© 2019 IJSRST | Volume 6 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : https://doi.org/10.32628/IJSRST196215

Analysis Report on Attacks and Defence Modeling Approach to Cyber Security

Dr. Bechoo Lal[1], Dr. Chandrahauns R Chavan[2]
[1]Assistant Professor, Department of Information Technology, Western College, University of Mumbai, Maharashtra, India
[2]Professor and Former Director, JBIMS, University of Mumbai, Mumbai, Maharashtra, India

ABSTRACT

The researcher stated that critical analysis on attacks and defense modeling approach to cyber security which is one of the significant research issues in the computing environment. The researcher focused on some of the factors such as control the side of damage, perform forensic analysis, executive standard counter measures, perform threat detection and hunting, and gather threat intelligence. These all are the defense parameters which are stated to modeling approach in cyber security. During the research the researcher evaluated the security parameters including password strength, fraud detection system, firewall and others security parameters which are significant with respect to cyber attach and environment. The researcher shown statistical report on industries impacted by cyber-attacks worldwide as of September 2017. The researcher stated that passwords are basic cyber-security tool that people encounter nearly every day to prevent valuable data and highly sensitive information from unauthorized persons. The researcher represented an attack and defense modeling approach with the help of cyber security attributes such as information security, network security, operational security, end-user protection and application security. The researcher also stated that a case study of the 2016 Korean cyber command compromise: the victim of a prospering cyber-attack that allowed access to internal networks. Per usual with massive scale attacks against South Korean entities, the hack was straight off attributed to DPRK. Case study-2: cyber warfare conflict analysis and case studies, to analysis historical cyber warfare incidents from the past to the current and capture relevant information in a very information acquisition section.

Keywords : NIST, IS, CIS, MIA, CYBER ATTACK, DEFENSE

I. INTRODUCTION

Cyber security is that the protection of internet-connected systems, beside hardware, code and data, from cyber-attacks. In associate extremely computing context, security includes cyber security and physical security -- every are used by enterprises to safeguard against unauthorized access to info centres and various computerised systems. data security, the researcher declared that cyber security is one in all the various analysis issues in current computing environments, that's meant to require care of the confidentiality, integrity and availableness of data, could also be a group of cyber security [1].

One of the foremost problematic elements of cyber security is that the constantly evolving nature of security risks. the traditional approach has been to focus resources on crucial system elements and defend against the biggest noted threats, and to

safeguard system from the external linear unitvironments that are creating problems among the computing nut which meant exploit elements open and not protecting systems against less dangerous risks[1][2].

The researcher conferred analysis problems and analysis issues among the computing environments, to pander to this environments, consulted organizations are promoting loads of proactive and adaptation approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated tips in its risk assessment framework that advocate a shift toward continuous observation and amount assessments [3]. The process of maintaining with new technologies, security trends and threat intelligence could also be a tough task among the computing environments. However, it's necessary thus on safeguard data and system security and various assets from cyber threats that take many forms [4].

1. Ransom ware could also be a method of malware that involves academic degree bad person lockup the victim's system files -- typically through cryptography and exigent a payment to rewrite and unlock them.
2. Malware is any file or program won't to harm a somebody, like worms, portable computer viruses, Trojan horses and spyware.
3. Social engineering is academic degree attack that depends on human interaction to trick users into breaking security procedures thus on succeed sensitive data that is typically protected.
4. Phishing could also be a range of fraud where dishonest emails are sent that match emails from reputable sources; however, the intention of these emails is to steal sensitive info, like MasterCard or login data.

The researcher focused on the analysis issues and necessary impact on use of cyber security can facilitate stop cyber-attacks, info breaches and fraud and should aid in risk management. Once an organization includes a sturdy sense of network security and a decent incident response prepare, it's higher able to stop and mitigate these attacks with connection computing environments. Cyber security refers to preventative ways that won't to defend data from being taken, compromised or attacked. It wants academic degree understanding of potential data threats, like viruses and various malicious code [5].

