Security Implementations In Loon Data Center

Vishal Kumar Singh, Kalyan Chakravarthi Bathena, Bino Annamma Varghese
{x18201687, x19106513, x18141633}@student.ncirl.ie
Cloud Security, M.Sc Cloud Computing
National College of Ireland
Dublin, Ireland.

***Abstract*—Security is one of the main concerns for the cloud providers and the customers. Data stored in data centers are confidential and is increasing day by day, customers want their data to be secure and except some privacy from the service provider. The idea of having a loon data center up into the sky was proposed in the geo-location field of having a data center. Having a data center in the sky not only prevents human interaction from the data center, but also secure the data centers location from the customers. The loon will be connected with the ground base station using a secure channel of laser communication, which is undetected by the normal crowd. In this paper we will see the important security implementations to secure data in the data center in many ways and with many tools and methods to make the data center and the data in it completely secured.**

Keywords — Loon data center, portable data center, security in loon data center, secure data center, flying secure data center.

I. INTRODUCTION.

Security of the data is becoming the most crucial issue these days, as huge amount of data is being stored at a data center. The data that is being stored is increasing, most of the companies and private organizations are storing their data in a data center. While the data needs to be made secure and confidential from external attacks and threats. The service provider or the data center holders are trying to implement the security aspects to the data that is stored.

The loon data center is built to provide the utmost security to the data present in it by using the techniques for their physical and software as well. Physical security includes wide range of strategies to prevent their interface from outer section. While the software security is trained by the virtual strategies that prevents the data from cybercrimes. The data center will be handling the most sensitive data of an organization so the security measures should be more critical. The protection levels of security practices are made complex to protect them from external attacks. Elements like physical, data, operational and network security measures are included for the loon data center. The report addresses all the security issues of the loon data center which make it more comparing with other services and types of data centers.

II. APPORACH AND PLANNING.

Securing the data center and the data is one of the important aspects of data center functioning. To achieve this goal to deliver security to our data center, we consider 5 levels or different security technique to implement best security features into our loon data center. The five categories and approach we plan are as follows: -

1) **Geo-location Level Security.**
2) **Physical Level Security.**
3) **Data Level Security.**
4) **Operational Level Security.**
5) **Network Level Security.**

Geo-location Level security- Protecting the data center from natural disasters, threats and attacks in the sky, so that our data center is safe and secure in the sky.

Physical Level Security- This combines the ways of protecting the data center from physical damages and the base station from unauthorized access and the hardware of the data center protected from fire and other damages.

Data Level Security- Considering the security of data on the data center by enabling data encryption, multi-level security and backups of the data.

Operational Level Security- Having a loon data center which needs to be monitored and controlled constantly from the base station, we need to implement security there as well.

Network Level Security- Securing the network and ways of communicating with the loon and the data center must be considered and implemented as well.

In this paper we will explore many ways to secure our loon data center in each of these security levels.

III. TOOLS, METHODOLOGIES AND FRAMEWORKS.

A. *Geo-location Level Security.*

Figure 1: - Geo-location of our loon data center.

The loon data center will be plcaed up into the atmosphere in the stratosphere layer, which is safe from natural disiaters like earthquake, floods which can be an issue if the data center is on land and water. The stratosphere layer of the atmosphere is 20 – 25km away from the earth surface and is wirelessly connected using laser and radio communication systems. The stratosphere layer has nothing but empty space and air in it, so there's nothing it can collide with to get damaged.

The geo-location of this data center is one of the main advantages of having this type of data center. It uses all nautal resources to work and is 100% dependent on it. It uses solar energy using solar panels to power the data center and the equipment's on the loon. The cooling is also natural, as the temperature in the stratosphere is always below zero and is around -50 Celsius, we only need to use the cold air to cool the data center using fans.

B. *Physical Level Security.*

As we know our loon data center is in the sky and is constantly moving with the wind directions, there is no human interaction possible with the data center. But we must consider other aspects to save the data center from attacks.

1) **Collision avoidance system.**
The data center is flying in the sky with the wind directions. We use radar technology to detect if there's an object coming towards the loon or if the loon is about to hit another loon. In this case the operator in the ground base station can change the course of the loon to catch different wind current and avoid collision of the loon data center. However, the chances of this happening is almost negligible.

