International Journal of Engineering Innovations in Advanced Technology
ISSN: 2582-1431 (Online), Volume-4 Issue-2, June 2022

An Investigation on Cybersecurity Threats and Security Models

P Vinaya Sree
Assistant Professor, Department of CSE, Anurag Group of Institutions, Hyderabad, India.
Email: vinayasreecse@anurag.edu.in

H Sindhu, K Vineela
UG Student, Department of CSE, Anurag Group of Institutions, Hyderabad, India.
Email: hsindhu55482@gmail.com ,Vineelakonda78@gmail.com

***Abstract* - Cyber security has been used interchangeably for information security, where later considers the role of the human in the security process while former consider this as an additional dimension and also, focus person has a potential targe+. However, such discussion on cyber security has important implication as it focuses on the ethical part of the society as a whole. To address the issue of cyber security, various frameworks and models have been developed. It also introduces the concepts of cyber security in terms of its framework, workforces and information related to protecting personal information in the computer. This paper reviews these models along with their limitations and review the past techniques used to mitigate these threats. Furthermore, the report also provides recommendations for future research.**

***Index Terms* - Cybersecurity, frameworks, workforces, threats, techniques**.

I INTRODUCTION

Cyber security has been used interchangeably for information security, where later considers the role of the human in the security process while former consider this as an additional dimension and also, focus person has a potential target.

However, such discussion on cyber security has an important implication asitfocuses on the ethical part of the society as a whole. There are various definitions of the concept of cyber security with varied aspects such as secured sharing, confidential and access to information. But still, the definitions lack clarity and consensus.

.

II LITERATURE SURVEY

A "Security-aware optimization for ubiquitous computing systems with SEAT graph approach"

For ubiquitous computing systems, security has become a new metric that designers should consider throughout the design process, along with other metrics such as performance and energy consumption. A combination of selected cryptographic algorithms for required security services forms a security strategy for the application.

In this paper, we propose methods to generate security strategies to achieve the maximal overall security strength while meeting the real-time constraint. In order to express security requirements of an application, we propose a novel graph model called Security-Aware Task (SEAT) graph model to represent real-time constraints and precedence relationships among tasks. Based on the SEAT graph approach, we propose an optimal algorithm, Integer Linear Programming Security Optimization (ILP-SOP). For the special structures such as simple path graph and tree, we propose two dynamic programming-based algorithms (DPSOP-path/tree) to generate the optimal security strategy.

Experiment results demonstrate the correctness and efficiency of our proposed method. The experimental results show that, by using our proposed techniques, the security strength can be improved by 44.3% on average. As local descriptors, and as we shall see, it is not only fixed-size features, but also offers the advantage of being highly efficient. The proposed approach allows distinguishing the destination after converting the image to the HSV system, after which the force field features will be extracted using the fast algorithm and then classification by using the distance for three methods (Manhattan, Euclidean, and Cosine) through which a comparison is made to choose the best resolution, as it was found that the resulting accuracy of the two dataset (ORL and UFI) is 99.9%.

Manuscript received April 04, 2022; Revised May 01, 2022; Accepted May 10, 2022.

B "Attack Detection and Identification in Cyber-Physical Systems -- Part I:

Models and Fundamental Limitations" Cyber-physical systems integrate computation, communication, and physical capabilities to interact with the physical world and humans. Besides failures of components, cyber-physical systems are prone to malignant attacks, and specific analysis tools as well as monitoring mechanisms need to be developed to enforce system security and reliability. This paper proposes a unified framework to analyze the resilience of cyber-physical systems against attacks cast by an omniscient adversary. We model cyber-physical systems as linear descriptor systems, and attacks as exogenous unknown inputs. Despite its simplicity, our model captures various realworld cyber-physical systems, and it includes and generalizes many prototypical attacks, including stealth, (dynamic) false-data injection and replay attacks. First, we characterize fundamental limitations of static, dynamic, and active monitors for attack detection and identification. Second, we provide constructive algebraic conditions to cast undetectable and unidentifiable attacks. Third, by using the system interconnection structure, we describe graph-theoretic conditions for the existence of undetectable and unidentifiable attacks. Finally, we validate our findings through some illustrative examples with different cyber-physical systems, such as a municipal water supply network and two electrical power grids.

