should be done as a mandatory to check whether the employees has no criminal records and there is no proper process to maintain these background check records.
   Risk rating: medium

5. **Authorization documentation** should be included in the policy to authorize the key cards. Staff members who have key cards should also have form stating the reason for accessing particular doors with necessary approvals and signatures.
   Risk rating: medium

6. **Environmental security** consists of several factors like wind flow, abundant water availability, fire protection or heating problem and natural disasters. Considering all these factors, area chosen should satisfy all the environmental factors.
   Risk rating: high

7. **Incidents and recovery** play a crucial role in data security, where in cases of unexpected failure of controls might require recovery to bring back to working condition.
   Risk rating: High

8. **Disaster recovery** is a mandatory plan where in the data redundancy comes into play. Hence residing the data in multiple locations helps to ensure the continuity of data center operations in case of any natural disasters.
   Risk rating: High

9. **Intrusion detection system** are important in finding if any unauthorized access is taking place but it has a drawback of false alarming sometimes[26].
   Risk rating: low

VII. CHALLENGES AND LIMITATIONS

Security in a data center is extremely complex, and hence any counter threat strategy of completely removing risk is impossible.

1. Use of HTTPS is more secure than using HTTP to facilitate encryption and avoid packet sniffing, however, it is impossible to cache pages in a shared cache. Additionally, since HTTPS is an end-to-end encryption, access to look inside the data stream cannot be done. [19]
2. Packet filtering is an efficient firewall procedure however, they require complex configurations. Furthermore, this process is unable to prevent attacks on application-layer. [20]
3. Although intrusion detection systems do a commendable job in detecting anomalies in the network, sometimes IDS can lead to false alarms identifying a legitimate behavior as an attack. [21]
4. Penetration Detection systems consists of a few limitations like lack of time, scope, accessibility, known exploits etc. [22]
5. In regards to the physical security, it is crucial to keep all the systems up and running at all times simultaneously since authorization consists of the each and every security system as a whole and not each being treated as individual access. Hence, consistent management and maintenance is required.
6. Implementation of security control required a lot of time. 69% of organizations claims to take up to 4 hours to set up a firewall for a new network application. Moreover, Updating of security devices can take up to weeks. [23]
7. Human error is inevitable and hence this could compromise the security system. More than half of organizations claim to have one or more human related errors in 2 years. [23]

VIII. CONCLUSION

Today, with so many innovations and range of technology options available, a data center project is an extremely huge task. Simultaneously, it is possible to develop efficient infrastructure with convenience. Hence, a lot of factors come in to play and security of the infrastructure is the most important aspect. Without a proper secure system, the data center will not have much use from the business point of view. Attacks on client data, downtimes will not just affect the availability of the system, but also the integrity of the company. It is highly advised to not compromise with the security system. Implementing a high quality security system will be expensive, but the returns are even greater. Top Cloud Computing companies experience negligible amount of downtime due to their highly secure systems and protocols. Higher availability is achieved and ultimately the integrity of the company is improved. As mentioned in the report, the security system in a data center covers not just the software aspects but also the physical ones. The security needs to be assured as soon as the border wall of the data center premise begins. From the entry gates to the server rooms, authentication of each and every personnel is very important. The global market for security in data center is predicted to reach USD 14.11 billion by 2022 [25]. Emergence of newer technologies has paved way for more challenging and competitive innovative methods that can be used in the security system in the data centers.

IX. REFERENCES:

[1] Cindy LaChapelle, Defining the right data protection strategy: The nuances of backup and recovery solutions. http://www.isg-one.com/index/module-article-detail/defining-the-right-data-protection-strategy-the-nuances-of-backup-and-recovery-solutions

[2] Mauricio Arregoces, *Data Center Fundamentals*,[ONLINE], Accessed on 9 December 2017, Available at: http://estigia.fi-b.unam.mx/maestria/Cisco%20Press%20-%20Data%20Center%20Fundamentals.pdf

[3] (May 2017) *Amazon Web Services: Overview of Security Processes*, [ONLINE], Accessed on 9 December 2017, Available at: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

[4] *Data Center Network Security*, [ONLINE], Accessed on 9 December 2017, Available at: https://cyrusone.com/resources/glossary/data-center-network-security/

[5] Atewologun Olumide and Abeer Alsadoon (November 2015), *Hybrid encryption model for secure cloud computing* http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=7368466