2) **Fire Protection system.**
The cabinet of the data center has a smoke detector, fire sensors and fire alarm inside the cabinet, when ever it detects smoke inside the cabinet or if any hardware, batteries, catches fire. There will a fire extinguisher placed on top inside the cabinet which would deploy automatically, and the fans would also start running and cold air starts flowing through the data center in on time.

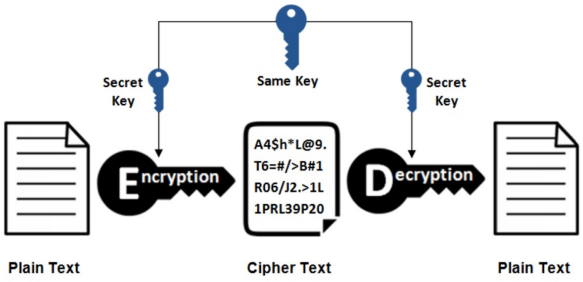
3) **Balloon Exploding.**
If the balloon at the top with helium gas in it, explodes or if there's a leakage of gas from the balloon. There will be 2 parachutes attached, one with the main balloon and other with the data center. These parachutes will be deployed automatically if there's a problem with the balloon and the data center will then be brought down to land safely.

4) **Loss of power supply.**
The data center is powered by solar energy using the solar panels attached with the loon. If the solar panels get damaged or stops working, the batteries on the loon to power the data center during night times will comes into action. The loon then must be guided to an easily reachable location and brought down to do the maintenance required and then launch it again.

C. *Data Level Security.*

The most important reason to have a loon data center is that, it can handle the crucial data as well as the confidentiality of the data as it has no direct human interaction. Now a days it is very hard to maintain the security intrusions for a data center. According to IBMs surveys only 20 percent of the US customers completely trust the data provides to have data privacy. Data breaches is the only problems faced by most of the large-scale organizations. However, these breaches can be prevented using some techniques such as Encryption, Backup and recovery, Compliance and transparency, Cyber insurance.
Apart from the physical security measure we've provided the data security is also much required for the loon data center. Considering the issues like encryption, backup and recovery and firewall protection which are further explained clearly in the following report. Additional to these types we also have terms like authentication, access control, data masking and tokenization. The loon data center provides high security measures by data encryption, software security and the firewall protection.

1) Encryption.
Encryption is the most commonly used technique to translate the data to from sender to client where the data can only be read by having the access key produced by the sender. The main objective of encryption is to transfer the data confidentially. Public key cryptography is the most secured encryption for the transfer of data while it is also called as the symmetric encryption. In symmetric encryption, it has same secret keys for encryption and decryption of the data known as public key which is used for encryption and private key which is used for decryption. Generally, the process of symmetric encryption and decryption takes as below



The loon data center has possibilities of data attacks as the data is being transferred using wireless connections. To solve and prevent the attacks we are using the encryption process so that any third-party user cannot attack the data center. As the symmetric AES encryption can be adopted to any hardware or software, we can use this encryption process to secure the data and prevent form security attacks.

The encryption process has many outdated types, considering the issues of them we planned to use the Advanced Encryption standard for encryption. The AES encryption process is faster and stronger than the 3DES. By adopting the AES encryption, we can get the results with strong security for the data, it is eased to implement in any software or hardware. It is also flexible to use for any kind of software. While it is designed to be resistant to the ones who is attacking the data and the speed of encryption and decryption is high to make sure that the systems adopt to the process.

2) ***Software security.***

Software is the only application through which data is being transferred to data center. The software shouldn't be attacked by any of the hackers, so some security measures are to be taken. While the loon data center has a wireless type of transferring the data, the software should have protection towards the malicious attacks. These attacks may cause the decommission for the software. Security of the software includes the integrity, authentication and availability. The failure of such functionalities may lead to the software attacks which ends with stealing of information, monitoring the content that is transferred and may have damage to the data that is being transferred or stored in a data center.

