Journal For Innovative Development in Pharmaceutical and Technical Science (JIDPTS)
Volume:3, Issue:11, Nov:2020

(J I D P T S)
ISSN(O):2581-6934

STUDY OF EMERGING TRENDS ON LATEST TECHNOLOGIES AND ITS CYBERSECURITY CHALLENGES

Anusha Chitneni [1]

[1]Dept of Research & Development, Electrogenics, Telangana

Abstract : Cyber Security assumes a significant part in the field of information technology. Securing the data have gotten perhaps the most crucial test in the current day. At whatever point we consider cybersecurity, the main thing that rings a bell is 'cyber crimes,' which are expanding hugely step by step. Different Governments and organizations are taking numerous measures to forestall these cybercrimes. Other than different measures, cybersecurity is as yet a significant worry to many. This paper focuses on centers around challenges looked at by cybersecurity on the most recent advances. It additionally centers around the most recent cybersecurity techniques, morals, and the patterns changing the essence of cybersecurity.

Keywords: cybersecurity, cybercrime, cloud computing

I. INTRODUCTION

Today man can send and get any information, might be an email, or a sound or video just by the snap of a catch, yet did he think how safely his information is being communicated or shipped off the other individual securely with no spillage of data? The appropriate response lies in cybersecurity. Today the Internet is the quickest developing framework for inconsistent life. In the present specialized climate, numerous most recent innovations are changing the substance of humankind. However, because of these arising advancements, we cannot compellingly shield our private data, and subsequently, these days, cybercrimes are expanding step by step. Today more than 60% of absolute business exchanges are done on the web, so this field required a high caliber of security for straightforward and best exchanges. Henceforth cybersecurity has become a most recent issue. The extent of cybersecurity is not merely restricted to making sure about the data in the IT industry yet in different fields like cyberspace etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking[1]. Additionally needs a significant level of security. Since these technologies hold some important data regarding a person, their security has become unquestionable. Enhancing cybersecurity and protecting necessary data infrastructures are essential to each country's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to developing new services just as governmental policy. Against cybercrime needs a comprehensive and safer methodology. Given that technical measures alone cannot prevent any crime, law enforcement agencies must be allowed to investigate and prosecute cybercrime effectively[2]. Today, numerous countries and governments are forcing severe cyber securities laws to prevent some essential data loss.

II. CYBERSECURITY

Privacy and security of the information will consistently be top security measures that any association takes care of. We are presently experiencing a daily reality such that all the data is maintained in a computerized or a cyber-structure. Social networking sites provide a space where users feel safe as they interact with friends and family. On account of home users,

cyber-criminals would continue to target social media sites to steal personal information. Social networking and bank exchanges require a person to take all the required security measures. As crime is expanding, even the security measures are additionally expanding[3]. As per the review of U.S.technology and healthcare heads across the country, Silicon Valley Bank found that companies accept cyber attacks as a severe threat to their data and business coherence.

There will be new attacks on Android operating system based devices, yet it will not be for enormous scope. The reality tablets share similar operating system as PDAs implies the equivalent malware will before long focus them as those stages. The number of malware examples for Macs would keep developing, however substantially less than on account of PCs. Windows 8 will permit clients to create applications for virtually any gadget (PCs, tablets, and PDAs) running Windows 8, so it will be conceivable to create killer applications like those for Android. Thus these are a portion of the anticipated patterns in cybersecurity[4].

III. TRENDS CHANGING CYBERSECURITY

Here mentioned below are some of the trends that are having a significant impact on cybersecurity.

1. Web servers

The threat of attacks on web applications to separate data or to distribute malicious code endures. Cybercriminals distribute their malicious code through real web workers they have undermined. Be that as it may, data-taking attacks, a considerable lot of which get the consideration of media, are additionally a significant threat. Presently, we need a more noteworthy accentuation on securing web workers and web applications[5]. Web workers are mainly the best stage for these cybercriminals to take the data. Henceforth one should consistently utilize a more secure program, particularly during significant exchanges, not to fall prey to these crimes.

2. Cloud computing and its services

Nowadays, all small, medium and enormous companies are gradually receiving cloud services. As such, the world is gradually moving towards the clouds. This most recent pattern presents a significant test for cybersecurity, as traffic can circumvent customary examination purposes. Furthermore, as the quantity of applications accessible in the cloud develops, strategy controls for web applications and cloud services will likewise need to advance to forestall the loss of essential data. Even though cloud services are building up their models, many issues are being raised about their security. Cloud may give gigantic chances; however, as the cloud advances, it should consistently be noticed as its security concerns increment.

3. APT's and targeted attacks

Adept (Advanced Persistent Threat) is an unheard-of level of cybercrime product. For quite a long time, network security capacities, for example, web separating or IPS, have had a critical impact in distinguishing such focused on attacks (generally after the underlying trade-off). As assailants become bolder and utilize more dubious strategies, network security must coordinate with other security services to identify attacks[6]. Subsequently, one must improve our security procedures to forestall more threats coming later on.