II. LITERATURE REVIEW

The research focused on "disruption of electrical power operations is ruinous on national security and jointly the economy. Will quality of wide unfold assets and jointly the interdependences among laptop computer, communication, and power infrastructures, the necessity to satisfy security and quality compliance on operations might even be a troublesome issue"(Chee-Woo 10 et. al (2010)).

The research emphasized that "the communication networks linking the massive sources of unfold all over the earth and data college field of study consultants area unit troubled to vogue the high performance hardware and coding system package that might cater the wants of today's' hi college corporations. The potential threat to secure monumental volume of data with a varied community of cyber criminals might even be a challenge within the current digital era"(Atul Bamrara et.,al(2013))

The researcher stated that "cyber-attack techniques area unit perpetually evolving and creating use of lessons learned over time. To stay pace with attackers and defend essential info systems in our ever additional connected world, defense mechanisms have to be compelled to additionally become additional refined. Usually understanding attack

techniques additional clearly is that the start toward increasing security. Intrusion detection systems (IDS) area unit around for form of years to warn of cyber strikes, however the suggests that they presently analyze data offers a restricted browse of cyber-attack activity" (Eric Goetz entail (2002)).

The researcher emphasized that "the success of a business mission is very obsessional concerning the Communications and information Systems (CIS) that support the mission. Mission Impact Assessment (MIA) seeks to help the combo of business or military operations with cyber defense, significantly in bridging the psychological feature gap between operational decision-makers and cyber defenders" Alexander Kott et. Al (2018)).

The researcher focused on " nuclear weapons systems were initial developed at a time once laptop computer capabilities were in their infancy and small thought was given to potential malicious cyber vulnerabilities. Several of the assumptions on that current nuclear ways that area unit based mostly pre-date this widespread use of digital technology in nuclear command, management and communication systems"(Beyza Unal and Patricia Lewis (2018)).

The researcher focused on " cyber-attack might even be a sensitive issue within the earth of web security. Governments and business organizations round the world area unit providing monumental effort to secure their data. Understanding attack models give additional insight into network vulnerability; that successively is employed to defend the network from future attacks. Within the cyber security world, it's difficult to predict a possible attack whereas not understanding the vulnerability of the network"(Hamad AL-Mahanadi (2016)).

The researcher focused on "the opportunities provided by the data and technology, with a special stress on the net, became associate integral a component of life. However, area unit we tend to tend to tend to sufficiently aware and ready as people, nations or the international community for the threats coming back from web or for the denial of the utilization of that dimension of communication, commerce and even warfare? Specifically, despite the growing reasonably users, the net continues to air the most side or below minimum regulation"(Duic et. al (2017)).

The researcher emphasized on " a part of Chatham House's Project on Cyber Security and area Security, a multiyear scientific research among the International section examining the protection challenges at the intersection of cyber security and area security, drawn from assume tanks, domain and business, launched into their views on their country's cyber security and area security policies"(Caroline metropolis (2014)).

The researcher focused on "the augmented dependency on the net, cyber-attacks area unit quick turning into an exquisite various for state adversaries, part thanks to the advantage of activity a perpetrator's identity. In response, governments round the world area unit taking measures to boost their national cyber defenses. However, these defenses, that area unit usually passive in nature, area unit deficient to handle the threats"(Tiong Pern Wong (2011)). It is also focused on "technology continues to evolve so else do the opportunities and challenges it provides. It tends to maneuver from a society already entwined with the net to the approaching age of automation, Big Data, and jointly the net of Things (IoT). Attack vectors like botnets, autonomous cars and ransom ware. Threats at the side of info manipulation, establish stealing, and cyber warfare. Tangential problems like info sovereignty, digital trails, and leverage technology talent"(Clive James (2016)).

The researcher emphasized that " non-public business encompasses a very important impact on economic and national security and governments should own a stake in protective essential personal infrastructure as a results of it will with totally different government assets. As nations push to spice up their cyber capabilities the flexibility of state to incentivize the personal sector to share info in an especially timely manner can greatly impact the effectiveness of cyber security management"(Bryan Watkins (2014)).