The software security threats should be kept in mind while developing the software itself and by continuously monitoring the software performance the attacks can be prevented and new security measure can be implemented for the further use.

a) ***Integrity.***

The software integrity mainly used for the protection for hacks and the privacy violations of the developed software. When the code integrity is high, the software will have the most security measure which includes the security features, limited access control. The software is developed in a way that it has the limited access control which gives the authorization to the users depending on their roles. While the stack and buffer overflow and the command and SQL injections are the prominent attackers of a software.

b) ***Authentication.***

Authentication with appropriate authorization is the most secured way to protect the data gains the data breaches. This gives access to the databases by verifying the user credentials. For loon data center it can be used for getting the access to the data that has been stored in the data center. The authentication process can also be used for the software side to access the right option to get the desired outcome. Only the authorized user can use the data or the software that is present in the data center. It can also give access to the multiple systems and platforms. By accessing the information from the software there can't be any data breaches and the hacker cannot even check for the information that is placed on the application.

c) ***Availability.***

The security impacts of software integrity and authentication achieves high performance of it, where the performance is proportional to the availability of the software. The software reliability increases the availability of it by achieving the aligned goals. The users need to monitor the performance of the software in order to update the software with high availability.

3) ***Data Backups of the backups.***

It is important to have backups of the data on the data center. One of the aims of having a loon data center, is to have backup of the data center on land to safeguard data during natural disaster. But the data on the loon data center also must have backup on some other place on a data center. It is always better to have backup of the backups, so that there are many ways to prevent data loss and data privacy.

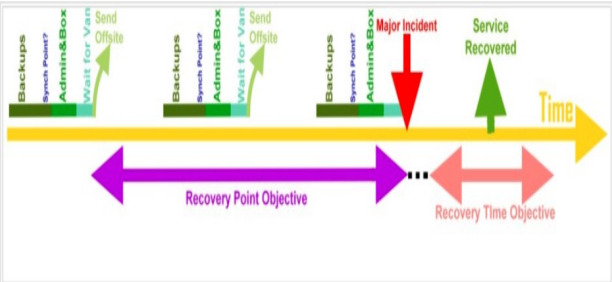
D. ***Operational Level Security.***

This level of security deals with the operations of data center and the loon and its security implementations. There is a team, which works to make sure the operations are running well and is secure from threats and attacks. This team also deals with the solutions to come up when there is a disaster and issues in the data center.

1) ***Disaster Recovery.***

Disaster recovery is designed to avert the data loss as well as business disruption resulting the civil emergencies, equipment failures, cyberattacks and

natural disaster. Most of the small and mid-sized business organizations are neglecting to have a disaster recovery plan. Due to lack of the planning, infrastructure failure itself may have a loss whereas critical application failure may lead to 5-10 times of infrastructure failure. Because of such failures 40% of small organizations are closed and 25% of organizations got shut in the first year itself due to the crisis. The following figure represents some of the options to improve the disaster recovery planning.



Considering the Loon data center location, it's easy to plan for the disaster recovery. As it is placed in air there are very less possibilities for natural disaster. Even though there are very less possibilities for such things, it will be brought down according to the climatic conditions over there. As there will be no human interaction with the data center directly unless its connection is interrupted. Anyway, they can be sorted of by providing the backup connections. The disaster recovery should be continuously planned it is mandatory to use the data center monitoring tools in order to safeguard the data center.

These monitoring tools helps the data center from risk. In case of any disaster due to fire or short-circuit it will be automated so that it falls back to earth using the parachutes at the top of the container and at the bottom air bags will be placed for safe landing. Also, for such fire emergency scenarios the automatic fire extinguishers will be placed.

In case of any system failure there will backup of data stored on the ground data center, so that data losses can be recovered. The backup of loon data center will be placed confidentially at a portable location. As it is an edge data center it can be on earth and can be stored easily in container and moved to different places through different means so that no human will be able to trace the backup data except who has access over the main data center. In order to protect the data, we will be using encryption and decryption to access the data.

*2) **Ground Base station Security.***

The ground base station is the place from where the loon will be controlled and monitored. This station will have CCTV surveillance system to monitor unauthorized user access and prevention.

*a) **Two-Factor Authorization.***

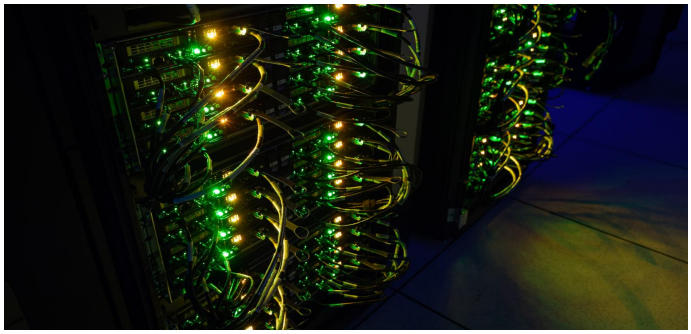
The authorized user must go through 2FA to enter the station and to control the loon and data center. One would be biometric fingerprint scanner and iris/retinal scan to gain access into the station.

