Research Article

Mozamel M. Saeed*

Comparing the influence of cybersecurity knowledge on attack detection: insights from experts and novice cybersecurity professionals

https://doi.org/10.1515/comp-2024-0016
received March 2, 2024; accepted August 30, 2024

Abstract: This article investigates the effect of cybersecurity knowledge on the ability to detect malicious events in a network. We developed a simplified intrusion detection system (IDS) to simulate real-world scenarios and assess detection capabilities. The IDS features typical network intrusion characteristics, such as signature-based detection and anomaly detection, providing a realistic environment for participants. A cross-sectional study was conducted by recruiting 75 respondents who were from Al Neelain University, with novices observing ten distinct cyber-attack scenarios, including phishing, malware, and denial-of-service attacks. At the same time, experts examined three complex scenarios involving advanced persistent threats and zero-day exploits. Among these participants, 35 were considered novices (students) in cybersecurity, while 40 were security professionals from technical communities. The study procedure involved novices observing ten scenarios and completing a questionnaire assessing their detection accuracy, while experts observed three scenarios and filled out a similar questionnaire. The specific measures used to determine detection capabilities included the accuracy of identifying malicious events, the rate of false positives (mislabelling benign events as malicious), and the rate of false negatives (failing to identify malicious events). The findings of this study demonstrate that cybersecurity knowledge facilitates the accurate detection of malicious events and reduces mislabelling benign events as malicious. A deep understanding of a particular network is necessary for making precise detection decisions, which rely on cybersecurity knowledge. Experts exhibit the capability to differentiate different types of cyber-attacks. They accurately assess various network settings and determine the maliciousness of networking events with greater precision. In conclusion, this study highlights the importance of cybersecurity knowledge in detecting and differentiating cyber-attacks. The expertise of experts in network analysis and precise determination of malicious events emphasizes their significance. These findings have practical implications for enhancing attack detection capabilities.

Keywords: intrusion detection system, knowledge, security, data-breach prevention, attack detection capabilities

1 Introduction

The rapid advancement of smart grid technologies has revolutionized the utilization and asset management of power grids, enhancing their capacity to respond effectively to grid problems [1]. However, this increased connectivity has also given rise to cybersecurity concerns in industrial control system (ICS) environments, both at national and global levels. The emergence of Internet of Things devices has introduced new vulnerabilities, allowing malicious actors to exploit botnets for various purposes, including distributed denial of service attacks, information collection, and unauthorized cryptocurrency mining [2].

The operational profitability and success of businesses rely on the functional integrity of modern ICS systems. Unfortunately, there has been a concerning rise in cyber-attacks and threats targeting ICSs worldwide. Addressing these cybersecurity challenges is crucial to protecting critical infrastructure and maintaining trust in industrial domains. The prospects of cybersecurity are being remarkably restructured through the emergence of advanced technologies. Artificial intelligence (AI) has emerged as a significant technology influencing cybersecurity. Consequently, machine learning brings an opportunity specifically deep learning (DL) in cyberspace as a countermeasure for cyber-attacks. Moreover, machine learning delivers more potency in anomaly detection. Generally, DL provides paramount concert to machine learning due to its layered atmosphere and its operational algorithms for extricating effective

* **Corresponding author: Mozamel M. Saeed,** Department of Computer Science, Prince Sattam bin Abdulaziz University, Al Kharj, Saudi Arabia, e-mail: m.musa@psau.edu.sa, mozamel8888@gmail.com

information from training data [3]. Previous studies have discussed machines and DL as battling tools for cyber threats and their implementation for cybersecurity [4–7]. Therefore, Choudhary et al. [8] advocated that the integration of AI with machine learning, cloud computing, and blockchain technology has revolutionized the practices of cybersecurity. In addition, as the landscape of security threats progresses, the approaches of DL represented by recurrent neural networks (RNNs) and convolutional neural networks have manifested substantial favourable outcomes across various areas such as face, image recognition, and voice detection. Long short-term memory, a specified method of RNN, evolved as the dynamic and effective contender for intrusion detection, outperforming in demonstrating sequential data and captivating long-term contingencies [9]. Leevy et al. [10] highlighted that the algorithms of machine learning effectively trained on the datasets of intrusion detection can determine the traffic for the network which can be threatening to the information system.

However, these technological innovation provides advanced results and improved competencies but also bring forward new intricacies and complications in the domain of cybersecurity, as it is an imperative dimension of attention for institutions struggling to protect their digital assets in a continuously growing interrelated world [11]. Llanten-Lucio et al. [12] also discussed amalgamation of technological advancement with the strategies of cybersecurity does not happen without complexities since it needs companies and corporations to perpetually upgrade and remodel their measures of cybersecurity to manage new jeopardized related to these innovations. Moreover, these emerging technologies also influence the dimensions of global geopolitics. Popescu [13] stated that technological innovations including AI, cloud computing, and 5G have an influential impact on the dynamics of geopolitics. Thus, the involvement of these technologies with cybersecurity surpassed the boundary of individual organizations and involved security concerns at nationwide and worldwide levels. The critical use of these emerging technologies by government and non-government agencies in surveillance activities and cyber warfare reinforces the demand for strong cybersecurity methods in organizations. Furthermore, the challenges and complications of cyber threats have increased due to the integration of advanced technologies. Cyberpunks and hackers are exploiting these emerging technologies to generate more innovative attack procedures, which incur serious complications to the available cybersecurity defences [11]. Alshaikh et al. [14] observed that machine learning cybersecurity interacts with presented data due to its trained function and is unable to handle new and formerly obscured data. In addition, machine learning is a learning instrument without cognizance and other human characteristics that distinguish machines from humans. Further, Zwilling et al. [15] argued that these countermeasures do not comprehensively alleviate the cybersecurity violation. Thus, these emerging technologies with cybersecurity solutions cannot be perceived as the all-inclusive solution to stop cyber-attacks encouraging cooperation and institutions to proceed towards more human-centric methods to reduce their threats and vulnerability to cyber-attacks [16].

Since the usage of data and internet consumption persistently grow to continue, the knowledge and awareness related to cybersecurity have become exceptionally crucial. In recent years, cybersecurity experts have focused on securing substations and developing standards such as IEC 62443 and IEC 62351 for supervisory control and data acquisition systems, ICS security, and power system information infrastructure [17]. However, despite their extensive training, cybersecurity analysts may still possess incomplete or outdated domain knowledge due to the dynamic nature of the field. Furthermore, the lack of cybersecurity awareness among employees poses additional vulnerabilities, as human error and exploitation of limitations can compromise system security [18].

