IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

The Future of Cyber Security

Adharsh Krishnan
adharshsanthi@gmail.com
Sri Krishna College of Technology,
Coimbatore, Tamil Nadu

M. Deva Priya
m.devapriya@skct.edu.in
Sri Krishna College of Technology,
Coimbatore, Tamil Nadu

ABSTRACT

In the near future, cyber security will play a dominant role in personal and business applications. As society is becoming more and more digitized, there are more chances to win by exploiting this. As a result of the growing proliferation of digitization and connected devices, the demand for cyber security solutions is growing at a relatively high rate. The complexity and connectivity of digitized systems have a direct impact on their security. The goal of this review is to summarize the logical predictions of the future of cybersecurity.

Keywords— *Cyber security, Information security, Cloud systems, IoT systems, Digitization, Cyberspace, Cyber defense*

1. INTRODUCTION

Today, most of the critical and important systems are interconnected and driven by computers. It will increase in the near future resulting in more and more things being automated. Personal lives will entirely depend on interconnected devices which would make everyday lives easier and smarter.[1] Almost all the data will reside on the cloud, making it vulnerable to data theft and leakage if preventive measures aren't implemented. The role of cybersecurity in everyday lives will increase tremendously within the next 10 years because of the increase in internet-connected devices.[2] Every data must be protected and several policy frameworks have to be created to manage it.

2. IMPACT OF INTERCONNECTED DEVICES

It is estimated that in 10 years, the number of Internet of Things (IoT) devices will be more than 10 times the human population seen today.[3] Each day, thousands of new devices come online into the cyberspace and each one of them is susceptible to a security breach in one way or the other. Figure 1 shows the increase in the number of devices used between 2015 and 2020.

At present, as per the data are shown in figure1, the number of connected devices is more than the number of humans on this planet and this will triple in the next 5 years.

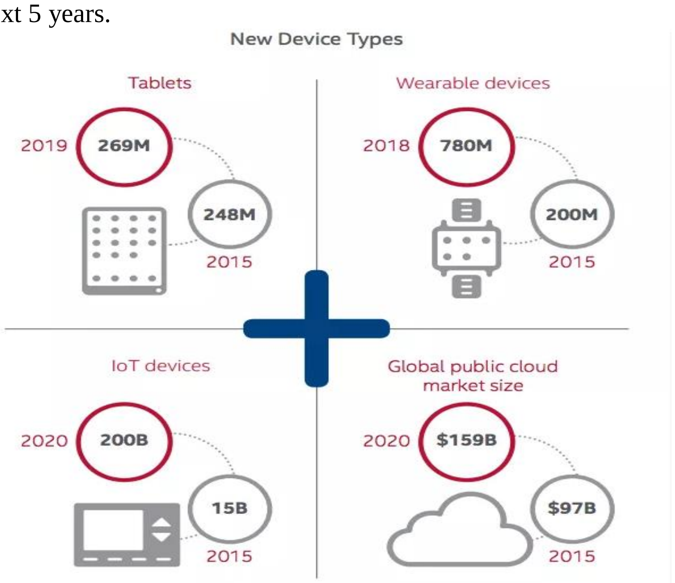


Fig. 1: Estimation of the number of new devices (2015 - 2020)

3. CYBERCRIME

Cybercrimes are increasing every day. The important factor is the lack of forecasting of the impact of cybersecurity. So the future predictions should be able to bring stable but not susceptible policies that should likely reduce the cybercrime activities that are being carried out worldwide. One of the predictions is that cybercriminals will find more ways to break and that should be avoided by writing new security policies and implement them across the industry.

Every year, the number of cyber crimes increase, costing countries and companies billions of dollars. The total cost shows that even though there are systems to defend such attacks, criminals have not stopped disrupting the system (figure 2). To tackle this, the UN, other institutions and bilateral have come together to create seamless web enforcement against cybercriminals. This should continue and be given more importance to ensure the safety of the countries and companies from cybercriminals.

