International Journal of Engineering Inventions
e-ISSN: 2278-7461, p-ISSN: 2319-6491
Volume 13, Issue 3 [March. 2024] PP: 06-10

A Comprehensive Review of Cyber Security In Cloud Infrastrucutre

[1]Rajan Kumar Yadav, [2]Munish Saran, [3]Upendra Nath Tripathi
[1]Research Scholar, Deen Dayal Upadhyaya Gorakhpur University Gorakhpur, U.P., India
[2]Research Scholar, Deen Dayal Upadhyaya Gorakhpur University Gorakhpur, U.P., India
[3]Associate Professor, Deen Dayal Upadhyaya Gorakhpur University Gorakhpur, U.P., India
[1]rkyd94@rediffmail.com,[2]munishsaran@gmail.com,[3]untripathi@gmail.com
Corresponding Author : rkyd94@rediffmail.com

ABSTRACT : *With the development of cloud computing the importance of cyber security has also increased. In this research paper we will try to understand in detail the interconnection between cloud computing, cyber security, cyber attacks and cyber security techniques and their impact. With the rapidly increasing use of cloud computing many questions of security and privacy have been faced. In fact the nature of cyber attacks and their impact on cloud systems and infrastructure is also considered. Here the impact of cyber security techniques and their use in cloud computing environment is discussed. We will also look at how cyber security techniques protect cloud systems and what measures can be taken to protect against cyber attacks. In this research paper we will understand the importance of cyber security and study in detail the security practices associated with cloud computing. This paper will also try to highlight the practice of cyber security and create awareness from a business perspective.*

Keywords: *Cloud Computing, Cyber Security, Cybercrime.*

Date of Submission: 22-02-2024 Date of acceptance: 04-03-2024

I. INTRODUCTION

Cloud Computing : Cloud computing is a computing model that provides on demand, scalable, measured and secure services to end users via the internet. Due to these benefits cloud computing is used in many use cases. There are many cloud service providers in today's market who provide different types of cloud services to their customers. Some major cloud service providers include IBM Cloud, Oracle Cloud, Amazon Web Services and Google Cloud[1].

Cloud systems are widely used due to their cost-effectiveness, convenience of access, and benefits of data backup. However these face significant security and privacy challenges compared to traditional storage technologies. The purpose of this area is to evaluate prior research and examine cloud systems in the context of cyber threats. Various policies, technologies, and protection are important to ensure their safety. But also increase the associated threats. Handing over data to cloud providers regardless of their reliability can put customer privacy at risk.[2]

In today's time, a lot of expansion of technology is being seen, internet and computer are being used in almost every field like education, business, transaction etc. It means that almost every type of data or information is being exchanged through devices such as computer, laptop, mobile etc., and situation, it is very important of users or any organization. Special care should be taken because there is a danger of theft of data or information by the unauthorized person. At present, there is a continuous increases in the cases of cyber-attacks around the world [3].

Cyber Security – Cyber security refers to an effective security technology in which different types of layers are used for security which protects computer, network, data or information etc., score from unauthorized attacks [4]. Because users or any type of organizations want to keep their data or information safe and cybercriminals also want to steal user's information through social media platforms. Cyber Security is a very important part for any user's, organizations or company because in this the information and data of the user's or any organizations gets security and in this various types of security are provided to the users or any organizations like any type of applications, information, network, infrastructure, data used through the internet, its security. Security of user's and data of any organizations which is stored or received on the cloud etc,. Therefore, Cyber Security especially provides security to these various aspects in which any confidentiality, availability and integrity of information should not be violated [5].

