A DETAILED STUDY ON CYBER SECURITY FRAMEWORKS

[1]Ms.P ALEKHYA, [2]Ms.G LAXMISAI, [3]Mr .D. REDHIMA, [4]Ms.G BHARGAVI
Department of Computer Science and Engineering
Balaji Institute of Technology and Science, Narsampet, Warangal, Telangana, India.

ABSTRACT:
Cyber Security is mainly used for the security purpose, where later it is considered as the human role for the security process and other formers are considering this as an extra measure. However, cyber security is mainly focusing on the moral part of the society. For addressing the issue of cyber security, we are developing various frameworks and models. And cyber security is also introducing some concepts in terms of its framework, workforces and also protecting personal information in the computer.

Keywords: Indulgent, quest, unauthorized, nascent cankers

1. INTRODUCTION:

We are having various definitions for the concept of cyber security with different aspects such as secured sharing, confidential sharing and providing access to the information. But still, some of the definitions lacks clearness and unity. Moreover, cyber security is definitely measured with respect to the accessing of the data, integration of data, shared security, storage and transfer of data through electronic modes[1][2]. Cyber security introduces 3 major factors. Cyber security is having a measure protecting computer systems, networks, and information disruption or unauthorized access[3][5]

Fig1: Areas of cyber security issues reviewed in this paper or destruction.

This paper mainly focuses the issues of summarizes the existing security models and cyber security threats [4][6]. Fig. 1 represents the main areas reviewed in this paper, which include cyber security personnel, vulnerability scanning, email virus filtering, personal information protection, and firewall services. The significance of this paper are assisting both academics and professionals gain a holistic view about contemporary cyber security field. The main purpose of this paper having two aspects:

1) This paper summarizes critical issues in cyber security domains by a literature review.
2) This paper offers a number of research directions for future research in the field. The remainder of this paper is organized by taking some reviews and organizes crucial issues in cyber security [6].

2. CRUCIAL ISSUES IN CYBER SECURITY:

Many efforts have been made for finding the solution for cyber security problems and different frameworks have been introduced. These frameworks faced different situations even it was working outstanding initially at the time of development. The limitations deduct from different content, such as future technologies and utility limitations. Security problems are often taken an deal between security demands and other benefits [6][7].

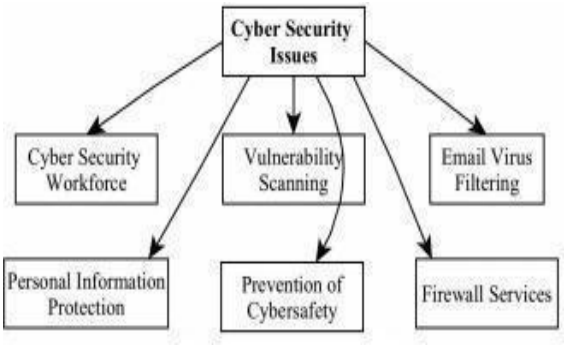

Fig2: Viewpoints of cyber security issues

A. Cyber security workforce:

The framework of National Initiative for Cyber security Education (NICE) is an inter- agency Endeavour by the National Institute of Standards and Technology (NIST). The agency focuses on awareness, cyber security Education, training and professional development. NICE came up with the Cyber security Workforce simulation. This framework implore on recognition by the process of training. Also, accomplishes secure cyber infrastructure as defined in the environment and the framework has not been added the factor that new technologies are rapidly nascent that improved the challenges in cyber security threats. The scholars also mentioned that there is need to be enough cyber security controls and procedures, which need to be oftentimes reviewed [7][8]. The researchers further indicated some of the possibility that had not added the substance of threats that utilize dangerous. Hence strategies of risk management needs to be addressed. Also, the authors provide that cybercrime civil law is not in place to handle the criminals. Finally, an effective security strategy can be active in cooperation with modeling business processes.

B. Cyber safety for authenticating personal data incomputer:

Cyber-safety is a concept that has been used to explain a set of measures, practices, and actions that help in the protection of computer and privacy from various operations. In any company, there is a Cyber-safety Program policy, PPM 310-22, which provides the devices attached to any company where electronic communications network must meet definite security standards. As required by the system, most departments offer final reports defining their levels of the observance. And also, different services are in place to teach all faculty, staff and students to meet the cyber safety standards. Specific information about these services is provided [8][9]. The cyber safety problems can be caused due to viruses, hackers, finding thieves, spyware. The virus cankers the computer through the email attachment and file sharing. One cankered computer can cause problems to all the Computer networks. A people who “trespass” the computer from a remote location are taken as Hackers. These people use a computer to send email or viruses or do other activities that cause computer malfunction. In the case of finding thieves, the people who have unauthorized access to the personal data like social security, and financial account numbers are taken. Spyware is software that “piggybacks” on programs that are downloaded and gathers data about online habits and transfers personal data without the user’s brain. In addition to the above-discussed threat, a company may face a number of other phenomenon’s if they fail to take actions to authorize personal data and user’s computer. The phenomenon indulgent such as loss in the access of campus computer network, confidential data, integration and access to data, research on personal electronic data lawsuits, loss of public trust and loss of opportunities, quest, internal conflict action and or employment termination.