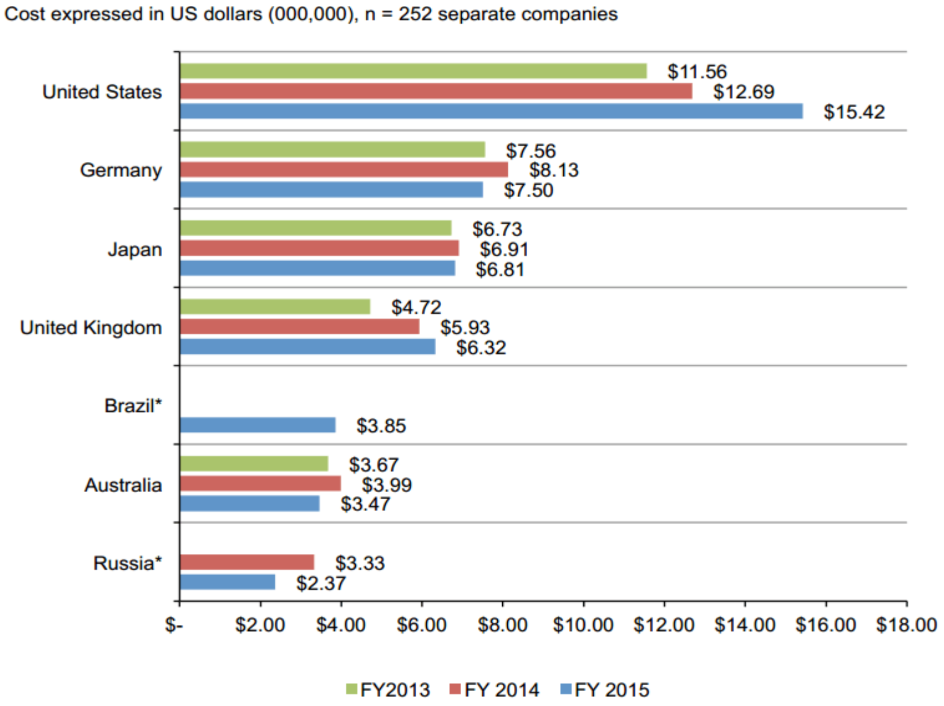


Fig. 2: Total Cost of Cyber Crimes in Seven Countries (2013 - 2015)

4. ROLE OF IoT IN CYBER LANDSCAPE

In IoT, objects identify each other and share information that can help each other in real-time. This technology thrives well as any object can represent itself in the shared world and become more usable. It is about a world where anything can be connected online and produce intelligent data. However, this also means that the system is susceptible to weakness and this is where the role of cybersecurity comes in.

Privacy becomes the major concern when IoT is involved because an object which belongs to a person is shared to the online world. If an object has a flaw, it can be accessed by attackers and the person's privacy is breached.

One major concern is that of all these connected devices around 70 percent are vulnerable to attacks. This makes almost everyone who owns a connected device vulnerable to attack and lose private information. Open Web Application Security Project (OWASP) is an online community that provides solutions to problems of major concerns and IoT is one of them for sure. Figure 3 shows the IoT landscape.

