IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 May 2024, accepted 14 June 2024, date of publication 17 June 2024, date of current version 26 June 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3416045

RESEARCH ARTICLE

Cybersecurity Education and Awareness Among Parents and Teachers: A Survey of Bahrain

MOHAMED AYYASH[1], TARIQ ALSBOUI[2], OMAR ALSHAIKH[2], ISA INUWA-DUTSE[2], SAAD KHAN[2], AND SIMON PARKINSON[2]
[1]Royal Academy of Police, Ministry of Interior, Manama 33305, Bahrain
[2]Department of Computer Science, University of Huddersfield, HD1 3DH Huddersfield, U.K.

Corresponding author: Simon Parkinson (s.parkinson@hud.ac.uk)

ABSTRACT In today's interconnected and digital world, the need to safeguard sensitive and personal information is vital. The rise in cybercrime, especially that involving minors and vulnerable groups, is alarming. Creating awareness of online risks and safe online behaviour is critical. The purpose of this study is to explore the importance of integrating cybersecurity education in schools, with a focus on practices within Bahrain. We explore prevention measures through user studies ($n = 251$) with parents and teachers. The survey was designed and conducted that included 19 questions for parents ($n = 157$) and 10 for teachers ($n = 94$). The findings revealed that children are highly vulnerable and exposed to various risks, with inadequate awareness of cybersecurity among parents and inadequate parental supervision. Parents and teachers have identified that some of the most common risks children face online are exposure to inappropriate content, such as pornography and interactions with strangers, as well as financial fraud. Three out of four parents are aware of the risks, yet only half apply parental controls to protect their children. Parents and teachers (69% parents, 64% teachers) strongly believe that educational institutions have the responsibility to improve cybersecurity awareness among children, and 87% of the participants reported that it is a key priority. However, awareness and distribution of information to students has been established as a key challenge and many believe that the most effective teaching mechanism is reported to be narrative-based, problem solving and video-based. Therefore, it is imperative to adopt proactive measures to improve the cybersecurity education process in Bahrain.

INDEX TERMS Cybersecurity, education, awareness, parents, teachers.

I. INTRODUCTION

The rapid development of technology has transformed the world into a highly connected cyberspace [1]. The Internet, remote communication, and novel applications have significantly influenced people's lives, leading to considerable online time and, in some cases, to internet addiction [2]. Children are an important part of society and have been affected by the digital revolution. The amount of time 10-year-old children spend on digital devices has increased considerably in the last decade. According to the Organisation for Economic Cooperation and Development (OECD) [3], children spent 40 minutes a day on digital devices in 2012, which increased to 2 hours in 2015 and more than 3 hours on weekends in 2017. Research suggests that young people use the Internet more frequently and start doing so at increasingly younger ages [4]. Even preschool children have familiarised themselves with digital devices before being exposed to more traditional educational resources, such as books [5]. A comprehensive study conducted by Boston Consulting Group (BCG) in 2022 revealed that 95% of children in the Middle East are online at the age of 12 [6]. Furthermore, 65% accessed the Internet as young as 8 years of age and 87% accessed it at age 10. The study also revealed that 81% of the children are daily users and most spend 1-5 hours per day.

The increased use of technology by children has led to an alarming rise in cyber threats and risks. Due to their lack of

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamed Elhoseny.

awareness and knowledge, they are particularly vulnerable to these dangers. According to the FBI Internet Crimes Report (2015-2022), cybercrimes against children have increased by 20% annually, with approximately 14,500 children becoming victims during the reporting period, resulting in a financial loss estimated at $2.9 million [7]. Different forms of cyber threats have been identified to have a significant impact on children's lives, including blackmail [8], [9], phishing [10], cyberbullying [11], [12], pornography [13], [73], and privacy breach [14]. Consequently, many of these hazards could be reflected in the physical or psychological life of the child. Bahrain's Telecommunication Regulatory Authority (TRA) has published a comprehensive national report on Internet safety to promote a culture of cyber safety and increase knowledge in this area [15]. The report focusses on cyberbullying as a major threat to children, highlighting its complexity and impact on young people. Furthermore, online activities and related cyber violence could cause severe problems such as academic failure [16], pathological addiction, sleep problems [17], and even attempts to commit suicide [18].

Consequently, the importance of spreading cybersecurity awareness and culture among child societies and academic institutes must be considered in today's digital age. Schools and parents are the main sources of educational resources and training providers. Although parents have traditionally been viewed as the primary parties responsible for protecting their children, statistics indicate that there is a need for children to be more aware of cybersecurity. Studies conducted in Malaysia [19], Saudi Arabia [20], [21], and Cyprus [22] suggested that technical knowledge and skills are a significant challenge for parents. About 38% of parents need to be more aware of cybersecurity and threats. Furthermore, almost half of the parents surveyed do not believe that they are the right party to turn to for their children if they encounter any cyber threat [15]. The lack and inefficiency of communication between parents and their children is the most serious problem faced in the process. Most parents do not apply or have technical control over their children's Internet usage and do not discuss cyber threats with their children.

