 ISSN 2776-8007


# Using Information Technology to Quantitatively Evaluate and Prevent Cybersecurity Threats in a Hierarchical Manner

Rui Mai [1,*] and Mingzhu Wu [1]

Hainan College of Economics and Business, China
mairui@hceb.edu.cn*;
* corresponding author

(Received: December 10 , 2022; Revised: January 1, 2023; Accepted: January 22, 2023; Available online: April 4, 2023)

**Abstract**

The vulnerability of traditional network security technology in the face of rapid advancements in information technology and the constant changes in network security. As a result, hackers can easily exploit loopholes in traditional security measures, such as cracking cryptographic algorithms, and stealing sensitive user information and data, which has led to a crisis of trust in recent years. To ensure safe and effective operation of massive data on the network, this article presents a quantitative assessment of the network's threat situation. The assessment is divided into two parts: support evaluation and credibility evaluation. These parts are further broken down into three levels of evaluation and severity evaluation. The article also provides a list of network security-related precautions that can be taken to mitigate potential risks. The experimental results show that implementing these hierarchical security measures can improve the security rate of Internet users' information by 4%-5%. Overall, the article highlights the importance of adopting more advanced and sophisticated security measures to combat the increasingly complex threats posed by cybercriminals.

*Keywords:* Information Technology, Network Security Threat Situation, Hierarchical Network, Quantitative Assessment, Security Precautions

## 1. Introduction

In today's world, cyber attacks have become an increasingly significant threat to businesses, organizations, and individuals. With the growth of technology and the internet, the risk of cyber attacks has also increased, leading to a greater need for effective cybersecurity measures [1]. While there are numerous methods of addressing cyber threats, using information technology to quantitatively evaluate and prevent such threats in a hierarchical manner has gained considerable attention as a potential solution [2].

The primary problem addressed by this research is the need for effective cybersecurity measures in the face of growing cyber threats. Traditional cybersecurity methods often rely on reactive measures, such as firewalls and antivirus software, to prevent attacks. However, such measures are not always effective in preventing sophisticated and targeted cyber attacks [3,4]. Using information technology to quantitatively evaluate and prevent cyber threats in a hierarchical manner is a proactive approach that enables organizations to identify and address vulnerabilities before they can be exploited.

Another challenge facing organizations is the complexity of cyber threats. Cyber attacks can take many forms, and they often target multiple areas of an organization's network simultaneously [5]. Using information technology to evaluate and prevent cyber threats in a hierarchical manner allows for a more comprehensive understanding of the

risks and vulnerabilities present in a network, enabling organizations to take a more targeted and effective approach to cybersecurity [6].

Furthermore, many organizations face the challenge of limited resources when it comes to cybersecurity. Implementing effective cybersecurity measures can be costly and time-consuming, and smaller organizations may not have the resources to invest in such measures. Using information technology to evaluate and prevent cyber threats in a hierarchical manner can help organizations make better use of their limited resources by identifying the areas of greatest risk and focusing their efforts on those areas [7-9].

Finally, the lack of standardization in cybersecurity practices is another problem that this research seeks to address. There is currently no universal standard for cybersecurity practices, and different organizations may take vastly different approaches to cybersecurity. Using information technology to quantitatively evaluate and prevent cyber threats in a hierarchical manner provides a standardized approach to cybersecurity that can be adapted to the specific needs of individual organizations [10].

Using information technology to quantitatively evaluate and prevent cybersecurity threats in a hierarchical manner offers a proactive, comprehensive, and standardized approach to cybersecurity that addresses many of the challenges facing organizations today. This research aims to explore the potential of this approach and develop practical strategies for implementing it effectively [3]. By doing so, it is hoped that organizations of all sizes can better protect themselves against the growing threat of cyber attacks.