4. Mobile Networks

Today we can interface with anybody in any piece of the world. Be that as it may, for these mobile networks, security is a too huge concern. Nowadays, firewalls and other security measures are getting permeable as individuals are utilizing devices, for example, tablets, phones, PC's and so forth, all of which again require additional protections separated from those present in the applications utilized. We should consistently consider the security issues of these mobile networks. Other mobile networks are exceptionally inclined to these cybercrimes[7]. A great deal of care must be taken if there should arise an occurrence of their security issues.

5. IPv6: New internet protocol

IPv6 is the new Internet convention that is supplanting IPv4 (the more seasoned rendition), which has been a spine of our networks all in all and the Internet on the loose.

Ensuring IPv6 is not only an issue of porting IPv4 capacities. While IPv6 is a discount substitution in making more IP tends to accessible, some principal changes to the convention should be considered in security policy. Subsequently, it is in every case, better to change to IPv6 at the earliest opportunity to decrease the dangers concerning cybercrime.

ISSN:-2581-6934 |Available at : www.jidps.com | pp :(15-18)

IV. CYBERSECURITY TECHNIQUES

1. Access control and password security

The idea of user name and password has been a critical method of securing our data. This might be one of the principal measures concerning cybersecurity.

2. Authentication of data

The reports that we get should consistently be verified be before downloading that is it ought to be checked on the off chance that it has begun from a trusted and a dependable source and that they are not changed. Confirming of these reports is generally done by the antivirus programming present in the devices. In this way, decent antivirus programming is additionally essential to shield the devices from viruses[8].

3. Malware scanners

This software usually examines all the records and archives present in the system for malicious code or dangerous viruses[9]. Viruses, worms, and Trojan ponies are malicious software regularly gathered and alluded to as malware.

4. Firewalls

A firewall is a software program or bit of hardware that assists screen with trip programmers, viruses, and worms that attempt to arrive at your PC over the Internet. All messages entering or leaving the web go through the firewall present, which analyzes each message and squares those that do not meet the predetermined security models[10]. Consequently, firewalls assume a significant function in distinguishing the malware.

V. CONCLUSION

PC security is a big theme that is becoming more significant because the world is getting exceptionally interconnected, with networks being utilized to do essential exchanges. Cybercrime keeps on veering down various ways with each New Year that passes, thus protecting the data. The most recent and troublesome technologies, alongside the new cyber tools and threats that become visible every day, are testing organizations to secure their framework. However, they require new stages and insight to do as such. There is no ideal answer for cyber crimes except for we should attempt our level best to limit them to have a sheltered and secure future in cyberspace.

REFERENCES

[1] International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, “Study of Cloud Computing in HealthCare Industry “ by G.Nikhita Reddy, G.J.Ugander Reddy

[2] Soni, Vishal Dineshkumar and Soni, Ankit Narendrakumar and POTHUGANTI, KARUNAKAR, Student Body Temperature and Physical Distance Management Device in Classroom Using 3d Stereoscopic Distance Measurement (2020). International Journal of Innovative Research in Science Engineering and Technology 9(9):9294-9299,

[3] IEEE Security and Privacy Magazine – IEEECS “Safety Critical Systems – Next Generation “July/ Aug 2013.

[4] Vishal Dineshkumar Soni. (2018). IOT BASED PARKING LOT. International Engineering Journal For Research & Development, 3(1), 9. https://doi.org/10.17605/OSF.IO/9GSAR

[5] CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

[6] Vishal Dineshkumar Soni. (2019). IOT connected with e-learning . International Journal on Integrated Education, 2(5), 273-277. https://doi.org/10.31149/ijie.v2i5.496

[7] J. Yang, D. Zhang, A. Frangi, and J. Yang, “Two-dimensional PCA: a new approach to appearance-based face representation and recognition,”IEEE. Trans. Pattern Analysis and Machine Intelligence, vol. 26, No. 1, 2004.

[8] Soni, Ankit Narendrakumar, Diabetes Mellitus Prediction Using Ensemble Machine Learning Techniques (July 3, 2020). Available at SSRN: https://ssrn.com/abstract=3642877 or http://dx.doi.org/10.2139/ssrn.3642877

[9] I. Ahmad and K. Pothuganti, "Smart Field Monitoring using ToxTrac: A Cyber-Physical System Approach in Agriculture," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 723-727, doi: 10.1109/ICOSEC49089.2020.9215282.

[10] Ankit Narendrakumar Soni (2019). Spam-e-mail-detection-using-advanced-deep-convolution-neural-network-algorithms. JOURNAL FOR INNOVATIVE

ISSN:-2581-6934 |Available at : www.jidps.com | pp :(15-18)

DEVELOPMENT IN PHARMACEUTICAL AND TECHNICAL SCIENCE, 2(5), 74-80.

ISSN:-2581-6934 |Available at : www.jidps.com | pp :(15-18)