American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-8, Issue-5, pp-52-58
www.ajer.org
Research Paper Open Access

# Computer Network Security: Risks and Protective Measures

Benjamin Sarpong[1] and Dr. Zhihua Li[2]
[1]School of Internet of Things and Engineering Jiangnan University-China,
[2]School of Internet of Things and Engineering Jiangnan University-China,
Corresponding Author: Benjamin Sarpong

***ABSTRACT:*** *With the ushering in of the information age, a wide range of technologies in the field of computer science have emerged such that many network techniques are broadly utilized in different sectors of the society at large and in its wake not only have made great economic and social impact, but also have immensely promoted the rapid development in culture and systems. While the openness and adaptability of computer network has brought us a ton of benefits both throughout our lives and work, it also has caused a series of information security problems which put our life at risk. With the fast advancement of computer network technology, ensuring the security of the computer becomes a very essential factor that cannot be disregarded. Three major threats confronting computer network security include: threat from hackers, computer virus and denial of service attacks whiles some measures leading to the safety of the network also include legal measures, technical measures as well as management measures. This paper seeks to investigate the primary risk confronting computer network security, address system security innovations and advances to help tackle the shrouded risk of the current basic system security.*
***KEYWORDS****-Information age, Computer network, information security*

---

Date of Submission: 25-04-2019 Date of acceptance: 05-05-2019

---

## I. INTRODUCTION

With the improvement of Internet technology, computer networks have gradually transformed people's way of life as well as method of work. This factor has driven us into another period of data and digitalization, the wide utilization of computer networks has likewise brought about emotional improvements in our life and work. For instance, with the network system, students can submit their projects with less hustle directly to their professors, accounting professionals can accomplish data sharing with the synchronous transmission of financial findings, a branch office can make a constant correspondence with the headquarters to become more acquainted with the advancement and changes as well as carry out new plans. In addition, the government-affiliated institutions can learn to appreciate the paperless office and handle administration with the assistance of the network and finally individuals can at the comfort of their homes shop, pay and entertain themselves online. In the process of fast advancement of computer networks, shrouded risks of computer security turn out to be progressively conspicuous. This demands the adaptation of solid measures to guarantee the wellbeing of the network.

In light of computer science, the network has as of now not become only a key component of our lives, work and research, but a scaffold of correspondence. However, there are a few flaws about the computer network as it is evolving beyond our creative ability, among which the network security is dominant. The instance there is an abnormality in behavior or complete breakdown of the network, it will result in severe financial loss. The regular service will be placed in turmoil and each field of public activity, such as the telecommunication, defense, finance and the education sectors will all be affected. In this manner, it is dire to advance the system security, protect the huge information, improve the network methodically as well as make the network environment suitable [1].{Sun, 2011 #306}

## II. CONCEPT OF COMPUTER NETWORK SECURITY: MEANING AND IMPORTANCE

The computer network security can be referred to as the utilization of network management and technical measures to control and ensure data privacy, integrity and availability in a network environment are protected. This is usually classified into two groups; physical security and logical security. The physical security

simply refers to the computer equipment and its associated facilities are being kept safe from destruction, theft, mishandling, etc. Whereas the logical security includes the integrity, secrecy and accessibility of information [2].

The meaning of computer network security varies from user to user and X. Zheng explains network security as ensuring that the mobile and static information in a network can be accessed by the authorized users but not the unauthorized users and furthermore explains that the aim of network security is to ensure the confidentiality , integrity and availability of information [3].To the lay man, network security will mean that the information being transmitted via the network is well secured such that privacy is maintained, cannot be tampered with, eavesdropped or duplicated where as to the network administrator, it would include how to manage the harm caused by an unexpected natural disaster; how to reestablish the operation when the hardware is wrecked in order to guarantee the coherence and smoothness of the network system. Basically, network security incorporates equipment that includes the network system, software and its transmission over a secured channel which protects it from malicious attack. Also, the network security is not only related to technology but management as well since they complement each other.

Presently, the network security of Ghana is confronted with the challenges of man-made attacks and network intrusion. In this information era, with the wide utilization of computer networks and the quickly expanding interest of data transmission, a few institutions such as banks have derived benefits, yet a great deal of information has been lost thanks to attacks such as identity theft, eavesdropping and duplication of data. Some hackers have gone to the extent of penetrating some databases and destroying information through the introduction of a virus.

