The Seybold Report

ISSN 1533-9211

DOI: 10.5281/zenodo.10404088

A REVIEW ON DETERMINING CYBER SECURITY RISKS USING ESLs AND AI TECHNIQUES IN COMSEC

GURJEET KAUR

Research Scholar, M.Tech, Department of CSE, Rayat Bahra University, Mohali, Punjab, India.
Email: 99kgurjeet@gmail.com

Er. ASHIMA

Assistant Professor, Department of CSE, Rayat Bahra University, Mohali, Punajb, India.
Email: ashima.18621@rayatbahrauniversity.edu.in

Dr. PUNEET SAPRA

Associate Professor, Department of CSE, Rayat Bahra University, Mohali, Punjab, India.
Email: puneetsapra91@gmail.com

Abstract

Knowing what cyber security is and being able to use it successfully are essential skills in today's society, which is powered by technology and network connections. Without security to safeguard it, systems, crucial files, data, and other crucial virtual items are at risk. The relevance of the network unit is evaluated in conjunction with the network's cyber security risk assessment, utilizing the AHP approach and security status to estimate risk. Based on experimental results, this approach may determine each network unit's security level in addition to the primary network dangers. Threat hackers will also have greater access to an expanded attack surface due to the enhanced connection. Blackouts that were common in the past have been caused by cyber-attacks on energy networks using ESLs which stands for Electronic Shelf labels. In addition to raising the bar for digital and intelligent advancement, the Artificial intelligence Ubiquitous Power Internet of Things (UPIoT) for the Energy Internet also introduces unforeseen social variables, which change the environment for the emergence and propagation of its cyber dangers.

Keywords: Cyber Security, Electronic Shelf Labels.

INTRODUCTION

Many layers of defense are scattered throughout the networks, computers, programmes, and information that one wants to protect safe from harm in an efficient cyber security strategy. For a society to effectively defend against or recover from cyber-attacks, all of the systems, people, and tools must work together. The tasks of discovery, inspection, and remediation are three crucial security procedures that can be accelerated by a unified threat management system and cyber systems. People - Customers must understand and adhere to fundamental information security principles including choosing secure passwords, being cautious of attachments in email, and backing up their data. Learn more about fundamental cyber security principles and rules for accuracy. Processes - Governments need a plan on how to respond to both successful and common cyber-attacks. You might be escorted by a well-known outline. It makes it clear how to identify outbreaks, safeguard organizations, identify and address hazards, and learn from positive outcomes.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10404088

Technology - In order to provide people and organizations with the system security tools they need to defend themselves against cyber-attacks, technology is essential. Endpoint strategies, including PCs, mobile phones, and routers; systems; and the cloud are the three main targets that are most at risk. Next-generation firewalls, DNS filters, malware protection, antivirus programmers, and email security outcomes are examples of shared technology discarded to secure these things. Cyber may be distinguished as being in some way associated with the group of workstations or the network. Security also refers to the system used to safeguard anything.

As a result, the phrases "Cyber" and "safety" were developed to define the method of protecting user information during or following malicious attacks that could reveal a security breach. It is the period of time that was set aside for a while after the internet started developing rapidly. Any community or user can secure their vital data from hackers thanks to the asset of cyber security. Although it is wary of hacking at this stage, it has really used ethical hacking to implement cyber security in any building.

TYPES OF CYBER SECURITY

Phishing

The practice of disseminating false emails that appear to be from reliable sources is known as phishing. A meaningful data exchange that includes login information and credit card information is the aim. This type of cyber-attack is the worst.

Ransomware

It belongs to the category of malicious software. By preventing access to files or the computer system until the transaction is paid, it is regarded to be cash extraction. Payment of the ransom does not guarantee that the system or records will be recovered.

Malware

It is a sort of software made with the goal of obtaining an unauthorized permission to use or impairing a system. Engineering on the social web Opponents employ this strategy to trick you into disclosing sensitive information. They have the power to demand a financial settlement or better access to your protected information. Social engineering can be combined with some of the factors mentioned above to make you more likely to click on links, spread malware, or support bad causes.

GOALS OF CYBER SECURITY

Confidentiality

Ensuring that only authorized people can access your complicated data and ensuring that no information is disclosed to unwanted parties.

In the event that your key is secret and won't be disclosed to anybody, this compromises confidentiality.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10404088

How to protect confidentiality are as follows:

- Two- or multifactor verification; data encryption;
- Biometric confirmation

Integrity

Ensure that all of your information is accurate, reliable, and does not alter from one fact to another during the presentation. Integrity assurance techniques are as follows:

- No unlawful person shall have access to the records, which also violates privacy. Therefore, there will be controls for operator contact for worth working of the devices.
- Accessible backups that can return quickly are required.
- Version supervisory must be close by to check the change log.