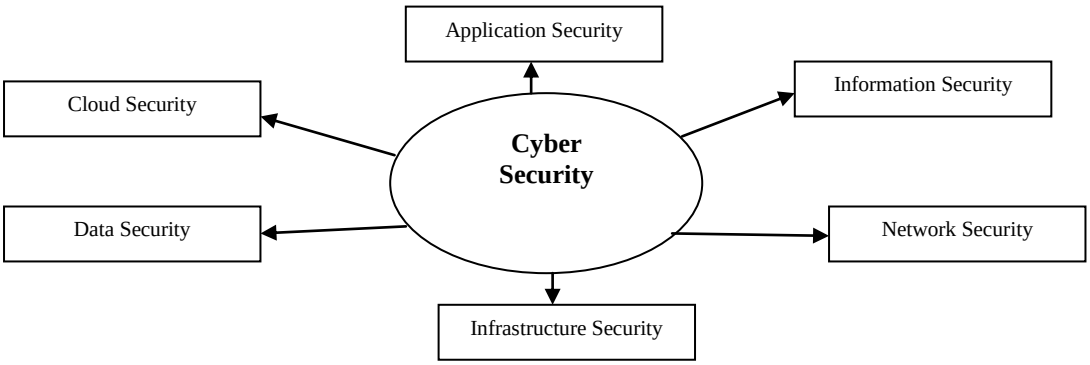

Figure1. Different types of Cyber Security

Cyber Crime – Cyber Crime is any kind of illegal act done through the internet. At present, an increase in the number of this type of crime is being seen. In this, cyber criminals use any devices (computer, laptop, mobile etc.) and with the help of the internet, the data of any user or organization or steal and misuse information [6].

II. LITERATURE REVIEW

In the last few years, Research Papers based on cyber security and its use in various fields, challenges and attacks researchers have told that –

According to Joachim Bjorge Ulven et al. [7] still, cyber security remains a very serious subject, so there is a need to make cyber security more strong because due to the weakness of cyber security, there is a threat to the user's data loss, forgery and the confidentiality of the data. They have said that in higher education cyber security risk remains a very serious problem and more work needs to be done on it.

According to Zeinab El-Rewini et et. al. [8] various types of unauthorized attackers are attacking the vehicular sensors in the risk of cyber security because different types of sensors are used in whatever modern developments are currently available in the market and in this cyber-attacks on the communication layer and control layer of those sensors. They have told that technologies like Machine learning in IoT, Cryptography and Blockchain are being used in vehicular security.

According to Deval Bhamare et. at. [9] cyber Security Plays a very important role for industrial control system, he says that by using cloud platform, cyber security can be strengthened in the industrial sector and industrial control system can be saved from cyber-attacks.

According to Diptiben Ghelani [10] energy sectors security can be perform in a really safe operation with the help of cyber security. Cyber security helps in securing its various areas like privacy, security and connectivity. He has told that the cyber security which is being used at present most of them have been taken from old telecommunication which provides very weak security, so they have highlighted the weaknesses of cyber security and smart grid.

According to Mahesh Kumar et. al. [11] The risks of user's online, private and public banks security in E-Banking have been discussed. They have told that technology is used in the e-banking system of private and foreign banks in India in which it completely helps them to grow their business. In order to go digital, users are not paying full attention to security. He said that private and public banks need to improve the existing security technology. So that the financial transactions and security of the users can be further strengthened.

III. CYBER SECURITY ATTACKS

The risk associated with any attack is based on three security principles the threat that is who is carrying out the attack. Weakness that is those who are weak are attacked and effect that is what the attack does. A security breach is an action that threatens the confidentiality, integrity or security of information assets and systems. There are many types of cyber security attacks that can put the security of an organization's systems and network or an individual at risk [12].