## III. EXISTING ISSUES AND THREATS ON COMPUTER NETWORK SECURITY

- **Flaws in Operating System and Application Software**

The computer operating system is a kind framework responsible for managing the computer hardware and software resources operation environment. An operating system functioning in a network environment becomes a security risk when there is a bug that enables hackers take advantage and attack the network system. In the development phase of some applications, there are some defects that are ignored and when this softwareis allowed to operate in a network, it gives way for the introduction of some malicious code into the operating system to help hackers gain control of the system [4].

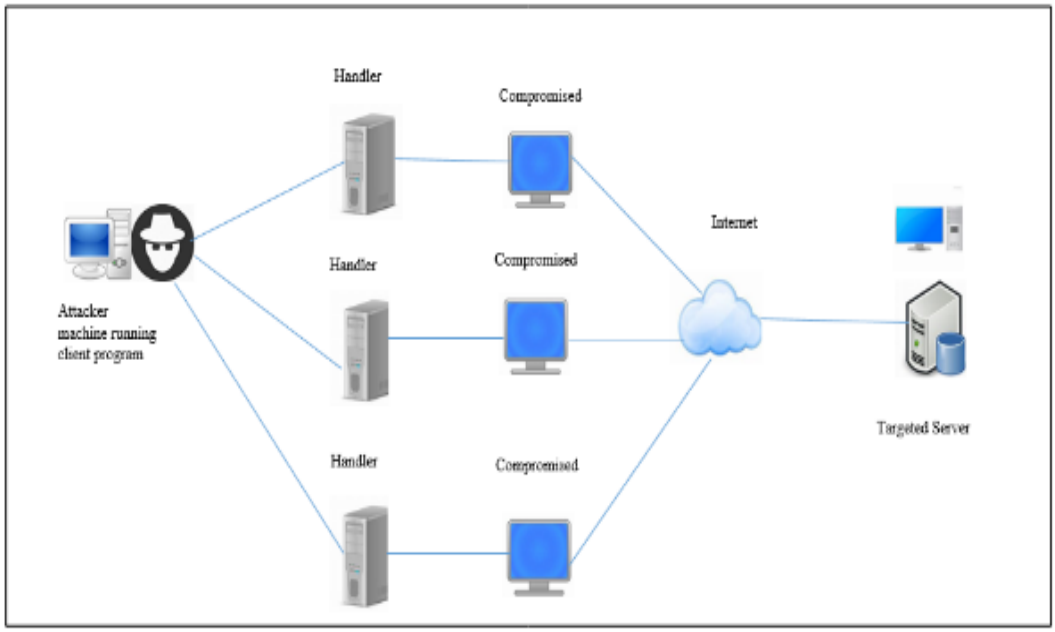
- **Human Attacks**

These attacks can be classified into two groups and they are usually carried out by internal or external attackers [5]. Internal attackers are the ones who figure out how to take control of a network system by partaking in communications legitimately. These individuals are usually workers or staff of the organization so they usually can easily send/receive messages to/from other network hubs because they have access to any encryption keys that may be requested by the system. Then again, the external attackers ‘tune in” to the remote communications, endeavor to comprehend the network’s functionality, and discover any flaw. The external attacks are less difficult to defend against since they do not have access to any essential data such as cryptographic keys or log in access [6]. Some examples of external attacks are:

- Man in the Middle Attack(MITM): In this attack, the hacker first listens on the communication channels to gather much information about a network to possibly find a way to intrude (eavesdropping). Once this is achieved successfully, the hacker now pretends to be one party by controlling the messages and then eventually takes over the whole communication. This situation can be curbed through the use of secure communication links between communication nodes and the utilization of modern cryptographic algorithms. [7]


Figure 1:Man in the middle attack (MITM)

- Denial of Service Attacks (DoS): These attacks mainly focus on the network system's operation and plan to reduce its usefulness or even completely shut it down for a brief period of time. At the point a DoS attack happens, a hacker intends to debilitate the network's assets or resources by consistently flooding the network with high traffic and in the long run preventing genuine users from utilizing the system. This is a very risky attack in the network environment where the exhaustion of the system's resources is vital for its performance [8].