Firewalls

A firewall is a piece of hardware or software that aids in blocking hackers, viruses, and worms from trying to access your computer over the Internet. Firewall always checks the communication whenever it enters and leaves the internet. It is an interface which is used to validate the communication first to block any kind of Trojan or virus into the system. Consequently, firewalls are crucial in the detection of malware.

Anti-virus Software

A computer programme known as antivirus software works to identify, stop, and take action against dangerous software programmes, such as worms and viruses. The majority of antivirus programmes have an auto-update capability that enables the programme to download profiles of fresh viruses so that it can scan for them as soon as they are found. Every system must have anti-virus software as a minimum need.

Availability

There must not be any bout alerts such as Denial of Service (DoS) every time the operator has requested a resource for a piece of statistics. The entire body of evidence must be accessible. For instance, if an attacker controls a website, the DoS that results will make it harder to get.

INSPECTING CYBER SECURITY RISKS

Although the power grid is a ubiquitous network, it only represents electric energy—not information or data. Astute energy with a significant proportion of renewable energy, changes to the "Internet" and the electrical market. Vitality and power user-side, data transformation, and transmission all stand for various fundamentally little facts that need to be joined. Huge data has a high value density, while single data has a low value density. High value. By means of the clever interconnection of sizable small data volumes, UPIoT offers ubiquitous perception of information and data. At the moment, UPIoT is in the planning phases at the moment.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10404088

The most important feature of it's the center of UPIoT cyber security development is the network of support and its availability.

To evaluate the risk of cyber security, a cyber-security evaluation model must be created indicates that the risk, susceptibility, and value of the asset that impact the cyber security risk of UPloT are connected. The danger rises in proportion to the quantity and intensity of vulnerability as well as asset worth. Vulnerability (V), threat (T), the elements of UPIoT cyber security include asset (A) and R TVA is one way to express risk (R). As such, the this is an expression for the network unit's risk (r). I in the network (NU).Considering that every node in the network with varying effects on network risk, the weighted total of all the total risk (R) of the network can be defined using unit risks.

Often, a security risk assessment includes many objectives. For example, asset appraisal calls for integrity, accessibility, and discretion. This is an example of a multi-objective decision-making conundrum. Furthermore, the evaluation process's goals and criteria frequently lack a standard measurement unit. These elements of safety risk assessment give rise to the advantages of AHP algorithm with ESLs. AHP (Analytic Hierarchy Process) is a simple method for doing quantitative analyses of qualitative problems. According to the AHP concept, the weight assessment of each risk aspect is split into three levels: the target level, the standard level (criterion level), and the scheme level complementation level. The AHP algorithm is used to establish the scheme level indicators' weight, and the indicators' quantitative values are then used to evaluate the risk components.

An AHP-based risk element evaluation using ESLs follows these steps:

Accompanying us

1. Based on the network architecture and service quality, select the AHP model.
2. Define the judgment matrix using expert scoring and ESLs for fast findings.
3. A determined the significance of every assessing factor.
4. Calculate the scheme-level metrics.
5. Examine the risks.

Using both math and psychology, the Analytic Hierarchy Process (AHP) is a way to organize and analyze complicated decisions. Thomas L. Saaty created it in the 1970s, and since then, it has been improved. It is divided into three sections: the main objective or issue you are attempting to solve, all potential answers, or alternatives, and the standards by which you will evaluate the alternatives. By quantifying the criteria and other choices involved in a decision and connecting them to the main objective, AHP offers a logical framework for making necessary decisions.

When making decisions about difficult problems with significant consequences, the AHP is most helpful. It differs from other methods of making decisions because it puts figures on options and criteria that are typically hard to assess. AHP assists decision makers in selecting

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10404088

the course of action that best aligns with their beliefs and problem-solving expertise, as opposed to dictating the "correct" course of action.

ELECTRONIC SHELF LABEL

Retailers employ electronic shelf label (ESL) systems to display product pricing on shelves that may be automatically updated or changed under the direction of a central server. These systems are often located on the front edge of retail shelving.

Electronic paper (E-paper) or liquid crystal display (LCD) are the two ways that ESL tag modules show the buyer the current product pricing. On ESLs, e-paper is frequently utilized since it offers clear visuals and complete graphic imagery, requiring no power to store an image and only electricity for updates. Unlike static placards, a communication network from the central server enables the price display to be automatically updated anytime a product price is modified. Reliability, battery life, speed, and application range must all be supported by wireless communication. Radio, infrared, or even visible light communication can all be used as wireless communication methods. The ESL market currently favors radio frequency communication a lot.