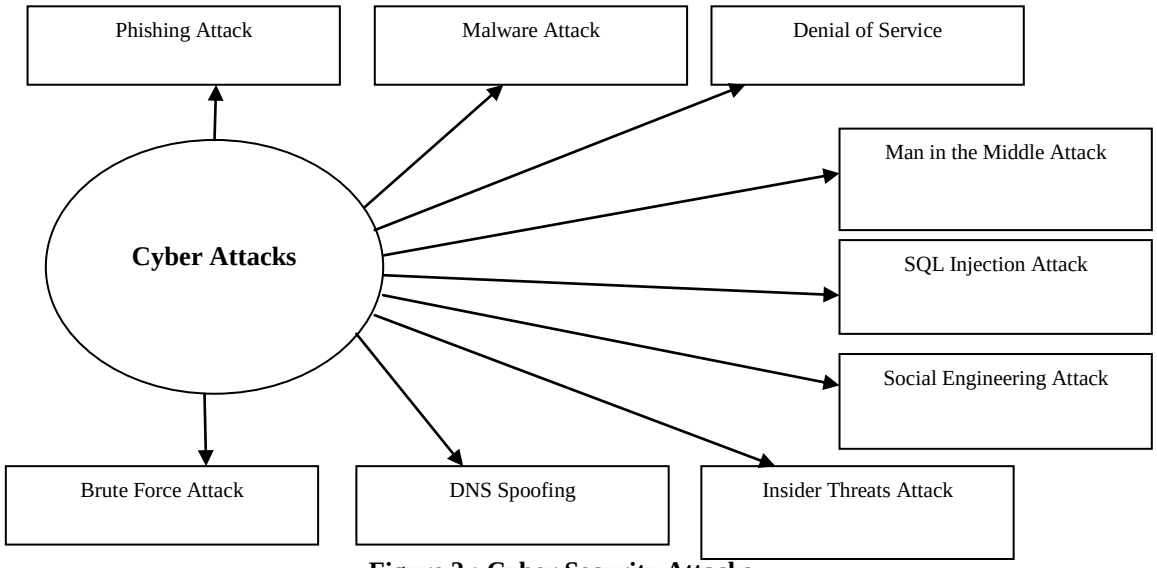

Figure 2 : Cyber Security Attacks

Phishing Attacks – According to Verizon's latest data breach survey 32 percent of confirmed breaches are from phishing. These attacks are aimed at scaring people into sharing valuable information like their user names, passwords, social security numbers and credit card details. Whether through email, text or more commonly phone calls [6]

Malware Attacks – Malware is a type of dangerous software designed to disrupt the normal functioning of any device such as mobile phones, desktop, laptop and servers. The user clicks on the malware source which is often presented in the form of a script or executable code and accidentally installs the malware. Some malware types are designed to gain persistent network access while others are designed to spy on user activities or steal vital information and some are designed simply to cause disturbance. Some malware is designed to extort money. Ransomware like malware, encrypts files and then demands payment in exchange for the decryption key [13].

Denial-of-Service Attacks – In this attacks hackers overload a server or network so much that legitimate users have trouble accessing services.

Man-in-the-Middle Attacks – In this attacks hackers interfere in the communication and steal data when information is exchanged between two parties.

SQL Injection Attacks – In this attacks hackers gain unauthorized access to the database of websites or applications, which can compromise sensitive information.

Social Engineering Attacks – In this attack attackers take advantage of people's emotions and human behaviour so that they can obtain information through any means, such as passwords or confidential data.

Insider Threats – These types of attacks often come from employees within an organization contractors or suppliers who may by suggestion or by omission reveal confidential information or cause damage.

DNS Spoofing – In this attack hackers modify Domain Name System records so that genuine users can be sent to fake websites and information can be stolen from them.

Brute Force Attacks – In this attack, hackers use automated tools to scan passwords thereby gaining unauthorized access to systems or accounts.

IV. CYBER SECURITY TECHNIQUES

Cyber attackers try to accomplish their objectives by changing their operations using technologies. They often modify the malware's signature so that they can take advantage of those techniques and sometimes they find ways to exploit the malware so that it can be successful in entering. The rapid development of internet

technologies and its use by millions of people provides cyber criminals with easy access to large numbers of people [6].

