2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT) | 979-8-3503-4438-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAICCIT60255.2023.10466175

Honeypot Networks in Deception Technology for IOT Devices

Deepti Sharma[1], Amandeep Singh[2], Shikhar Chitkara[3], Tanmay Sharma[4]
[1]*AIT-CSE, Chandigarh University, Punjab.*
[2,3]*Department of Internetworking, Dalhousie University, Halifax, Canada.*
[4]*CSE , KIIT Kalinga University*

***Abstract*— In this Digitized world, everyone is looking up for options for which there is no need to go out and perform some specific tasks such as Shopping, transferring money, etc. With all these advantages the problem which has been raised is of Cybercrimes with which everyone is scared of these days. Cybercrimes may occur due to the viruses which can enter into devices using insecure websites and can eventually lead us towards being a victim of cybercrime. In this chapter, the Honeypot Networks and frameworks in deception technology for IoT devices has been discussed. Since IoT has taken over every single device in the market and so the risk associated with them is also higher as compared to any other end device. Some novel and enhanced traps are used to engage the hackers for a longer duration and keeping all the essential data secured. The prime constituents of data captured and data control in honeypot has expatriated and presents a categorization for honeypot as per the targets specified. The technical progress and security contribution of nowadays production and research honeypots will be reviewed. This paper highlights the scenarios of the virtualization and integration of upcoming Honeypots and sees how the fusion of Honeypot networks in Cyber security will be helpful for the better tomorrow.**

***Keywords*— Honeypots, Deception Technology, IoT devices, Cyber security, Malicious Activities, Attacks.**

I. INTRODUCTION

In this cutthroat competitive world, everyone is taking a step towards digitization which is itself a very crucial thing, especially for the present modern world. People have been constantly working in improvising modern technology so that people can securely perform various actions, but with all this modernization it can be noticed that several malicious activities have constantly increased in a decade. The main victims of such malicious activities are those people who have been using the Internet frequently and for a longer time. These malicious activities [1]are usually encountered in the form of broadcast email Viruses, Internet scanning worms. No major virus or worm attacks for a long period were seen, it's not just because the Internet connections have become more secure but it is because that the hackers have stopped targeting a large number of systems instead of that they have started controlling and compromising the host system. Day by day things were getting

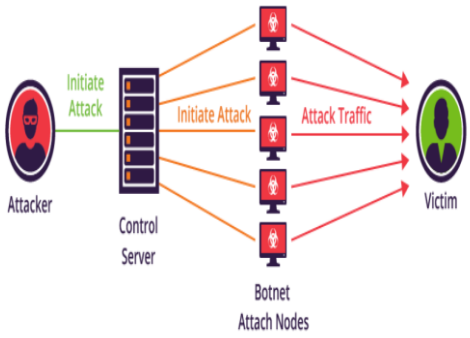

Fig. 1 DDoS Botnet[3]

As an initial enhancement, the "Botnets" on the internet were introduced. A botnet is referred to as computer network which is intruded and managed by an attacker. In this method, every system is contaminated by a malicious set of instructions also known as "bots" which communicate with other devices connected in the botnet. The attackers [2] maintain proper control over the systems and manipulate the devices according to them by using Distributed Denial of service (DDoS) attacks, and various other types of attacks. Turning the tables towards the recent advancements in network security to prevent malicious activities , the "Honeypot networks" introduced. A honeypot network is a unique trap that attracts hackers towards it and when the hacker is attacking the honeypot network then it detects the malicious activity. Recently, researchers have developed various honeypot based attack detection [4,5,6,7,8,9] and analysis systems. Honeypots are used in monitoring defense systems in which attackers who are keeping the botnets will attempt to find means to escape honeypot traps.

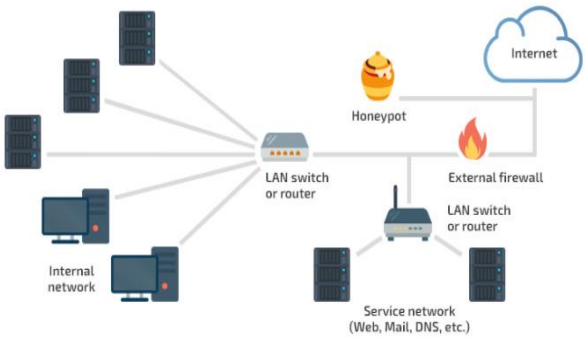

Fig. 2 Deployment of Honeypot networks.[10]

979-8-3503-4438-7/23/$31.00 ©2023 IEEE

Honeypot traps are derived from a well-known technology that is used to prevent any sort of damage in a network in cybercriminal activities. This technology is known as "Deception Technology" which works by developing traps or deception decoys that resemble the actual network which distracts the attacker from getting the actual network attacked. Deception decoys are free to work in a real time or virtual Operating environment and are devised in such a way that it can trick the cybercriminal by making them realize [11] that they have targeted the actual network.

