CYBER SECURITY IN SDN NETWORKS

[1]K.Priyadharshini, [2]Navaneetha Krishnan.S, [3]D.Karthik, [4]M.Santhanaraj

[1]Assistant Professor, [2]Student, [3]Student, [4]Student
Computer Science
[1]Sri Krishna Adithya College of Arts and Science, Coimabatore, India

***Abstract*: Cyber Security plays an important role in the field of information technology. Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.**

***Keywords*: Cyber security, Cyber crime, cyber ethics, social media, cloud computing, android apps.**

I. INTRODUCTION:

The ability to accumulate massive amounts of knowledge provides the chance to look at, observe, and see irregularities to discover network problems. Higher unjust security data reduces the essential time from detection to correction, enabling cyber specialists to predict and stop the attack with none delays. Information is analyzed mistreatment algorithms that provide essential insight to organizations so as to produce help in up their services. Massive information is continuous to be used on larger platforms as well as money services, health services, weather, politics, sports, science and analysis, vehicles, assets, and currently cyber security. A very important thanks to monitor your network is to line up a giant information analysis program. A typical response to evolving attacks is to either add a lot of security tools or increase the sensitivity of the safety tools already in situ. Massive information analysis is that the method of viewing massive information sets to reveal hidden patterns, unknown correlations, market trends, client preferences and different necessary data. To ingest all the information, filter and combination the information 1st, however it's tough and troublesome to come to a decision what to filtrate and what to stay.

II. ROLES HUMANS PLAY IN CYBERSECURITY SCIENCE

• Humans as developers and designers:
We will be talking a lot about cybersecurity practitioners in their roles thinking and acting as scientists.

• Humans as users and consumers:
Humans as users and consumers often throw a wrench into cybersecurity. Users are commonly described as the weakest link in cybersecurity.

• Humans as orchestrators and practitioners:
Our goal is to defend a network, data, or users, and we decide how to achieve the desired goal. Defenders must be knowledgeable of the environment, the tools at their disposal, and the state of security at a given time. Human defenders bring their own limitations to cyber defense, including their incomplete picture of the environment and their human biases.

• Humans as active adversaries:
Human adversaries can be unpredictable, inconsistent, and irrational. They are difficult to attribute definitively, and they masquerade and hide easily online. Worse, the best human adversaries abandon specific attacks more quickly than defenders like you can discover them. Scientific inquiry in chemistry and physics have no analogous opponent.

III. METHODS USED TO PREVENT OF CYBER THREATS

With the help of Big Data log analytics we can prevent cyber threats by monitoring data. When Big Data log analytics is combined with JIT (Just in Time) analysis it collects information on the machines that have an open connection with locations outside the local network. It also predicts future attacks and gives you information about previous attacks that might have occurred on your system. An IBM report shows us that forty-six (46) percent of businesses are experiencing security breaches; which shows that the need to protect our information is very high. IBM developed a solution using Big Data that protects data from threats and fraud. IBM's solution detects risk and intrusion while analyzing structured and unstructured data.

Crucial issues in cyber security:
Cyber security relies upon the care that individuals can take and conclusions they conduct while they organize, manage and utilize systems and internet. Numerous efforts have been made to find the solution for cyber security evaluation challenge and various frameworks have been constructed. However, the frameworks encounter different difficulties though it was working fine initially

at the time of development. The restrictions derive from different aspects, such as emerging technologies and facility limitations. Security issues are often considered a tradeoff between security requirements and other benefits.

IV. PREVENTION OF CYBER SECURITY:

There are seven significant cyber-safety actions which are Running Anti-virus Software, Installing OS/Software Updates, Preventing Identity Theft, Switch on the Personal Firewalls, Prevent Adware/Spyware, protection of Passwords and Backing up Important Files.

1) Install OS/Software updates:

• Installing software updates are also known as patches that helps to fix issues of operating system (OS) (e.g., Mac OS X, Windows Vista, Windows XP,) and software programs such as Microsoft applications.
• Many of the latest operating systems are arranged to download updates automatically by default. Once the updates have been downloaded, a confirmation prompt is displayed for installation. Click yes
• Once the updates are complete, make sure to restart the computer for the patches to be applied.

