IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ANALYTICAL SYSTEM FOR NETWORK SECURITY ON SITUATIONAL AWARENESS AND ITS COMPARISON OF IMPLEMENTATION METHODS

[1]Sumiyah khaja, [2]Syed Faizuddin Ahmed Quadri.

Coding Instructor, Whitehat jr, Online platform

Technical Lead (SME), IT DEPARTEMENT/ Vertafore, HYDERABAD

ABSTRACT

The information technology industry has made significant advances into many facets of society, including its politics, business, and culture. The digital revolution has not only contributed to the enormous growth of human society but has also brought an unprecedented amount of attention to the challenges of maintaining network security. There are four main phases that researchers who focus on network security go through: network security best practises, complementary research and passive defence, proactive analysis and plan development, and a holistic perspective and forward-looking forecasting. Against the background of the new strategic command for the digital control, which all countries are competing for, new features arise in the debate over network security situational awareness, both in academic study and industrialisation. To that purpose, a thorough literature evaluation of situational awareness in network security was done for this study. In this paper, we lay out the national and international landscape of current research, and then provide the analytical framework necessary to place network security awareness within the context of the data value chain. Finally, some conclusions and recommendations are offered. The entirety of the procedure is broken down into five distinct steps that occur in sequential order: the factor acquisition stage, the model representation stage, the measurement establishment stage, the solution analysis stage, and the scenario prediction stage. Next, the function of each stage, the prevalent methods currently in use, the results of applying the methods to the experimental objects, and a side-by-side comparison of the various approaches are discussed. The purpose of this paper is to serve as a resource for researchers and engineers in the field of network security, offering them a bird's-eye view of the current state of the field and some supplementary ideas for its eventual industrialization. The paper will also make an effort to offer some recommendations for bettering the safety of computer networks.

Keywords: Network security, Network situational awareness, Big data network security, Intrusion detection.

1. INTRODUCTION

Mobile devices, systems with embedded software, computers, servers, networks, and the Internet all play a significant role in today's world. Recent advancements and publications in the news demonstrate that such systems are continuously being attacked. The government's highly secure systems have also been the target of successful intrusions, along with those of less security-conscious end users.

Common types of cyber threats include APTs, DDoS attacks, CPMs (cross-platform malware), metamorphic and polymorphic malware, phishing, BGP hijacks, cyber espionage, data breaches, vulnerabilities, malicious websites, social media scams, credit card fraud, and identity theft. Symantec states that "the only constant that can be said about the threat landscape, and Internet security in general, is that change is the only constant" in their 2015 Internet Security Threat Report. Research in the field of cyber security is essential due to the increasing number of sophisticated attacks and the wide variety of attack vectors. Social engineering and a weak link, like a user opening a seemingly legitimate e-mail attachment, have been the starting point for many successful attacks

against highly protected networks in recent years. One of the most crucial objectives is to better inform users, as social engineering and a vulnerable link have often been the starting points for attacks on highly secured networks.

The data, the computing resources, the cyber security, and the software programmes are all safeguarded from attack by a combination of different policies, strategies, and technologies [1]. Cyber security encompasses a wide range of operational best practises, tools, and protocols [2]. Data-level, application-level, network-level, and host-level security measures can all be implemented in the cyber world. Security breaches and attacks can be prevented and detected using a variety of techniques [3, 4]. Firewalls, anti-virus programs, IDSs, and IPSs are all examples of such security measures. Other tools include intrusion prevention systems (IPSs). Despite this, many of the adversaries still have an edge because all they have to do in order to benefit from a weakness in the systems that need to be safeguarded is locate one. As more and more systems become internet-connected, there is a greater potential target pool available to cybercriminals. As attackers gain in sophistication, they are creating zero-day exploits and malware that can hide from security systems for much longer [5].

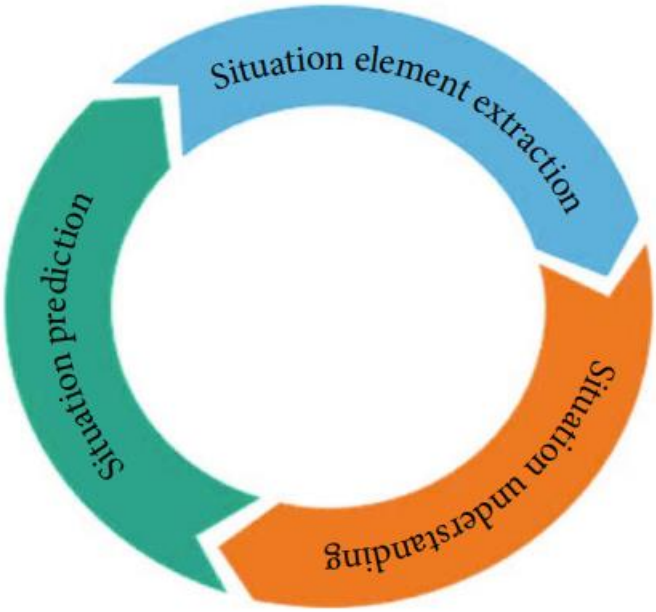


Figure 1: Security in Cyberspace Situational Awareness Cycle.