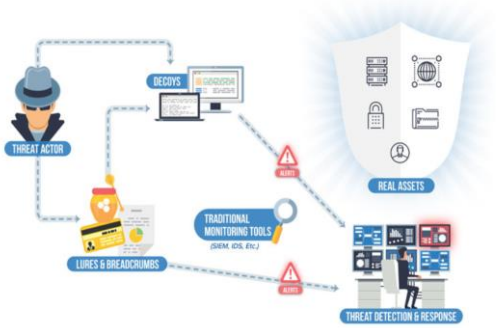

Fig. 3 Deception Technology[12]

Figure 3 illustrates how Deception technology works in an Operating system and how honeypots are deployed. Suppose a threat actor is trying to attack the real assets with the help of Deception Technology, honeypots, and decoys are deployed to prevent a cyber attack on the real assets. These networks fully devote themselves to the attackers and whenever the cybercriminal tries any malicious activity then it is informed to the Threat detection and response through which the user gets the Internet Protocol address of the attacker and protects the real assets from the risk of theft.

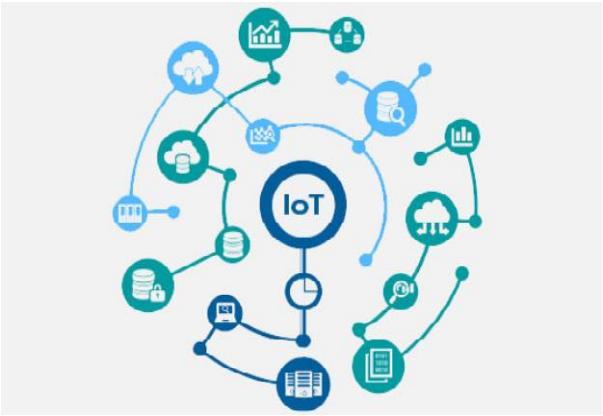

Fig. 4 IoT Network[13]

Since network security has been a major concern in all the networks whether it be normal devices or smart devices everyone wants them to be secured. Several steps have been taken towards the security of the IoT devices such as Authentication and controlled access has been provided to IoT devices to be secure but what about the IoT network? Is it possible for us to make IoT networks secure? To know the answers to several such questions, [14]one need to dig deeper into the fundamental concepts to make IoT networks more secure and sustainable. Further in the chapter the deception technology, Honeypot Networks, and how they could be implemented in IoT Devices is detailed.

II. Deception Technology

Spiteful attacks generally have significant involvements in organizations and businesses but its consequences can be hazardous for a company's value in the market. Whenever an attacker attacks the network then it is very important to acknowledge the crime to the threat detection and repository unit. This facilitates provides the knowledge about the crime and thus find the hope for solution. Therefore, the technique of cyber-provenance is [15] about finding out the attacker behind the malicious activities associated with the network. It includes tracking and policing the hacker, whether it be an individual or a group of people behind the cybercrime. Cyber-criminals can make cyber-attribution more difficult for forensic teams to trace back their traces. With the help of IP Spoofing or proxy servers, criminals can erase their traces for the moment and can confuse the policing team to investigate further.

These challenges are really difficult to resolve and one-sided technology can not help in changing things a lot. In this part of the paper, a technical solution will be studied that assist the investigators in successful cyber-provenance that is Deception Technology. The primary goal of deception technology [16] is to identify anomalous activities happening in the system, Deception Technology works by developing a fake network that resembles the actual network and is generally used for fooling the attacker. These fake networks are also known as decoys which can be operated either on virtual or real operating systems and are designed in such a way that they could trick the criminal to commit a cybercrime.

Most of the traditional methodologies are not helpful in preventing today's cyber-attacks [17, 18, 19] such as advanced persistent threats (APT). Because these methods have now been useless in keeping the network safe so one need some novel technology to tackle situations in a better manner. Deception Technology has been found as one of the best methods in preventing the attackers to meet his or her objective. Traditional methods are proven to be more effective in saving the adversary's malicious attacks directly for example [20, 21] a firewall helps in protecting any unauthorized actions from infiltrating the computer or network whereas the encryption method helps in encrypting the data in such a way that it cannot be decrypted by anyone except the destination address.

The fundamental objective [22]of deception is to manipulate the attacker so that the actual network could be saved from the attack. By studying deception in-depth [23] It is well studied that deception can compensate for limitations in the old defensive methodologies; moreover, deception can be utilized to get additional product information on opponents end when the attacker falls into the defender's trap.

A. Reason of Using Deception Technology

Since now all are familiar with what deception technology is, so it is the time to learn the reason of using deception

technology. In the favour to support the answer of this section, following accountable points are as follows:

1) Post Breach Approach used in earlier times: Breach is a definite incident in which confidential or secure [24] data has been retrieved by cybercriminals or unauthorized users. Basically, the Breach detection system (BDS) [25] is a category of applications and security devices designed in such a way that they can easily detect the malicious activity in the network after a breach has occurred.