Indeed, the focus of research on the contribution of human behaviour in the mitigation of cyber risks has increased in recent times [15]. However, comprehensive insights related to how knowledge, awareness, and behaviour towards cybersecurity vary across individuals when encountered with different types of cyber threats are still relatively limited. Therefore, this study aims to investigate the knowledge and skills of beginners and professionals in the domain of threat detection in cybersecurity, specifically in Sudan. The study examines the reasoning processes employed during the detection of cyber-attacks and compares the cognitive skills of experts with the domain knowledge of novices. To the best of our understanding, this study endeavours to contribute to the existing literature by evaluating variations in cyber-attack awareness knowledge and behaviour towards its defence among the cybersecurity professionals and students at the Al Neelain University of Sudan. The results of this study will provide valuable insights to security auditors, managers, and analysts in conducting comprehensive threat and vulnerability assessments at the human level. To achieve the aim of the study a cross-sectional study was conducted by recruiting students of Al Neelain University. These participants were instructed to perform their task online and earned one point for correct classification of attack and no-attack and *vice versa*.

The study contributes significantly by raising awareness of information security among both experts and novices, examining the impact of cybersecurity knowledge on accurately detecting malicious events within networks.

It involves the development of a simplified Intrusion Detection System (IDS) to investigate the efficacy of individuals with varying levels of cybersecurity knowledge. The research is likely to demonstrate that experts are notably better at differentiating and detecting various types of cyber-attacks compared to novices. This highlights the importance of deep domain knowledge in cybersecurity. The findings would suggest practical implications for enhancing attack detection capabilities and advocate for increased investment in cybersecurity training and education to improve threat detection and response.

The remainder of this article is structured as follows: Section 2 presents a focused literature review, highlighting the gaps and controversies in the existing research. Section 3 describes the materials and procedures used in the study, while Section 4 presents the findings. Subsequently, Section 5 provides a comprehensive discussion of the results, Section 6 discusses the study implications, and Section 7 concludes the article by summarizing the key findings and their implications. Finally, Section 8 outlines the action plan.

2 Literature review

A cyber-attack is an unauthorized attempt to access private and confidential data with the intent to steal, damage, or eliminate entire systems or networks. Individuals, businesses, and organizations must understand the inheritable risks of utilizing a network and how to defend against inevitable attacks. In active attacks, an attacker aims to disrupt the system by injecting malicious traffic which is malicious or performing illegal commands [19]. Common active attacks consist of malware and DoS-type attacks. Malware or malicious software simplifies damaged computer systems [20]. This is also known as any software code whose intent is to cause harm and damage. Scareware is a properly tagged malware as it intends to scare victims into sending them money.

Since cybersecurity analysts go through extensive certification programs and training, they possess broad knowledge of information security and network operation. There is a possibility of incomplete and outdated domain knowledge as security analysts operate in a highly dynamic environment. In such a setting, problem-solving, decision-making, inventive thinking, and learning depend on the thinking strategies, as it is generally considered that the central aspect of cybersecurity expertise is the mastery of independent cognitive skills. Alhashmi et al. [18] have also asserted that a lack of cybersecurity awareness is also a major factor responsible for the increased vulnerability of an organization regarding cyber-attacks where human error and limitations are exploited illegally to intervene in the systems and deteriorate the security fabric. Therefore, employing security awareness methods such as contextual training, web-based training, and embedded training can be useful in increasing information and system security within an organization.

Alharbi and Tassaddiq [21] investigated the level of cybersecurity awareness among the university students of Majmaah, Saudi Arabia, and explored the defence skills and knowledge of students regarding cybercrimes and information security. They concluded that the security management plan should involve awareness and training programs for learners related to cybersecurity and should also be supported by top management so that students become able to recognize and handle these cyber susceptibility and threats. Similarly, Ghelani [22] advocated that expertise in cybersecurity is the significant constitutes of effective operation of businesses as the ability of companies and corporations to successfully handle cyber hazards relies on their capabilities to execute appropriate knowledge. Cain et al. [23] examined cyber knowledge (“Cyber Hygiene”) among aged between 18 and over 55 of 268 users of the computer. The study focused on how they manage tools of online security like software anti-virus and firewalls. The research was carried out utilizing Amazon Mechanical Turk, which is a marketplace for crowdsourcing. The result of the study found that experts who were self-identified had less knowledge of cyber-attacks theoretically as compared to those who were non-experts.

Al-Ghamdi [24] conducted a study to evaluate the degree of awareness among different IT employees related to cyber hazards since the expertise and knowledge of the cybersecurity team are essential in alleviating cyber threats. This study found a huge knowledge gap among the security operation team and other IT workers that should be narrowed. It is worth mentioning that security operation teams are more capable of handling cyber hazards after recognition of these attacks. Furthermore, Dash et al. [25] highlighted the significance of the behaviour of workers and the efficiency of security awareness programs based on AI to deal with cyber hazards. They concluded that the behaviour of workers is observed as the significant determinant for a strong information system, as inadequate knowledge can damage even the most consistent information system. Consequently, the implementation of AI-driven interactive security programs is growing in start-ups and hi-tech enterprises. Moreover, Frati et al. [26] highlighted the importance of cybersecurity training programs to create awareness among healthcare staff since the cybersecurity system of healthcare organizations is vulnerable to versatile cyber hazards and turned out to be interesting targets for cyberpunks as they have profound data. They observed that the

promotion of awareness regarding cyber-attacks among personnel so that they can adopt protected practices while handling the patients' information and the adoption of performant technologies by the organization are requisite for a strong defence system of cybersecurity.

Zwilling et al. [15] examined user-specific factors associated with the degree of cybersecurity knowledge and skills among cyber experts across different economies with varying values of GDPs and found that cyber awareness has a strong association with cyber knowledge irrespective of included nations or gender. Additionally, protection instruments were also associated to.

Baraković and Baraković Husić [27] explored and investigated the degree of cyber awareness, hygiene, knowledge, and behavioural practice by surveying university students and they found that students have low cyber knowledge and awareness quite unsatisfactory but they have an adequate level of behavioural hygiene. Sheng et al. [28] developed the concept of gamification successfully to educate about phishing, which they explain in their research as "Anti Phishing Phil: an examination and design of a game that educates individuals to not get trapped under phishing attack." The game concentrated on predicting those URLs that may be malicious. The result of the study showed that games influenced individuals to be attentive more when detecting phishing attacks in the future. The study initiates an idea of the significance of gamification for identifying phishing attacks to evaluate the users. Chi [29] stated that an expert in cybersecurity might be considered a person with a high level of knowledge and proficiency in networks and information security as compared to a person who has less amount of knowledge ("novice"). Asgharpour et al. [30] revealed how users with several knowledge levels in information security and years of exposure might have dissimilar mental models of cybersecurity. A high level of experience in information security recommends enhanced performance in detecting cyber-attacks as compared to those who have a low level of knowledge. Those individuals who are experienced in this field make more correct decisions than those who are not experienced. The researcher stated that it is expected from an expert to detect more meaningful and featured patterns.