- **Malware**

Malware is any software specially designed with the intention to cause harm to a computer system or network. It usually causes harm after it is introduced in one way or another into a target system and it most often exists as an executable code or another software. They are mostly referred to as computer viruses, worms, Trojan horses, ransomware etc. [9] [10].

A computer virus is a sort of vindictive software that, when executed, reproduces itself by altering other computer programs and embedding its own code. When this replication succeeds, the influenced regions are then said to be "infected" with a virus [11]. Viruses are obtrusive and transmissive and they tend to make systems operate at lower proficiency and eventually lead to system failure and as result a lot of data and equipment are lost. Spyware on the other hand operates differently with its primary intent to take over a network to steal information.

Under the network environment, it is very important to fully comprehend the implications of virus attacks so as to attach incredible significance so as to ensure the smooth running of the network system. It is very essential to select the best antivirus software for a network to help facilitate the smooth running of the computer network.

## IV. DEFENSIVE MECHANISMS OF COMPUTER NETWORK SECURITY

In computer network security a defensive mechanism is an activity, device, strategy or procedure carried out to help decrease a risk, flaw, or an attack by disposing or preventing it, by limiting the damage it can cause, or by finding and bringing it to light with the goal that a corrective action can be carried out [12].The ways and means to counter or help protect a computer network system can be classified into three main groups namely: Technical defensive mechanisms, which usually involves the application of encryption technologies, firewall and anti-virus technologies as well as network access control. The Physical defensive mechanisms entails the computer system environment, computer room environment selection and the computer room safety protection. The Management defensive mechanism covers the Training of end users and the legalities [2]

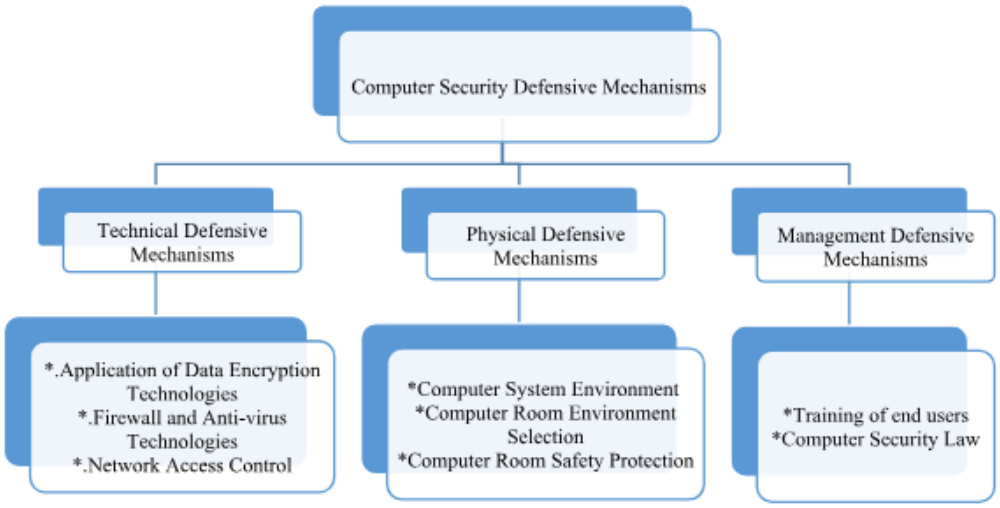



**Figure 3:** Typesof Computer Security Defensive Mechanisms

- **Technical Defensive Mechanisms**
- Application of Data Encryption Technologies

In an attempt to prevent unapproved users from getting access to a network, data encrypting technologies and batch signature verification techniques should be applied. With data transmission taking place via computer network, it will be essential to utilize signature verification techniques to identify the sender as well as the contents [13]. Potential security issues such as forging, denying and adulteration can be curbed through the use of signature verification techniques to ensure that the information and the sender are in conformity. Additionally, we can utilize cryptographic technologies, which falls into encryption and decryption, to update and revamp the data as per a specific structure, therefore making it quite impossible for users without access to comprehend let alone to tamper or even steal the information [14]. When there is a need to use these documents, they can simply be decrypted by users with the appropriate keys. Presently, some of the encryption innovations include but not limited to RSA which is named after its creators Rivest, Shamir and Adelman, Advance Encryption Standard and Data Encryption Standard [1]. So as to confirm the information and the user's identity, we can authenticate the actual identity and check the user's access request, the origination of the information to ensure its integrity in order to the threats of misrepresentation and unapproved users. Below in figures 4 and 5 are the types of encryption: Symmetric and Asymmetric encryption.