A recent study has shown that less than 6% of children stated that they would turn to their parents if faced with a cyber threat [15]. Children often create Internet accounts without parental knowledge. Most parents may not know what to do, with only 13% of adolescents believing that their parents fully understand online activities [23]. Therefore, raising awareness among parents and teachers is crucial. Schools must provide cybersecurity education to equip children with the skills to deal with threats. Developing awareness and a cybersecurity culture within educational institutions is one way to provide these skills and expertise.

The implementation of cybersecurity and Internet safety awareness and training programmes in educational institutions is often considered a priority to protect children digitally [24], [25], [26] and a requirement to achieve a safe cyber environment [27], [28]. Efficient cyber risk prevention can be achieved by creating a culture around children, including schools, neighbourhoods, and societies, targeting behaviours, skills, and attitudes, and spreading awareness among teaching parties, that is, parents, teachers, and related institutions are required to build a robust training programme approach [29], [30]. In the UAE, cybersecurity programmes were implemented in several schools and achieved promising results in increasing cyber safety and awareness among children [31]. In Bahrain, the Telecommunications Regulatory Authority published several online guides and awareness programmes for young people; however, studies show that children are not interested in these types of awareness, especially the youngest, who have difficulty accessing such content [17], [32]. Therefore, awareness and training programmes must have long-term continuity to consolidate the information received and adapt it to become a culture among the communities concerned [33], [34], which can be applied in school stages. This study investigates the importance of integrating cybersecurity education in schools, with an emphasis on practices within Bahrain. The main objective is to understand the level of awareness about cybersecurity among parents and teachers to identify risks, methods, and strategies to increase awareness. The main findings of the study include:

- **Common risks and challenges:** The most common risks, whether experienced or more likely, are exposure to inappropriate content, engaging in suspicious or dangerous relationships, and financial fraud. Possible challenges facing cybersecurity education include the need to increase awareness among educational parties, logistic support, and the delivery of information to the student.
- **Internet access by children:** We found that 3 out of every 4 children in Bahrain have access to the Internet before entering middle school with daily use for 3 hours or more. Meanwhile, only one of them received sufficient cybersecurity awareness.
- **Awareness among parents and teachers:** Three out of every four parents in Bahrain are aware of the risks facing their children and are concerned about the issue. Only half of them apply parental control techniques and are familiar with the concepts of cybersecurity and related laws, which led them to state that they cannot handle the situation if their children are exposed to a risk on the Internet. 69% of parents and 64% of teachers believe that educational institutions are the most responsible party for raising children's awareness, supported by an average of 88% for both reporting that it is a priority to include it in schools.
- **Improve cybersecurity awareness:** One of the most effective methodologies to improve cyber threats, especially among students, is through narrative, problem solving and video-based techniques. Based on the common risks identified, we recommend video-based education as the most convenient method to raise awareness.

The remainder of this paper is structured as follows. We begin by providing an overview of the background and current literature in Section II. Sections III and IV describe the research questions and methodology, respectively. Sections V and VI present relevant results and a discussion, respectively. Finally, Section VII concludes the study.

II. BACKGROUND AND RELATED WORK

This section presents the background and related studies on the main topics addressed in this study.

A. CYBERSECURITY

Cybersecurity is a relatively recent and increasingly significant concept that has received substantial attention in recent years. Craigen et al., in their comprehensive analysis of various research articles, distilled the essence of cybersecurity and concluded that the definition of "cybersecurity is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems" [35]. Despite the global recognition of cybersecurity as a critical element within the security frameworks of different countries, there exist variations in how nations define it, where several countries published their national cybersecurity strategy (NCSS) [36], [37]. For example, the UK defines cybersecurity as the practice of protecting IT devices of individuals and organisations from unauthorised access and cyberattacks [38], while Australia and France have referred to cybersecurity as measures and resistance to confidentiality, integrity, and availability of data stored in the process [39]. In contrast, India describes it as the activity of protecting information and information systems [40]. In Bahrain, according to NCSC cybersecurity is the process of protecting systems, data, networks, and information from cyberattacks. The cyber threat landscape is evolving as new technologies are developed and deployed, e.g., autonomous vehicles [41], [42], [43], generative AI [44], [45], and authentication technologies [46], [47], [48]. This further motivates the need to educate children to increase awareness levels to accommodate new threats. In this study, we focus mainly on the awareness aspect, which we prefer to identify as [49]: increasing the level of knowledge about online risks and practices to stay safe online.

B. CYBER RISKS FACING CHILDREN

The Internet is a vast and constantly changing space, with rapid changes appear in the last decade due to the uptake of social media services. The risks for children and minors have diversified, taking various forms, whether under the well-known label of cybercrimes such as hacking and information theft, or other risks related to specific segments of society, such as bullying, online grooming, and electronic extortion, which may primarily target children [50]. With the significant increase in the use of the Internet among children at an early age [51], many researchers specialising in cybersecurity and online safety have directed their studies in recent years toward examining the risks faced by children and minors during their use of the Internet in its various forms and platforms. In the following paragraphs, we review some relevant studies aimed at identifying the significant threats and dangers they may encounter.

1) CLASSIFICATION OF CYBER RISKS

According to Hasebrink et al. [52] and Livingstone [53], cyber risks from a general perspective are classified into the following three main sections:

(A) **Content** that explains the web findings, including exploiting personal information, violet content, pornography, and sexual content.