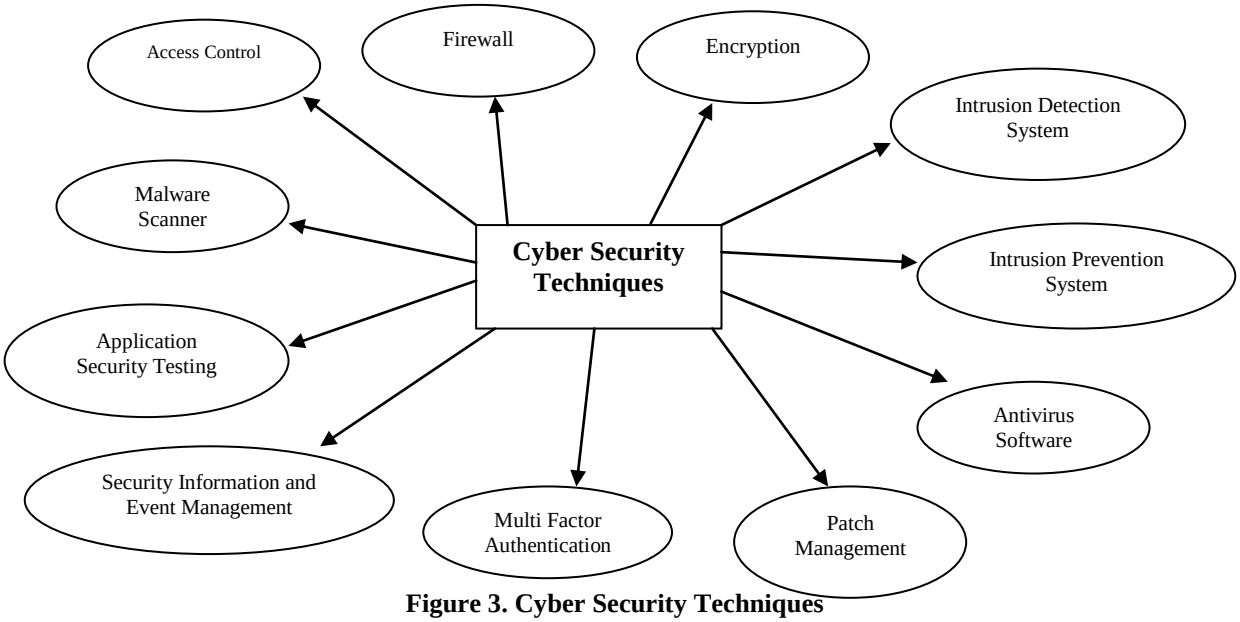

Figure 3. Cyber Security Techniques

Access Control – In this type of technology users are given special permissions so that only authorized users can access specific information.

Firewall – A firewall is a software or hardware package that helps prevent hackers, viruses and worms from trying to access you Personal Computers or Laptop through the web. It checks all incoming messages and block those that do not meet security criteria. Firewalls play a vital role in detecting malware or it can also be said that this is a network security device which blocks unauthorized access and malicious traffic [6].

Encryption – In this type of technology while security the data it is converted into plain form so that unauthorized access can be avoided.

Intrusion Detection System – This system detects attempts to enter the network and generates messages when any suspicious activity occurs. Intrusion Detection System (IDs) is an effective tool that helps business detect and prevent unauthorized entry into their networks [14].

Intrusion Prevention Systems – These are advanced forms of detection that not only detect attacks but also try to stop them.

Antivirus Software – This software is used to protect computers and networks against malware and viruses.

Patch Management – In this systems and software are kept up to date within a stipulated period so that the weaknesses detected in them can be removed.

Multi-factor Authentication (MFA) – In this process authentication is done using two or more factors such as a fingerprint or biometric authentication along with a password.

Security Information and Event Management - Security Information and Event Management tools monitor network and system events to identify and respond to potential security incidents.

Application Security Testing - These techniques are used to identify and fix vulnerabilities in software and applications, so that no security vulnerabilities can be exploited.

Malware Scanner – Malware scanner is a software tool that protects computers and networks from malware and viruses. It scans files, programs and memory and identifies or isolates malware which keeps systems secure and reduces the possibility of malware.

V. CONCLUSION

Cloud computing is increasing and with it, the importance of cyber security is also increasing. The entry and development of cloud systems is a major step but along with it also faces many questions of security and privacy. The threat of Cyber attacks in this region is also increasing becoming more serious and widespread. Thus, development of cyber security techniques and practices and their application is essential in every cloud environment. In just a short time the development of progress combined with the depth and breadth of powerful cloud computing and strong cyber security. Which even ordinary people cannot understand is monumental. To achieve this objective more effective security measures should be developed so that an environment of security and trust can developed in the digital world.

ACKNOWLEDGMENTS

This paper and the research behind it would not have been possible without the exceptional support of my supervisor Dr. Upendra Nath Tripathi. I would also like to acknowledge the invaluable contributions of my research colleagues and advisors who provided guidance and support throughout the research process.