*b) **Limited user access.***

The people having access to this station should be limited and should only be given to higher authorities. To prevent attacks and maintain confidentiality of the details of the loon data center.

E. Network Level Security.

The loon data center uses laser and radio communication systems to be connected with the loon and data center to exchange data. Securing the network with the loon and data center is also important and necessary to have a secure channel to communicate and deliver services.



*1) **Securing communicating systems.***

The loon uses laser communication to communicate and exchange data with the data center and loon. As we know that laser communication is one of the fastest and secure way of communicating with long distance devices. It uses a specific channel and frequency to connect with the data center, which is confidential and not disclosed to anyone except the data center operators in the ground base station.

*2) **Firewall Protection.***

The prevention of unauthorized access by the third party in a private network can be attained by providing firewall protection. While the loon data center is using unwired type of transferring and storing the data, we need to be more conscious about the hacker attacks. The firewall protection helps to monitor and control the flow of data between the private networks and the internet by using set of user defined instructions. These instructions keep monitoring of the data and devices to be out of network destructive elements. There are various types of firewalls depending on the use.

*a) **Packet filtering.***

Based on the user defined instructions the system checks and verifies the packets entering and leaving, will be accepted or rejected by the system. It sets the threshold point and then checks for the proper origin of

the system they are entering through without reading the content in a packet. The packets that are entering the loon data center are first filtered using this technique.

b) ***Proxy Firewall.***

These firewalls are used to filter the incoming protocols from the application and delivered through another proxy devices. It keeps verifying the input packets and establishes the connection. It verifies the actual content of the information and checks the information for malware. Only when the data is approved then it is transferred to the data center. While it also has the details of sender and usage of the information so that the data is protected from the attackers.

c) ***Software and Hardware Firewall.***

The single software firewall will be the most compatible which provides several firewalls that can satisfy each system goal. The software used for the data center can be protected and prevented by using this firewall. While the hardware security is also added to this, so that the risk of attacking the hardware appliances can be reduced. The devices which are used for the loon data center like routers, data racks and servers can be secured without getting them hacked. By authenticating the hardware appliances such that only limited people access the data, this will make the data more secure and the appliances too get secured by providing hardware firewall.

3) ***IP spoofing.***

To prevent IP spoofing in our network, we monitor networks, use latest ipv6 internet protocol, use network attack blocker and many validation and verification methods.

4) ***Man in the middle attack.***

These types of attack happens when a third party host enters the network between the two legal hosts, and the legal hosts are unaware of this illegal host. To avoid this type pf attack we use VPN and make sure that the source and destination hosts are well authenticated and secure.

5) ***DOS Attack (Denial of service).***

To prevent DOS attack, we use redundancy into our infrastructure, have specific Dos anti-virus software and configure network against Dos attacks.

IV. TECHNICAL TESTING APPORACH.

A. ***Physical Intrusion testing.***

The objective is to record the physical security aspects of the loon data center and remove if any failure issues are discovered. It also finds the finds the reasons for malicious attacks that accommodate the physical barriers like sensors, cameras, human traps to unauthorize the access to the data center appliance. To solve such issues, we are using the tools which can improve the physical security concerns which includes

1. Passive Reconnaissance
2. Open source intelligence (OSINT)
3. Active Reconnaissance (On-site observation)
4. Vulnerability identification

The recording of the failures will make you understand the places to be updated and save the ground station and the loon data center from security aspects. For the physical security flaws there will be continuous remedies to make them work appropriate.

B. ***Data encryption testing.***

The encryption is the strongest security that can be provides to the data. While the symmetric AES encryption doesn't provide the hacker to get the data at any cost. The AES encryption is hard to crack due to its strength, anyway before using launching the loon data center it is mandatory to verify that the algorithm is perfectly implemented so that no one can hack or get the key by ease. Only after proper testing the loon data center will be launched and then it should be continuously monitored in order to make it even harder for the attacker.