The researcher focused on a " robust U.S.A. cyber deterrence strategy can have the foremost immediate result on nation-states whose actions area unit influenced by U.S.A. instruments of national power. However, nations like D.P.R.K. And Persia have shown associate out of this world resistance to U.S.A. political and economic pressure and will be powerful to discourage whereas not credible threats of military actions.it ought to else pursue the simplest way to discourage common hackers, criminals, violent no state actors, and totally different non-nation-state actors"(Timothy M. McKenzie (2018)).

The researcher emphasize that almost all of the " cyber security analysis specialize in either presenting a specific vulnerability or proposing a specific defense formula to defend against a well-defined attack theme. To analysis the interactions between the bad person and jointly the defender as a non-cooperative security game. The key came upon is to model attackers/defenders to possess multiple levels of attack/defense ways in which area unit completely utterly totally different in terms of effectiveness, strategy prices, and attack"(Afraa Attiah et. al (2018)).

The researcher focused on " cyber warfare might even be a Brobdingnagian one, with various sub topics receiving attention from the analysis community. The researcher tend to first examine the foremost basic question of what cyber warfare is, scrutiny existing definitions to find footing or disagreements. The terms cyber war and cyber warfare don't seem to be tolerably differentiated. To handle these problems, we tend to tend to tend to gift a definition model to assist define each cyber warfare and cyber war"(Michael Robinson et.al (2015)).

The researcher focused on " the conventional network defense tools like intrusion detection systems and anti-virus specialize in the vulnerability element of risk, and ancient incident response methodology presupposes a no-hit intrusion. Associate evolution at intervals the goals and class of network intrusions has rendered these approaches insufficient sure actors. A clean category of threats, befittingly dubbed the "Advanced Persistent Threat" (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting sensitive economic, proprietary, or national security info"(Eric M. parliamentarian Maynard educator et. al (2005)). The research also focused on "laptop computer security has evolved from a technical discipline to a strategic conception. The world's growing dependence on a strong however vulnerable web – combined with the turbulent capabilities of cyber attackers – presently threatens national and international security. Strategic challenges wish strategic solutions. The researcher examines four nation-state approaches to cyber-attack mitigation"(Cm Kenneth Geers (2011)).

The researcher focused on "Defense, cyber resiliency ought to be incorporated across the entire capability lifecycle, and conjointly the associated policy development needs to be cognizant of this holistic would really like. The specification of cyber-resiliency requirements needs to be improved, additional importance needs to be placed on cyber security at intervals the look and magnificence phases, to realize this, a spanking new Defense organization

has been planned and its broad responsibilities created public"(Stuart Fowler (2018)).

III. PROBLEM STATEMENT AND RESEARCH OBJECTIVES

The researcher stated the some of the significant research issues in cyber security with respect to attacks and defense modeling approach.

1. To study the significant factors of cyber-attack.
2. To study the defense factors which are capable to protect cyber- attack in computing environment.

To study the current research issues on Industries and cases impacted by cyber-attacks worldwide.

IV. Attack and Defense Modeling Approach

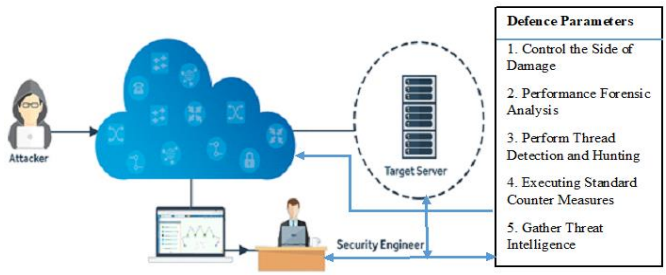

Fig 1. Adapted- Attack and Defense Modeling Approach

The researcher developed a framework of the analysis study to " identify the cyber-attack and defense modeling approach. It constitutes a fairly trade-off in terms of readability, modeling power, quality and quantification capabilities. This paper develops associated completes the theoretical foundations of such

Cyber security adaptation and presents new developments on defensive aspects. Notably, detection associated reaction modeling are fully integrated in cyber security enhanced theoretical framework. Fully completely different use-cases and quantification examples illustrate the connectedness of the final approach"(Kotenko and V. Skormin (2010)).