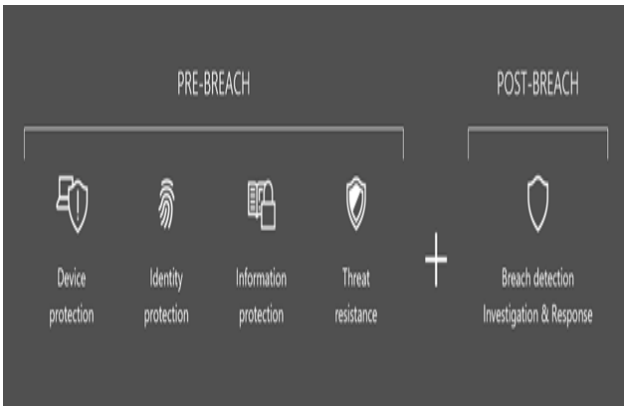

Fig. 5 Steps of Breach Detection with windows defender[26]

No other technology can actually prevent the system or device from being attacked by the hacker although deception technology helps in distracting the attackers and gives them a sense of attacking on a pseudo network. From here one can observe and note the activity of the attacker and [27] hence necessary actions can be taken in accordance to their behavior. In [28] authors have focused the Post Breaching of the customers while doing online shopping for different age groups in which they have seen the variations which can be observed in the age group of 55 years (adults) and below with that to people of beyond 55 years of age (senior Citizens). The study shows the perceptions of both the age groups and also explains how much of a risk factor is associated with the young generation getting their information hacked by the hackers whereas the trust issue of the old generation on online shopping will not allow them to share essential information frequently and hence they are on the safe side.

2) Reduction in fake alerts and risks: Loose ends and fake alerts can all destroy the security endeavors and restrict the resources even if they all are analyzed at all. A lot of noise leads IT teams towards complacent and neglecting which could be a legitimate threat. Through deception technology one can reduce noise and it is associated [29,30]with low risk as it has no risk on data or any sort of impact on the resources and functioning. Whenever a hacker tries to attack on the network a true and genuine message is generated and acknowledges the administrator to take necessary actions in time.

3) On demand automation and scaling: The threat to the data and enterprise network is the most worrying concern and to take some measures regarding this security teams are not funded sufficiently so that they could implement changes and provide a higher level security. Just because of this reason people are heading towards deception technology as it provides a high level security at minimal expenses. It not only eliminates the need of manual endeavors to scale the network but also invents the network automatically according to the demand.

B. Deception Technology and IoT

So far it is discussed that the deception technology has been used for a long span of time. Initially it was used in the defense system for both defensive as well as offensive purposes but as the years passed. It has seen that deception technology [31] has started getting utilized in computer network to provide more security to data and network in the form of Honeypots, Honey nets and in the form of canary files.

For the protection of IoT devices and the users of the services to replicate the decoys. IoT deception is expanded beyond the utilization of honey nets and honeypots This IoT devices replication process confuses the attack targets [32,33,34,35] provided there should be a proper ratio of imposer devices must be working in order to prevent the attack and hence results in making a breach less methodology for the attackers to access the data over the intended IoT network endpoints.

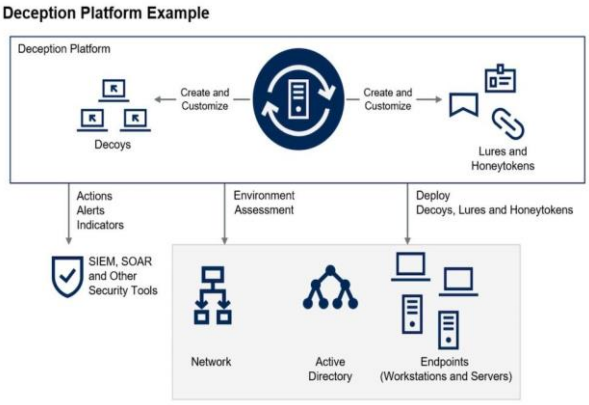

Fig. 6 Deception Technology in IoT Devices[36]

C. Necessity of Dynamic Deception

This section of the chapter is going to highlight the facts about the deception technology and some of the limitations which network technicians came across while establishing the network frames. With time the requirement of the networks has also changed, now businesses have expanded and hence the network does too. With this expansion of the networks, it is quite difficult to add another system in the pseudo network or deception network manually every time one add on a system to actual network.

To resolve this major issue It has decided to make the system from manual working to the automated working system. This drift was not at all possible without the Dynamic Deception technology. One of the most incumbent requirement regarding the successful implementation of deception technology is that there should be identical networks and there must be fresh set of data if these requirements do not match then the attacker may invade to the actual network and try to use other methods to skip this deception network and eventually harm the real system. With recent advancements and keeping in view about the technological changes in terms of Artificial Intelligence and Machine learning world, [37,38]

Many researchers have given their contribution in making the deception networks enabled with these technologies and which are really helping a lot in making them more effective and secured in a way or the other.