The process of assessing network security situations involves examining the risk management perspective and utilizing scientific methods and techniques to analyze various elements of the network, including potential security threats and vulnerabilities [9]. By quantifying the risk associated with potential threats, it becomes possible to develop effective protective measures and defense countermeasures to mitigate, avoid, or resist risks while keeping them within acceptable levels. There are two primary methods for assessing network security threats: qualitative and quantitative assessments.

Qualitative assessment involves describing the status assessment using descriptive language, while quantitative assessment involves classifying risks based on evaluation indicators that represent the results of the status assessment in mathematical form. Quantitative assessment is preferred because it is easier to calculate and interpret, and it reduces the potential for significant differences in results due to subjective human allocation. However, quantitative assessment results are not entirely accurate and can still be subjective. This method also tends to be more costly than qualitative assessment.

Overall, a thorough network security situation assessment is critical for identifying and addressing potential threats to network systems effectively. By utilizing both qualitative and quantitative assessment methods, network administrators can gain a comprehensive understanding of the risks and vulnerabilities present in their network and develop effective strategies to mitigate those risks.

## 2. Literature Review

### 2.1. Cybersecurity Situational Awareness

Cybersecurity situational awareness refers to the ability to identify and respond to potential cyber threats in real-time. It involves continuously monitoring a network's security status and identifying any suspicious activities that may pose a risk to the system. The importance of cybersecurity situational awareness has become increasingly evident in recent years, as cyber attacks have become more sophisticated and frequent [11].

The first step in achieving cybersecurity situational awareness is to establish a robust monitoring system that can detect and alert network administrators to potential threats. This system should be able to monitor various types of

activity, including network traffic, user activity, and application activity. The system should also be able to identify anomalous behavior that may indicate a potential threat [12].

Once potential threats are identified, it is essential to have a well-defined incident response plan in place to respond to them quickly and effectively. This plan should outline the steps to be taken in the event of a cyber attack, including isolating affected systems, containing the attack, and restoring normal operations. It should also include procedures for communicating with internal stakeholders and external partners, such as law enforcement agencies.

To effectively respond to potential cyber threats, network administrators must have access to timely and accurate information. This information can be obtained through threat intelligence, which involves gathering data on the tactics, techniques, and procedures used by cybercriminals to carry out attacks. Threat intelligence can help network administrators identify and mitigate potential threats before they can cause significant harm.

Overall, cybersecurity situational awareness is critical for protecting network systems from cyber attacks. By establishing a robust monitoring system, implementing an incident response plan, and utilizing threat intelligence, network administrators can identify and respond to potential threats quickly and effectively, minimizing the damage caused by cyber attacks. As cyber threats continue to evolve, it is essential to maintain a high level of situational awareness and adapt security strategies accordingly.

## 2.2. Situational Quantitative Assessment

Situational quantitative assessment is a critical process used to evaluate and mitigate various risks and threats faced by individuals, organizations, and even nations. This assessment involves utilizing various mathematical and statistical tools to quantify the likelihood of different risks and to assess the potential impact of such risks if they occur. The aim of situational quantitative assessment is to provide decision-makers with the necessary information to develop effective mitigation strategies, contingency plans, and response actions [13].

One significant advantage of situational quantitative assessment is its ability to provide an objective and data-driven analysis of different risks. By using mathematical models and statistical tools, this assessment can provide a clear understanding of the probability and impact of various risks. This can help decision-makers to make informed decisions and to develop effective strategies that can reduce the impact of such risks on the system [14].

Another advantage of situational quantitative assessment is its ability to identify previously unknown risks. This is because quantitative assessment techniques can identify risks that may be overlooked in a qualitative assessment. This can help organizations to identify and develop strategies to mitigate these risks before they cause significant harm.

However, one limitation of situational quantitative assessment is its reliance on historical data. This means that if there is no relevant historical data available, the assessment may not be entirely accurate. Also, the assessment can only provide insights based on available data, which means that new risks that have not yet been encountered may not be considered.