3 Methods

3.1 Study design and participants

A cross-sectional study was conducted by recruiting 75 respondents who were from Al Neelain University, Sudan. To ensure the representativeness and generalizability of the findings, careful participant selection criteria and recruitment process were implemented. The selection criteria included a diverse range of participants, including students and professionals, with varying levels of cybersecurity knowledge, encompassing different genders, age groups, and educational backgrounds. The recruitment process involved collaboration with Al Neelain University and other relevant institutions, engagement with student organizations, utilization of professional networks, information sessions, snowball sampling, and provision of incentives. By adopting these strategies, the study aimed to include a representative sample that reflects the broader population, thereby enhancing the applicability and transferability of the findings to similar contexts and populations within the field of cybersecurity.

The respondents were invited to the computer laboratory of the university. They were considered novices in cybersecurity because they were not part of the cybersecurity workforce. These 35 students earned one point for correctly identifying an under-attack network and a network with no cyber-attack and lost one point for incorrect classification. Besides, 40 security professionals were recruited from technical communities such as professionally oriented networks (LinkedIn) or computer emergency response teams. These participants were instructed to perform their task online and earned one point for correct classification of attack and no-attack and *vice versa*.

3.2 Study instrument

The current study aims to differentiate the level of understanding of novices with little or no expertise from experts who have a profound knowledge of cybersecurity. For this purpose, the study adopted a questionnaire designed by Ben-Asher and Gonzalez [31], which was carefully developed based on inputs from expert security analysts. The questionnaire consisted of a comprehensive set of items aimed at assessing participants' knowledge and understanding of various aspects of cybersecurity. The questionnaire comprised a total of 50 items, covering different domains within cybersecurity, including network security, information security, cyber-attack types, and the use of security tools. Each item was designed to evaluate participants' theoretical knowledge and practical understanding of the field. For each item, participants were provided with multiple-choice response options to select from, allowing them to indicate their level of familiarity or understanding. The response options were structured to capture a range

of possible answers, including correct and incorrect choices, as well as partially correct or uncertain responses.

To ensure the validity and reliability of the questionnaire, several measures were taken. The content validity of the questionnaire was established by consulting with a panel of cybersecurity experts and incorporating their feedback into the item selection and formulation. Additionally, the questionnaire underwent a pilot testing phase with a small group of participants to assess its clarity, comprehensibility, and relevance. Regarding reliability, internal consistency measures such as Cronbach's alpha coefficient were computed to assess the reliability of the questionnaire. A high Cronbach's alpha value, above 0.70, was obtained, indicating good internal consistency and reliability of the questionnaire items.

3.3 Study procedure and analysis

The generation and validation of network scenarios in the study were conducted with meticulous care to ensure their accuracy and relevance. The process involved several steps to create and validate the scenarios, as described below:

- Scenario generation: The generation of network scenarios was based on established principles and guidelines in the field of cybersecurity. The researchers considered various types of cyber-attacks such as MITM attacks or SQL injection and their potential impact on network systems. They carefully selected a set of attack scenarios that represented realistic and commonly encountered situations in cybersecurity.
- Base rate assignment: A base rate of malicious events was assigned to the network scenarios. This base rate represented the probability of encountering a malicious event within the network. The assignment of the base rate was informed by prior research and empirical data to ensure a reasonable approximation of real-world scenarios.
- Attack definition and classification: Each network scenario was designed to simulate a specific type of attack, such as MITM attacks or SQL injection. The researchers precisely defined the characteristics and behaviours associated with each attack type, ensuring consistency and clarity in the scenarios.
- Probable attack tendency: The probable tendency of attacks within the potential state space and the network state was considered during scenario generation. This involved considering the likelihood of certain attack patterns and behaviours occurring in different network states. The researchers followed established methodologies, such as those described by Lye and Wing [32], to determine the probable attack tendencies within the generated scenarios.
- Validation and expert input: The generated network scenarios were subjected to rigorous validation procedures. This involved seeking expert input from cybersecurity specialists, including practitioners from the university's information and network security office and faculty members from the Department of Computer Science with expertise in intrusion detection. These experts reviewed the scenarios, ensuring their alignment with real-world cyber-attack scenarios and providing valuable insights and feedback.

The proposed network structure shows certain arrangements in the network events that show the development of cyber-attacks (Figure 1). Twenty network events took place in all scenarios. A value of 0.35 was assigned as the base rate of malicious events. Seven out of 20 events were considered malicious. The definition of the probable tendency of attacks in the potential state space and the network state, as stated by Lye and Wing [32], was followed to generate ten network scenarios. The difference in network scenario was based on the type of attack. Service is used to gain control over the webserver and store sensitive data. A design representing regular network operation was also constructed to monitor ongoing traffic within a network. It was observed that there was a decrease in the frequency of inaccurate detection in network scenarios in comparison with an increased ratio of fake signs generated by IDS. However, some differences were there in the real task of security professionals owing to simple interpretations that were taken into consideration for accommodating novices.

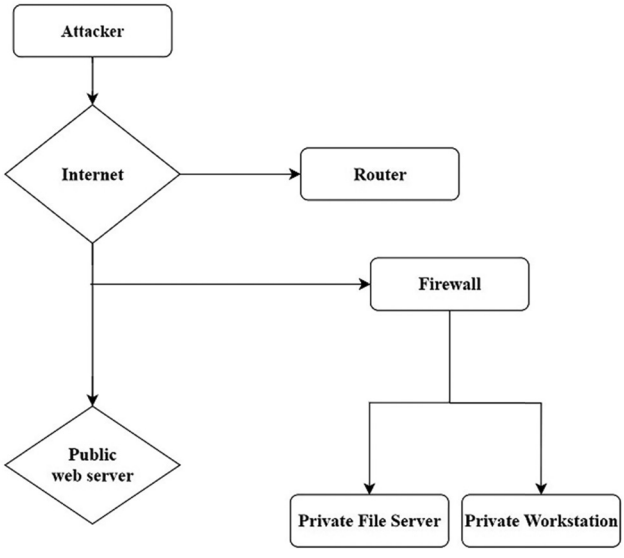

Figure 1: Progress of cyberattacks.

The participants in the study, both novices and experts, were asked to classify networks as being under attack or not based on the observed scenarios. The criteria or indicators used by the participants to make these classifications were based on their domain knowledge and understanding of cybersecurity. While the specific details of the criteria and indicators may vary depending on individual participants, some common factors that could have been considered include the following:

- Anomalous network behaviour: Participants may have looked for any unusual or abnormal network behaviour that could indicate a potential cyber-attack. This could include sudden spikes in network traffic, unauthorized access attempts, unusual patterns of communication, or unexpected network connections.
- Known attack signatures: Participants may have relied on their knowledge of known attack signatures or patterns. They might have compared the observed network behaviour with well-documented attack signatures to identify any matches or similarities.
- System alerts or warnings: Participants might have paid attention to system alerts or warnings generated by IDS or other security tools. These alerts could provide valuable information about potential attacks or suspicious network activities.
- Changes in network performance: Participants may have considered any significant degradation in network performance as a possible indication of a cyber-attack. This could include slower response times, increased latency, or network unavailability, which could be indicative of malicious activity impacting the network.
- Suspicious outbound or inbound connections: Participants might have focused on identifying any suspicious outbound or inbound connections from the network. This could involve examining the destination or source of network traffic and assessing whether it aligns with known malicious entities or patterns.