V. METHODS AND MATERIAL

This research study is based on the secondary data which are collected from the different sources and current research articles and the researcher emphasized on some of the significant research issues with respect to attack and defense modeling approach in cyber security. The researcher used the statistical tools to represents the Cyber-attacks on industries worldwide with multiple factors in tabular and pictorial representation. With the help of secondary data the research identify the attack and defense modelling approach of a standardized strategy document with such complicated needs ought to be supported a way which will assure consistency of the results obtained through the varied development phases and numerous stakeholders that require to participate within the strategy development method. Exploitation such technique for a method development ought to additionally afford a lot of easier thanks to sporadically update or revise the strategy with relevancy cyber-attack and defense.

VI. CASE STUDY

CASE STUDY-1: A CASE STUDY OF THE 2016 KOREAN CYBER COMMAND COMPROMISE

On Gregorian calendar month 2016 the South Korean cyber unit was the victim of a successful cyber-attack that allowed access to internal networks. " Per usual with huge scale attacks against South Korean entities, the hack was in real time attributed to Democratic People's Republic of Korea. Also, per completely different large-scale cyber security incidents, the identical kinds of 'evidence' were used for attribution functions. Disclosed ways in which of attribution provide weak proof, and so the procedure Korean

organizations tend to use for information revealing lead many to question any conclusions. The man of science analyzed and mentioned form of issues with this suggests that South Korean organizations disclose cyber-attack data to the overall public. A time line of events and disclosures area unit aiming to be created and analyzed at intervals the context of acceptable measures for cyber warfare. Finally, the man of science examined the South Korean cyber military attack in terms previously planned cyber warfare response tips. Specifically, whether or not or not any of the foundations is applied to the present real-world case, and if so, is Asian nation even in declaring war supported the foremost recent cyber-attack" (Kotenko and V. Skormin (2010)).

One issue that has to be mentioned specific to " South Korea's situation with Democratic People's Republic of Korea, is that applying law of states itself could also be problematic. Democratic People's Republic of Korea could also be a state with restricted recognition; Asian nation considers Democratic People's Republic of Korea to be an element of the identical nation and therefore the alternative method around (Scoffed, 2005). Therefore, in theory, got to associate offensive cyber operation be verified to be North Korea's doing, they could form up Korean code. However, very makes a shot to push South Korea's code to Democratic People's Republic of Korea would heaps have in all probability be harmful. Potential solutions and responses got to be found among international law; even in cases whereas not physical damages"(Aleksandar KLAIC (2018)).

CASE STUDY-2: CYBER WARFARE CONFLICT ANALYSIS AND CASE STUDIES

The first objective was to analysis historical cyber warfare incidents from the past to the present and capture relevant data in an exceedingly} very data acquisition section. the first section needed to analysis the timeline of events throughout this incident and develop the specified insight to be ready to analyze the parties involved thus on mark them as established order side or non-status-quo side. This provided a signal of motive from the no status-quo side and so the progression of change of magnitude. The second objective involved mapping the cyber-warfare incidents to MIT's CASCON framework. The CASCON mapping given {the data the knowledge the data} collected from the incidents in an exceedingly} very structured kind that's very important since its information of kinetic warfare was intensive [20].

The CASCON based totally analysis for cyber-incidents not only discovered insights into what actually happened throughout a cyber-incident, but helped answer key queries that may in all probability cowl some fateful behavior of involved states and conflicts in an exceedingly} very region. There's on the far side associate doubt an outsized amount of data that is to be learned and regarded, every from the historical purpose of scan that CASCON provides and from current affairs. The results of this thesis are not meant to be conclusive, but a study of state-sponsored cyber- cases exploitation MIT's CASCON to map and reason data for future learning regarding conflicts involving states [20]. The man of science found that variety of the next facts:

1. Reduced costs compared to plain strikes.
2. Higher efficiency in achieving the goal.
3. The uneven nature of the cyber-attacks makes defense powerful.
4. The anonymous nature of the offense permits the offensive government to bypass approval by the world community compared with a military offensive.
5. Probability to conduct cyber-attacks in amount for immediate government ends, nevertheless on steel oneself against accomplishable future kinetic attacks.