They are attacks that have never been seen before, but in most cases, they are variations of attacks that have been seen before. Commoditization of exploitation tactics is making the problem significantly worse since it makes rapid distribution possible without the involvement of entities that exploit the privileges granted to them [6]. Indications of a compromise are present at every stage of the lifecycle of an assault, and there may even be strong warning signs of an impending attack. A challenge lies in the task of locating these markers, which may be spread across the environment. The cycle of situational awareness for cyber security is depicted in Figure 1.

This study offers a thorough analysis of the research on situational awareness in network security. The aim of this guide is to aid in the understanding of linked ideas, the promotion of their application, and the development of new connections. Meanwhile, a generic analysis framework of network security situational awareness has been constructed from the standpoint of the value chain. The framework breaks down the five main phases of situational awareness for network security: acquiring relevant factors, representing the model, establishing appropriate measurements, analysing possible solutions, and forecasting future events. At each step, we discuss the outcomes of typical procedures in practise and provide an overview of the relevant research. Not only does this article provide an overview of the most pressing difficulties and emerging research trends in this area, but it also digs deeper into the visualisation of perception analysis results and situational awareness in the context of enormous data environments.

2. LITERATURE REVIEW

2.1 Cyber situational awareness

By describing and analysing the published research on CSA from the angles of national cyber policy and science, Franke et al. [7] conducted a systematic literature review. This was found by Franke et al. In order to detect, identify, and respond to a wide variety of threats and attacks in the field of cyber security, SA needs a deep understanding of the organization's current and historical cyber actions. Organizations are able to quickly recognise, process, and grasp information thanks to the information that is provided by CSA, which is both comprehensive and

specialised in nature and relates to cyber threats and vulnerabilities. Low-level network sniffing is one example, but these suspicious and intriguing behaviours can also be gleaned from external data sources like social media. They can also be rather interesting. In turn, CSA assists organisations in gaining an understanding of their present and future risk situations, as well as their position in terms of the protection systems they have in place.

In order to accomplish CSA, the roles that humans and robots need play in a Cyber Common Operating Picture were outlined by Conti et al. [8]. They contended that it is crucial to distinguish between jobs that require human cognition and those that can be easily mechanised and processed by computers while constructing CCOPs.

2.2 Cyber situational awareness visualizations

Several research investigate the use of visualisations in relation to the investigation of networks and malware. A good case in point is the SLR on network security visualisations provided by Shirave et al. [9]. Five broad types of network security visualisations were discovered by the authors. Monitoring host servers, both inside and outside the network, monitoring port traffic, spotting attack trends, and analysing routing behaviour are just some of the subjects covered in these training sessions.

When it comes to managing networks and services, Guimaraes et al. [10] provide an SLR of information visualisation. When researching the use of information visualisation in managing networks and services, they came across some well-explored subjects. Some of the things that can be measured and monitored using IP networks come into this category. Furthermore, they looked into the duties and interactions involved in employing network and service management information visualisations, as well as the visualisation approaches used in such visualisations. This research was carried out in the United Kingdom. In terms of network and service management visualizations, their research indicates that standard 2D/3D displays are most commonly employed. They also suggest several avenues for further study of information visualisations in the context of network and service management. A few examples are the IoT, Big Data, Cloud Computing, SDN, and Human-Centered Evaluation.

Wagner et al. [11] compile a list of available malware analysis visualisation tools. To do this, they applied a malware visualisation taxonomy to the existing literature and categorised it according to a standard method of data processing and visualization. The authors further classified the results based on the file and format types that were used in their creation, the visualisation techniques that were applied, the representation space and the mapping to time, the time periods that were considered, the authors' interactive abilities, and the available user actions.

Staheli et al. [12] provide a comprehensive review of several visualisation assessments related to cyber security. The authors outline potential future possibilities after identifying the most prevalent forms of evaluations used for security applications.

Franke et al. [7] carried out a systematic literature review that zeroed in specifically on CSA. Their review covers a wide range of topics and incorporates papers that have nothing to do with visualisation. From the earliest works on CSA and SA in industrial control systems to the most up-to-date emergency management and SA structures, algorithms, and visualisations, this book covers it all. Franke et al. [7] suggest that it is crucial to look beyond the technical aspects of visualisations in order to completely appreciate the connection between CSA levels and the visualisations of CSA. This is done so that a more in-depth comprehension of the correlation between CSA levels and CSA visualisations can be attained.

3. THE THEORETICAL MODEL OF SITUATIONAL AWARENESS

The term "situational awareness" in the context of network security refers to the use of technical means to obtain, from a wide range of time and space in a massive network environment, all elements of network security, including the status of various network equipment, network behaviour, and user behaviour. And by integrating and analysing the collected data from various sources, we can assess the current state of network security and project its future evolution.