The study procedure involved novices observing ten scenarios and completing the questionnaire, while experts observed three scenarios and filled out the questionnaire. The rationale behind the different numbers of scenarios for novices and experts was based on the aim of the study to compare the detection performance between these two diverse populations, taking into consideration their varying levels of expertise and familiarity with cybersecurity. The decision to assign ten scenarios to novices and three scenarios to experts was made to balance the time and effort required from participants while still ensuring sufficient data for analysis. Novices, being relatively less experienced in the field of cybersecurity, were given a larger number of scenarios to provide them with more exposure and opportunities to apply their developing knowledge and skills. This larger set of scenarios aimed to capture a broader range of their detection capabilities and to provide a more comprehensive assessment of their performance. Conversely, experts, who already possessed a profound knowledge of cybersecurity, were assigned a smaller number of scenarios. This decision was made considering their expertise and efficiency in analysing and classifying network scenarios. By focusing on a smaller set of scenarios, the study aimed to assess the experts' ability to quickly and accurately identify potential cyber-attacks based on their extensive knowledge and experience.

Table 1 shows scenarios presented through the IDS tool. The respondents had to classify networks that are suspected to attack or have no tendency to attack as network events appeared. The participants had to positively determine the presence or absence of a cyber-attack. The novices filled out the questionnaire after randomly observing ten scenarios, and the online version of the IDS tool was used by the participants of the experts' group. They randomly observed three scenarios and then filled out the questionnaire. The experiment was completed in 25 min by experts, while the novices took 60 min to perform it thoroughly.

The difference in time required by experts and novices to complete the experiment is attributed to several factors related to their varying levels of knowledge, experience, and familiarity with the subject matter. Novices, who are relatively new to the field of cybersecurity, may require

Table 1: Scenarios in IDS

ID	Threat detection	Explanation
1		Running of ftpd and http services. The traffic between the internet and the web server is 3.3 Mbps. While the traffic between the web server and workstation is 3.3 Mbps
2	Running of ftpd on a web server	Running of ftpd and http services. The traffic between the internet and the web server is 3.3 Mbps. While the traffic between the web server and workstation is 3.3 Mbps. ftpd operation was executed
3		The workstation has been executing the user process the traffic between the internet and the web server is 3.3 Mbps. While the traffic between the web server and workstation is 3.3 Mbps

more time to carefully analyse and interpret the network scenarios presented to them. They may need additional time to understand the concepts, assess the indicators of attacks, and make informed classifications. Novices may also rely on the provided questionnaire to guide their decision-making process, which could further contribute to the longer duration. Conversely, experts, who have extensive knowledge and experience in cybersecurity, are likely to possess a higher level of familiarity with the patterns and indicators of attacks. They can quickly recognize relevant cues, evaluate network scenarios, and make accurate classifications based on their expertise. Due to their proficiency in the subject matter, experts can often perform the task more efficiently and with less deliberation, leading to a shorter completion time.

4 Results

The analysis of the questionnaire of experts revealed a clear differentiation between the two groups involved in this study. The majority of the participants of the expert group (80%) had experience of >1 year in the field of network operation and information security. In contrast, others had practical experience of >10 years. On the contrary, the majority of the participants in the novice group (90%) had no exposure to working in network operation and information security. Around 80% of the expert group participants had handled at least one or more cybersecurity events. In comparison, 60% of experts had spent one or more hours addressing network operation and security issues. Conversely, most of the participants of the novice group (60%) had handled cybersecurity issues once a year, and approximately 95% had not dealt with network operation and security issues daily. Moreover, 90% of novices had never used IDS, while 60% of experts had exposure to using IDS monthly.

The evaluation of theoretical knowledge revealed that all the experts were well aware of the definition and nature of the DoS attack. At the same time, only 36% of novices knew the definition of the DoS attack. Moreover, all experts and 85% of novices knew the correct definition of a phishing attack. The main target of the DoS attack is the network while phishing attacks mainly target the end-users. This knowledge helps evaluate the minor difference between both groups regarding their understanding of DoS and phishing attacks. 90% of experts knew the difference between passive and reactive IDS; however, only 25% of novices knew about it.

The theoretical and practical knowledge of participants of both groups was calculated based on a scale ranging between 0 and 1 by integrating their responses about theoretical and practical knowledge separately. The theoretical and practical base of knowledge was represented as two autonomous aspects for the novices (Cronbach's α = 0.463) and experts (Cronbach's $\alpha < 0.01$). However, there was an increased dissociation found in both the theoretical and practical fields of knowledge among the experts as compared to the novice. The distinct characteristics of participants from both groups are illustrated in Figure 2. The figure clearly shows that in comparison with the theoretical and practical knowledge of novices and experts, the theoretical (t (73) = 13.115, $p < 0.001$) and practical knowledge (t (73) = 13.286, $p < 0.001$) of the experts was much higher. Although they were not regularly associated with IDS monitoring tasks, these findings also highlight the experts' advanced knowledge and experience in cybersecurity and network operation.

Moreover, optimal/near-optimal scores were obtained by experts in the questions that assessed theoretical knowledge as well as practice dimensions. On the contrary, novices' variability and practical understanding were limited; however, they showed higher variability in theoretical knowledge. The results depicted that the number of detected events significantly impacted the decision power of the participants (z = 9.152, $p < 0.001$), as there was an increased tendency to construe threat as a cyber-attack.

Figure 3 clearly shows a significant interaction between the frequency of events declared as having malicious activities and the group of participants involved in the detection. Furthermore, most experts got ideal or near-optimal scores based on the theoretical questions, with the majority of the variation finding in the practical aspect. Beginners exhibited low knowledge of practical aspects with lower variation and higher theoretical knowledge variability. These results

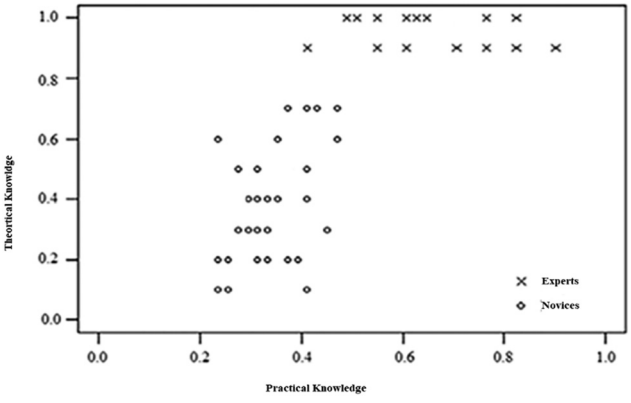

Figure 2: The theoretical and practical knowledge base of beginners and experts about network security.