REFERENCES

[1]. Munish Saran, Rajan Kumar Yadav and Upendra Nath Tripathi, "Machine Learning based Security for Cloud Computing : A Survey", International Journal of Applied Engineering Research, ISSN 0973-4562, Volume 17, Number 4 (2022), pp. 332-337.

[2]. Roaa Al Nafea and Mohammed Amin Almaiah, "Cyber Security Threats in Cloud : Literature Review", 2021 Internation Conference on Information Technology (ICIT), 2021 IEEE, DOI : 10.1109/ICIT52682.2021.9491638.

[3]. Somesh Rai, Dr. K. Singh and A. K. Varma, "Global Research Trend on Cyber Security : A scientometric Analysis", (2019), Library Philosphy and Practice (e-journal), 3769, https://digitalcommons.unl.edu/libphilprac/3769.

[4]. Mrs. Ashwini, Mr. Sachin Bbosale, Mr. Farisb Kurupkar, "RESEARCH PAPER ON CYBER SECURITY", CONTEMPORARY RESEARCH IN INDIA (ISSN 2231-2137) : SPECIAL ISSUE : APRIL, 2021.

[5]. Yuchong Li and Qinghui Liu, "A comprehensive review study of cyber-attacks and cyber security ; Emerging trends and recent developments", Elsevier, Energy Reports 7 (2021) 8176-8186.

[6]. Dr. Prof. Rajasekharaiah K.M., Chhaya S Dule, Sudarshan E, " Cyber Security Challenges and its Emerging Trends on Latest Technologies", IOP Conf. Series : Materials Science and Engineering 981 (2020) 022062, doi : 10.1088/1757-899X/981/2/022062.

[7]. Joachim Bjorge Ulven and Gaute Wangen, "A Systematic Review of Cybersecurity Risk in Higher Education", Future Internet 2021, 13, 39. https://doi.org/10.3390/fil3020039.

[8]. Zeinab El-Rewini, Karthikeyan Sadatsharan, Niroop Sugunaraj, Daisy Flora Selvaraj, Siby Jose Plathottam and Prakash Ranganathan, " Cybersecurity Attacks in Vehicular Sensors", IEEE Sensors Journal, Vol. XX, April 2020.

[9]. Deval Bhamare, Maede Zolanvari, Aiman Erbad, Raj Jain, Khaled Khan, Nader Meskin, "CyberSecurity for Industrial Control Systems : A Survey", ePrint Computers and Security, Elseveir, Accepted November 2019.

[10]. Diptiben Ghelani, "Cyber Security in Smart Grids, Threats and Possible Solutions", American Journal of Applied Scientific Research, 2022, doi : 10.11648/j.XXXX.2022XXXX.XX, https://www.sciencepublishinggroup.com/j/ajasr.

[11]. Mahesh Kumar and Sanjay Gupta, "Security perception of e-banking users in India", An Analytical Hierarchy Process. Bank and Bank Systems, 15(1), 11-20, doi : 10.21511/bbs.15(1).2020.02.

[12]. Iqbal H. Sarker, A.S.M. Kayes, Shahriar Badsha, Hamed Alqahtani, Paul Watters and Alex Ng, "Cybersecurity data science : an overview from machine learning perspective", Journal of Big Data, 2020, DOI : 10.1186/s40537-020-00318-5.

[13]. Dr. Yusuf Perwej, Prof. (Dr.) Syed Qamar Abbas, Jai Pratap Dixit, Dr. Nikhat Akhtar and Anurag Kumar Jaiswal, "A Systematic Literature Review on the Cyber Security", International Journal of Scientific Research and Management (IJSRM), Volume 09, Issue 12, Pages EC-2021-669-719, 2021.

[14]. Munish Saran, Rajan Kumar Yadav, Pranjal Maurya, Sangeeta Devi and Upendra Nath Tripathi, " A Novel Methodology For Enhancing Intrusion Detection System", i-manager's Journal on Software Engineering, Vol. 17, No. 4, April-June 2023.