The software like Disk Cryptor can be used for managing the encryption algorithms. It can also save multiple passwords and uses the two-factor authentication to make it complicated. The software is easy to use so that the keys can be secured by having the premium account. As it is handling the multiple encryption algorithms male the AES testing and execution easy.

C. ***Software security testing.***

The software application that is to be deployed in the loon data center, initially it should include the security measure in the development stage itself. Missing of any security issue in the application during the development will lead to get hacked easily which end up with data breaches. So before deploying the application it should be thoroughly tested to its maximum potential to secure the data and the software. To monitor the software issues many tools have been used to checks their integrity, authentication and availability of the application is getting the appropriate results or not.

Considering the security issues of an application, we will be using the Zed Attack proxy tool which is an open sourced security testing tool. The tool can handle the multiple platforms for testing the security vulnerabilities. IT uses the command lines for the expert users. ZAP consists the feature of

1. Application error disclosure
2. Cookie not HTTP Only flag
3. Missing anti-CSRF tokens
4. Private IP disclosure
5. Session ID in URL
6. SQL injection
7. XSS injection

D. ***Network security testing.***

The network security is most important thing that need to have the continuous monitoring techniques. For the network security we are using the techniques of firewall protection, IP spoofing, DOS (Denial of Service). The IP spoofing can be monitored by the tools that ae used for firewall protection and DOS. Monitoring these network security aspects, we are using the tools such as Wireshark and LOIC

Wireshark: is a network penetrating tool which will monitoring the network that assist the user to get the exact details of the activities taking place in the network. It captures the data packets from different individual packets and their details of destination and source will be

determined by the used protocols in the network. By getting the information from the Wireshark, we can find the weak points of the network and can improve its standards.

LOIC (Low Orbit Ion Canon): The LOIC tool is used to test the DOS attacks that are happening to the network. It sends the TCP or HTTP requests to the servers that are used by the customers and if accepted users can have the access to the network servers. It doesn't hide the IP address of the network, but it keeps a track of it. While the proxy server cannot help for requesting the access because the request will be directed to the proxy server and not the target server that a user should access.

E. Power Supply Testing.

The loon will be powered using solar energy and the energy is also stored in batteries, which will power the data center at nighttime. We use Resolver tool to monitor the power usage by the hardware's and equipment's on the loon data center and to check the battery capacity and amount of power left in batteries, and how long can it power the data center. This tool monitors the current battery usage and battery health as well. It also monitors the amount of energy converted from solar panels into electrical energy, to keep track of the data center performance.

V. FINDINGS AND RISKS RATINGS.

Finding the risks on any data center before implementing it is a must, we must identify the possible risks involved in our loon data center. It is always better to take precautions rather than solving it when the problems arise. The loon data center has many security implementations to be deployed before or after implementing this idea. Availability, integrity and proper authentications techniques must be considered before the data center is placed in orbit, and regular checkups and monitoring is required to have best possible outcomes from this data center.

The loon data center has many aspects to consider and implement security for it to work and give services to the customers and discussing solutions to the risks that may arise after it is implemented. The loon data center has the balloon risks, communicating with lasers and radio equipment's also has some challenges and requires effective monitoring and controlling to be done. The possible risks and rating of this loon data center are shown below:

- **Compliance Risks.**

Risk Control Area.	Description.	Risk Likelihood.	Risk Impact.	Risk Product.
Data Protection.	The data on the loon is least likely to get attacked.	Likely	Serious	LOW.
Legal Issues.	Loon might fly into restricted area or licensing issues.	Slight	Mild	Very Low.
Incident Response.	Failure to identify the problem and overcome it.	Likely	Severe	Moderate.

- **Strategic Risks.**

Risk Control Area.	Description.	Risk Likelihood.	Risk Impact.	Risk Product.
Information and data security.	The loss of data and breach of data privacy.	Likely	Serious	LOW.
Data Migration.	The data of loon is difficult to move into legacy data center.	Slight	Mild	Very Low.
Loon placement location.	The loon must be placed in a legal location and be controlled in a particular region only.	Slight	Mild	Very Low.