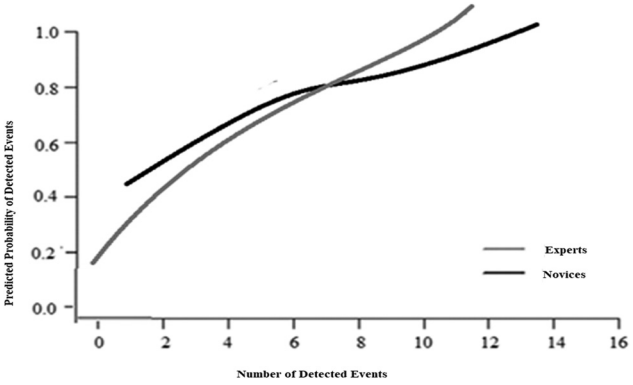

Figure 3: Probability of novices and professionals in declaring cyber-attacks considering the number of malicious events detected.

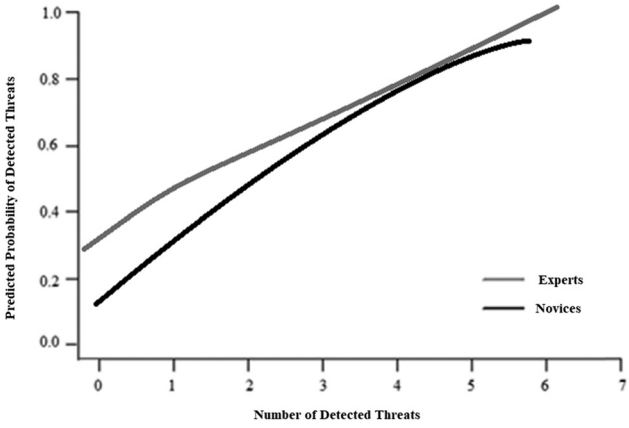

Figure 4: The probability of declaring cyber-attacks in novices and experts depends on the number of total detected attacks.

indicate the usability of the questionnaire for the identification of groups with varying degrees of expertise.

4.1 Detecting attack scenarios

Security experts are trained to protect networks against attacks; however, the current study showed no difference in the conduct of novices and experts. A logistic regression model examined the relationship between decisions that declare a network either as malicious or as a cyber-attack representation. The dependent variables in this model were binary decisions: under-attack or under no attack, while the independent variables were the group of participants as well as the frequency of network events. These results highlight that as far as novices are concerned, there is an increased likelihood of declaring a malicious event as a cyber-attack (z = 3.816, p < 0.001). When many detected cases are involved, experts are more than likely to declare such events as cyber-attacks.

The study findings also exhibited a difference in the novices' performance and experts' performance as the association between several properly categorized malicious events and the judgment about network scenarios presenting cyber-attacks was examined. Concerning both experts and novices, a significant increase in the likelihood of deciding about a cyber-attack was observed with the rise in the number of detected malicious events (z = 8.194, p < 0.001). After detecting a few actual threats, the novices showed an increased likelihood of deciding about the sequence of network events that show a cyber-attack (Figure 4). On the contrary, while detecting a few threats, the experts did not show such a likelihood of deciding about a cyber-attack (z = 2.070, p = 0.038). The assessment of the relationship between the frequency of events accurately identified as harmful and the determination of a cyber-attack indicated a comparable disparity in expert and beginner conduct. Through an accurate detection and frequency of threats with a logistic regression model, by taking participants as independent variables and the decision regarding the whole scenario, it was unveiled that there was an increase in the tendency the detect malicious events as well as both the experts and novices also concluded that a cyber-attack was placed. However, in case of an increase in the frequency of threat detection, both the experts and the novices likely decided about the cyber-attack.

4.2 Detection of malicious events

All the 20 network events taken into consideration for these scenarios of this study were classified either as malicious or non-malicious by the participants. There were 11,000 and 1,200 network events for novices and experts, respectively. A huge pool of malicious events at the network was classified as threats by the experts (χ (1, N = 3,829) = 15.651, p < 0.001) in comparison with the novices (χ (1, N = 8,371) = 15.068, p = 0.024). The experts correctly detected approximately 55% of malicious network events, while the other 15% were false detections (Figure 5). On the contrary, only 44% of novices correctly detected malicious network events, while 18% were false detections (Figure 5).

The results depicted significant variation in detection rate across diverse scenarios of the network (F (3,539) = 6.767, p < 0.001). The Sniffer detected scenario showed a significant increase in the tendency of detecting events of the malicious network, as compared to detection rates calculated for deface websites (mean = 41%, SD = 30%) and DoS (mean = 45%, SD = 28%). There was a significant interaction between the type of scenario and the group of

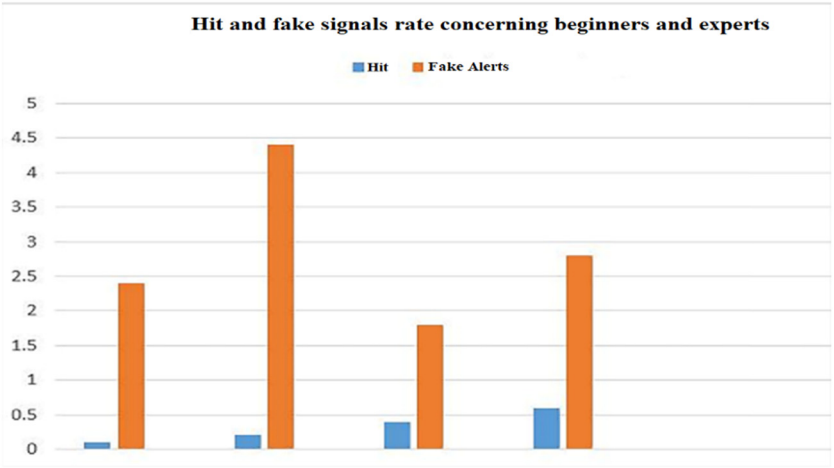

Figure 5: Hit and fake signals rate concerning beginners and experts during the detection of malicious network events.

participants (F (3,539) = 2.715, p = 0.044). This clearly showed that there is a significant impact of the experience of cybersecurity on stealing confidential data (t (240) = 4.105, p < 0.001) and Sniffer detected scenarios (t (116) = 1.948, p = 0.054). No difference was observed between experts and novices in different scenarios, except for Sniffer-detected scenarios and stealing confidential data.