Situational quantitative assessment is a critical tool for risk management and mitigation. Its ability to provide objective and data-driven analysis of various risks can help decision-makers to develop effective strategies to reduce the impact of such risks. Although it has some limitations, such as its reliance on historical data and inability to identify new risks, it remains a valuable tool in risk management and should be employed as part of an overall risk management strategy.

ISSN 2776-8007


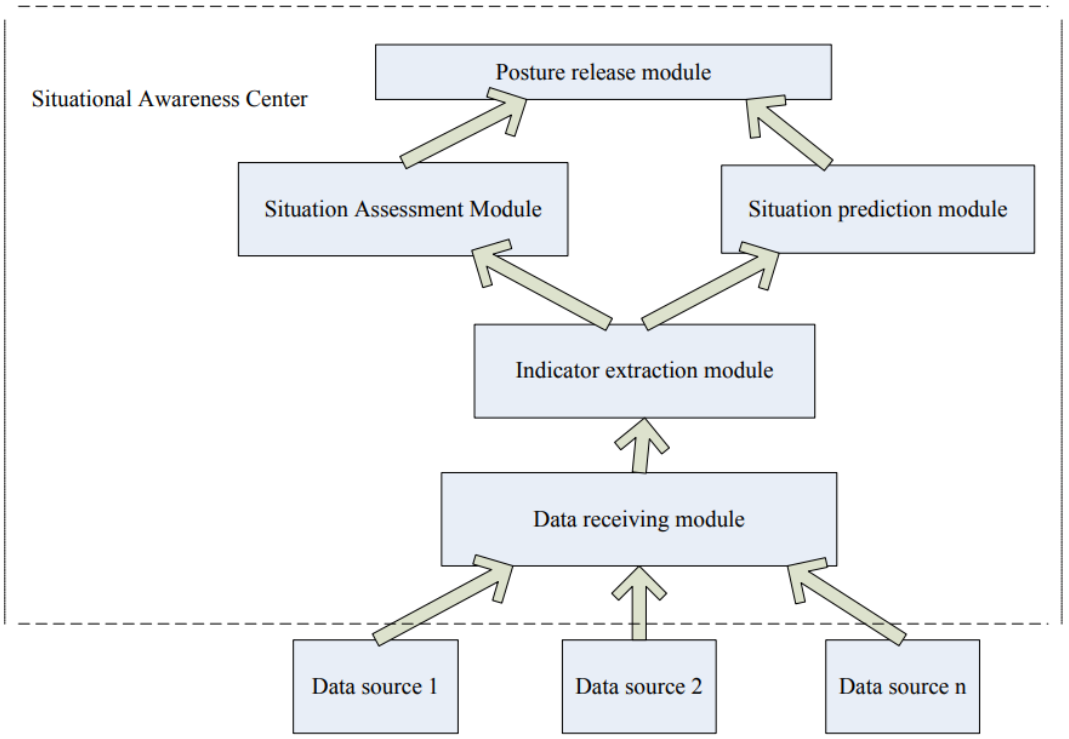


Figure. 1. Situational quantitative assessment model

## 2.3. Situational Quantitative Assessment

Situational quantitative assessment is a critical process used to evaluate and mitigate various risks and threats faced by individuals, organizations, and even nations [15]. This assessment involves utilizing various mathematical and statistical tools to quantify the likelihood of different risks and to assess the potential impact of such risks if they occur. The aim of situational quantitative assessment is to provide decision-makers with the necessary information to develop effective mitigation strategies, contingency plans, and response actions [16].

One significant advantage of situational quantitative assessment is its ability to provide an objective and data-driven analysis of different risks. By using mathematical models and statistical tools, this assessment can provide a clear understanding of the probability and impact of various risks. This can help decision-makers to make informed decisions and to develop effective strategies that can reduce the impact of such risks on the system.

Another advantage of situational quantitative assessment is its ability to identify previously unknown risks. This is because quantitative assessment techniques can identify risks that may be overlooked in a qualitative assessment. This can help organizations to identify and develop strategies to mitigate these risks before they cause significant harm.