- **Operational Risks.**

Risk Control Area.	Description.	Risk Likelihood.	Risk Impact.	Risk Product.
Balloon Risks.	The balloon can explode, or leakage of gas can happen.	Slight	Severe	Moderate.
Natural Disasters.	The loon can be damaged by this.	Slight	Mild	High
Power loss.	Solar panels can disfunction.	Likely	Mild	Moderate.
Network Risks.	The network must be disconnected during maintenance.	Highly likely	Mild	Low
Collision Risks.	The loon data center can collide with other balloon or objects in the sky.	Slight	Mild	Very Low.

- **Market and Financial Risks.**

Risk Control Area.	Description.	Risk Likelihood.	Risk Impact.	Risk Product.
Capacity Management.	The infrastructure on the loon is limited.	Likely	Serious	LOW.
Service termination or failure.	The loon will be of no use if the service is terminated.	Slight	Mild	Very Low.

VI. Challenges and Limitations.

Even though the loon data center gives solution to many of the challenges and problems faced by todays data center on land and water, it also have some limitations which has scope for improvement in the near future. However, the loon data center has a few drawbacks and challenges which can be fixed and deployed again into the atmosphere. Few of them are listed below:

- The balloon used in this prototype is filled with helium gas and eventually the gas gets dissolved and reduces the altitude of the loon, so the loon must be brought down to refill the helium gas and then launched again into the atmosphere. The balloon can last for up to 200 days without any modifications.

- The loon has many equipment's installed on it, if one of them fails to function or is damaged for any reason. The loon must be landed to the surface and the necessary maintenance must be done.

- When the loon is on the ground for maintenance, during this time the communication system will be inactive, and the data center will be disconnected for a small period of time.

- The communication systems used in loon data center is laser communication and radio communication system as backup, due to bad weather conditions (which in stratosphere layer is almost negligible) the laser systems may not deliver high data transfer rates. However, radio systems are reliable and works every time.

- If the loon data center flies far away from the ground base station and is out of range for the communication systems, then it would be a huge problem. As we can no longer control the loon speed and directions. To solve this issue, we can have multiple base station with communication systems at different locations.

These are the challenges and limitations of the loon data center. However, loon data center has these few faults and drawbacks but has many more advantages and reasons to use this a type for data centers.

VII. Conclusion and Findings.

The loon data center includes the security measure in terms of physical, security, geographical, data, network and operational security. However, they are dependent on the size and operations processed by the organization. Though the data center is possessed with the utmost security, it should be continuously upgraded with the future innovative measures, as the technology is growing immensely.

The attackers may find some parts of securities easy to crash. Considering them the data center security measure should be modified with the future technologies. But as of present technologies the loon data center has the most secured way of protecting the data. Self-destructive measures can be implemented in the critical scenarios by having the backup of the backup in some other data center.

VIII. References.

1. "Technology," *Loon*. [Online]. Available: https://loon.com/technology/. [Accessed: 08-Dec-2019].
2. "Loon LLC," *Wikipedia*, 04-Dec-2019. [Online]. Available: https://en.wikipedia.org/wiki/Loon_LLC. [Accessed: 08-Dec-2019].
3. [1]"Data Center Network Security - CyrusOne", *CyrusOne*, 2019. [Online]. Available: https://cyrusone.com/resources/tools/data-center-network-security/. [Accessed: 08- Dec- 2019].
4. "How to Prevent DDoS Attacks: 6 Tips to Keep Your Website Safe," *eSecurity Planet: Internet Security for IT Professionals*. [Online]. Available: https://www.esecurityplanet.com/network-security/how-to-prevent-ddos-attacks.html. [Accessed: 08-Dec-2019].
5. *usa.kaspersky.com*. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/ip-spoofing. [Accessed: 08-Dec-2019].
6. "5 data security techniques that help boost consumer confidence," *Cloud computing news*, 24-Apr-2019. [Online]. Available: https://www.ibm.com/blogs/cloud-computing/2019/04/24/data-security-techniques-boost-confidence/. [Accessed: 08-Dec-2019].
7. "Data Security," *Looker*. [Online]. Available: https://looker.com/definitions/data-security. [Accessed: 08-Dec-2019].
8. "What Is Data Encryption? Definition, Best Practices & More," *Digital Guardian*, 15-Jul-2019. [Online]. Available: https://digitalguardian.com/blog/what-data-encryption. [Accessed: 08-Dec-2019].
9. J. Parms, "Symmetric vs. Asymmetric Encryption – What are differences?," *SSL2BUY Wiki - Get Solution for SSL Certificate Queries*, 07-Feb-2019. [Online]. Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. [Accessed: 08-Dec-2019].
10. "What is Software Security? - Definition from Techopedia," *Techopedia.com*. [Online]. Available: https://www.techopedia.com/definition/24866/software-security. [Accessed: 08-Dec-2019].