Retailers who sell their products in physical storefronts are the main users of electronic shelf labels, which are often affixed to the front edge of the retail shelves and show the product's price. Depending on the type of ESL, additional data may also be presented, such as stock levels, expiration dates, or product information for accuracy in results. Paper labels are replaced with electronic shelf labels (ESLs), which are tiny, battery-operated electronic paper (e-paper) displays that provide product and pricing details at the shelf edge. To create a dynamic pricing automation network, ESLs connect wirelessly to a central hub to get the accurate result.

EXAMINING AND ESTIMATION

Our analysis demonstrates the correlation between specific personality traits and noncompliance with cyber and network security standards, including impulsivity, risk-taking, and failure to consider the long-term effects of activities. The development of a battery of tests to include personality characteristics and cognitive processes relevant to cyber and network security behaviors into one framework should be the main goal of future study. This battery of tests ought to examine the cognitive abilities covered previously, such as impulsivity, risk-taking, and considering the effects of actions in the future to get the results to be done based upon ESLs.

Additionally, we demonstrate here how specific psychological techniques, such as rewarding and punishing security-related conduct, employing innovative polymorphic security alerts, and utilizing psychological techniques to encourage consideration of potential repercussions of actions, may boost pro-security behavior. Additionally, there are cognitive training techniques that assist in lowering impulsivity, risk-taking, and procrastination in the general population, such as working memory training and extra technical lectures.

ISSN 1533-9211

DOI: 10.5281/zenodo.10404088

Next, the probability that an IoT device will be the target of an attack is determined. In our fictitious example, we estimated the risk of this attack at 70%. Based on the experts' analysis, this possibility could evolve.

Attackers can choose to attack any or all of all three of the following: vulnerability, attack, and interdependence layer as well as susceptibility. So, the Internet of Things system's backing for environmental, social, and economic aspects will have an effect on the achievement of the company. Other approaches could be created in consideration of the suggested IoT system security to reduce the possibility of this impact by detecting it earlier using ESLs.

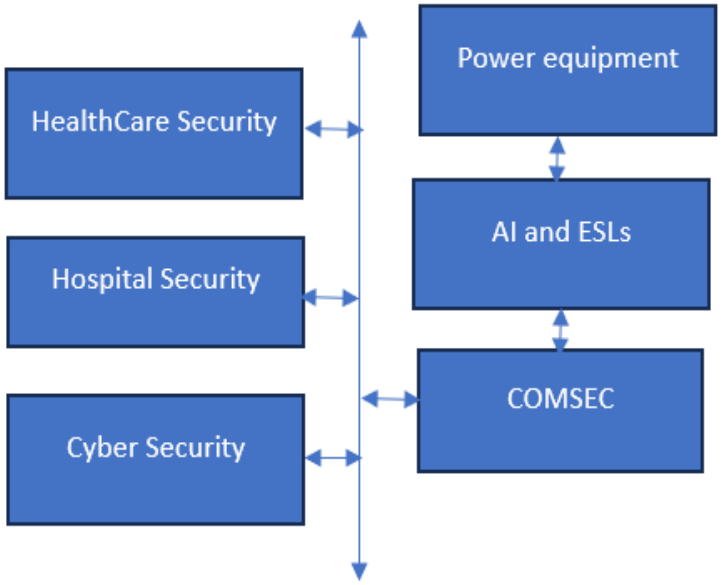

Figure 1: Block Diagram of Cyber Security

As was previously mentioned, there are numerous human errors that can compromise computer and security systems. These errors include sharing passwords, oversharing information on social media, accessing dubious websites, using unapproved external media, clicking links randomly, using weak passwords, opening attachments from dubious sources, sending sensitive information via mobile networks, and not physically securing p However, phishing emails and password sharing have been the focus of the majority of studies on human mistakes.

Future studies should examine how individual differences and contextual factors (such as emotional state, job urgency, or multitasking) contribute to various types of cyber security failures, such as using the same or weak passwords.

ISSN 1533-9211

DOI: 10.5281/zenodo.10404088

RESULTS

Benefits of the real model of architecture include the following, for instance, in comparison to other general-purpose IoT designs:

1) Data availability - exclusively trustworthy interfaces that pair certificates and use tokens are allowed to access the information. There should be a thorough examination of the processing results while considering the proprietary a process for producing the data request format dynamically as well as a breakdown to reduce the intricacy of the process of registration. A data center stores information and efficiently manages data access. Failure of a data center's operations is unavoidable and potentially catastrophic.