5 Discussion

The study analysis revealed several significant patterns and differences between novices and experts in detecting cyber-attacks. The accuracy rates of both groups in classifying networks as under attack or not were examined, shedding light on their respective capabilities and limitations. The results indicated that experts, despite their extensive knowledge and experience in the field of cybersecurity, did not exhibit a significantly higher accuracy rate compared to novices. This finding challenges the notion that expertise alone guarantees superior performance in detecting cyber-attacks. The study highlighted that expertise does not necessarily translate into higher detection accuracy, especially when confronted with complex and evolving attack scenarios. Conversely, novices demonstrated a noteworthy capability in judging network scenarios that involved a limited number of malicious events. Their ability to identify and interpret indicative events towards the end of the network scenarios was more satisfactory compared to experts. This finding suggests that novices may rely on observable patterns and indicators to make accurate classifications, compensating for their relative lack of domain expertise.

Previous studies have highlighted the significance of human decision-making in keeping IT systems safe and secure [29,32,33]. IDS possesses an effective information security design, which supports security analysts by increasing their apprehending related to strengths and shortcomings of decisions by humans. Decision-making in the cyber world is affected by past knowledge and experiences. Therefore, the current study's findings have improved the quality of the decisions taken by humans for detecting cyber-attacks concerning cybersecurity experts and novices. The knowledge and experience of cybersecurity professionals related to information and network security were extensive. The cybersecurity experts used a completely different approach to network security tasks than the novices, although the experts did not use IDS daily. The significant difference between experts and novices was observed in their capabilities to detect malicious activities that take place through a sequence of events; a trivial difference concerning declaring an entire sequence as a cyber-attack was also observed between these two groups. This clearly showed that knowledge and experience enhance an individual's ability to detect malicious cyber events.

The experts may lack situated knowledge as they are taken away from the familiar operation environment. Previous studies have confirmed the significance of situated knowledge [33]. Experts are likely to take two substitute descriptions regarding the behaviour of the network: legitimate maintenance of web servers and behavioural network that corresponds with the breach. The status of the network can be disambiguated as the experts benefit from situated knowledge.

Novices benefit from events that are indicative and appear at the end scenarios of the network while detecting cyber-attacks. The capability to judge network scenarios considering a limited number of malicious events was

more satisfactory among the novices than the experts. The differences between novices and experts may be ignored as the decision about cyber-attacks is taken after observing all the network events. However, experts are expected to play an essential role in detecting cyber-attacks and preventing damage by propagating attacks through networks.

Sarno and Neider [34] advocated that professionals seem to have over-confident and more vulnerable behaviour as compared to students in terms of cyber-hygiene. In addition, novices reported having more knowledge than the experts, this indicated that cyber experience can be different from cyber hygiene as experience does not constantly anticipate the actions. The notion of adopting cybersecurity cautious behaviour during monitoring is supported by the fact that the confidence level of experts while making a positive decision about an attack is higher compared to lower levels of confidence while making adverse decisions about an attack. All the directors in the domain of cybersecurity are responsible for chalking out more effective security plans to mitigate the risk and attacks. Along with it, it is also one of their functions to specify the instructions to ensure the safety of internal users and deal with cyber-attacks. A schedule is created and staff is trained to minimize the likelihood of human error and how to deal with the scenario when a human error is involved. Therefore, the significance of cybersecurity awareness cannot be overlooked in reinforcing security and transparency. Similarly, Ghelani [22] also argued that awareness related to cybersecurity enables organizations to operate their businesses effectively by avoiding cyberattacks. Another aspect of cybersecurity awareness is to create security mindfulness so that critical procedures can be carried out for all internal users. It also provides individuals regarding the aspects of security control to be followed regularly. Moreover, there are numerous advantages of cyber training and awareness programs as they provide new exposure and insights related to the potential risks in the cyber world that in turn also help in minimizing the number of cyber-attacks. More advantages include that these awareness programs are imperative in saving time in terms of early recognition and detection of cyber-attacks through risk assessment so these potential threats and risks can be countered and mitigated at their initial stages. At the organizational level, these programs set the organizational culture and involve an early risk assessment. Crimes in cyberspace represent a plethora of security issues related to compliance, incorporation of security protocols, and digital rights.

Keeping up appropriate cybersecurity for a whole organization takes a ton of thought, arranging, experimentation, and system. Investigating different organizations tends to resolve what turned out badly, how an assault happened, and what steps could have been taken to forestall that assault. When that has been resolved, academic institutions can actualize safety efforts to help forestall clear dangers against their organization. Thinking about the numerous instruments and techniques that are usually used to actualize security, for example, client accounts having solid, one-of-a-kind, pivoting login information, firewalls, representative preparing, and guaranteeing Skyward uses those related to visiting infiltration testing, and weakness examines, academic institutions can find a way to make sure about the entirety of their information. Arrangements must be executed throughout the organization with clear rules concerning all parts of cybersecurity inside the organization, extending from what computerized security perspectives are required, physical security viewpoints, precisely what role representatives play in looking after security, and how to appropriately report any issues. Generally, cybersecurity is an essential angle to keeping up the respectability of the most significant resources.

The current study does have certain limitations that should be acknowledged. First, the number of events in the network scenarios used for the analysis was relatively small compared to real-life scenarios of network traffic. This limited number of events may restrict the generalizability of the findings to more complex and diverse cyber-attack scenarios encountered in practical settings. It is important to recognize that real-world cyber-attacks can involve a wide range of tactics and behaviours, and the findings of this study may not fully capture the intricacies and variations present in those scenarios. Moreover, the simplified IDS used in this study, while effective for educational purposes, may not have encompassed all possible network behaviours and attack vectors found in real-world environments. This could limit the realism of the scenarios and influence the participants' performance.

Additionally, the study employed a logistic regression approach, which is a standard and commonly used statistical method in this field. However, it is worth noting that over the past few years, there have been significant advancements in DL techniques for IDS. These DL techniques have shown promising potential in enhancing the accuracy and effectiveness of detecting cyber-attacks. By utilizing alternative statistical approaches or incorporating machine learning techniques, the analysis could have benefited from more advanced methods that capture complex patterns and improve predictive performance. Furthermore, the recruitment of participants from a single university may introduce selection bias, as the sample may not be representative of the broader population of cybersecurity professionals and novices.

6 Study implications

The findings of this study have important practical implications for organizations seeking to enhance their cybersecurity measures and decision-making processes. By understanding the differences in the capabilities and decision-making approaches of novices and experts in detecting cyber-attacks, organizations can tailor their strategies to effectively address the challenges posed by evolving cyber threats.

First, the study highlights the value of expertise and experience in detecting malicious activities within a network. Organizations can leverage this insight by investing in ongoing training and professional development programs for their cybersecurity teams. To do this effectively, organizations should implement a structured training curriculum that focuses on the latest threat trends and advanced detection techniques. They should also introduce regular simulation exercises and real-world threat scenarios to test and enhance their teams' response capabilities. Furthermore, establishing mentorship programs where experienced professionals guide less experienced staff can facilitate the transfer of knowledge and best practices. Organizations should also promote continuous learning by supporting cybersecurity personnel in obtaining advanced certifications and engaging in specialized workshops.