C. Studies of email virus filtering:

Several studies have been conducted on the filtering of email virus and Prior study had addressed that various existing spam detection methods, precise, and dependable spam detection process had introduced. The applications that currently applied by various anti-spam software are considered to be static, which mean that it is quite easy to elude by tweaking the messages. For performing, the spammer we would evaluate the current anti-spam methods and regulate the modes to play around. To encounter the spam effectively, it is important to adopt a new technique [9][10]. This new approach needs to be complete the spammer’s strategies as they are changing from time to time. It must able to adapt the particular organization that it is protecting for the answer which lies in Bayesian mathematics. The study findings indicated that some of the spam detection methods and also numerous issues associated with the spam. From various studies, it is understood that we will not be able to stop the spam and will be done effectively using Bayesian method when compared to other methods. Moreover, Research also explored various problems associated with spam and spam filtering methods. Some of the different spam method are Bayesian analysis, Blacklist/White list, and also Mail header analysis. The different spam filtering techniques adopted Distributed adaptive blacklists, Rule-based filtering,Bayesianclassifier,

K-nearest neighbors, Support Vector Machine (SVM), Content based Spam Filtering Techniques - Neural Networks, The multi-layer networks, Technique of search engines, Technique of genetic engineering, Technique of artificial immune system. Moreover, prior research also explored various problems associated with spam and spam filtering methods. These methods determine the incoming spam methods are Bayesian analysis, Blacklist/White list and also Mail header analysis. The different spam filtering techniques adopted Distributed adaptive blacklists, Rule-based filtering, Bayesian classifier, K-nearest neighbors, Support Vector Machine (SVM), Content-based Spam Filtering Techniques - Neural Networks, The multi-layer networks, Technique of search engines, Technique of genetic engineering, Technique of artificial immune system. The study findings disclosed that several of the filtering techniques are based on text categorization methods, and there is no technique will claim to supply a perfect resolution with 0% false positive and 0% false negative. There are a lot of analysis opportunities to classify transmission and text messages. Kumar et al. indicated that the spam data set is examined with the employment of TANAGRA data processing tool that determine the efficient classifier in the classification of email spam. Firstly, feature choice and have construction is conducted to get the specified characteristics. After that different classification algorithms would be Applied to the data set and a cross- validation would be done on every classifier. In the end, the most effective classifier in email spam is determined on the aspects of preciseness, error rate and recall. From the obtained results, fisher filtering, runs filtering feature choice algorithms perform higher classification for several classifiers. The Rnd tree classification algorithm applied to relevant options when fisher filtering has made more than 99% accuracy for spam detection. This Rnd classifier is additionally checked with test data set which supplies correct results than other classifiers for this spam data set.

D. Studies of firewall service:

Al-Fayyad et al.evaluated the performance of personal firewall systems by organizing an arranged walk through to see the planning factors that might violate the usage standards. In the study of private firewalls usability on Windows XP platform four trendy firewalls particularly Norton 360 V.2.0.0.242, Trend small web Security Version sixteen.00.1412, Zone AlarmV.7.1.248 and ESETNod32 Smart Security. The study results indicated that non-public firewalls encounter poor usability that might result in vulnerabilities in security. The usability problems could be due to the difficulty that the information given by the firewalls (could be throughout the method of putting in, configuration or during interaction) was not clear or misleading. Various usability problems are noticed thanks to the reduced clarity of alerts. Li evaluated the problems in inserting the firewalls within the topology of networking style and the way to border the routing tables within the method in order that a Maximized firewall rule set could be negligible that helps to avoid performance bottleneck and limits the security loopholes. There have been two significant contributions that the problems are NP- complete, and that a heuristic resolution has been projected and illustrate the efficiency of algorithms using simulations. The outcome of the check indicates that the advised algorithmic program has restricted the multi-firewall rule set than other algorithms[10][11].

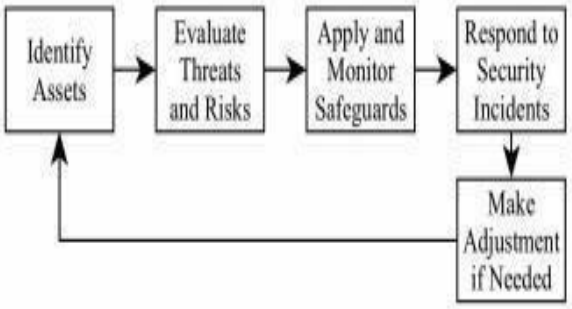

Fig. 3: General operation flow of cyber safety prevention

E. Studies of vulnerability scanning:

SudhaRanietal. Analyzed Intrusion Detection System (IDS) methods to identify an attack of a computer network. In order to prevent vulnerable virtual machines network, intrusion detection system is proposed. In addition, the study has taken potential security risks also because the security considerations taken into account for implementing a virtual private network [11][12].

F. Prevention of Cyber safety:

There are six significant cyber-safety actions they are Running Anti-virus Software, Installing OS/Software Updates, Preventing Identity Theft, Switch on the Personal Firewalls, protection of Passwords and Backing up Important Files [12].