III. Honeypot Computing

In computer security terms, Honeypots are the computer security mechanisms established in such a way that they detect, rebound and also counteract the unapproved access to the systems. Usually, a honeypot incorporates the data into it which appears to be the important part of the resource but is completely isolated and monitored from unauthorized access. Honeypot mimics the real [39] network and prevent the actual network from being attacked by any sort of malicious activities.

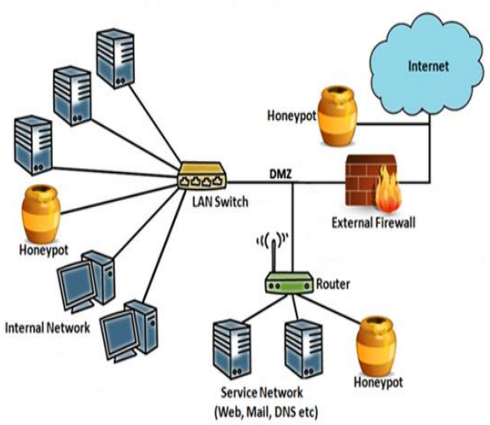

Fig. 7 Honeypot Computing [40]

The figure 7 illustrates the Honeypots in a network to prevent malicious activities in a system. [41]In this section of the chapter Honeypots, Its uses, types and the advantages and limitation of the honeypot networks will be discussed.

A. *Working of Honeypots*

Honeypots are very much identical to the real networks not just the topology but with the applications and data which leads towards fooling the cyber criminals to hack the devices. For instance, a honeypot can impersonate a company's billing system that is a regular target of the attackers to find the credit/debit card details of the customers. Once the hackers attack on the system then their behaviour is recorded and moreover using[42] Artificial Intelligence and Machine learning the Network will automatically learn ways to provide more security and prevent the system to be hacked again.

Honeypots are made to attract the cybercriminals and to prevent the system from being attacked[43] i.e. Honeypot may have ports which responds to the weak passwords and such ports may be provided with open access so that to attract attackers from accessing into the honey pot environment, rather than a safe live network. Honeypots set up to the address specific problem. Moreover, it is an informative tool which can help in understanding threats.

B. *Types of Honeypots*

Depending upon the purpose and the extent of security which is needed as well as the type of choose the type of honeypot which are described below:

1) Email Traps: In Email Traps, an email is placed which contains a malicious email address or link. Once the user opens that link it will take it to an unseen location from where only the device that assigns the automated addresses, can find it. As these addresses will only be used for spam traps so it is confirmed that the mail will go into spam. The mails with the same content are returned to the spam trap and can be blocked automatically and the source IP is added to the blacklist.

2) Decoy Database: A decoy Database is established to screen software limitations and attacks destroying insecure network topology or injecting Structured Query Language or privilege abuse.

3) Malware Honeypot: A malware honeypot makes identical copies of applications and APIs to invite attacks. Malwares can be analysed to create anti-malware software or to shut down the weaknesses in the APIs.

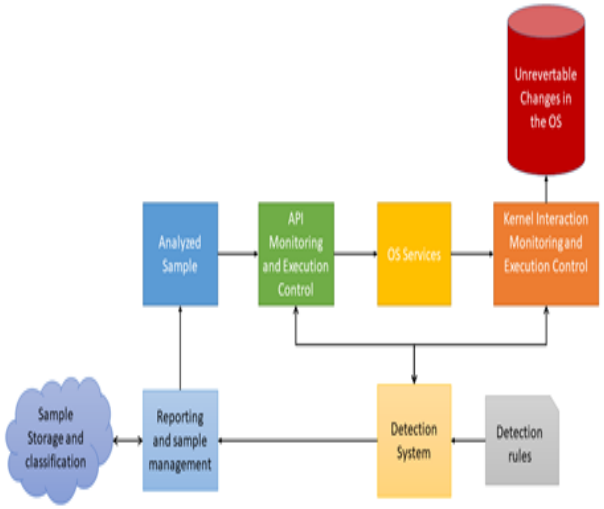

Fig. 8 Malware detection in honeypot [44]

4) Spider Honeypot: A spider honey pot is envisioned to trick the WebCrawler by creating links and web pages which are only available for WebCrawler. The process of getting Crawlers will help in preventing malicious bots to access the information.