[6] Tom Brewster (April 2014), *Protect your business by encrypting your network*, [ONLINE] Accessed on 8 December 2017, Available at: http://www.computerweekly.com/feature/Protect-your-business-by-encrypting-the-network

[7] *Physical Penetration Testing*, [ONLINE], Accessed on 8 November 2017, Available at: https://www.redteamsecure.com/physical-penetration-testing/

[8] (2013)*Iris ID systems Inc, Security and Data Protection in a Google Data Center*, [ONLINE], Accessed 8 December 2017, Available at: https://www.youtube.com/watch?v=4IDD8BP2EmU

[9] Jaspreet Singh (2008), *Understanding RPO and RTO*, [ONLINE], Accessed 8 December 2017, Available at: https://www.druva.com/blog/understanding-rpo-and-rto

[10] Zaid Karkit, Mohamed El Marraki (17 November, 2015), *Applying Encryption Algorithm to enhance data security in cloud storage* [Accessed 8 December 2017,

[11] *Advanced Encryption Standard*, [ONLINE], Accessed 8 December 2017, Available at: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[12] ISO 27001:2013 – Information Security Management Systems, [ONLINE], Accessed 8 December 2017, Available at: https://www.certificationeurope.com/certification/iso-27001-information-security/

[13] Parag Shelke, Sneha Sontake, A.D, Gawande, (May 2012), *Intrusion Detection System for Cloud Computing*, International Journal of Science and Technology Research Volume 1, Issue 4, [ONLINE], Available at: http://www.ijstr.org/paper-references.php?ref=IJSTR-0512-5114

[14] *Intrusion Detection System*, [ONLINE], Accessed 8 December 2017, Available at: https://www.alienvault.com/solutions/intrusion-detection-system

[15] *Penetration Testing Overview*, [ONLINE], Accessed 9 December 201, Available at: https://www.coresecurity.com/content/penetration-testing

[16] Tarun Gupta (2010), *5 Penetration Tools To Secure Your Network*, [ONLINE], Accessed 9 December 2017, Available at: http://www.computerweekly.com/tip/5-penetration-test-tools-to-secure-your-network

[17] *Physical Penetration testing*, [ONLINE], Accessed 9 December 2017, Available at: https://www.redteamsecure.com/physical-penetration-testing/

[18] (2013) *Testing the Data Center Network: Best Practices*, [ONLINE], Accessed 9 December 2017, Available at: https://www.infopoint-security.de/medien/testing_the_data_center_network-best_practices_whitepaper.pdf

[19] *The downside of using HTTPS*. In: *Web Server Management: Securing Access to Web Servers*, [ONLINE], Accessed 10 December, Available at: http://people.ds.cam.ac.uk/jw35/courses/using_https/html/x183.htm

[20] *Firewall Categories*, [ONLINE], Accessed 8 December, Available at: http://etutorials.org/Networking/Router+firewall+security/Part+I+Security+Overview+and+Firewalls/Chapter+2.+Introduction+to+Firewalls/Firewall+Categories/

[21] Lynn Rademacher, *The Disadvantages of Intrusion Detection Systems*,[ONLINE], Accessed 10 December 2017, Available at: https://www.techwalla.com/articles/the-disadvantages-of-intrusion-detection-systems

[22] *Penetration Testing- Limitations*, [ONLINE], Accessed 10 December 2017, Available at: https://www.tutorialspoint.com/penetration_testing/penetration_testing_limitations.htm

[23] (May 18 2015), *Data Center Security Challenges*, [ONLINE], Accessed on 10 December 2017, Available at:)https://www.slideshare.net/CiscoSecurity/data-center-security-challenges-infographic

[24] *Data Center Security- A Global Strategic Business Report*, [ONLINE], Accessed on 10 December 2017, Available at: http://www.strategyr.com/MCP-7014.asp#sthash.ELI9HA1O.dpbs

[25] (July 2017), *Global data center security market will reach USD 14.11 Billion by 2020: Zion Market Research*, [ONLINE], Accessed on 9 December 2017, Available at: https://globenewswire.com/news-release/2017/07/27/1063255/0/en/Global-Data-Center-Security-Market-Will-Reach-USD-14-11-Billion-by-2022-Zion-Market-Research.html

[26] (June 2006), *Data Center Review*, [ONLINE], Accessed on 9 December 2017, Available at: http://leg.mt.gov/content/Publications/Audit/Report/06DP-05.pdf