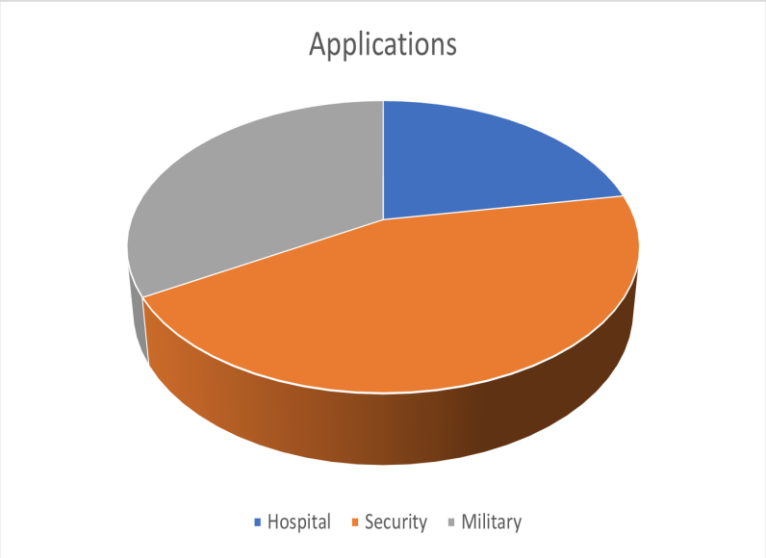

Figure 2: Security Authorities

IoT devices in data centers can reduce the requirement for human error and interaction by automating administrative tasks. Numerous typical data center tasks, such as network traffic monitoring, software and configuration upgrades, physical infrastructure monitoring, and automating alert notifications to relevant authorities, can be managed by IoT devices.

CONCLUSION

The growth of IR4.0 technologies has increased the demand for data centers to securely allow communication between different enterprises and to store, process, and analyze data in a suitable manner. In order to address the problem of recognizing cyber security risk of UPIoT, this study presents a cyber-security risk-assessment strategy based on AHP with ESLs and an importance evaluation method of node taking service features. Offering a new viewpoint on the assessment of security risks and the identification of Internet of things, the example shows that the method can not only intuitively quantify security risks but also identify the key security risks in the network as well as the security threats and vulnerabilities of a node.

The Seybold Report
ISSN 1533-9211
DOI: 10.5281/zenodo.10404088

References

1) Ullah, S., Zahilah, R. Curve25519 based lightweight end-to-endencryption in resource constrained autonomous 8-bit IoTdevices. Cybersecur 4, 11 (2021). https://doi.org/10.1186/s42400-021-00078-6.

2) P. A., B. Seth and G. Ramachandran, "Analysis of Current SmartWearable Trends using Internet of Medical Things," 2023 ThirdInternational Conference on Artificial Intelligence and Smart Energy(ICAIS), Coimbatore, India, 2023, pp. 19-22, doi:10.1109/ICAIS56108.2023.10073832.

3) P. A., G. V. Reddy "Artificial Intelligence Techniques for the wirelesswearable Smart Healthcare Prediction System Applications," 2023Second International Conference on Electronics and RenewableSystems (ICEARS), Tuticorin, India, 2023, pp. 879-884, doi:10.1109/ICEARS56392.2023.10085051.

4) Manzil, H.H.R., Manohar Naik, S. Android malware categorydetection using a novel feature vector-based machine learningmodel. Cybersecurity 6, 6 (2023). https://doi.org/10.1186/s42400-023-00139-y.

5) Wang, H., Singhal, A. & Liu, P. Tackling imbalanced data incybersecurity with transfer learning: a case with ROP payloaddetection. Cybersecurity 6, 2 (2023). https://doi.org/10.1186/s42400-022-00135-8.

6) Renganathan, V., Yurtsever, E., Ahmed, Q. et al. Valet attack onprivacy: a cybersecurity threat in automotive Bluetooth infotainmentsystems. Cybersecurity 5, 30 (2022). https://doi.org/10.1186/s42400-022-00132-x.

7) Wohwe Sambo, D., Yenke, B.O., Förster, A. et al. A new fuzzy logicapproach for reliable communications in wireless underground sensornetworks. Wireless Netw 28, 3275–3292 2022).https://doi.org/10.1007/s11276-022-03008-7.

8) Rahaman, S.M.A., Azharuddin, M. A cluster based charging schedulefor wireless rechargeable sensor networks using gravitational searchalgorithm. Wireless Netw 28, 3323–3336 (2022).https://doi.org/10.1007/s11276-022-03049-y.

9) Kumar, Naween, Dash, Dinesh, & Kumar, Mukesh. (2021). Anefficient on-demand charging schedule method in rechargeable sensornetworks. Journal of Ambient Intelligence and HumanizedComputing, 12(7), 8041–8058

10) Vishnu P Parandhaman, Analysis Techniques Artificial intelligence forDetection of Cyber Security Risks in a Communication and Information Security (2023)