By examining the traffic coming to the honey pot system, admin can access the level of the threat, from where the

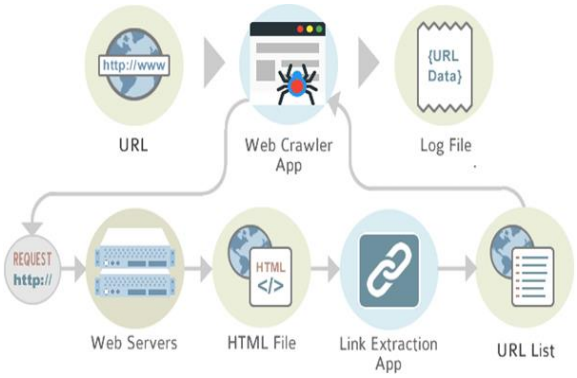

Fig. 9 Web Crawling [45]

cybercriminals are coming from? What is their method of operation? In which data or applications, [46] they are interested in and the most important thing up to what extent system is secure to prevent cyber-attack.

C. *Honeypot and IoT*

Several researchers have paid their significant contribution towards enhancing the technology in securing the devices as well as the networks by amending some changes in the traditional technology such as Deception Technology from which the honeypots were derived and now in this section the application of this fusion of traditional technology with the advanced new networks and end devices will be decided.

In [47] the authors have given emphasis on the problems which were faced during the attacks on honeypots in game-theoretical model of deception using a defender and an attacker. The attacker is managing to deceive the defending wall by deploying various kinds of attacks depending upon mild to severe activities. This behaviour makes honey pots as a tool of deception technology to fool hackers. Authors have utilised the Bayesian Networks to automatically learn the behaviour of the attacker.

In [48], Authors focus upon the mitigation of DoS attacks on IoT devices and tries to make them more secure and protected. Since, Honeypots are generally used in the online servers to decoy systems to prevent the attacks on the main server. In this paper, similar practices have been introduced to prevent the whole IoT system from shutting down due to a Denial of service attack.

Honeypot Internet of Things (IoT) (HIoTPOT) helps in secretly monitoring the IoT devices and analyzing the latest threats those are harmful for the IoT devices. In [49] the Research Honeypots are deployed which are intelligent enough to memorise the latest schemes and ethics used by hackers for attack over the IoT network. As a preventive measure, intruders were introduced to make HIoTPOT networks more secure and reliable. Several peripheral modules and sensors like zigbee module [50] can also be connected to the Honeypot networks as end-devices and once they are connected to honeypot of things (HoT). The zigbee modules will help the network to communicate with the admin once the attack is initiated by the hacker.

From the above research one gets a clear idea about how vast the domain of Honeypot and IoT technology has taken place in surrounding these days. This fusion of the two technologies plays a vital role in this modern society in making every online or offline communication more secure and reliable.

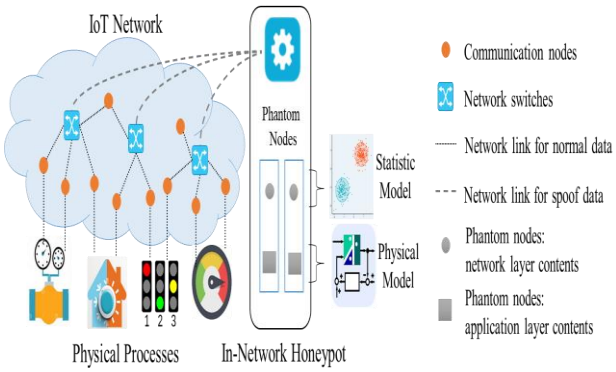

Fig. 10 HIoTPOT[51]

IV SECURITY IN IoT DEVICES

So far it is seen that the deception technology can be useful in securing networks and prevents end-devices from being attacked with any sort of malicious activities. Recently the world has stepped into the IoT era in which everything is not just digitalised but have also become smart to communicate with other machines and take decisions on their own. There are a lot of algorithms which are being used in order to make decisions more effectively for instance some machine learning algorithms such as Back-Propagation Algorithm[52], Bayesian Theorem[53], K Nearest Neighbour[54], etc.

These smart devices are generally enabled with a network of sensors that provides various functionalities to the device which can be a boon or bane to the user. Although these sensors are really helpful in performing tasks such as reading temperature, monitoring home and performing actions on commands such as google home or Amazon Alexa but on the other hand these devices can be very hazardous for us and useful for the cyber criminals as they can see whatever web camera is capturing, they can listen whatever microphone listens so security is in user's hand and manufactures should give equal emphasis to the modern technology and how secure this technology is.a

Since IoT is a very vast field to study as there are several different kinds of sensors available in the market these days and to study the insights of each sensor is really impractical due to which the challenges which are associated with securing the IoT devices and their network is really challenging.

Internet Technology is very wide spread these days. The count of the devices which are being connected to the internetwork is increasing with every passing day. Through recent advancements in technology and the technical drifts which are pervading across the globe and made IoT an essential need for the human race to survive in this world. However, it is not properly defined and reliable. IoT does not stick to a single protocol but has an open platform [55, 56,57] for everyone to see use and edit utilities according to their usage. The efficiency of the data management [58,59] can be enhanced by using the M2M interactions when everything surrounding us has become smart enough.