6. Chance to conduct cyber-attacks in period for immediate government ends, yet on steel oneself against doable future kinetic attacks.

VII. STATISTICS OF CYBER ATTACKS

Table 1 : Cyber-attacks on industries worldwide 2017		
Industries impacted by cyber-attacks worldwide as of September 2017		
	Share of respondents	
Energy	26	in %
Healthcare	25	in %
Retail and wholesale	25	in %
Manufacturing	22	in %
Infrastructure	19	in %
Financial institutions	17	in %
Automotive	15	in %
Professional services	15	in %
Power and utilities	14	in %
Martine	14	in %
Communications, media and technology	13	in %
Aviation and aerospace	9	in %

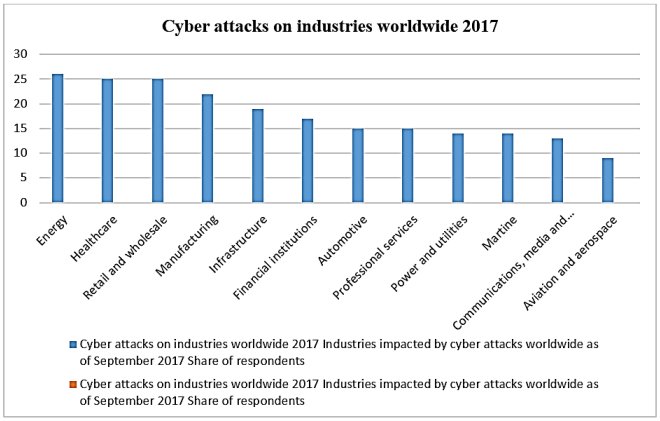

Fig 2. Cyber-attacks on industries worldwide 2017

VIII. RESULTS AND DISCUSSION

Cyber-attacks unit of measurement an unbroken threat to businesses around the world with immense sums of money being spent to protect against them. The image of some wicked character plotting in his or her sleeping room is one most folk have once puzzling over hackers and cyber criminals. Whereas in 2015, 40 the look after attacks stemmed from 'outsiders', a shocking hour were extremely perpetrated by company insiders. IBM, World Health Organization created the figures supported knowledge from over 8,000 of their purchasers devices, disclosed that the' 5.5 you look after such 'attacks' were caused unwittingly, 44.5 there have been deemed to possess been malicious.

An executive is made public as anyone World Health Organization has physical or remote access to a company's assets. IBM note that the' this can be ready to usually be Associate in Technical employee, it can also mean business partners or maintenance contractors – people you trust enough to grant system access to. Insiders not entirely have this access, they're going to even be responsive to your weaknesses and then exploit those tons of effectively than an out of doors agent will be able to.

IX. CONCLUSION

In this research paper the researcher focused on the significant research issues on attack and defense modeling approach to cyber security in computing environment. The researcher proposed a modeling approach to spot and therefore the causes of cyber-attack and providing a virtual primarily based answer that are having restricted access and value within the computing environments. The researcher additionally expressed this statistical analysis problems with cyber- attack and defense in different Industries. Through the modelling construct, the researcher planned a model to stop cyber-attack and

defense to stop the cyber-attack services within the computing environments. The researcher also analyzed and mentioned variety of problems with this means that South Korean organizations disclose cyber-attack info to the general public. A time line of events and disclosures are going to be created and analyzed within the context of acceptable measures for cyber warfare. In another cases cyber warfare incidents from the past to the current and capture relevant information in a very information acquisition section from the incidents in a very structured kind that is vital since its information of kinetic warfare were more intensive.

X. REFERENCES

[1]. Chee-Woo 10 et. al (2010),' Cyber security for vital Infrastructures: Attack and Defense Modeling', revealed in: IEEE Transactions on Systems, Man, and information science - half A: Systems and Humans (Volume: 40, Issue: 4, July 2010), Page(s): 853 - 865.