However, one limitation of situational quantitative assessment is its reliance on historical data. This means that if there is no relevant historical data available, the assessment may not be entirely accurate. Also, the assessment can only provide insights based on available data, which means that new risks that have not yet been encountered may not be considered.

Situational quantitative assessment is a critical tool for risk management and mitigation. Its ability to provide objective and data-driven analysis of various risks can help decision-makers to develop effective strategies to reduce the impact of such risks. Although it has some limitations, such as its reliance on historical data and inability to identify new risks, it remains a valuable tool in risk management and should be employed as part of an overall risk management strategy.

The network security situation assessment algorithm uses the network security information of each server node in the network (including intrusion information, network node topology information, vulnerability information performance information service information, and log information) to obtain the vulnerability situation, threat situation, and System operation situation, combined with the distribution of nodes in the network cluster to determine the vulnerability situation, threat situation and the degree of influence of the system operation situation on different nodes, then the security situation assessment value of the entire network can be expressed by formula (1):

$$Y = \sum_{j=1}^{k} (D_j, E_j, F_j) * (U_{jD} U_{jE} U_{jF}) \quad (1)$$

## 3. Methodology

### 3.1. Support Evaluation

Support evaluation is an essential aspect of any system that involves providing support services to clients or users. The process involves assessing the effectiveness of the support provided, identifying areas for improvement, and implementing changes to enhance the quality of support [3, 17-19]. The following is a five-paragraph methodology for conducting support evaluation.

The first step in support evaluation is to define the goals and objectives of the evaluation process. The goals should be specific, measurable, achievable, relevant, and time-bound (SMART). The objectives should include the identification of the key performance indicators (KPIs) to be used to evaluate the effectiveness of the support services provided. These KPIs could include response time, customer satisfaction, and first-time resolution rate, among others.

The second step is to collect data related to the identified KPIs. This could involve gathering feedback from customers, analyzing support logs and tickets, and conducting surveys. The data collected should be accurate, reliable, and relevant to the evaluation process.

The third step is to analyze the data collected to identify trends and patterns that could indicate areas of strength and weakness in the support services provided. This could involve using statistical tools and techniques such as regression analysis, correlation analysis, and factor analysis. The analysis should provide insights into the factors that are affecting the quality of support provided and identify areas for improvement.

The fourth step is to develop an action plan to address the areas of improvement identified in the analysis. The action plan should include specific, measurable, achievable, relevant, and time-bound (SMART) objectives and should be designed to enhance the quality of support provided. The action plan should be communicated to all stakeholders involved in the support services, including the support staff, management, and customers.

The fifth and final step is to monitor the implementation of the action plan and assess its effectiveness in improving the quality of support services provided. This could involve conducting follow-up surveys, analyzing support logs

and tickets, and tracking the identified KPIs. The results of the monitoring process should be used to refine the action plan and ensure continuous improvement of the support services provided.

In conclusion, support evaluation is a crucial process for ensuring the quality of support services provided to clients or users. The five-step methodology outlined above provides a structured approach for conducting support evaluation that involves defining goals and objectives, collecting data, analyzing the data, developing an action plan, and monitoring the implementation of the action plan. By following this methodology, organizations can continuously improve the quality of their support services and enhance customer satisfaction.

## 3.2. Attack Severity Classification

Attack Severity Classification is a critical concept in cybersecurity that refers to the process of categorizing attacks based on their severity. This concept is essential for organizations to develop appropriate responses and strategies to prevent or mitigate attacks [6]. Attack severity classification helps organizations to understand the potential impact of an attack, including its scope, duration, and level of damage. By assessing the severity of an attack, organizations can prioritize their response and allocate resources appropriately to minimize the impact of the attack.

There are several methods for classifying attack severity, including using vulnerability scores, incident response procedures, and security information and event management (SIEM) systems [20]. Vulnerability scores involve rating the severity of an attack based on the vulnerability that the attack targets. Incident response procedures involve assigning severity levels to potential threats based on their potential impact. SIEM systems automatically categorize attacks based on the severity of the event and notify security personnel to respond appropriately.