Endsley established the theoretical groundwork for situational awareness through methodical research on its evaluation process. Schematically depicted in Fig. 2 is the theoretical paradigm of situational awareness:

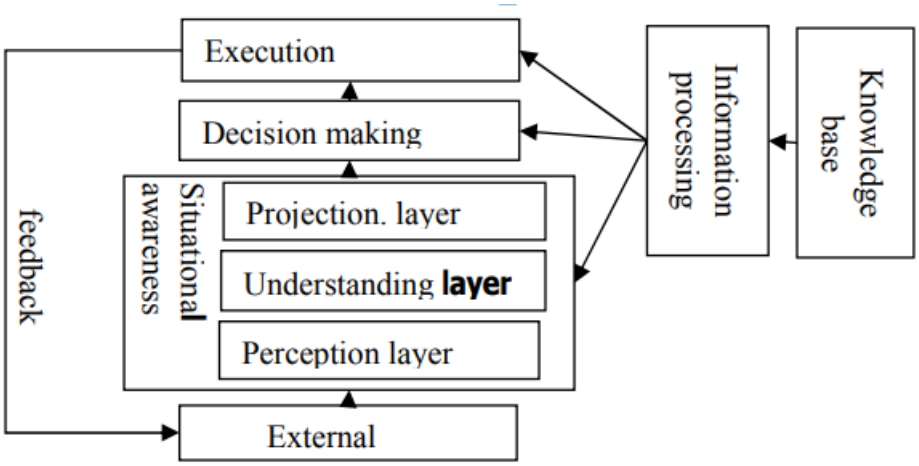


Fig. 2. Situational Awareness: A Theoretical Model

Perception, comprehension, and projection are the three components that make up situational awareness.

Perception layer: This system is in charge of taking in information about the external world, such as its current state, its qualities, and the dynamic changes taking place there. The human senses, including sight, sound, and touch, are responsible for such detailed work.

Comprehension layer: It is based on the perceptual layer, determining how important certain aspects of the environment are to accomplishing goals, and putting all of those aspects together to have a better understanding of everything.

Prediction layer: By integrating the perception and knowledge layers, we can anticipate the future state of each component of our environment and the behaviour of those components with the highest possible degree of accuracy.

The model for Network Security Situational Awareness

In order to thoroughly, accurately, and objectively assess the state of operation of a network, researchers have examined a wide variety of perceptual models. Figure 3 shows a typical situational awareness model for network security.

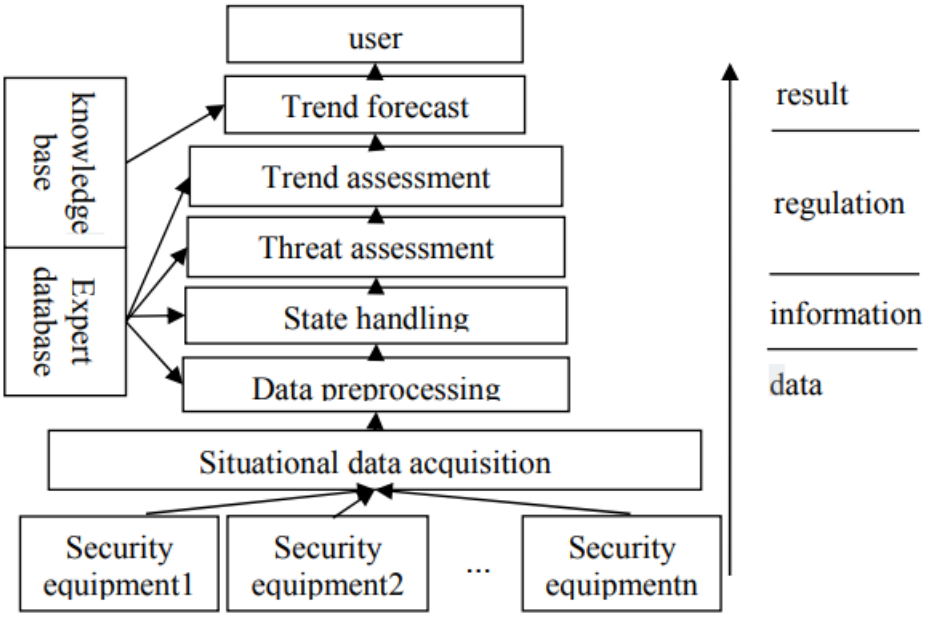


Fig. 3. Typical Model for Network Security Situational Awareness

There are 5 distinct phases of realisation identified in this model of situational awareness. Human-computer interaction is achieved by situational visualisation after IT resources are gathered, analysed, and fed back on several levels.

The five processing levels are:

Data preprocessing: Some forms of preparation, such as user distributed processing, impurity filtering, etc., can be performed on unstructured data, but doing so is optional. Take out the event and get the data. What this means in practise is that after collecting data, decisions are made to standardise and adjust the occurrences in question. This

also implies that the most fundamental aspects of an occurrence are expanded.

Situation assessment: includes statistical analysis and qualitative evaluation of the situation The scenario analysis report and the network comprehensive situation map are the products of the evaluation, which also serves to inform administrators' decision-making processes.

Impact assessment: It will project the present state of affairs into the future and evaluate how the participants' beliefs or prediction behaviours affected the outcome.

Resource management, process control and optimization: Indicators for optimization can be set up to allow for real-time monitoring and evaluation of the entire integration process, and optimal allocation of relevant resources can be attained.