[2]. Atul Bamrara et. al (2013),' Cyber Attacks and Defense methods in India: Associate in Nursing Empirical Assessment of Banking Sector', International Journal of Cyber sociology Vol.7 Issue.1 January - Gregorian calendar month 2013.

[3]. Eric Goetz et.,al(2002),' Cyber Attack Techniques And Defense Mechanisms', fact-finding analysis for Infrastructure Assurance (IRIA) cluster - Institute for Security Technology Studies, June-2002.

[4]. Alexander Kott et.al (2018),' Approaches to Modelling the Impact of Cyber Attacks on a Mission' USA work, USA, 2018.

[5]. Beyza Unal and Patricia Lewis (2018),' Cyber security of Nuclear Weapons Systems Threats, Vulnerabilities and Consequences', International department, January 2018.

[6]. Hamad AL-Mahanadi (2016),' Cyber-Attack Modeling Associate in Nursingalysis Techniques: An Overview', 2016 fourth International Conference on Future net of Things and Cloud Workshops, 978-1-5090-3946-3/16, 2016 IEEE Interior Department ten.1109/W-FiCloud.2016.29.

[7]. Duic et.,al(2017),' International cyber security challenges', MIPRO 2017/ISS, University of Applied Sciences Vern, Zagreb, Croatia,2017.

[8]. King of Great Britain Baylon (2014),' Challenges at the Intersection of Cyber Security and area Security Country and International establishment Perspectives', International Security, December 2014.

[9]. Baron Clive of Plassey James (2016),' Cyber security Threats Challenges Opportunities', ACS, November-2016.

[10]. Bryan Watkins (2014),' the Impact of Cyber Attacks on the non-public Sector', Association for world affairs, August-2014.

[11]. Timothy M. McKenzie (2018),' Is Cyber Deterrence Possible?' Air University Press Air Force analysis Institute Maxwell Air Force Base, Alabama, 2018.

[12]. Afraa Attiah et.al (2018),' A Game metaphysical Approach to Model Cyber Attack and Defense Strategies', school of Engineering and engineering, University of Central FL, Florida, USA.

[13]. Archangel Robinson et. al (2015),' Cyber Warfare: problems and Challenges', Article in Computers & Security, March 2015.

[14]. Eric M. pedagogue et.,al(2005),' Intelligence-Driven electronic network Defense sophisticated by Analysis of mortal Campaigns and Intrusion Kill Chain', U.K. National Infrastructure Security Co-ordination Centre (UK-NISCC) and therefore the U.S., July -2005.

[15]. Kenneth Geers (2011),' Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation methods with Dematel', capital University of Technology school of data Technology Department of information

science, treatise was accepted for the defense of the degree of Doctor of Philosophy in information science on might six, 2011.

[16]. Stuart Fowler (2018),' Developing cyber-security policies that penetrate Australian defense acquisitions', Australian military Journal, 2018.

[17]. Joshua I. James(2016),' A Case Study of the 2016 Korean Cyber Command Compromise', Legal information science and rhetorical Science Institute, Hallym University, Chuncheon, Republic of Korea.

[18]. Mohan B. Gazula(2017),' Cyber Warfare Conflict Analysis and Case Studies', Cyber security knowledge base Systems Laboratory (CISL),Sloan faculty of Management, area E62-422 Massachusetts Institute of Technology, Cambridge, MA 02142.

[19]. Kotenko and V. Skormin (2010), 'Attack and Defense Modeling with BDMP', MMM-ACNS 2010, LNCS 6258, pp. 86-101, 2010. C Springer-Verlag Berlin Heidelberg 2010.

[20]. Aleksandar KLAIC (2018),' a way for the event of Cyber Security Strategies', workplace of the National SC, Croatia.

Cite this article as :

Dr. Bechoo Lal, Dr. Chandrahauns R Chavan, "Analysis Report on Attacks and Defence Modeling Approach to Cyber Security ", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 2, pp. 52-60, March-April 2019. Available at doi :
https://doi.org/10.32628/IJSRST196215
Journal URL : http://ijsrst.com/IJSRST196215