A lot of security challenges are there, which through the help of topologies and some new architectures can be utilised to make the backbone of the full-fledged IoT environment. Vivid and interesting challenges in the [65] security of the IoT are faced while taking out the data. Since one cannot say IoT is a fully developed environment and still the limitations and challenges are yet to be explored in respect to security. WSN and IP-based WSN are considered as the basic data collecting spots in the majority of the IoT systems. Attacks on these structures may cause some serious troubles [60]of data theft. If the nodes are used as the bait then the cybercriminal may be able to retrieve the information which is being sent to the higher level and can cause some serious problems after effect over the processing of the data. Destruction of the security vulnerabilities especially in sensor networks can lead towards DoS.

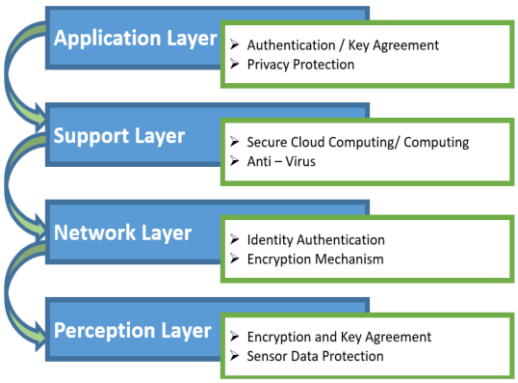

Fig.11 Multilayered structure of IOT

In Fig. 11 It is shown that the multilayered structure of the security over various TCP-IP model layers of the operating system. It is clear that at each layer, some security mechanisms which are handling the processes smoothly and preventing data to be breached easily. Just for the sake of providing more security to the above described security systems using previously discussed Deception Technology and its derivative Honeypot networks.

V. CONCLUSION AND FUTURE SCOPE

Now a days the use of technology is improving and enhancing with every passing day but along with the advanced technology, Some advanced methods were needed to keep protected. Hackers are getting advanced day by day. Here in This paper It is seen how traditional technology can be utilized in such a way that it creates a revolution in the technology and sets a bench mark in the market. Deception Technology is considered to be the oldest technology which is being used to provide security to the networks and devices but later on its derivatives were used to take best out of the fundamental technology such as Honeypots and Honeynets. This evolution helps in achieving various targets and removes the vulnerabilities which are caused while making IoT network strong with and without Deception Technology and its derivatives. In future this technology can also be utilized in establishing the 5G Technology. Since 5G is itself an emerging technology and hence can face some more challenges while becoming a trend in every country around the world. With the application of small cell and Device to Device connections, the usage of antennas, and the investigation of the less used millimeter Wave frequency spectrum, it is believed that the 5G network is well established to reach to the rising demand applications which are data centric in near future. With the emerging growth of 5G network that will definitely need the enhanced security, the novel solution will take the data confidentiality to the new heights.

REFERENCES

[1] C. C. Zou and R. Cunningham, "Honeypot-Aware Advanced Botnet Construction and Maintenance," International Conference on Dependable Systems and Networks (DSN'06), Philadelphia, PA, 2006, pp. 199-208, doi: 10.1109/DSN.2006.38.

[2] H. Project (2005). Know your enemy: Tracking botnets. http://www.honeynet.org/papers/bots/

[3] Guest Author (2017, Apr) , “How to identify a Mirai-Style DDos Attack” https://www.imperva.com/blog/how-to-identify-a-mirai-style-ddos-attack/

[4] K. Anagnostakis, S. Sidiroglou, P. Akritidis, K. Xinidis, E. Markatos, and A. Keromytis. Detecting targeted attacks using shadow honeypots. In Proceedings of 14th USENIX Security Symposium, August 2005.

[5] D. Dagon, X. Qin, G. Gu, W. Lee, J. Grizzard, J. Levin, and H. Owen. Honeystat: Local worm detection using honeypots. In Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID), 2004.

[6] X. Jiang and D. Xu. Collapsar: A vm-based architecture for network attack detention center. In Proceedings of 13th USENIX Security Symposium, August 2004.

[7] J. Levine, R. LaBella, H. Owen, D. Contis, and B. Culver. The use of honeynets to detect exploited systems across large enterprise networks. In Proceedings of IEEE Workshop on Information Assurance, June 2003.

[8] N. Provos. A virtual honeypot framework. In Proceedings of 13th USENIX Security Symposium, August 2004.

[9] M. Vrable, J. Ma, J. chen, D. Moore, E. Vandekieft, A. Snoeren, G. Voelker, and S. Savage. Scalability, fidelity and containment in the potemkin virtual honeyfarm. In Proceedings of the ACM Symposium on Operating System Principles (SOSP), October 2005.