III ANALYSIS

A Existing System

Al-Fayyad et al.evaluated the performance of personal firewall systems by organizing an arranged walkthrough to determine the design factors that could violate the usage standards. In the study of personal firewalls usability on Windows XP platform, four modern firewalls namely Norton 360 V. 2.0.0.242, Trend Micro Internet Security Version 16.00.1412, Zone Alarm V. 7.1.248 and ESET Nod32 Smart Security. The study results indicated that Personal firewalls encounter poor usability that could lead to vulnerabilities in security. The usability problems could be due to the issue that the data given by the firewalls (could be during the process of installing, configuration or during interaction) was not clear or misleading. Various usability problems have been noticed because of the reduced clarity of alerts

IV METHODOLOGY

In addition, proposed solution provides information on how to use programmability of software switches based on the solutions that improve the detection accuracy and defeat. Other research focused on the vulnerability assessment for automatic environments along with the web applications and various threats which are detected during the vulnerability assessment for different networking products.

The study has adopted OpenVas tool with exploratory research method. The study findings revealed some of the methods that can fix vulnerability for removing threats using the function PHP info () and other methods like Trojan helps in keeping networking systems safe

V ARCHITECTURE

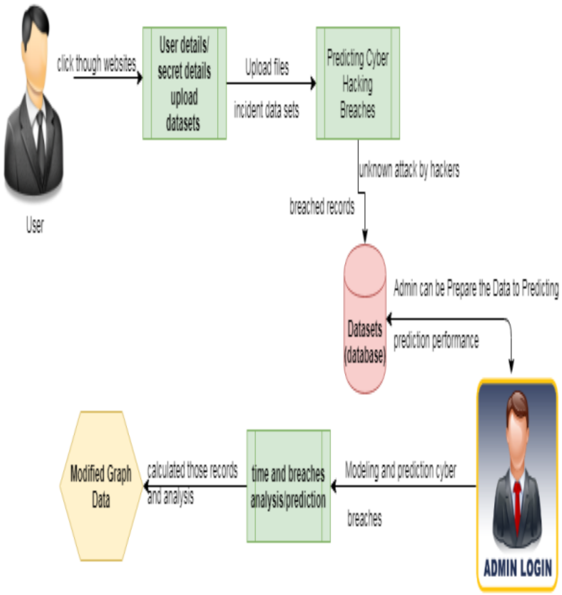
User
click though websites
User details/ secret details upload datasets
Upload files
incident data sets
Predicting Cyber Hacking Breaches
unknown attack by hackers
breached records
Datasets (database)
Admin can be Prepare the Data to Predicting
prediction performance
ADMIN LOGIN
Modeling and prediction cyber
breaches
time and breaches analysis/prediction
calculated those records and analysis
Modified Graph Data

Figure 1: Architecture diagram

VI RESULT

A

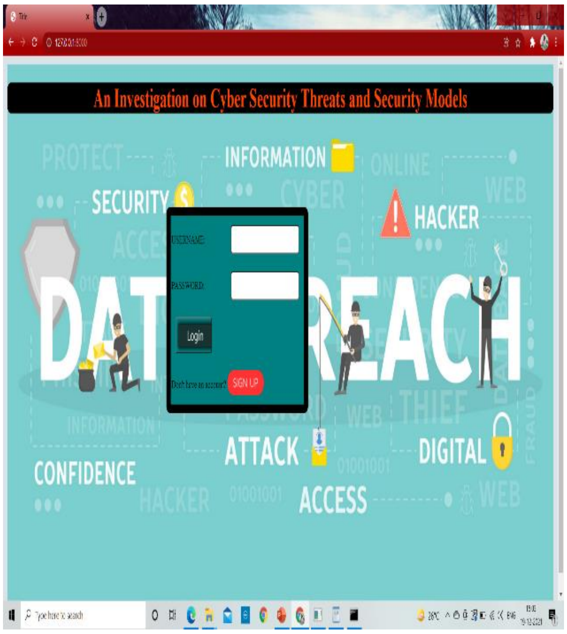
An Investigation on Cyber Security Threats and Security Models