3. DISCUSSIONS:

From the review it had been determined that, there are various studies conducted on cyber safety especially earlier studies have tried to aim the issues connected to spam and spam filtering techniques. In specific, spam dataset is analyzed victimization TANAGRA data processing tool to explore the efficient classifier for email spam classification. Further studies also analyzed various existing spam detection methods and identified an efficient, accurate, and reliable spam detection method .The usage of personal firewall systems by performing a cognitive analysis in deciding style components which might violate the principles of usability. The issue of how to prepare the topology of firewalls in a very network style and how the frame the routing tables in execution so the max firewall rule set may be restricted. Attribute-based solutions are often associate choice for specific security needs. The usage of Intrusion Detection System (IDS) procedure to seek out a network attack. The vulnerability assessment in automatic setups together with web applications and different threats, such as data validations. A Creative quantitative vulnerability assessment model on cyber security for DAS is evaluated. Further the analysis indicated varied safety and interference functionalities.

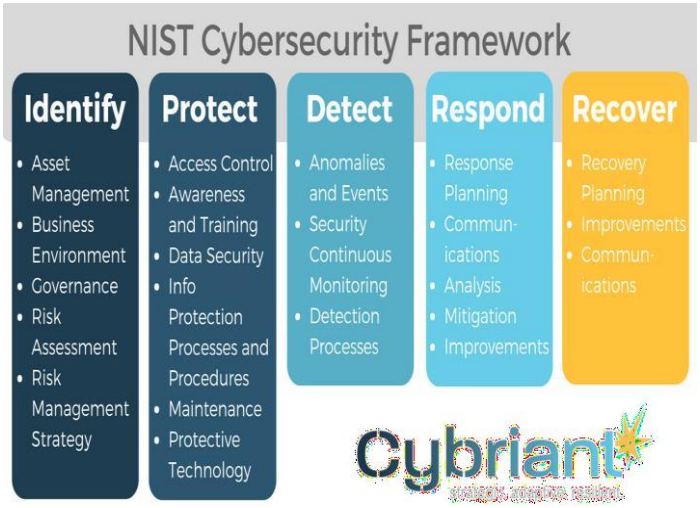

Fig 4: Cyber security Frameworks

4. CONCLUSIONS:

From the review, it had been found that majority of the studies have been conducted on the e-mail security, firewalls, and vulnerabilities. Yet, not several studies from the angle of countersign security. There are general recommendations on the way to secure the positive identification however not any protocol to protect the system inherently. Therefore, there is a would like for a lot of studies in terms of techniques and models from this angle to make sure that passwords are protected.

5. REFERENCES:

[1] Manikandan, v., v. Porkodi, aminsalihmohammed, and m. Sivaram. "Privacy Preserving Data Mining Using Threshold Based Fuzzy Cmeans Clustering." ICTACT Journal on Soft Computing 9, no. 1 (2018).

[2] D.Yuvaraj,D., & Balaji, S.(2018). Smart Junkyard Using Iot. International Journal of Pure and Applied Mathematics, V118, No.22,P 1103-1108.

[3] Ahamed, B. B., & Hariharan, S. (2012). Implementation of Network Level Security Process through Stepping Stones by Watermarking Methodology. International Journal of Future Generation Communication and Networking, 5(4), 123-130.

[4] M. Gallaher, A. Link, and B. Rowe. Cyber Security: Economic Strategies and Public Policy Alternatives. Edward Elgar Publishing, 2008.

[5] F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber- physical systems. IEEE Transactions on automatic control

[6] Y. Yan, Y. Qian, H. Sharif, and D. Tipper. A survey on cyber security for smart grid communications. IEEE Communications Surveys & Tutorials, 14(4):998–1010, 2012.

[7] A. Tonge, S. Kasture, and S. Chaudhari. Cyber security: challenges for society-literature review. IOSR Journal of Computer Engineering, 2(12):67–75, 2013.

[8] S. Subashini and V. Kavitha. A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1):1–11, 2011.

[9] K. Gai and S. Li. Towards cloud computing: a literature review on cloud computing and its development trends.

[10] M. Qiu, H. Su, M. Chen, Z. Ming, and L. Yang. Balance of security strength and energy for a PMU monitoring system in smart grid. IEEE Communications Magazine, 50(5):142–149, 2012.

[11] M. Qiu, W. Gao, M. Chen, J. Niu, and L. Zhang. Energy efficient security algorithm for power grid wide area monitoring system. IEEE Transactions on Smart Grid, 2(4):715–723, 2011.

AUTHORS BIBILIOGRAPHY:

	**P ALEKHYA:** PURSING BTECH IN BALAJI INSTITUTE OF TECHNOLOGY AND SCIENCES
	**G LAXMISAI:** PURSING BTECH IN BALAJI INSTITUTE OF TECHNOLOGY AND SCIENCES
	**D REDHIMA:** PURSING BTECH IN BALAJI INSTITUTE OF TECHNOLOGY AND SCIENCES
	**G BHARGAVI:** PURSUING BTECH IN BALAJI INSTITUTE OF TECHNOLOGY AND SCIENCES