[10] Stanlslav (2019, June) Creating and deploying honeypots in kubernetes https://www.apriorit.com/dev-blog/619-web-cybersecurity-honeypots-in-kubernetes

[11] Article “Deception Technology” , Forcepoint.com https://www.forcepoint.com/cyber-edu/deception-technology

[12] Article “Deception Technology-fooling the enemy” , Forcesite.com https://foresite.com/deception-technology-fooling-the-enemy

[13] Dave Kjendal (2018,June), “The modernization of iot networks” https://www.senetco.com/blog/the-modernization-of-iot-networks/

[14] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, Internet of Things: A survey on the security of IoT frameworks, Journal of Information Security and Applications, Volume 38, 2018, Pages 8-27, ISSN 2214-2126,

[15] Lin, H.: Attribution of malicious cyber incidents: from soup to nuts. J. Int. Aff. 70(1), 75–137 (2016)

[16] Rauti, S., Lepp¨anen, V.: A survey on fake entities as a method to detect and monitor malicious activity. In: 2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), pp. 386–390. IEEE (2017).

[17] Bejtlich, R.: The Practice of Network Security Monitoring: Understanding Incident Detection and Response. No Starch Press, San Francisco (2013)

[18] Karuna, P., Purohit, H., Ganesan, R., Jajodia, S.: Generating hard to comprehend fake documents for defensive cyber deception. IEEE Intell. Syst. 33(5), 16–25 (2018)