3.1 Visual analytics for network activity

Many different kinds of network monitoring are typically associated with use cases that involve network activity. Nevertheless, not only for monitoring but also for more in-depth research from a variety of perspectives, one might employ these strategies. As a result, we split up this category into three different use cases: I monitoring of host and server activity; (ii) monitoring of port activity; and (iii) monitoring of both internal and external traffic. In the end, getting a comprehensive picture regarding ongoing network activity and contributing to the state of situational awareness will require looking into all of these different areas as well as engaging in interactive investigation. This is necessary for a variety of reasons, including but not limited to the following: management concerns; keeping an overall perspective on how the network is typically utilized; and the detection of threats, attacks, or intrusions. However, this also has implications for computer network security because compromised systems typically display network activity patterns that are distinct from those of unaffected devices.

3.2 Visual Overview for Internal and External Monitoring

There are two main ways to approach analysing network activity: from within the network or from the outside looking in. Many companies and organisations previously relied on network routing devices like routers and firewalls in combination with a service like network address translation (NAT) to keep their internal networks secure. When it comes to monitoring the activities of the network, it is typically possible to differentiate between the machines that are part of the internal network and those that are part of the external network due to the topological layout.

However, in the most recent few years, this clear distinction has become problematic as a result of the fact that a significant number of successful attacks can be categorised as insider threats or were actually carried out on a compromised internal host. This is because of the fact that a significant number of successful attacks have been carried out on a compromised internal host. This is because the trustworthiness of internal hosts has been called into question. It is likely that the employee who received the well designed e-mail that was used in the initial attack on this internal server did not suspect anything fishy about the malware file that was attached to the e-mail and opened it when it arrived in their inbox. When criminals try to trick their victims into trusting them by using social engineering, the probability of this happening is significantly increased.

4. METHODOLOGY

This section begins with a condensed description of the experimental environment that was used in this study as the basis for the subsequent chapters, which will be used to compare and summarise the various strategies that were employed at various stages of the proposed framework. This section serves as the basis for the following section, which serves as the basis for the subsequent chapter. This section then moves on to discuss the implications of these findings. As the subject of this investigation, we have settled on a middle-sized software development company.

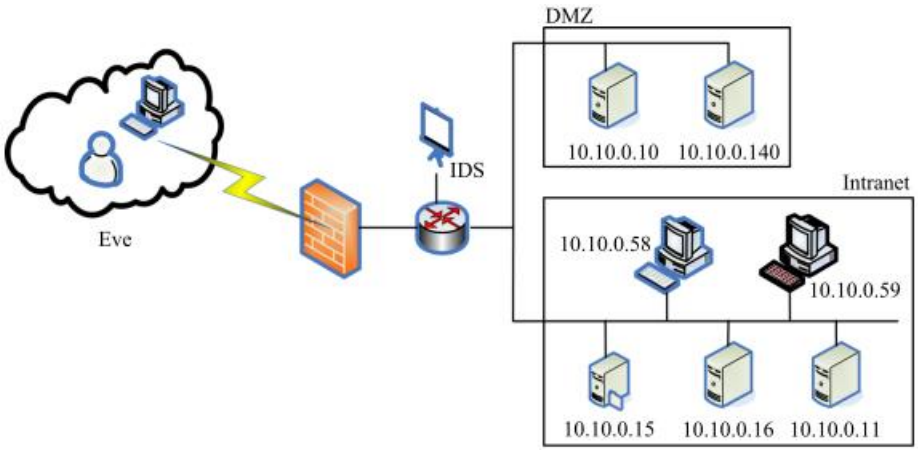


Fig. 4 The topology for experimental network.

A schematic of the company's network structure is shown in Figure 4. The system itself Through the use of dedicated telecommunication lines and external network linkages, God is a monitoring system that keeps tabs on both the internal network and the external network. The web server located at 10.10.10.10 is used for displaying advertisements and product demonstrations. 10.10.0.140 is the Internet Protocol address for the log server connection (because company personnel are often on business trips, both internal and external network access are required to go through the external network). In addition to SQL Server, Oracle, and the two relational databases that are utilised by the business, the no-relationship database known as MongoDB has been installed on the server located at 10.10.0.15. The most up-to-date versions of the deployments for all of the company's delivered and in-development products can be found on the test server (10.10.0.16). That machine at 10.10.0.11 is our private test environment. This server stores the entirety of the company's source code, as well as any critical project solutions, process information, etc. About one hundred employees work on the company's development team, who are mostly split in two groups according to the various development technologies used. The.net technical team is represented by 10.10.0.58, while theJava technical team is indicated by 10.10.0.59.