(B) **Contact** which includes other parties communicating with the child, such as bullying, grooming, or misinformation.

(C) **Conduct** where two or more children are parties to cyber-risk actions such as cyberbullying, illegal downloads, or phishing.

Furthermore, Livingstone et al. described risks from another point of view as opportunities and risks. Actions can be taken on both sides on a scale [53]. However, whether actions are classified, they eventually affect children legally or harmfully. In one article, various types of risk were mentioned: pornography, phishing online, and cyberbullying [54]. Although they stated that the most serious and dangerous risks are the rarest among all risks, the other common risks are dangerous and could be harmful to children. Researchers have widely discussed sexual risks due to their increasing occurrence. Farrukh et al. define sexual risks as harassment behaviours such as requests for sexual content, sexual stalking, and the trading of pornographic content; in addition, the disclosure of unwanted sexual content/information is the most likely risk for children [55]. Mitchell et al. mentioned another type of sexual solicitation that can be more aggressive even in offline situations, be it by email, phone, or text massages [56]. Furthermore, they state that sexting (sexual talking/texting) among children has increased significantly in recent years with the evolution of social networking platforms, while they mentioned in their research that both sexes have the same exposure to it.

Another significant risk that young people face online is cyberharassment, which can be defined as repeated, persistent, and unwanted interpersonal aggression facilitated by information and communication technology (ICT) [57]. Sexual/aggressive harassment was discussed by Pereira et al. [58]. They conducted a local survey in Portugal among more than 600 young people. Their study highlighted cyber-harvesting as a growing risk recently in their circles. A total of 66% of the parties surveyed said that they had been exposed to an act of cyber-harassment at least once in their lives. Cyberbullying is one of the most common risks in children's societies. Any action that uses a technological medium to intimidate or convey an intention to harm is considered [55]. Many studies relate cyberbullying to a serious and harmful problem, physically and psychologically, including depression and suicide [59], which has led many specialists and researchers to strongly advise addressing causes beyond the growing trend of cyberbullying in schools and social institutions [60]. In Bahrain, a national study published in 2015 by TRA shows that 50% of children who faced cyberbullying suffered consequences such as depression and school absences [15].

Privacy is another risk that has been widely spread among children, mainly through social media platforms such as Facebook and Instagram, making parents extremely concerned about their children's private information on the Internet [61]. Privacy breaches can cause identity theft, such as the name and date of birth, which can be used to commit cyber or physical crimes [49], [62]. Furthermore, various universal studies discussed multiple cybercrimes related to different age groups of children, where some risks target younger ages 8-12, such as privacy breaches and identity theft, while contact threats and related crimes affect mostly older ages 12 and above. Other risks affect both age groups, such as cyberbullying, phishing, racism, and pornography [10], [63]. Pereira et al. conducted a local survey among more than 600 young people in Portugal. They recently discussed cyber-harassment as a growing risk in their circles [58]. A total of 66% of the surveyed parties said that they had been exposed to cyber harassment at least once in their lives. Locally, during their study in Bahrain, Al-Naser et al. found that inappropriate or unethical content represents the most prevalent risk among children under 6. This is followed by downloading malicious and harmful content onto your devices [64].

C. CYBERSECURITY EDUCATION

Access to the digital devices is fast growing. Almost 70% of children aged 8-18 years have a smart device that can access the Internet in the Middle East, and 23% of younger children aged 4-8 years have access to the Internet. Furthermore, in 2016, 608 of the 3,100 cybercrimes were related to child sexual abuse [65]. With the growing risks and cyber threats, the need for educational processes and culture is a must, considering the responsibilities of governments to secure a safe online space for children and protect them from threats, including cyber ones. In this section, we discuss relevant approaches to generating awareness of cybersecurity education.

1) INTERNATIONAL STANDARDS

As a crucial element in national security, cybersecurity is a defining factor in the level of security in a particular country. It pertains to a state's ability to confront cyber threats and the general public's awareness, proactive and preemptive measures, and training initiatives in this domain. Consequently, most international standards emphasise the importance of training and education with respect to national cybersecurity and cyber safety. For example, Sarri et al. in the National Capabilities Assessment Framework (NCAF) mentioned that education and training capabilities are necessary as an essential section of the framework, where the country encompasses cybersecurity awareness at the early stage of the student's education path [66]. Robust education and training courses are crucial to ensure a safe online environment for children, as outlined by the Oxford Global Cybersecurity Scholarship Challenge (GCSC) in 2021. The Cybersecurity Capacity Maturity Model for Nations emphasises that cybersecurity education should not be limited to universities and workplaces, but should also be integrated into primary, secondary and higher education [67]. Furthermore, AlDaajeh et al. proposed a national guide based on the NSCS of countries of world leaders, highlighting the importance of cybersecurity training as the initial phase of a nation's cybersecurity culture [68].