Attack severity classification is also an essential component of risk management. By classifying attacks based on their severity, organizations can develop and implement risk mitigation strategies. These strategies may include investing in new security measures, such as firewalls, intrusion detection systems, and access controls. They may also involve training employees on how to recognize and respond to potential attacks, creating backup and recovery procedures, and developing incident response plans.

Attack Severity Classification is a crucial concept in cybersecurity that helps organizations assess and prioritize potential threats. By categorizing attacks based on their severity, organizations can allocate resources appropriately and develop effective response strategies. This concept is also a critical component of risk management, helping organizations to mitigate the impact of potential attacks and minimize damage to their systems and data. Therefore, understanding the severity of attacks is essential for any organization that wants to maintain the integrity and security of its systems and data.

The severity of the attack is classified according to the degree of damage to the target network environment according to the attack intent, from 0 to 9 divided into ten levels, the higher the level, the higher the severity of the consequences of the attack [9]. The classification is mainly based on the destructiveness of the attack and the purpose and means of the invasion. The classification of threat attack severity levels is shown in Table 1:

Table. 1. Classification of attack severity

| Grade | Evaluation Criteria |
|---|---|
| 0 | Get OS, apply version information. |

| | |
|---|---|
| 1 | Get system sensitive information. |
| 2 | Read the unrestricted file and data. |
| 3 | Read more important or limited files and data. |
| 4 | Make a restricted file and data. |
| 5 | Move a restricted important document and data. |
| 6 | For unrestricted important documents, data is modified, or DOS attacks on ordinary services. |
| 7 | Execute the command or perform the system as a normal user, the network-level DOS attack. |
| 8 | Execute commands as managed (limited, not easy to use). |
| 9 | Execute commands as managed (not limited, easy to use). |

### 3.3. Credibility assessment

Credibility assessment is the process of evaluating the reliability and trustworthiness of information or individuals. The concept of credibility assessment is widely used in various fields, including law enforcement, journalism, psychology, and social sciences. The aim of credibility assessment is to determine the accuracy and credibility of a statement or source of information to make informed decisions.

One of the most common methods of credibility assessment is based on the cues of deception. These cues include verbal, nonverbal, and behavioral indicators that suggest whether an individual is telling the truth or lying. Examples of verbal cues include inconsistent statements, excessive detail, and a lack of spontaneity. Nonverbal cues may include avoiding eye contact, fidgeting, and nervous behavior. Behavioral cues include changes in vocal pitch or tone, body posture, and facial expressions.

Another approach to credibility assessment is to evaluate the credibility of the source of information rather than the information itself. The source of information can influence the credibility of the information, and this approach seeks to determine whether the source is trustworthy, reliable, and competent. This is especially important in fields such as journalism and academia, where the reputation of the source is a significant factor in determining the credibility of the information.

Credibility assessment can also be achieved through the use of technology. For instance, lie detector tests (polygraphs) are used to measure physiological responses that indicate deception, such as changes in heart rate and blood pressure. However, the use of polygraphs in legal contexts is highly controversial, and their accuracy is still a subject of debate.

Finally, credibility assessment is not a foolproof method and can be influenced by factors such as bias, context, and cultural differences. Therefore, it is essential to approach credibility assessment with caution and employ multiple methods of evaluation to increase accuracy and reduce potential biases. In conclusion, credibility assessment is a critical process in various fields that seeks to evaluate the reliability and trustworthiness of information or

individuals. It is achieved through various methods, including verbal, nonverbal, and behavioral cues, evaluating the credibility of the source of information, using technology, and being mindful of potential biases.

## 4. Discussion

To assess the situation of network security, various sources of data are required, such as the results of asset value and vulnerability assessments, and credibility, support, and severity outcomes in the threat assessment process. From these sources of data, the probability of a successful attack can be calculated by using the credibility and support degrees of the threat, and the likelihood of a security event's intrusion can be calculated based on the results of the vulnerability assessment. In addition, the loss level resulting from the security incident can be determined from the threat severity and asset value evaluation results. These parameters are then used to assess the security situation of the target system, and the outcome is presented in the form of a threat situation map.