4.1 Logical analysis framework

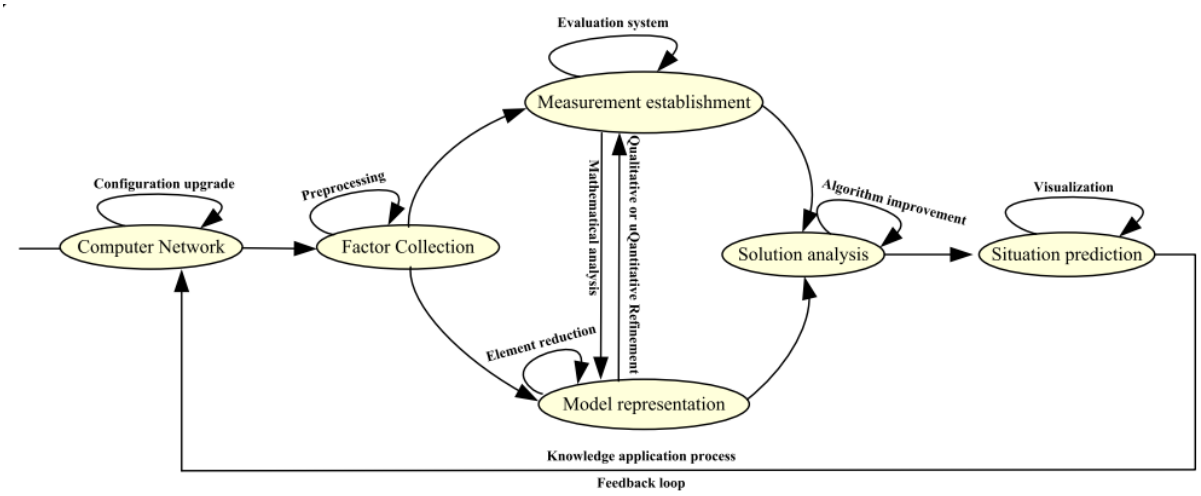


Fig. 5 network-based operational framework for situational awareness about network security

The standard procedure for cyber situational awareness is broken down into five discrete processing stages using the systematic engineering approach taken in this research. Figure 5 depicts these steps, which comprise data collection, model representation, metric setup, solution analysis, and future prediction. In this study, we apply the systematic engineering approach to the data value chain.

(1) The data collection and data preparation tasks make up the bulk of the element acquisition phase, the primary focus of which is on how to successfully acquire the security-related data in the greatest quantity possible. During this stage, the focus shifts to figuring out how to collect the data in the most productive way feasible. The act of effectively storing information is referred to as "data capture," and it has a specific name. This procedure includes the collecting of information regarding network configuration, information regarding network behaviour seen within the log, and information regarding network vulnerabilities. Utilizing a scanner, a sensor, or a tool that has been developed particularly for the purpose of data collection is one way to gather the required information. Another option is to use a tool that has been designed for the task. Before data modelling or analysis and utilisation, there is a step known as "data preprocessing," in which the original data is made more orderly.

(2) The stage of model representation places a primary emphasis on the correlative expression of the effective elements, which is essentially broken down into two tasks: element reduction and formal representation. During this stage, the model is represented graphically. Both of these jobs are subdivided further into subtasks. In order to accomplish the goal of the analysis in a manner that is both successful and efficient, it is important to perform an effective reduction of the objects that have been obtained throughout the process of element acquisition. The formal statement is making a reference to the process of precision abstraction, which includes the characteristics of the reduced elements as well as the link between the elements and the order relationship.

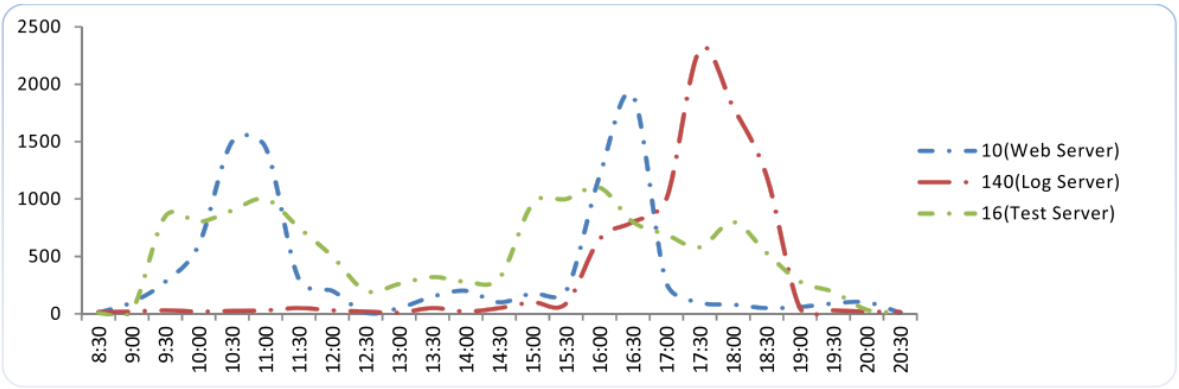
(3) Before diving into an investigation of the answer, it's important to do some fine-tuning of the values assigned to each component object, or "metric setup." At this point, a substantial amount of the quantitative classification and evaluation index system is utilised in order to articulate the two goals. For the purposes of this investigation, the qualitative classification is assumed to be a subset of the quantitative classification. Furthermore, the process of confirming the evaluation index system is defined as the act of standardising the connection that exists between the attribute values of the elements. The quantitative method involves assigning

mathematical values to each element's attributes, whereas the qualitative classification is simply viewed as a subset of the quantitative method. The quantitative method involves assigning mathematical values to each element's attributes.