2) THE ROLE OF PARENTS

Many researchers discussed and studied the role of parents in the cybersecurity education process. Multiple studies have consistently demonstrated a significant need for cybersecurity awareness among parents to protect their children, which poses a severe challenge when it comes to ensuring children's online safety. For example, Ahmad et al. conducted a comprehensive study on parental awareness of cybersecurity in Malaysia [19]. They found that a staggering 50% of the parents surveyed are unaware of their children's use and threats of online use. Compared to other studies, 69% of the parents did not attend any cybersecurity awareness programme. Another study by Cassidy et al. concluded that 30% of parents said that they never supervised their children [69]. Similarly, [70] discussed the lack of awareness of cybersecurity during childhood, leading to a lack of experience dealing with their children. Their study found that very few of them played a role in the use of the Internet compared to 50% of them who played a role in watching television. Furthermore, according to NCSA research, the findings indicate that approximately 60% of teenage users have created an online account that their parents do not know, while 31% of parents feel suspicious of their children's online behaviour [23]. Furthermore, miscommunication has been found, with 63% stating that their children must ask for help if they face a threat online, but only half of them have notified their children about this role [23].

In Bahrain, teachers stated that it is generally difficult for parents to participate due to their lack of awareness of their children's online activities [15]. In one study, the authors identified that only 25% parents have been exposed to cyber threats in their lives, making them more alert to children's behaviours on the internet; nevertheless, most of them were not exposed to this experience, making most of them unaware or less alert or concerned about their children on the Internet [22]. Similarly, in a local investigation among parents and children, it was found that there is a clear communication gap between them in terms of Internet behaviour and information sharing 50%, and children say that they do not trust the knowledge of their parents about the Internet [20]. Collectively, these findings emphasise the urgent need to improve parental education and awareness of cybersecurity before turning to them to protect children from cyber risks to which they are exposed.

3) THE ROLE OF SCHOOLS

The importance of incorporating cybersecurity into the educational system has been discussed by several researchers. According to Rahman et al., the inclusion of early cybersecurity education can cultivate a generation that respects cyber laws and is aware of the threats associated with the use of the Internet [25]. Furthermore, it has the potential to address the emerging issue of internet addiction in the current generation. In a case study of cybersecurity programmes for students, educational programmes were reported to improve the level of awareness of cybersecurity, create positive usage behaviour among children, and efficiently help students protect themselves online [31].

According to a study by Aloul 2010, the importance and need for security awareness to improve cybersecurity was examined [24]. Research revealed that implementing cybersecurity awareness education and training is crucial for Internet users around the world. Such activity is essential in government institutions, schools, universities, and organisations. Furthermore, in a qualitative study in the UK, it was concluded that children can understand and benefit from educational tools and cybersecurity programmes to help them become aware of their privacy and cybersecurity between Internet platforms [14]. The increase in Internet access in South Africa can be attributed to the wide availability and affordability of smartphones [71], [72]. Therefore, young people in these countries should learn more about protecting their devices from external threats. This lack of awareness is mainly due to the fact that knowledge about the use of the Internet is typically reserved for those studying computer-related courses at higher education institutions. The authors emphasised the need for a comprehensive awareness programme on the use of the Internet in South Africa that would be incorporated into all levels of education, including primary and secondary schools.

In 2020, the World Health Organisation (WHO) suggested that education and skills programmes are the most effective and promising method to help children become aware of online child sexual abuse (OCSA) [73], [74], [75] and protect themselves from related threats. Similarly, the Child Molestation Research Institute [27] stated that more than 90% of sexual abuse could be prevented through education and awareness programmes. Patterson et al. found the same results in their systematic review of the most effective methods for raising awareness of sexual abuse [30]. They found that spreading awareness among educational institutions and applying training and skill programmes in schools significantly protect children against related threats and decrease crimes of sexual abuse.

D. METHODS OF CYBERSECURITY EDUCATION

Several studies discussed and evaluated education and training methods to apply cybersecurity programmes and online safety awareness. Abawajy et al. examined the effectiveness of various methods to increase awareness of information security [76]. The findings of the study support the idea that such programmes are effective in improving the awareness and behaviour of end users about the security of information. The study emphasised the importance of countering cyberattacks that exploit human factors and reducing vulnerabilities associated with human behaviour. By evaluating different delivery methods, such as text-based, game-based, and video-based approaches, the study concludes that the component and video-based methods are very effective in providing information to students. Boulton et al. discussed the cooperative cross-age teaching intervention (‘CATZ’) in a pilot study [77]. They conducted a test and evaluation of their model through the application of various teaching and training methods to students on cybersecurity safety. They found that the students were more receptive and had a better comprehension of the information and training when they received it from the older students than any other method. This further enhanced the results of the evaluation of the online safety of the students.

Ebooks were used to effectively distribute related information in which they designed a digital book for online safety and evaluated its effects on children, finding that their e-book, carefully designed and directed to a specific group of children, gained wide and effective acceptance, contributing to raising awareness of children's cyber privacy and online activities [78]. In a classroom, Lastdrager et al. applied storytelling methods to assess the feasibility of anti-phishing programmes [79]. Testing the children before and after the programme with another untrained student found that most of the trained students were aware of phishing attempts. The current trends in school cybersecurity education for application in the short term are not promising and effective in the long term [72].