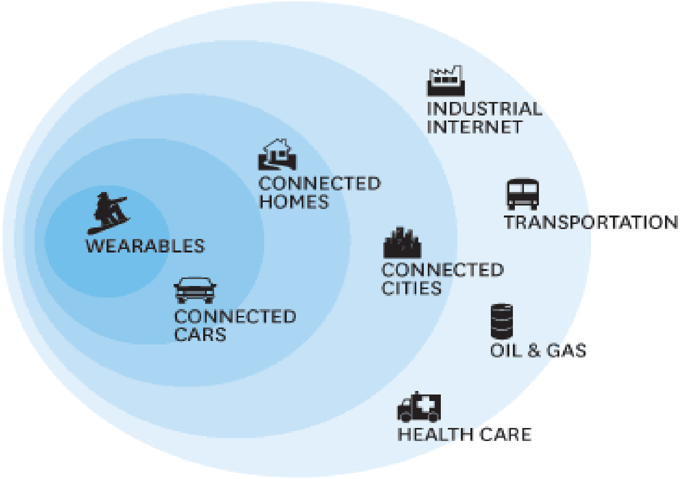


Fig. 3: IoT Landscape

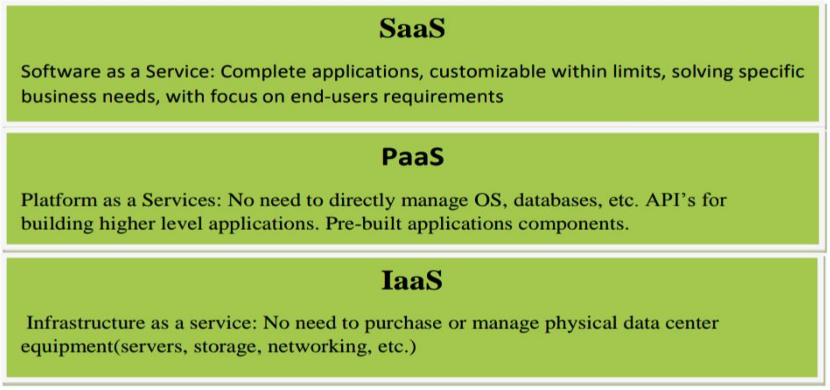
Some of the security flaws in the community are listed below:

- Web Interface is insecure
- Authentication and Authorization are insecure
- Cloud Interface is insecure
- Mobile Interface is insecure
- Data transmission and encryption are insecure
- Software is insecure
- Framework is insecure

The cyber landscape has evolved a lot in the past 10 years solving many flaws and insecurities. IoT will be a big challenge for the next 5 to 10 years.

5. CLOUD SECURITY

Cloud Security deals with the protection of information of billions of data which are shared over the cloud services. Cloud is reliable and cost-effective for sharing and maintaining resources over a short span of time. But, the cloud has its disadvantages when it comes to security because it is not secure due to various factors. The three layers of the cloud services are commonly known as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). There are several issues on all of these services on both customer and provider views (figure 4).



SaaS

Software as a Service: Complete applications, customizable within limits, solving specific business needs, with focus on end-users requirements

PaaS

Platform as a Services: No need to directly manage OS, databases, etc. API's for building higher level applications. Pre-built applications components.

IaaS

Infrastructure as a service: No need to purchase or manage physical data center equipment(servers, storage, networking, etc.)

Fig. 4: Cloud Services

Following are the security issues seen in Cloud Services.

- Multi-tenancy
- Insider Attack
- Outsider Attack
- Loss of Control
- Data Loss
- Elasticity

5.1 Multi-tenancy

It refers to providing shared computational resources, storage to all the clients who reside on the same physical storage of the person providing the resources. This may lead to data leakage, thus resulting in a privacy breach.

5.2 Insider Attack

A cloud vendor cannot trust the third party services and hence anyone in the organization can hack the resources of the cloud system.

5.3 Outsider Attack

The outsider attacks are not as dangerous as an insider but are prevalent. Cloud services are not private and so hackable at the Application Program Interfaces (APIs) and prone to vulnerabilities.

5.4 Loss of Control

Loss of control over data is the top area on which data loss happens for cloud organizations. Since the cloud can be hosted anywhere, it is hard for companies to keep track of the data.

5.5 Data Loss

Backing up data is very important on cloud services as recovering deleted original content is tedious. Organizations are not ready to spend time and money on recovering data which costs more than the installation costs.

5.6 Elasticity

Elasticity mainly leads to confidentiality issues. Scalability is the main goal of elasticity and it will provide resources to customers on demand and scale based on data.

Several solutions have been identified for some of the problems like malware injection attack problem, flooding attack problem and security information management. Many solutions have to be found for making the cloud much more secure because the cloud is definitely the future of data access and storage.

6. DEFENSE SECURITY SYSTEMS

Cybersecurity defence systems should be improved to cope-up with the proliferating data landscape. The defence systems should be able to analyze the data in real-time and to do that, they should be interconnected.[13] As network devices are interconnected, the existing security measures and policies should be updated to deal with that kind of data.[4]

The cyber knowledge gap is huge in the industry and with the rise of Artificial Intelligence (AI), cyber systems rely on it for more accurate information. Hence, the next generation of cybersecurity experts should be cultivated to efficiently handle the improved systems. Countries should give more importance to protect large scale environments like traffic controls and educate the public on safety measures.[8] Cloud services should have equal protection as data centres and their integrity in sending and receiving the user data should be maintained.