The process of evaluating the security situation is based on warnings, using quantitative indicators of threat elements and a gradual fusion of the values of various indicators. This results in a real-time representation of the threat situation for the object of evaluation. Hence, it is both feasible and necessary to develop a hierarchical model for assessing network security threats and proposing appropriate security measures.

In summary, constructing a model for network security threat assessment requires the use of data from various sources, including asset value and vulnerability assessments, and credibility, support, and severity results from threat assessment processes. The model should take into account the probability of a successful attack and the likelihood of intrusion based on vulnerability assessment results, as well as the potential loss level. By combining these factors, a security situation assessment can be conducted, and a real-time threat situation map can be created for the evaluation object. This method is based on warnings, quantitative indicators, and gradual fusion of values, providing a comprehensive and accurate evaluation of the network security situation.

## 5. Conclusion

In this article, the primary focus is on the concepts of hierarchical quantitative assessment of cybersecurity threat situations. This method involves analyzing various elements of network systems, assessing the severity of potential threats and vulnerabilities, and developing appropriate countermeasures to reduce online risks for users. To achieve this, the article provides an indicator system and corresponding theory for large-scale network situation assessment.

The process of network security threat situation assessment is divided into three main areas: credibility assessment, support assessment, and seriousness assessment. Credibility assessment involves evaluating the reliability and trustworthiness of information sources, while support assessment involves analyzing the infrastructure and technical support available for network systems. Finally, seriousness assessment involves evaluating the severity of potential threats and vulnerabilities.

According to the experimental results presented in the article, the hierarchical quantitative assessment of network security threat situations can significantly reduce online risks for netizens. This method provides a green and reliable network environment for users to access and interact with online content. This approach also helps network administrators develop effective protection measures and defense countermeasures to mitigate, avoid, or resist risks while keeping them within acceptable levels.

Overall, the hierarchical quantitative assessment of network security threat situations is a critical process in ensuring the safety and reliability of online networks. By analyzing various elements of network systems and assessing potential risks and vulnerabilities, network administrators can develop effective strategies to protect users and reduce online risks. The indicator system and corresponding theory provided in the article can serve as a valuable resource for network administrators seeking to enhance the security and reliability of their systems.

## References

[1] M. H. Rahman, T. Wuest, and M. Shafae, "Manufacturing cybersecurity threat attributes and countermeasures: Review, meta-taxonomy, and use cases of cyberattack taxonomies," J. Manuf. Syst., vol. 68, pp. 196–208, 2023, doi: 10.1016/j.jmsy.2023.03.009.

[2] R. Beuran, J. Vykopal, D. Belajová, P. Čeleda, Y. Tan, and Y. Shinoda, "Capability Assessment Methodology and Comparative Analysis of Cybersecurity Training Platforms," Comput. Secur., vol. 128, 2023, doi: 10.1016/j.cose.2023.103120.

[3] A. A. Fröhlich, L. P. Horstmann, and J. L. C. Hoffmann, "A Secure IIoT Gateway Architecture based on Trusted Execution Environments," J. Netw. Syst. Manag., vol. 31, no. 2, 2023, doi: 10.1007/s10922-023-09723-6.

[4] W. M. Pecena, "Can I Really Protect My Broadcast Plant From a Cybersecurity Attack?," SMPTE Motion Imaging J., vol. 132, no. 2, pp. 57–64, 2023, doi: 10.5594/JMI.2023.3239646.

[5] P. Ford, "The Quantum Cybersecurity Threat May Arrive Sooner Than You Think," Computer (Long. Beach. Calif)., vol. 56, no. 2, pp. 134–136, 2023, doi: 10.1109/MC.2022.3227657.