Additionally, organizations should foster collaboration and knowledge sharing among experts. This can be achieved by creating internal forums or knowledge-sharing platforms where cybersecurity professionals can discuss emerging threats and effective strategies. Encouraging participation in industry conferences and professional networks will also help teams stay informed about the latest developments and build a robust network of peers.

Furthermore, the study emphasizes the importance of both practical knowledge and theoretical knowledge in cybersecurity decision-making. Organizations should ensure that their security teams have a strong foundation in both areas. This can be accomplished by integrating academic training with practical exercises, such as conducting hands-on labs and red-team-blue team simulations. Additionally, organizations should support their teams in pursuing industry certifications and real-world scenario training to ensure they have both the theoretical knowledge and practical skills required to address complex cyber threats.

Another practical implication of the study is the need for cybersecurity professionals to maintain a cautious approach and avoid overconfidence. To address this, organizations should promote a culture of vigilance and continuous learning, emphasizing that security threats are constantly evolving. Implementing regular security awareness training programs, conducting awareness campaigns, and ensuring clear communication of security protocols and reporting procedures can help reinforce a proactive and cautious security stance among all employees. Additionally, periodic security drills and simulations can help maintain high levels of preparedness and vigilance.

To further improve cybersecurity measures, organizations should consider integrating advanced technologies and techniques into their intrusion detection systems. Specifically, they should adopt machine learning and AI tools to enhance their threat detection capabilities. These technologies can analyse large volumes of data to identify patterns and anomalies indicative of potential threats. Organizations should also regularly update and fine-tune these technologies to adapt to evolving attack methods. Combining these technological solutions with human oversight ensures that automated alerts are reviewed and validated by skilled professionals, enhancing the overall effectiveness of the detection system.

7 Conclusion

In conclusion, this study highlights the importance of practical knowledge and experience in effectively classifying network events as threats or non-threats in the context of cybersecurity. The findings indicate that decision-making in cybersecurity is influenced by the sequence of network events and the ability to discern key occurrences within the network. It is worth noting that the study focused on a limited number of network events, which may have implications for the generalizability of the findings. Future research should aim to address this limitation by incorporating more extensive and complex network scenarios to capture a wider range of real-life network traffic patterns. This will provide cybersecurity professionals with a more realistic and comprehensive understanding of network behaviour. Moreover, the study suggests the need to explore alternative statistical approaches or machine learning techniques to enhance the analysis. By leveraging advanced techniques such as DL and machine learning algorithms, researchers can improve the accuracy and reliability of network event classification, leading to more effective decision-making in detecting and mitigating cyber-attacks.

8 Action plan

In light of the findings from this study, it is evident that bridging the gap between novices and experts in

cybersecurity requires targeted actions. Therefore, we propose the following action plan for universities and students to enhance cybersecurity education and practice:

8.1 Action plan for universities

1. Enhance curriculum:
- Integrate practical labs and simulations.
- Update course content regularly with industry input.

2. Foster industry collaboration:
- Partner with cybersecurity firms for internships and guest lectures.
- Host workshops and seminars with industry experts.

3. Support certifications and training:
- Offer preparatory courses and subsidies for certifications.
- Provide specialized training in advanced areas.

4. Facilitate research and practical experience:
- Encourage student participation in research projects.
- Develop modern lab facilities and host CTF competitions.

8.2 Action plan for students

1. Pursue additional learning:
- Take online courses and attend webinars.
- Engage in personal cybersecurity projects.

2. Gain practical experience:
- Apply for internships and co-op programs.
- Utilize online platforms for skill practice.

3. Network and seek mentorship:
- Join cybersecurity organizations and attend conferences.
- Find and engage with a mentor.

4. Continuous skill development:
- Stay updated on industry trends and best practices.
- Regularly practice in cybersecurity labs and training environments.

By implementing these strategies, universities can strengthen their educational offerings, and students can better prepare themselves for careers in cybersecurity. Together, these efforts will bridge the gap between novice and expert levels, contributing to a more skilled and capable cybersecurity workforce.

Acknowledgement: The author is very thankful to all the associated personnel in any reference that contributed to/for this research.

Funding information: This study is supported via funding from Prince Sattam bin Abdulaziz University project number (PSAU/2024/R/1445).

Author contributions: It is a single-author article and M.M.S. contributed to all parts of the manuscript idea to final proofreading.

Conflict of interest: The author declares no conflict of interest.

Ethical approval: The study was approved by the institutional ethics committee of Al Neelain University.

Informed consent: Not applicable.

Data availability statement: The datasets used and analysed during the current study are available from the corresponding author upon reasonable request.

References

[1] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, Mar. 2019. Doi: 10.1109/jsyst.2017.2741483.

[2] G. Bovenzi, G. Aceto, D. Ciuonzo, V. Persico, and A. Pescape, "A hierarchical hybrid intrusion detection approach in IoT scenarios," *GLOBECOM 2020 – 2020 IEEE Global Communications Conference*, Dec. 2020. Doi: 10.1109/globecom42002.2020.9348167.

[3] J. Zhang, L. Pan, Q.-L. Han, C. Chen, S. Wen, and Y. Xiang, "Deep learning based attack detection for cyber-physical system cybersecurity: a survey," *IEEE/CAA J. Autom. Sin.*, vol. 9, no. 3, pp. 377–391, Mar. 2022. Doi: 10.1109/jas.2021.1004261.

[4] J. Ahmad, M. U. Zia, I. H. Naqvi, J. N. Chattha, F. A. Butt, T. Huang, et al., "Machine learning and blockchain technologies for cybersecurity in connected vehicles," *Wiley Interdiscip. Rev.: Data Min. Knowl. Discov.*, vol. 14, no. 1, Sep. 2023. Doi: 10.1002/widm.1515.

[5] O. Alshaikh, S. Parkinson, and S. Khan, "Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: the need for a standardised approach," *Comput. Secur.*, vol. 139, p. 103694, Apr. 2024. Doi: 10.1016/j.cose.2023.103694.

[6] M. K. Hasan, R. A. Abdulkadir, S. Islam, T. R. Gadekallu, and N. Safie, "A review on machine learning techniques for secured cyber-physical systems in smart grid networks," *Energy Rep.*, vol. 11, pp. 1268–1290, Jun. 2024. Doi: 10.1016/j.egyr.2023.12.040.

[7] H. M. Saleh, H. Marouane, and A. Fakhfakh, "Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning," *IEEE Access*, vol. 12, pp. 3825–3836, 2024. Doi: 10.1109/access.2023.3349248.

[8] A. Choudhary, A. Chaudhary, and S. Devi, "Cyber security with emerging technologies & challenges," *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, Dec. 2022. Doi: 10.1109/icac3n56670.2022.10074579.