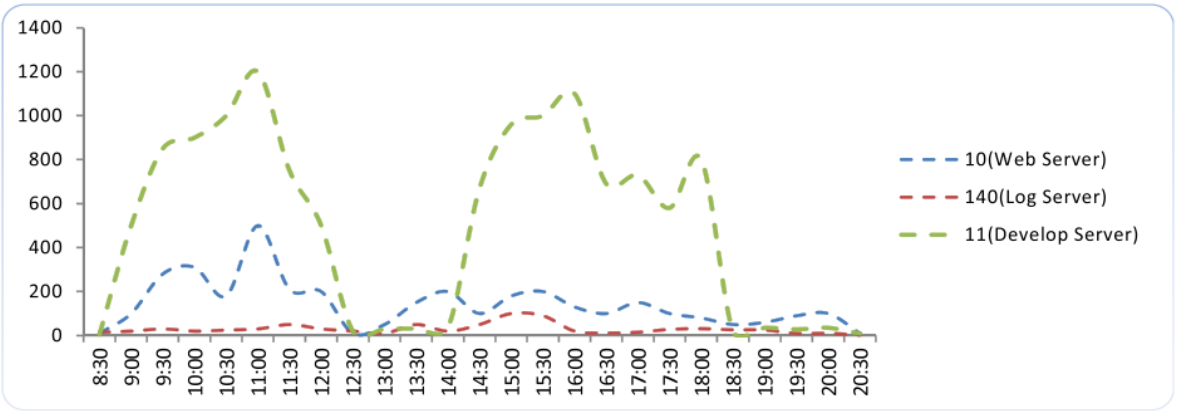
(4) The first three steps constitute the algorithmic process known as solution analysis. The main steps in this procedure include finding the solution algorithm, checking that it is correct, and refining it. The process of correctly combining the target with the model and the measure in order to decide the analysis step is referred to as the solution algorithm. In order to ensure the correctness of an algorithm, it must be checked if the inputs and results correspond correctly. On the basis of this, it should be considered to increase the efficiency of the algorithm so that it can expand in the environment of a true scale network.

(5) Predicting the future of a problem involves conducting an in-depth analysis and making decisions based on that judgement. This procedure consists mainly of two steps: visualising the analysis results and making a decision based on the knowledge gained. The process of generating and displaying the outcomes of the solution in a manner that is simple to comprehend is referred to as "result visualisation." After the data has been analysed and decisions have been made, the feedback loop will be applied to the existing network in order to strengthen cybersecurity by doing things like repairing vulnerabilities and upgrading configurations. This will complete a perceptual loop.