[19] Virvilis, N., Gritzalis, D.: The big four - what we did wrong in advanced persistent threat detection? In: 2013 International Conference on Availability, Reliability and Security, pp. 248–254 (2013)
[20] Al-Shaer, E., Wei, J., Hamlen, K.W., Wang, C.: Towards intelligent cyber deception systems. In: Al-Shaer, E., Wei, J., Hamlen, K., Wang, C. (eds.) Autonomous Cyber Deception, pp. 21–33. Springer, Cham
[21] Wang, C., Lu, Z.: Cyber deception: overview and the road ahead. IEEE Secur. Priv. 16(2), 80–85 (2018)
[22] Cohen, F., Koike, D.: Misleading attackers with deception. In: Proceedings from the Fifth Annual IEEE Information Assurance Workshop, pp. 30–37. IEEE (2004)
[23] Rauti S. (2021) Towards Cyber Attribution by Deception. In: Abraham A., Shandilya S., Garcia-Hernandez L., Varela M. (eds) Hybrid Intelligent Systems. HIS 2019. Advances in Intelligent Systems and Computing, vol 1179. Springer, Cham.
[24] Andrew Froehlich, "Data Breach" https://searchsecurity.techtarget.com/definition/data-breach?_ga=2.228851295.275768660.1604701000-594871215.1599086189
[25] Ben Lutkevich , "Intrusion Detection System" https://whatis.techtarget.com/definition/breach-detection-system-BDS
[26] Nathan Mercer, (2018, February) "Post breach detection with windows defender advanced threat protection" https://techcommunity.microsoft.com/t5/windows-blog-archive/post-breach-detection-with-windows-defender-advanced-threat/ba-p/166549
[27] Wasim Ahmad Bhat and S.M.K. Quadri. 2013. POSTER: Dr. Watson provides data for post-breach analysis. In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13). Association for Computing Machinery, New York, NY, USA, 1445–1448.
[28] Rajarshi Chakraborty, Jaeung Lee, Sharmistha Bagchi-Sen, Shambhu Upadhyaya, H. Raghav Rao, Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults, Decision Support Systems, Volume 83, 2016, Pages 47-56, ISSN 0167-9236,
[29] A. Yarali and F. G. Sahawneh, "Deception: Technologies and Strategy for Cybersecurity," 2019 IEEE International Conference on Smart Cloud (SmartCloud), Tokyo, Japan, 2019, pp. 110-120, doi: 10.1109/SmartCloud.2019.00029.
[30] Xiao Han, Nizar Kheir, and Davide Balzarotti. 2018. Deception Techniques in Computer Security: A Research Perspective. ACM Comput. Surv. 51, 4, Article 80 (September 2018), 36 pages.
[31] D. Weissman, "IoT Security Using Deception – Measuring Improved Risk Posture," 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2020, pp. 1-2, doi: 10.1109/WF-IoT48130.2020.9221223.
[32] Mohamad F. Razali et al., "IoT Honeypot: A Review from Researcher's Perspective," IEEE Conference on Applications, Information and Network Security (AINS), 2018.
[33] Quang Duy La et al., "Deceptive Attack and Defense Game in Honeypot-Enabled Networks for the Internet of Things," IEEE Internet of Things Journal, Vol 3, No. 6, December 2016
[34] Antara D. Oza et al., "Survey of Snaring Cyber Attacks on IoT Devices with Honeypots and Honeynets," 3rd International Conference for Convergence in Technology (I2CT), April 2018.
[35] Infosec Institute – "How To Protect Files With Canary Tokens," 2018.
[36] Jeremy Kirk,(2019 August) " Making the most of an investment in Deception Technology" https://www.bankinfosecurity.com/deception-technology-worth-investment-a-12881
[37] Kemi Ding, Xiaoqiang Ren, Daniel E. Quevedo, Subhrakanti Dey, Ling Shi, Defensive deception against reactive jamming attacks in remote state estimation, Automatica, Volume 113, 2020, 108680, SSN 0005-1098, B. Zhao, L. Huang and J. Zhang, "Single Channel SAR Deception Jamming Suppression via Dynamic Aperture Processing," in IEEE Sensors Journal, vol. 17, no. 13, pp. 4225-4230, 1 July1, 2017, doi: 10.1109/JSEN.2017.2695001.
[38] Burns, Bryan, Oskar Ibatullin, Oliver Tavakoli, Robert W. Cameron, and Daniel J. Quinlan. "Virtual honeypot." U.S. Patent Application 13/631,398, filed April 3, 2014.
[39] T. Holz and F. Raynal, "Detecting honeypots and other suspicious environments," Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop, West Point, NY, USA, 2005, pp. 29-36, doi: 10.1109/IAW.2005.1495930.
[40] Joshi, R. C., and Anjali Sardana, eds. Honeypots: a new paradigm to information security. CRC Press, 2011.Joshi, R. C., and Anjali Sardana, eds. Honeypots: a new paradigm to information security. CRC Press, 2011.
[41] Rodrigo , "Code a small web crawler" https://www.fiverr.com/rodrigo/code-a-small-web-crawler
[42] Q. D. La, T. Q. S. Quek and J. Lee, "A game theoretic model for enabling honeypots in IoT networks," 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, 2016, pp. 1-6, doi: 10.1109/ICC.2016.7510833.
[43] M. Anirudh, S. A. Thileeban and D. J. Nallathambi, "Use of honeypots for mitigating DoS attacks targeted on IoT networks," 2017 International Conference on
[44] Gandhi, U.D., Kumar, P.M., Varatharajan, R. et al. HIoTPOT: Surveillance on IoT Devices against Recent Threats. Wireless Pers Commun 103, 1179–1194 (2018).
[45] S. Dowling, M. Schukat and H. Melvin, "A ZigBee honeypot to assess IoT cyberattack behaviour," 2017 28th Irish Signals and Systems Conference (ISSC), Killarney, 2017, pp. 1-6, doi: 10.1109/ISSC.2017.7983603.
[46] Article " sdn based in network honeypot preemptively disrupt and mislead attacks in iot network" https://www.groundai.com/project/sdn-based-in-network-honeypot-preemptively-disrupt-and-mislead-attacks-in-iot-networks/1
[47] A. Van Ooyen, B. Nienhuis, Improving the convergence of the back-propagation algorithm, Neural Networks, Volume 5, Issue 3, 1992, Pages 465-471, ISSN 0893-6080,
[48] Friedman, N., Geiger, D. & Goldszmidt, M. Bayesian Network Classifiers. Machine Learning 29, 131–163 (1997).
[49] K. S. Ni and T. Q. Nguyen, "An Adaptable k -Nearest Neighbors Algorithm for MMSE Image Interpolation," in IEEE Transactions on Image Processing, vol. 18, no. 9, pp. 1976-1987, Sept. 2009, doi: 10.1109/TIP.2009.2023706.
[50] Ashton, K. (2009). That internet of things thing. RFiD Journal, 22(7), 97–114.
[51] Tewari, A., & Gupta, B. B. (2016). Cryptanalysis of a novel ultralightweight mutual authentication protocol for IoT devices using RFID tags. The Journal of
[52] Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2016). Secure integration of IoT and cloud computing. Future Generation Computer systems. doi:10.1016/j.future.2016.11.031.
[53] Odelu, V., Das, A. K., Khan, M. K., Choo, K. K. R., & Jo, M. (2017). Expressive CP-ABE scheme for mobile devices in IoT satisfying constant-size Keys and ciphertexts. IEEE Access, 5, 3273–3283.
[54] Kong, L., Khan, M. K., Wu, F., Chen, G., & Zeng, P. (2017). Millimeter-wave wireless communications for IoT-cloud supported autonomous vehicles: Overview, design, and challenges. IEEE Communications Magazine, 55(1), 62–68.
[55] Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. IEEE Communications Surveys & Tutorials, 8(2), 2–23.
[56] Mohammad Burhan et al. (2018, August), "IOT elements layered architectures and security issues: A comprehensive survey" https://www.mdpi.com/1424-8220/18/9/2796/htm
[57] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan and M. Di Renzo, "Safeguarding 5G wireless communication networks using physical layer security," in IEEE Communications Magazine, vol. 53, no. 4, pp. 20-27, April 2015,
[58] Resham Arya, "EEG Signals based Personality and Mood Recognition using Neural Network Approach" in Proceedings of 3rd International Conference on Intelligent Engineering and Management, ICIEM 2022