[9] A. Hasas, M. S. Zarinkhail, M. Hakimi, and M. M. Quchi, "Strengthening digital security: dynamic attack detection with LSTM, KNN, and random forest," *J. Comput. Sci. Technol. Stud.*, vol. 6, no. 1, pp. 49–57, Jan. 2024. Doi: 10.32996/jcsts.2024.6.1.6.

[10] J. L. Leevy, J. Hancock, R. Zuech, and T. M. Khoshgoftaar, "Detecting cybersecurity attacks across different network features and learners," *J. Big Data*, vol. 8, no. 1, Feb. 2021. Doi: 10.1186/s40537-021-00426-w.

[11] T. O. Abrahams, S. K. Ewuga, S. O. Dawodu, A. O. Adegbite, and A. O. Hassan, "A review of cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection," *Comput. Sci. IT Res. J.*, vol. 5, no. 1, pp. 1–25, Jan. 2024. Doi: 10.51594/csitrj.v5i1.699.

[12] Y.-I. Llanten-Lucio, S. Amador-Donado, and K. Marceles-Villalba, "Validation of cybersecurity framework for threat mitigation," *Rev. Fac. Ing.*, vol. 31, no. 62, p. e14840, Oct. 2022. Doi: 10.19053/01211129.v31.n62.2022.14840.

[13] A. I. C. Popescu, "The geopolitical impact of the emerging technologies," *Bull. "Carol I" Natl. Def. Univ.*, vol. 10, no. 4, pp. 7–21, Jan. 2022. Doi: 10.53477/2284-9378-21-38.

[14] O. Alshaikh, S. Parkinson, and S. Khan, "Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: the need for a standardised approach," *Comput. Secur.*, vol. 139, p. 103694, Apr. 2024. Doi: 10.1016/j.cose.2023.103694.

[15] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, "Cyber security awareness, knowledge and behavior: a comparative study," *J. Comput. Inf. Syst.*, vol. 62, no. 1, pp. 82–97, Feb. 2020. Doi: 10.1080/08874417.2020.1712269.

[16] O. Sarker, A. Jayatilaka, S. Haggag, C. Liu, and M. A. Babar, "A multivocal literature review on challenges and critical success factors of phishing education, training and awareness," *J. Syst. Softw*, vol. 208, p. 111899, Feb. 2024. Doi: 10.1016/j.jss.2023.111899.

[17] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, "Denial-of-service attack on IEC 61850-based substation automation system: a crucial cyber threat towards smart substation pathways," *Sensors*, vol. 21, no. 19, p. 6415, Sep. 2021. Doi: 10.3390/s21196415.

[18] A. A. Alhashmi, A. Darem, and J. H. Abawajy, "Taxonomy of cybersecurity awareness delivery methods: a countermeasure for phishing threats," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 10, 2021. Doi: 10.14569/ijacsa.2021.0121004.

[19] R. Bisht, "Active vs passive rotations," *A Mathematical Approach to Special Relativity*, pp. 291–295, 2023. Doi: 10.1016/b978-0-32-399708-9.00023-3.

[20] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: state-of-the-art," *Int. J. Electr. Power Energy Syst.*, vol. 99, pp. 45–56, Jul. 2018. Doi: 10.1016/j.ijepes.2017.12.020.

[21] T. Alharbi and A. Tassaddiq, "Assessment of cybersecurity awareness among Students of Majmaah University," *Big Data Cognit. Comput.*, vol. 5, no. 2, p. 23, May 2021. Doi: 10.3390/bdcc5020023.

[22] D. Ghelani, "Cyber security, cyber threats, implications and future perspectives: a review," *Authorea Prepr.*, Sep. 2022. Doi: 10.22541/au.166385207.73483369/v1.

[23] A. A. Cain, M. E. Edwards, and J. D. Still, "An exploratory study of cyber hygiene behaviours and knowledge," *J. Inf. Secur. Appl.*, vol. 42, pp. 36–45, Oct. 2018. Doi: 10.1016/j.jisa.2018.08.002.

[24] M. I. Al-Ghamdi, "Effects of knowledge of cyber security on prevention of attacks," *Mater. Today: Proc.*, Apr. 2021. Doi: 10.1016/j.matpr.2021.04.098.

[25] B. Dash, M. F. Ansari, P. Sharma, and S. S. Siddha, "Future ready banking with smart contracts – CBDC and impact on the indian economy," *Int. J. Netw Secur. Appl.*, vol. 14, no. 5, pp. 39–49, Sep. 2022. Doi: 10.5121/ijnsa.2022.14504.

[26] F. Frati, G. Darau, N. Salamanos, P. Leonidou, C. Iordanou, D. Plachouris, et al., "Cybersecurity training and healthcare: the AERAS approach," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1527–1539, Jan. 2024. Doi: 10.1007/s10207-023-00802-y.

[27] S. Baraković and J. Baraković Husić, "Cyber hygiene knowledge, awareness, and behavioural practices of university students," *Inf. Secur. J. Glob. Perspect.*, vol. 32, no. 5, pp. 347–370, Jun. 2022. Doi: 10.1080/19393555.2022.2088428.

[28] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, et al., "Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish," *Proceedings of the 3rd Symposium on Usable Privacy and Security*, Jul. 2007. Doi: 10.1145/1280680.1280692.

[29] M. T. H. Chi, "Two approaches to the study of experts' characteristics," *The Cambridge Handbook of Expertise and Expert Performance*, pp. 21–30, Jun. 2006. Doi: 10.1017/cbo9780511816796.002.

[30] F. Asgharpour, D. Liu, and L. J. Camp, "Mental models of security risks," *Lecture Notes in Computer Science*, pp. 367–377, 2007. Doi: 10.1007/978-3-540-77366-5_34.

[31] N. Ben-Asher and C. Gonzalez, "Effects of cyber security knowledge on attack detection," *Comput. Hum. Behav.*, vol. 48, pp. 51–61, Jul. 2015. Doi: 10.1016/j.chb.2015.01.039.

[32] K. Lye and J. M. Wing, "Game strategies in network security," *Int. J. Inf. Secur.*, vol. 4, no. 1–2, pp. 71–86, Feb. 2005. Doi: 10.1007/s10207-004-0060-x.

[33] D. Botta, R. Werlinger, A. Gagne, K. Beznosov, L. Iverson, S. Fels, et al., "Towards understanding IT security professionals and their tools," *Proceedings of the 3rd Symposium on Usable Privacy and Security*, Jul. 2007. Doi: 10.1145/1280680.1280693.

[34] D. M. Sarno and M. B. Neider, "So many phish, so little time: exploring email task factors and phishing susceptibility," *Hum. Factors: J. Hum. Factors Ergon. Soc.*, vol. 64, no. 8, pp. 1379–1403, Apr. 2021. Doi: 10.1177/0018720821999174.