Figure 2: An Investigation on cyber threats and security models

B

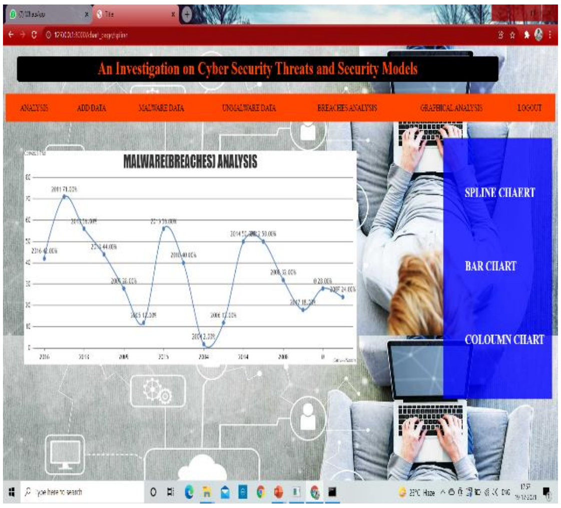

Figure 3 :Mallware breaches Analysis

CONCLUSIONS

From the review, it was found that majority of the studies have been conducted on the email security, firewalls, and vulnerabilities.There aregeneral recommendations on how to secure the password but not any authenticated protocol to protect the system inherently. Therefore, there is a need for more studies in terms of technics and models to ensure that passwords are protected.

REFERENCES

[1]J. Blackburn and G. Waters. Optimising Australia's Response to the Cyber Challenge. Kokoda Foundation, 2011.

[2] L. Bennett. Cyber security strategy. ITNOW, 54(1):10–11, 2012.

[3] M. Qiu, L. Zhang, Z. Ming, Z. Chen, X. Qin, and L. Yang. Securityaware optimization for ubiquitous computing systems with SEAT graph approach. J. of Computer andSyst. Sci., 79(5):518–529, 2013.

[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 cyberphysicalsystems. IEEE Transactions on Automatic Control, 58(11):2715–2729, 2013. [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 cloudcomputing. 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. In 2012 Fourth Int'l Conf. on Multimedia Information Networking and Security, pages 142–146, Nanjing, China, 2012.

[6] Viola, P. and Jones, M. Rapid object detection using boosted cascade of simple features. IEEE Conference on Computer Vision and Pattern Recognition, 2001.

AUTHORS PROFILE

P.Vinaya Sree is one of the authors of this paper. she completed her Master of Technology from JNTU Hyderabad in the year 2013 and B.Tech from JNTU Hyderabad in the year 2010. Worked as Asst. Professor at Mahaveer Institute of Science and Technology, Hyderabad. Presently working as Assistant Professor in the Department of Computer Science & Engineering at Anurag University, Hyderabad. She is the member of Cyber Security Research Wing and faculty coordinator of NULL club in the department. She handled diverse courses to under graduate students. She is a member of Indian Society for Technical Education (ISTE).

H.Sindhu is one of the co-authors of this paper. She was born in Telangana on August 2,2000. She is currently pursuing B.Tech. Degree in the field of computer science and engineering, from Anurag Group of Institutions, Hyderabad, Telangana, India. Her previous research interests are in the fields of Cyber Security. Her current field of Interest is Blockchain and Data Science. She is an active participant in the paper presentation events conducted at her college.

K.Vineela is one of the co-authors of this paper. She was born in Telangana on March 27,2001. She is currently pursuing B.Tech. Degree in the field of computer science and engineering, from Anurag Group of Institutions, Hyderabad, Telangana, India. She is currently working at cognizant as an intern in Hyderabad. Her previous research interests are in the fields of Cyber Security. Her current field of Interest is Blockchain and Data Science. She is an active participant in the paper presentation events conducted at her college.