Ondrušková t al., through a local survey in Czech schools, found that intermittent training does not significantly impact the response of students to online behaviour and is not an effective solution to improve online security skills [33]. Instead, it needed to engage cybersecurity awareness education throughout the educational process. Furthermore, cybersecurity training and education programmes must include practical and theoretical skills to be efficient and productive [80]. Cheung et al. tested and evaluated challenge-based learning strategies, where students trained using a challenge-and-solution approach in cybersecurity showed great benefits with a noticeable improvement in their computer skills, positive behaviour, and security skills [81]. Furthermore, providing cybersecurity knowledge and training to teachers and students helps these parties protect themselves from becoming cybercriminals and improve the effectiveness of the educational process [82], [83]. Furthermore, “simulation tools” have the potential to contribute significantly to improving information awareness and assurance levels among students, academic staff, and professionals [84]. These tools possess various attributes, such as user-friendly interfaces and comprehensibility, which enable students and users to conduct practical experiments and gain a deeper understanding of information security concepts.

1) CHALLENGES AND STRATEGIES

The multifaceted nature of cybersecurity concepts, both in theory and practice, presents a practical challenge in spreading awareness of this emerging technological field, especially through educational institutions. Rahmanet al. conducted a thorough analysis of various studies on cybersecurity education and concluded that the lack of teacher training and development in this area is a common challenge [25]. In addition, insufficient resources and funding, especially in underdeveloped countries, pose a problem. Salamzada et al. addressed logistic support and technical foundation requirements as the main challenges faced by the implementation of security in schools in developing countries [85]. Furthermore, teachers as the main participant in the educational process can have difficulty keeping up with the rapid development of technology developments and related cybersecurity aspects [86], thus being ineffective in providing information to students.

Al Shamsi et al. investigated a cybersecurity educational programme applied in the UAE [31]. The results of the interviews among the teachers showed some limitations in terms of the programme used, including a lack of methods of teaching of interest and practical activities. Furthermore, traditional narrative approaches were negatively affected. Regionally, Al-Janabi et al. conducted a small sample size survey in the Middle East to examine security awareness within educational settings, specifically among academic staff, researchers, and students [87]. The findings revealed a lack of essential awareness of the importance of cybersecurity among contributors in the Middle East. As a result, the study suggests that a comprehensive security management plan should incorporate security awareness and training for administrators and users to address this problem.

Meanwhile, the inclusion of cybersecurity in curricula has multiple requirements and conditions to be efficient and effective. Zepf et al. presented a proposal for a cybersecurity curriculum that aims to teach children the fundamental principles of cybersecurity and information assurance [88]. The authors outlined a set of criteria for evaluating the efficacy of digital security curricula. Subsequently, they recommended a cybersecurity curriculum designed for children with basic computer skills. They concluded that the cybersecurity education process should have the flexibility to cater to a diverse range of users, employ interactive and motivational techniques to enhance learning, and present computer security skills in a simplified way that is easily understandable to children. Conklin et al. discussed the main requirement for an efficient cybersecurity programme in the United States and the direction of related efforts [89]. They clearly stated that the student success element is the most critical factor for a successful evaluation programme. Both studies were limited in scope locally and more regionally and delved into a different specific research topic.

In addition to providing the necessary protective and security mechanisms, a good awareness programme must undergo proper design to provide compulsory awareness and active training and education programmes for users and employees as well. The programme should be instrumental in developing and spreading awareness of security between them, employing proper physical access controls, and obeying the security policies and rules established by the institution / organisation to achieve the best security [90]. In terms of evaluation elements, Kim's study emphasises the need for effective information security awareness training (ISAT) for college students [91]. Research finds that, although students recognise the importance of ISAT, many do not actively participate in such programmes. Furthermore, security topics not commonly covered in existing programmes or websites significantly impact student information security awareness. Therefore, the study recommends that educational institutions and universities assess and improve their ISAT offerings to better equip students to protect their information and systems in an increasingly connected world.

Al-Naser et al. presented a study on the level of parental supervision of their children, but the focus was only on children under 6 years of age [64]. TRA published a report and a research study on secure Internet use in Bahrain, where several statistics were reviewed, including children's Internet use and the types of platforms on which they spend their time [15]. However, with the spread of the COVID-19 pandemic and the significant increase in Internet use, especially among children, the study no longer represents the current reality of the data and does not cover the educational aspect of cybersecurity. Several studies have been conducted in other regions around the world, some of which we review in the following section. However, since they were carried out locally in different regions and cultures, they do not apply specifically to our target population. Our goal in this study is to examine the impact of integrating parental control and educational institutions towards improving cyber-related threat awareness in Bahrain.

III. RESEARCH QUESTIONS

The main objective of our research is to help protect children and young people from cyber risks. In this work, four research questions have been set to clarify the dangers to children and discuss one of the most appropriate ways to protect them from cyber dangers: by spreading the culture and awareness of safe use through educational institutions. The questions are generally divided into a section related to the current status of the problem and another section related to the educational process and related topics, as follows.

1) **RQ1:** What are the main risks facing children on the Internet?