7. PREDICTIONS FOR THE NEXT 10 YEARS

Every day, thousands of cyber-attacks are being carried in every part of the world. Predicting ‘Where, When and Why’ an attack will happen will save huge costs. Some of the predictions future predictions include:

- Data is accessible from any part of the world and an attacker can find a ‘Strategic method’ to compromise the system which does not require huge cost such as conventional systems.[3]
- Majority of us will be targeted since bots are taking over the tasks done by humans like scanning and finding vulnerabilities which will enable the attack to execute several times faster than normal ones.[4]
- Country-sponsored organizations and attackers will continue to develop new technologies.[5]
- Cybercriminals will find new ways to break the existing system to seek ways to monetize the data.[6]
- Terrorist groups will shift to cyberspace and will try to spread fear and rumours among the masses.[7]

8. SHAPING THE FUTURE OF CYBER SECURITY

Shaping the industry requires shaping the way in which defence systems work and update them to face the upcoming consequences of the cyber world. An agile and evolvable environment should be provided to develop solutions for hard problems.[9]

As the threats pose significant challenges to the industry, they increase as technologies develop and influence the online world in unprecedented ways.[11] The best cybersecurity expertise is measured by the integration of people, process, and technology.[8]

By educating more students on cybersecurity, the knowledge gap can be reduced which in turn would help shape the industry. Countries should focus on providing educational content from the industry to the masses so that they can learn, implement and develop new ways to protect themselves and others in the digital world. Digital security should also be shaped, as it will play a major part in every online user in the next 10 years.

9. CONCLUSION

The long-discussed need for a global cybersecurity forum would be a good start to implement and close the loopholes which make the defence system weak and insecure.[9] However, public awareness is also very important if policies favouring the masses are to be implemented. If people understand the importance of being digitally secure, then the solutions can be found without any difficulty.[10] Began from finding that a small computer program can leave a trail in a network without being detected, the security industry has come a long way in very less time. With more time and expertise, it will continue to evolve to become more secure and resilient.[12]

10. REFERENCES

[1] Thakur, K., Qiu, M., Gai, K., & Ali, M. L., An Investigation on Cyber Security Threats and Security Models, In Proceedings of 2nd IEEE International Conference on Cyber Security and Cloud Computing, pp. 307-311, 2015.

[2] Lohstroh, M., Kim, H., Eidson, J. C., Jerad, C., Osyk, B., & Lee, E. A., On Enabling Technologies for the Internet of Important Things, pp. 150-176, 2019.

[3] Taillat, S., Disrupt and restraint: The Evolution of Cyber Conflict and the Implications for Collective Security, pp. 1-14, 2019.

[4] Alsmadi, I. Cyber Policy and Strategy Management, The NICE Cybersecurity Framework, pp. 181-203, 2019.

[5] Ahmad, N., Mokhtar, U. A., Fauzi, W. F., Othman, Z. A., Yeop, Y. H., & Abdullah, S. N., Cyber Security Situational Awareness among Parents, In Proceedings of Cyber Resilience Conference, pp. 34-70, 2018.

[6] Sevis, K. N., & Seker, E., Cyberwarfare: Terms, Issues, Laws and Controversies, In Proceedings of 2nd IEEE International Conference on Cyber Security and Protection Of Digital Services, pp. 20-25, 2016.

[7] Abomhara, M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, Journal of Cyber Security and Mobility, pp. 65-88, 2015.

[8] Wei, D., Lu, Y., Jafari, M., Skare, P., & Rohde, K., An Integrated Security System of Protecting Smart Grid against Cyber Attacks, In Proceedings of Innovative Smart Grid Technologies Conference, pp. 1-7, 2010.

[9] Rid, T., & Buchanan, B., Attributing Cyber Attacks. Journal of Strategic Studies, pp. 4-37, 2015.

[10] Bajcsy, R., Benzel, T., Bishop, M., Braden, B., Brodley, C., Fahmy, S., & Levitt, K., Cyber Defense Technology Networking and Evaluation, Communications of the ACM, pp. 58-61, 2009.

[11] D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E., Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance analysts, In Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol. 49, No. 3, pp. 229-233, 2005.

[12] Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S., Team-based Cyber Defense Analysis, In Proceedings of IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, pp. 218-221, 2012.

[13] Lévy, P., & Bonanno, R., Collective intelligence: Mankind's Emerging World in Cyberspace, Perseus Books, pp. 200-250, 2017.