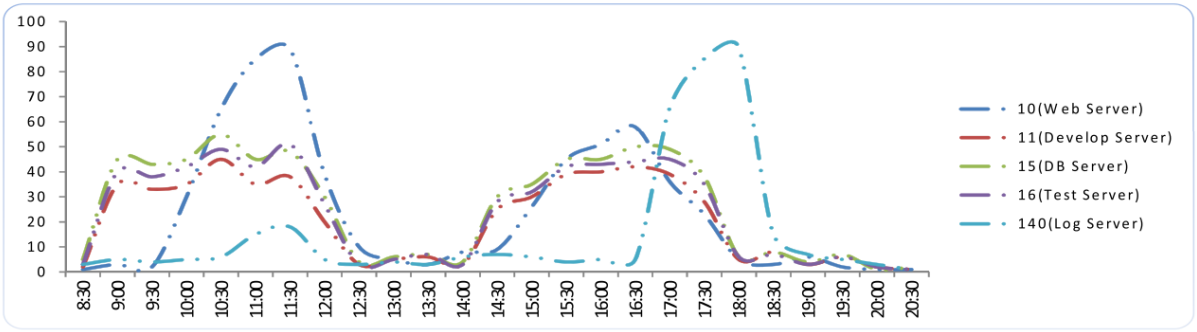
5. RESULTS IMPLECATIONS



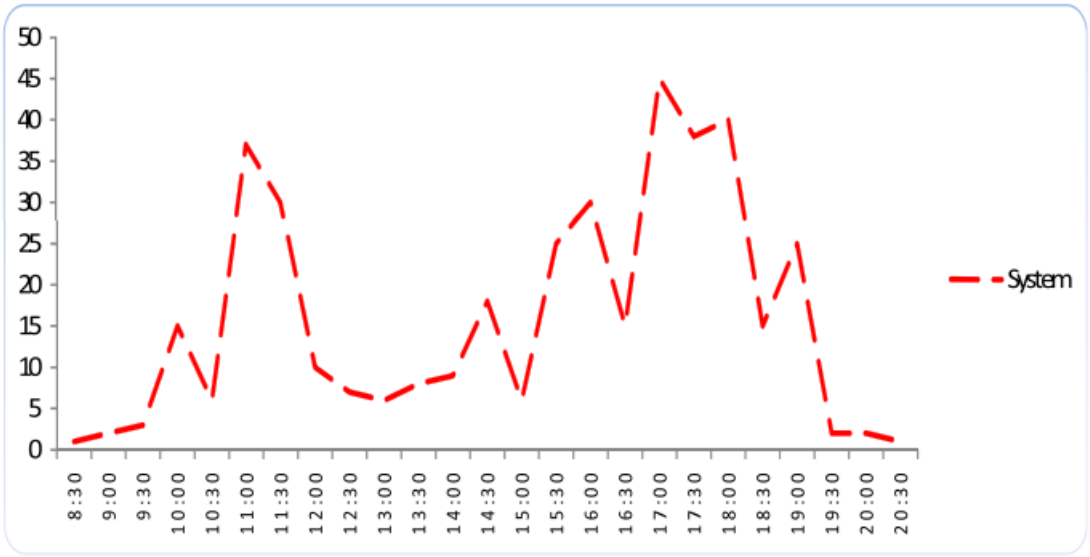
(a) Tomcat server security issue



(b) Threats posed by FTP on the server



(c) host level Threat situation.



(d) system level Threat situation

Fig. 6 The experimental network's resulting hierarchical situational awareness (a-d)

Quantification results for several security situations are displayed in Fig. 6; these include the Tomcat service, the FTP service, and the general security state of each host and local area network (a to d). The subjective quantization technique was used to produce these findings. Example measurable outcomes from the security scenario include the availability of Tomcat and FTP services and the general security status of each host and LAN. The hierarchical model aids in making sure that the results can be understood by intuition due to its consistency with the decision-thought maker's process throughout the analysis and calculation processes (for example, the security situation index is relatively high in Fig. 6 at around 17:30; because most people fill in the logs around this moment, the frequent external network mapping will lead to higher security risks).

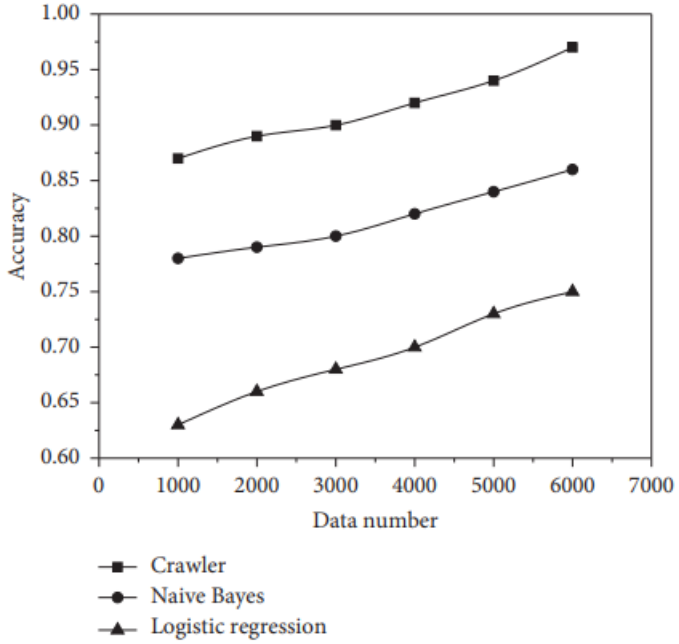


Figure 7: Classification model accuracy comparison.

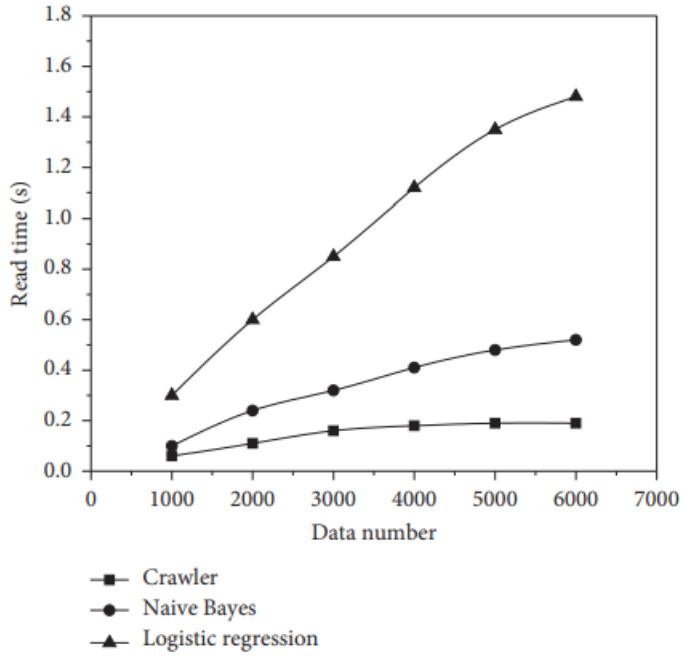


Figure 8: Classification model read time comparison.