2) **RQ2:** What is the level of awareness of cybersecurity among parents and teachers?
3) **RQ3:** What is the extent of parental control and its effectiveness on the use of the Internet by their children?
4) **RQ4:** What are the most suitable and effective methods to increase and improve awareness of cybersecurity?

IV. METHODOLOGY

In this section, we present the main research method including engagement with parents and teachers. The goal is to quantitatively and qualitatively assess the level of cyber threats and security awareness and recommend mitigation measures. Generally, this study has four main phases, as illustrated earlier in Table 1.

A. PROCEDURES AND PARTICIPANTS

To answer our research questions, we conducted a set of user studies involving parents and teachers. The research survey was designed using the Google Form and the target population consists of parents with children under 18 years of age and teachers, particularly those with a background or a role in computer education in Bahrain. To ensure a diverse and representative sample, we used various methods to reach these groups; we distributed the research article through school boards and individually used social media platforms to ensure credibility and maximise participation for both targeted groups. Participation is voluntary and no personally identifiable information was collected. The study was carried out according to the institution's ethics standards. We recruited $n = 215$ participants involving 49% male and 51% female. The $n = 215$ responses are made up of parents ($n = 157$) and teachers ($n = 94$). In terms of parents, 54% are male and 46% are female. With teachers we experience a change from parents where we received responses from 43% are male and 57% are female.

B. SURVEY STRUCTURE

The effective communication and understanding between parents and teachers are crucial to enhancing children's education, particularly in complex areas such as cybersecurity. Recognising the diverse perspectives and roles parents and teachers have in the educational journey of children [92], we crafted different sets of questions tailored to each group. Parents, who are intimately involved in their child's day-to-day activities and digital interactions at home, offer a unique vantage point on cybersecurity concerns. On the other hand, teachers, with their professional expertise and classroom experience, provide valuable information on how cybersecurity is addressed within the educational curriculum and the school environment. Furthermore, the nature of conversations surrounding a child's education differs between parents and teachers. Parents may prioritise aspects of cybersecurity that directly impact their child's safety and behaviour online, while teachers may focus on integrating cybersecurity education into lesson plans and addressing digital literacy within the classroom setting. The meticulous design of our questionnaires reflects a comprehensive understanding of these distinctions. By tailoring the questions to the specific needs and perspectives of parents and teachers, we ensure that the study provides insights that are not only relevant but also actionable to improve cybersecurity education in both home and school settings. This approach enables us to capture a holistic view of the challenges and opportunities to promote digital resilience among children, ultimately contributing to more effective strategies for cybersecurity education. The design of the questions followed a meticulous process. First, we design the following two questionnaires:

- **Questionnaire for Parents** The questionnaire for parents consists of 19 related questions around the themes of cybersecurity awareness, online risks, parental control, importance of education and challenges.
- **Questionnaire for Teachers** The second questionnaire is for teachers with 10 questions around themes of cybersecurity awareness, the importance of education, acceptance, challenges, and effective methods.

The targeted population consisted of parents with children under 18 years of age and teachers, particularly those with a background or role in computer education in Bahrain. To ensure a diverse and representative sample, we used various methods to reach these groups; we distributed the research article through school boards and individually used social media platforms to ensure credibility and maximise participation for both targeted groups.

1) SURVEY QUESTIONS

To maintain the integrity of our research, we took precautions to avoid guiding questions that could influence the responses of the respondents. We designed the questions to be neutral and unbiased, allowing participants to express their opinions and experiences. Furthermore, we based our decision on data from the literature review, including previous national reports [15], and previous similar regional studies (such as [64], [87]) to inform the design of our questions and the formulation of multiple choice / selection answer options. This integration of existing knowledge ensured the completeness and relevance of our questionnaire. We aligned the survey questions with specific research questions that captured the perspectives and experiences of parents and teachers. Each research question was carefully designed to encompass various dimensions of the research topic. Details about the questions are illustrated in Table 1. The types of answers were mainly scaled from 0-4, or were multiple choice selections or checkboxes where they could choose three selections at maximum. Numerical responses have been collected using a continuous 5-point Likert scale.

For the distribution and collection of responses, we use the Google Forms platform, which offers a user-friendly interface and allows efficient data management and analysis. We implemented various strategies within the survey to minimise the likelihood of incorrect or misleading responses, including providing clear instructions, incorporating validation checks, presenting logical and consistent answer

TABLE 1. Questionnaire questions according to research questions (RQ), themes and targeted group. Note: Cs=Cybersecurity. The parents (P#) and teachers (T#) questions are shown.