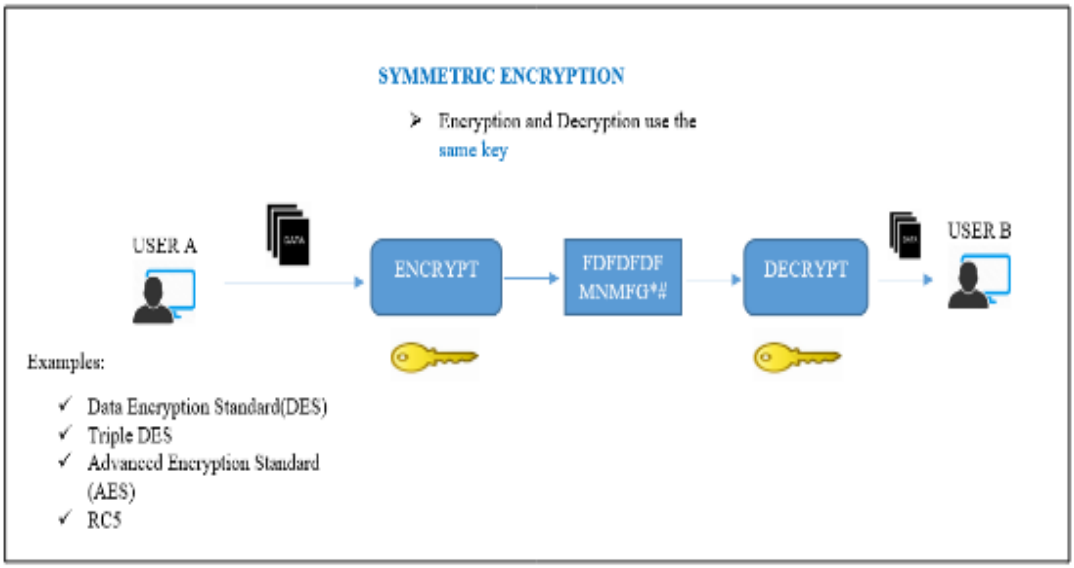



Figure 4:Symmetric Encryption

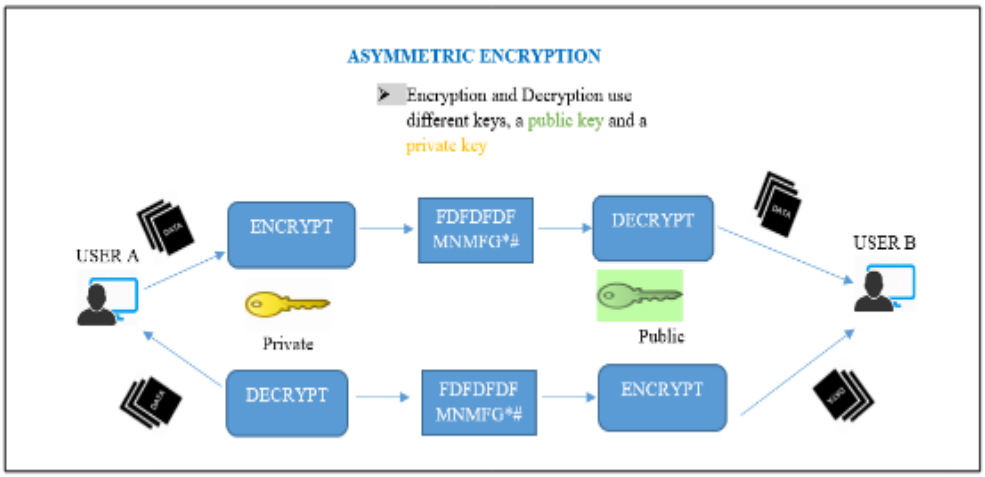


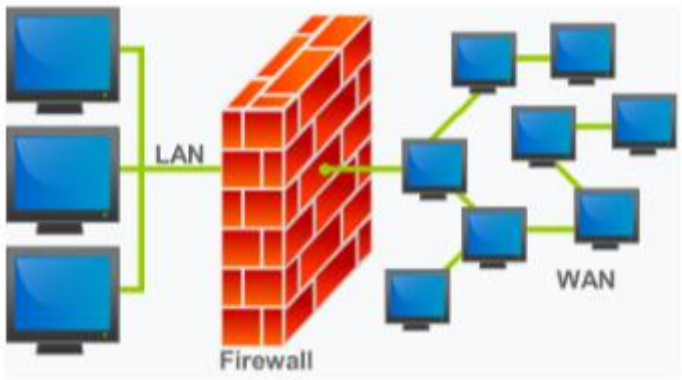

Figure 5: Asymmetric Encryption

- Firewall and Antivirus Technologies

The main function of a firewall is to serve as a network security framework that screens, monitors and controls approaching and active network traffic dependent on a set of foreordained security rules. A firewall ordinarily builds up a boundary between a trusted internal local network and an untrusted external network system, usually the Internet [15]. Firewalls are usually defined as either Network firewalls and Host-based firewalls: network firewalls channel traffic between at least two network systems and operate on network hardware such as a router, whiles host-based firewalls usually work on host computers and arrange network traffic all through those machines.

With firewalls functioning as a safe shield, they can be set as per application prerequisites and the pertinence of the network operation. By exploiting its scan features with regards to network communication, ports deemed unsafe can be monitored or even closed, thus avoiding or stopping Denial of service attacks as well malware attacks. Also with the prevention and control function, unauthorized users can be prevented from gaining access into the internal network. Finally, with the use of firewalls, limitations can be placed on some websites to enhance and simplify monitoring [16].

Concerning the issue of malware, effective prevention and control measures need to be observed to accomplish real-time protection and even controls such as the application of an intensive anti-virus software to affected computers on the network. Also, USB ports should be blocked to prevent the introduction of foreign media into the network as well as authentic anti-virus software should be installed with regular updates and installation of patches should be carried out regularly[1]




- Network Access Control

This ensures that information resources can only be accessed by authorized users and the models of access control may differ contingent upon the security approach. A few of these strategies are discretionary access control, mandatory access control, role-based access control, the rule set access control, list-based access control, and token-based access control. Access control mainly depends on identity authentication and some examples of network access control techniques are the enforcement of strong passwords (not date of births), the periodical change of passwords, use of hardware identity keys as well as biometrics [17]. Other ways to carry

out access control are through the filtration of the MAC address, isolation of Virtual Local Area Networks(VLAN) and access list control using the IP address.