Figures 7 and 8 show that the neural network improves classification accuracy by 12.79% and 29.33% over logistic regression and naive Bayes, respectively, while simultaneously reducing reading time by 63.5% and 87.2%. The reason for this is that the keywords for each category in the network security event classification are more unpredictable than in the news categorization. For instance, the category "entertainment" in the news information classification is where you'll most often see terms such as "star," "drama," and "variety show." Keywords like "athlete," "schedule," and "referee" are most commonly found in the "physical" section of the news. There are substantial distinctions between the various types of keywords. There is a high likelihood that the word "attack" will appear in certain subcategories of network security incidents. These subcategories can include things like "worm incidents," "mixed attack programme incidents," and "backdoor attack incidents," as few examples. It happens quite frequently in "vulnerability attack events" as well as "interference events," and as a consequence, the classification of network security events typically requires referring to the relationship between a large number of keywords all at the same time.

CONCLUSION

This article introduces the concept and core methods of network security situation awareness, and it focuses on the system engineering perception framework from the viewpoint of the data value chain. Obtaining the data,

representing the model, establishing the measurements, analysing the solutions, and forecasting the future are the five steps that make up the data value chain. Several steps of the process are introduced together with their key functions, methods, and the effects on applications that they have. During element acquisition, the perceptual data is compiled and summarised, and a brief overview of the database's standardised layout and implementation is given. Stages of model presentations include descriptions of each model's underlying principles, representative technology, and modelling results. This stage, known as "measurement establishment," involves quantifying the model elements and evaluating the index volume in light of those numbers. As part of the solution analysis phase, we talk about the underlying assumptions of the application, analyse common algorithms, and make a side-by-side comparison of the algorithms.

REFERENCES

[1] S. Li, L. Jiang, Q. Zhang, Z. Wang, Z. Tian, and M. Guizani, "A malicious mining code detection method based on multifeatures fusion," IEEE Transactions on Network Science and Engineering, 2022.

[2] O. Altay, T. Gurgenc, M. Ulas, and C. Özel,"Prediction of wear loss quantities of ferroalloy coating using different machine learning algorithms," Friction, vol. 8, no. 1, pp. 107–114, 2020.

[3] M. Ulas, O. Altay, T. Gurgenc, and C. Özel, "A new approach for prediction of the wear loss of PTA surface coatings using artificial neural network and basic, kernel-based, and weighted extreme learning machine," Friction, vol. 8, no. 6, pp. 1102– 1116, 2020.

[4] S. Li, Q. Zhang, X. Wu, W. Han, and Z. Tian, "Attribution classification method of APT malware in IoT using machine learning techniques," Security and Communication Networks, vol. 2021, Article ID 9396141, 12 pages, 2021.

[5] S. Li, Y. Li, W. Han, X. Du, M. Guizani, and Z. Tian,"Malicious mining code detection based on ensemble learning in cloud computing environment," Simulation Modelling Practice and Theory, vol. 113, article 102391, 2021.

[6] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Intrusion detection techniques in cloud environment: a survey," Journal of Network and Computer Applications, vol. 77, pp. 18–47, 2017.

[7] U. Franke and J. Brynielsson, "Cyber situational awareness - A systematic review of the literature," Computers and Security, vol. 46, pp. 18–31, 2014. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2014.06.008

[8] G. Conti, J. Nelson, and D. Raymond, "Towards a cyber common operating picture," in 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE, 2013, pp. 1–17.

[9] H. Shiravi, A. Shiravi, and A. A. Ghorbani, "A survey of visualization systems for network security," IEEE Transactions on visualization and computer graphics, vol. 18, no. 8, pp. 1313–1329, 2011.

[10] V. T. Guimaraes, C. M. D. S. Freitas, R. Sadre, L. M. R. Tarouco, and L. Z. Granville, "A survey on information visualization for network and service management," IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 285–323, 2015.

[11] M. Wagner, F. Fischer, R. Luh, A. Haberson, A. Rind, D. A. Keim, and W. Aigner, "A survey of visualization systems for malware analysis," in Eurographics Conference on Visualization (EuroVis), 2015, pp. 105–125.

[12] D. Staheli, T. Yu, R. J. Crouser, S. Damodaran, K. Nam, D. O'Gwynn, S. McKenna, and L. Harrison, "Visualization evaluation for cyber security: Trends and future directions," in Proceedings of the Eleventh Workshop on Visualization for Cyber Security, 2014, pp. 49–56.

[13] G. A. Fink, P. Muessig, and C. North. Visual Correlation of Host Processes and Network Traffic. In Visualization for Computer Security, IEEE Workshops on, volume 0, page 2, Los Alamitos, CA, USA, 2005. IEEE Computer Society. ISBN 0-7803-9477-1. doi:10.1109/VIZSEC.2005.18. [pages 15, 20, 28, and 70]

[14] F. Fischer and D. A. Keim. VACS: Visual Analytics Suite for Cyber Security - Visual Exploration of Cyber Security Datasets. In VAST Challenge 2013 - Honorable Mention, 2013. [pages 6, 14, 20, 28, and 42]

[15] F. Fischer and D. A. Keim. NStreamAware: Real-Time Visual Analytics for Data Streams to Enhance Situational Awareness. In Proceedings of the Eleventh Workshop on Visualization for Cyber Security, VizSec '14, pages 65–72, New York, NY, USA, 2014. ACM. ISBN 978-1-4503-2826-5.