Theme	Question	Research Questions	Parent Question Number	Teacher Question Number
Background	What school stage are your children in / or what school stage are you teaching?		P1	T1
Awareness	How would you rate your familiarity with the concept of Cs?	RQ2	P2	T2
Internet usage & Risks	At what age did your child access the Internet?	RQ1	P3	
	How long do your children spend on the Internet daily?		P4	
	Are you concerned about the use of your children and the risks online facing them?		P5	
	Have your children ever attended or received any Cs awareness programmes before?		P6	
	Have your children been exposed to any of the following online risks before?		P7	
	I think that my children are more likely to be exposed to these risks		P8	
Parental control	I am aware of the behaviour and use of my children on the Internet.	RQ2	P9	
	I am aware of the risks my children face online.		P10	
	How often do you apply risk mitigation strategies such as parental control and age content?		P11	
	If my child is exposed to any risks, I can effectively handle the issue.		P12	
	I am concerned about my children's online presence.		P13	
Education importance	Who do you think is the most responsible party to educate and raise children about cybersecurity and online safety?	RQ2	P14	T3
	How do you rate the importance of including cybersecurity education in schools?		P15	T4
	At which stage should we start teaching Cs in schools?		P16	
Challenges	What is the level of challenges and obstacles facing cybersecurity / safety education in schools?	RQ3	P17	
	What are the challenges facing Cs education in schools?		P18	T5
	Have you ever received or attended any of Cs education strategies and training?			T6
	How do you feel about your trust in teaching Cs to students?			T7
	I am interested in attending training courses regarding Cs education			T8
Methods & strategies	Which of the following are the most appropriate and effective methods for delivering information related to cybersecurity/safety?	RQ4	P19	T9
Solutions	What are the effective solutions to overcome challenges and obstacles?			T10

options, and not allowing for duplication attempts, as well as excluding suspicious answers and incomplete questionnaires. A pilot study was also conducted to address the level of response and identify any possible technical problems, questions, or misunderstandings. Thus, a total of 30 parents and 15 teachers participated in the pilot study. Furthermore, we should mention that we used Arabic to design and publish the questionnaire to avoid confusion, as it is the native language of the target population.

V. RESULTS

Reliability Analysis: The responses from the research participants were analysed for reliability and correlation analyses. We apply Cronbach's alpha [93], [94] to measure the internal consistencies among the responses given under the constructs in Table 2. An alpha value $\alpha \geq 0.7$ suggests that each experimental construct is reliable and consistent. A Cronbach's alpha above 0.7 suggests that the items in the scale or questionnaire are closely related to each other and are measuring the same underlying construct reliably. In other words, the items are consistent in their measurement of the targeted concept or trait. We can have confidence that the scale or questionnaire is producing consistent results and that the scores obtained from it are dependable representations of the construct being measured. Table 2 summarises the reliability analysis for each of the constructs applicable to the study. All constructs show reliable values.

Staff Readiness: Some of the questions in Table 1 have been designed to understand how parents and teachers can help to avoid the cyber-related risks facing children. For the reliability analysis that involves teachers' responses (Table 2), we are interested in understanding the readiness to address cyber risks that may emerge. The following questions have been presented and relevant responses have been collected:

- The level of awareness of cybersecurity
- Perception about the importance of cybersecurity awareness in schools
- Confidence/trust in teaching or raising awareness on cybersecurity
- Willingness to participate in creating cybersecurity awareness programme

There is a high level degree of internal consistency ($\alpha = 0.78$) for the items in the staff readiness.

As previously communicated, the survey was divided into two primary sections. The total responses received were 251, which is 157 from parents and 94 from teachers. The gender split of the responses overall is 123 male and 128 female, of which 84 males and 73 females are parents and 39 males and 55 females are teachers. Moving forward, we will examine the results regarding the specific groups and topics surveyed.

A. PARENT RESULTS

In addition to the specific questions provided in Table 1, parents are asked in what stage of school their children are currently at (P1). We included this question to segregate the target audience, where we specifically sought responses from parents who actively raise children aged 4 to 17 years.

TABLE 2. Survey questions and reliability analysis for all constructs pertaining to parents [P] and teachers [T] in the study using Cronbach's alpha (α). The alpha value for all aggregated constructs is approximately (≈ 0.80). A value above 0.7 is generally considered acceptable, indicating that the elements measure a cohesive concept.

Construct:	*Awareness* [P]	
Measure:	A) Awareness about cybersecurity B) Awareness about cybersecurity and cyber crime C) Exposure to cybersecurity risk D) I am aware about my child usage E) I am aware about cyber risks faced my children F) Exposure to cyber risks awareness by children	$\alpha = 0.79$
Construct:	*Internet Usage* [P]	
Measure:	A) Age of Internet access by children B) Daily time spent by children using the Internet	$\alpha = 0.63$
Construct:	*Preventive Measures* [P]	
Measure:	A) I can handle the situation if my child is exposed to cyber risks B) The more responsible	$\alpha = 0.85$
Construct:	*Staff Readiness* [T]	
Measure:	A) The level of awareness of cybersecurity B) Perception about the importance of cybersecurity awareness in schools C) Confidence/trust in teaching or raising awareness on cybersecurity D) Willingness to participate in creating cybersecurity awareness programme	$\alpha = 0.78$

Additionally, we aimed to gain a general understanding of the ages of the participants' children in terms of school stage. In Bahrain, there are mainly 4 stages of education, which are Preschool (4-6), Elementary (6-11), Middle (12-14), and High (15-17). The types of answers available were multiple selections or checkboxes in which participants could select multiple selections. Most of the responses indicated that they raised children in elementary schools (53%) followed by middle schools (43%). Figure 1 illustrates the responses and it can be seen that most children in the range of 6-14 years are young. This is explained by the fact that Elementary has the largest age range (6-11), which means that there will be more students in this range.