2) Running Anti-Virus Software:

• In order prevent computer virus issues install and then run the anti-virus software such as Sophos and check the last updated date.

• Make sure to check periodically if the installed antivirus is up to the date which helps to block current and future viruses. The anti-virus application removes detected viruses, quarantines it and finally repairs users system infected files.

• The students of UC Davis, staffs and faculty members can download Sophos software for both homes and work computers for free from the Internet Tools CD, which you can obtain from the Shields Library's IT Express.

3) Preventing Identity Theft:

• Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it. Protect others people's information as you would your own. • Never send personal or confidential information via email or instant messages as these can be easily intercepted.

• Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable business (often a financial institution) in an attempt to gain personal or account information. These often do not include a personal salutation. Never enter personal information into an online form you accessed via a link in and any email from an unknown email id. Generally authentic businesses do not request personal details online.

4) Switching on Personal Firewalls:

• Find under system's security setting for a default personal firewall and switchiton. MacOSC and Microsoft Vista have installed built-in firewalls. After turning on the firewall, check it for any open ports which would allow hackers and viruses.

• Firewalls work as the protection layers between the internet and computers.

• The standard process of hackers would be to send pings (calls) to various computers at random and check for their responses. The functionality of Firewalls is to block your computer which prevents any response calls from a computer.

5) Protecting passwords:

• Make sure that not to share your passwords, and make sure to create new passwords which are hard to guess. Avoid any dictionary works and establish a password by with mixed number, alphabets, and punctuation marks.

• Be sure not to use any common passwords or its variations such as abc123, iloveyou1, let me in, qwerty1, (yourname1), password1 and baseball.

• Change passwords periodically. • When choosing a password: – Mix upper and lower case letters – Use a minimum of 8 characters – Use mnemonics to help you remember a complicated password.

V. IMPLEMENTATION

When springing up with the long-standing time analysis, development and application of AI ways that in Cyber Security, one must distinguish between the immediate goals and long views. There square measure varied AI ways that directly applicable in

Cyber Security, and gift square measure immediate Cyber Security problems that has to plenty of intelligent solutions than square measure implemented these days. As nevertheless we tend to have mentioned these existing immediate applications. inside the future, one can see promising views of the appliance of totally new principles of knowledge handling in state of affairs management and deciding. These principles embrace introduction of a customary and stratified knowledge style inside the deciding software. This type of style has been planned. An application house is that the information management for net central warfare. solely automatic knowledge management can guarantee quick state of affairs assessment that gives an alternative superiority to leaders and call makers on any C2 level. Knowledgeable systems square measure already obtaining employed in many applications, usually hidden inside associate degree application, like inside the safety measures springing up with software. However, knowledgeable systems can get wider application, if huge knowledge bases measure going to be developed.

VI. CONCLUSION

From the review, it was found that majority of the studies have been conducted on the email security, firewalls, and vulnerabilities. Yet, not many studies from the perspective of password security. There are general recommendations on how to secure the password but not any authenticated protocol to protect the system inherently. Therefore, there is a need for more studies in terms of technics and models from this perspective to ensure that passwords are protected. The experience in DDoS mitigation has shown that even a security against large-scale attacks are unbowed with rather restricted resources once intelligent ways that square measure used. Obviously, the new developments in data understanding, illustration and handling what is more in machine learning will greatly enhance the cyber security capability of systems that may use them.

REFERENCES

[1]. (George, January 11, 2017) http://www.securityweek.com/role-artificialintelligence-cyber-security
[2]. E. Tyugu. Algorithms and Architectures of engineering. IOS Press. 2007.
[3]. B. Mayo, E. Tyugu, J. Penjam. Constraint Programming. Alignment ASI Series, v. 131, SpringerVerlag. 1994.
[4]. I. Bratko. Logic programming Programming for engineering. Addison-Wesley, 2001 (third edition).
[5]. http://singinst.org/overview/whatisthesingularity/
[6]. F. Rosenblatt. The Perceptron -- a perceiving and recognising automaton. Report 85-460-1, Cornell natural philosophy Laboratory, 1957.
[7]. F. Barika, K. Hadjar, and N. El-Kadhi, "Artificial neural network for mobile IDS resolution," in Security and Management, 2009.