[6] A. Alotaibi and M. A. Rassam, "Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense," Futur. Internet, vol. 15, no. 2, 2023, doi: 10.3390/fi15020062.

[7] Z. Muhammad, Z. Anwar, B. Saleem, and J. Shahid, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," Energies, vol. 16, no. 3, 2023, doi: 10.3390/en16031113.

[8] J. S. Fidelis, L. Joseph, K. D. Souza, K. Sankaranarayanan, and V. Agarwal, "Development of risk inventory for hospitals in India," J. Patient Saf. Risk Manag., vol. 28, no. 1, pp. 21–30, 2023, doi: 10.1177/25160435221142672.

[9] P. Sharma, S. Kapoor, and R. Sharma, "Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach," Int. J. Syst. Assur. Eng. Manag., vol. 14, no. 1, pp. 287–296, 2023, doi: 10.1007/s13198-022-01793-0.

[10] C. C. Trumbach, D. M. Payne, and K. Walsh, "Cybersecurity in business education: The 'how to' in incorporating education into practice," Ind. High. Educ., vol. 37, no. 1, pp. 35–45, 2023, doi: 10.1177/09504222221099389.

[11] S. B. Nazeer Khan, D. Richards, P. Formosa, and S. Bankins, "To breach or not? Profiling students' likelihood of breaching university ICT Codes of Conduct: Student Profiling of Breach of ICT Codes of Conduct," in ACM International Conference Proceeding Series, 2023, pp. 50–57. doi: 10.1145/3579375.3579382.

[12] P. Jenifer, A. R. Geebin, P. Brundha, and E. Manohar, "Differentially Distributed Private Intelligence Security in Cybersecurity Infrastructures," in Proceedings - 5th International Conference on Smart Systems and Inventive Technology, ICSSIT 2023, 2023, pp. 721–724. doi: 10.1109/ICSSIT55814.2023.10061092.

[13] O. Naim, D. Cohen, and I. Ben-Gal, "Malicious website identification using design attribute learning," Int. J. Inf. Secur., 2023, doi: 10.1007/s10207-023-00686-y.

[14] S. Ruiz-Villafranca, J. Carrillo-Mondéjar, J. M. Castelo Gómez, and J. Roldán-Gómez, "MECInOT: a multi-access edge computing and industrial internet of things emulator for the modelling and study of cybersecurity threats," J. Supercomput., 2023, doi: 10.1007/s11227-023-05098-2.

[15] J. Lourenço, J. C. Morais, S. Sá, N. Neves, F. Figueiredo, and M. C. Santos, "Cybersecurity Concerns Under COVID-19: Representations on Increasing Digital Literacy in Higher Education," Smart Innovation, Systems and Technologies, vol. 320. pp. 739–748, 2023. doi: 10.1007/978-981-19-6585-2_65.

[16] Z. Zhao et al., "ERNN: Error-Resilient RNN for Encrypted Traffic Detection towards Network-Induced Phenomena," IEEE Trans. Dependable Secur. Comput., pp. 1–18, 2023, doi: 10.1109/TDSC.2023.3242134.

[17] I. N. Kolosok and E. S. Korkina, "Applying Cyber-Physical Management to the Structure of the Demand Response Aggregator," Lecture Notes in Networks and Systems, vol. 460 LNNS. pp. 229–238, 2023. doi: 10.1007/978-3-031-20875-1_21.

[18] I. Lateș and C. Boja, "Cyber Range Technology Stack Review," Smart Innovation, Systems and Technologies, vol. 321. pp. 25–40, 2023. doi: 10.1007/978-981-19-6755-9_3.

[19] F. S. Alrayes et al., "Enhanced Gorilla Troops Optimizer with Deep Learning Enabled Cybersecurity Threat Detection," Comput. Syst. Sci. Eng., vol. 45, no. 3, pp. 3037–3052, 2023, doi: 10.32604/csse.2023.033970.

[20] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," Ocean &Coastal Manag., 2023, [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0964569123000182