- **Physical Defensive Mechanisms**

The computer room equipment and other related hardware should neither be placed beneath water level nor on the highest floor of high rise buildings. Environmental physical conditions for example, temperature ought to be considered so as to keep a safe space for local servers. The air surrounding the hardware more often than not should be in a scope of 68 to 72 degrees to shield servers from heat.

Essentially, there should be adequate space surrounding computer equipment for air to freely circulate. The space between the equipment is typically subject to their dimensions and ventilation is an exceptionally fundamental prerequisite to avert heat-generating data storage devices from overheating. Another potential environmental hazard that should be considered is vibration, which causes a disturbance to a hard drive or even dislodge the boards and microchips that make the framework to operate efficiently. Proper padding of walls will go a long way to help computer systems from getting disturbed by vibrations.

Some potential events that compromise the servers are power outages so it is fundamental to ensure that the system is secured by providing redundant power reinforcements such as – a standalone generator or an uninterruptible power supply (UPS) device. These power backup systems need to be tested and monitored regularly

In conclusion, acts of purposeful sabotage ought not be overlooked., no matter how impossible they may appear. It is very important to ensure that servers are secured against both physical and cyber intruders as security breaches are always a possibility. Surveillance cameras need to be fixed to capture anyone entering the server room without approval and the information recorded should be archived for recovery and review in the event of a breach. Locks that require a key or a combination ought to be introduced in the server room itself as well as installed server racks. [18]

- **Management Defensive Mechanisms**

In the network, information may often be interpolated or maliciously destroyed due to malicious intrusion. To handle this, users should pay attention to backups and recovery technology. Data backup and recovery should become a habit, because system failure is inevitable in database system operation and loss of data most often occurs. If database backup is well performed in advance, you do not need to worry even if a sudden system failure leads to the destruction of important data, because there is an intact backup of the data for restoration. After unpredictable failures, administrators can use the data backup to restore the database to the state before the failures. In this way, the integrity and consistency of the data can be guaranteed.