11. A. Wert, J. Kunz, A. Kraus, M. Oehler, C. Waldvogel, M. Oehler, J. Kunz, and A. Wert, “5 Things to Consider When Dealing with Availability of Software Systems,” *Novatec*, 04-Mar-2019. [Online]. Available: https://www.novatec-gmbh.de/en/blog/5-things-to-consider-when-dealing-with-availability-of-software-systems/. [Accessed: 08-Dec-2019].
12. “What is Data Center Security?,” *Forcepoint*, 30-Oct-2019. [Online]. Available: https://www.forcepoint.com/cyber-edu/data-center-security. [Accessed: 08-Dec-2019].
13. E. Dosal, “What is a Firewall? The Different Firewall Types & Architectures,” *Compuquip Cybersecurity*, 26-Nov-2019. [Online]. Available: https://www.compuquip.com/blog/the-different-types-of-firewall-architectures. [Accessed: 08-Dec-2019].
14. A. Steed, “Home,” *Business Technical Services*, 11-Oct-2017. [Online]. Available: https://bts-consulting.biz/2017/10/11/the-three-different-types-of-firewalls/. [Accessed: 08-Dec-2019].
15. G. Maria, “4 Common Encryption Methods and Use Cases,” *GetApp Lab*, 08-Jul-2019. [Online]. Available: https://lab.getapp.com/common-encryption-methods/. [Accessed: 08-Dec-2019].
16. R. Bellairs, “What Is Software Integrity? And How To Achieve It,” *Perforce Software*. [Online]. Available: https://www.perforce.com/blog/qac/what-is-software-integrity. [Accessed: 08-Dec-2019].
17. “Physical Penetration Testing - RedTeam Security,” *Red Team Security*, 26-Aug-2019. [Online]. Available: https://www.redteamsecure.com/services/penetration-testing/physical-penetration-testing/. [Accessed: 10-Dec-2019].
18. A. Steed, “Home,” *Business Technical Services*, 11-Oct-2017. [Online]. Available: https://bts-consulting.biz/2017/10/11/the-three-different-types-of-firewalls/. [Accessed: 08-Dec-2019].
19. G. Maria, “4 Common Encryption Methods and Use Cases,” *GetApp Lab*, 08-Jul-2019. [Online]. Available: https://lab.getapp.com/common-encryption-methods/. [Accessed: 08-Dec-2019].
20. R. Bellairs, “What Is Software Integrity? And How To Achieve It,” *Perforce Software*. [Online]. Available: https://www.perforce.com/blog/qac/what-is-software-integrity. [Accessed: 08-Dec-2019].
21. “Physical Penetration Testing - RedTeam Security,” *Red Team Security*, 26-Aug-2019. [Online]. Available: https://www.redteamsecure.com/services/penetration-testing/physical-penetration-testing/. [Accessed: 10-Dec-2019].
22. “The most Popular Free Encryption Software Tools to Protect Your Data,” *Heimdal Security Blog*, 04-Oct-2019. [Online]. Available: https://heimdalsecurity.com/blog/free-encryption-software-tools/. [Accessed: 10-Dec-2019].
23. “Top 10 Open Source Security Testing Tools for Web Applications (Updated),” *Hackr.io*. [Online]. Available: https://hackr.io/blog/top-10-open-source-security-testing-tools-for-web-applications. [Accessed: 10-Dec-2019].
24. “7 Best Cyber Security Penetration Testing Tools,” *Cybrary*. [Online]. Available: https://www.cybrary.it/0p3n/7-cyber-security-pentesting-tools/. [Accessed: 10-Dec-2019].
25. “Internal Audit Management & Internal Control,” *Resolver*. [Online]. Available: https://www.resolver.com/grc-software/audit-controls/?utm source=capterra&utm medium=directory&utm campaign=au-demo&utm_term=audit. [Accessed: 10-Dec-2019].