Computer users need to be educated on how to maintain proper computer security habits such as changing passwords from time to time and using stronger passwords rather than dates of birth as this will go a long way to strengthen network security awareness. Training programs, according to computer user's responsibilities should be carried out to help strengthen the management of the network safety consciousness, occupation morals as well as the cultivation of the sense of responsibility. This will help build a perfect safety management system to continuously strengthen the computer network information security standardization management as well as strengthen the construction of computer network security to provide a reliable guarantee for an organization.

Finally, it is very important to strengthen the legislation framework by amending the existing laws and regulations to help bring people who commit cyber-crimes to justice. There should be an introduction of more security personnel to easily detect security issues as well as easily carry out cyber-crimes [19]

## V. CONCLUSION

The computer network security is a complicated system of engineering, involving technology, hardware management and as a result, security solutions should be set and understood. The network security solution is a combination of various security technologies which entails a safe operating system technology, firewall technology, virus protection technology, computer legislation and enforcement of law which forms a complete set of network safety protection systems. Computer network security threats have become issues that pose as a big challenge to our lives. By making sure we identify the source of major possible threats, we can settle on the suitable prevention and control mechanisms by matching the technical requirements and working out the effective security precaution strategies. Hence a reliable and safe operation environment can be established to guarantee a sustainable innovation and development of network security techniques.

## REFERENCES

[1]. Sun, X. The study on computer network security and precaution. in Proceedings of 2011 International Conference on Computer Science and Network Technology. 2011.
[2]. Fuguo, L. Study on security and prevention strategies of computer network. in 2012 International Conference on Computer Science and Information Processing (CSIP). 2012.
[3]. Zheng, X. Computer network security and measures. in Proceedings of 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. 2011.
[4]. Qing, W. and C. Hongju. Computer Network Security and Defense Technology Research. in 2016 Eighth International Conference on Measuring Technology and Mechatronics Automation (ICMTMA). 2016.
[5]. Granjal, J., E. Monteiro, and J.S. Silva, Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey. Ad Hoc Networks, 2015. **24**: p. 264-287.
[6]. Tuna, G., et al., A survey on information security threats and solutions for Machine to Machine (M2M) communications. Journal of Parallel and Distributed Computing, 2017. **109**: p. 142-154.
[7]. OneM2MPartners, o.M.-T.-.-S.-V., 2014-April-10, OneM2MPartners, oneM2M-TR-0008-Security-V1.0.0 , 2014-April-10. 2014.
[8]. https://www.us-cert.gov/ncas/tips/ST04-015, https://www.us-cert.gov/ncas/tips/ST04-015. https://www.us-cert.gov/ncas/tips/ST04-015.
[9]. Microsoft. Defining Malware. 2009; Available from: https://technet.microsoft.com/en-us/library/dd632948.aspx.
[10]. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf.
[11]. Definitions and Timeline, in Computer Viruses and Malware, J. Aycock, Editor. 2006, Springer US: Boston, MA. p. 11-25.
[12]. Glossary, I.S., Internet Security Glossary. Internet Security Glossary.
[13]. Kittur, A.S. and A.R. Pais, Batch verification of Digital Signatures: Approaches and challenges. Journal of Information Security and Applications, 2017. **37**: p. 15-27.
[14]. Blahut, R.E., Cryptography and Secure Communication. 2014, Cambridge: Cambridge University Press.
[15]. Oppliger, R., Internet security: firewalls and beyond. Commun. ACM, 1997. **40**(5): p. 92-102.
[16]. Peltier, T., Peltier, J, Peltier, T., Peltier, J. (2007). Complete Guide to CISM Certification. New York: Auerbach Publications, https://doi.org/10.1201/9781420013252. 2007, New York: Auerbach Publications.
[17]. Servin, A., Distributed Network Defence and Reinforcement Learning. Conference Proceedings, 2006.
[18]. Collins, T., 7 Common Server Room Problems for Businesses to Consider. 2015.
[19]. Chunli, L. and L. DongHui. Computer network security issues and countermeasures. in 2012 IEEE Symposium on Robotics and Applications (ISRA). 2012.

Benjamin Sarpong" Computer Network Security: Risks and Protective Measures"American Journal of Engineering Research (AJER), vol.8, no.05, 2019, pp.52-58