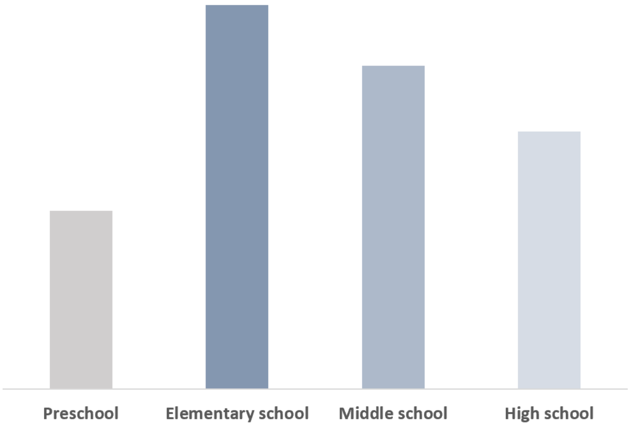


FIGURE 1. The distribution of school stages of the participants' children.

1) CYBERSECURITY AWARENESS

P2 was designed to address the level of awareness of cybersecurity among parents and their familiarity with the term. The responses were measured on a scale of 0 to 4, where each number indicates a level of familiarity. Almost half (46%) of the parents stated that they are familiar or well acquainted with the concept, while half of that number stated that they have a good understanding of cybersecurity. Alternately, 15% of them said that they are familiar with it and a similar percentage for parents who never heard about it.

2) INTERNET USAGE & RISKS

Figure 2 shows the aggregate responses on the age of Internet access and the level of awareness of cybersecurity, as well as the age of Internet access and the level of awareness of cyber crimes. Both images show the measures of awareness levels (0-5) dependent on the age of the child and the amount of time that they reported using the Internet, which is consistent with previous research [4]. Interestingly, as seen in the figure, the age of the individual does not necessarily mean that they are using the Internet more or understanding the risks more. This could be because younger children use the Internet more due to the amount of free time they have available and also because older children might be more aware of the risks and crimes, but this awareness makes them realise that there is so much more that they do not

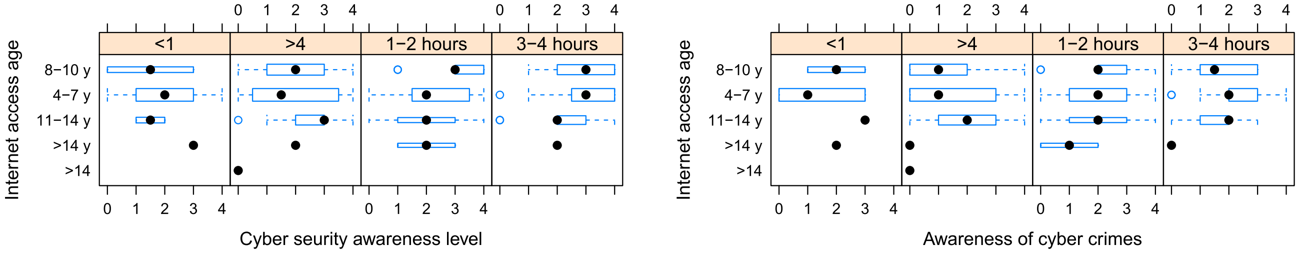


FIGURE 2. Internet access age, daily usage.

TABLE 3. Age of Internet access among children and their daily usage.

Access Age (years)	3-7	8-10	11-14	15 & older
Count	76	44	31	6
Daily use of children	**>4 hours**	**3-4 hours**	**1-2 hours**	**<1 hour**
Count	68	41	33	15

know. On the contrary, younger children may not have as much knowledge and therefore do not perceive a gap in their knowledge. In Table 1, questions P3-P8 have been proposed to examine the topic of Internet use and associated risks from the perspective of parents. Essentially, P3 aims to investigate the age at which children gained access to the Internet and participated in Internet-based activities. The result revealed that most of the children had early access to the Internet. Specifically, 76 parents reported that their children accessed the Internet or were online at 7 years of age or under, representing half of the children (49%) in the survey (120 of 244 children). Furthermore, 28% of the children started accessing it between the ages of 8 and 11, while only 23% waited until 11 years or older. These findings indicate that a significant proportion (82%) of children accessed the Internet before entering middle school.

P4 seeks to explore the daily usage patterns of the children of the participants in any of the various activities on the Internet. The results indicate an upward trend toward increased daily use. As illustrated in Table 3, 44% of the children spend more than four hours on the Internet daily, followed by 26 who spend three to four hours. On the contrary, 21% and 9%, respectively, reported limited daily use for two hours or less than an hour. These findings suggest that 70% of the children dedicate around half of their free time to activities on the Internet, which is similar to the 2015 study by TRA in Bahrain [15]. This is interesting and suggests that the amount of internet use has not changed significantly in the last 8 years.

P6 explores the level of awareness and knowledge among the children of the participants by measuring the factor of education or training. The results identified that three-quarters of the children did not receive sufficient specialised awareness (25%) or did not receive training-related awareness (51%). Only 24% of the children had previously received awareness training. This is an important finding, as it demonstrates that a significant portion (76%) of children have had no or insufficient levels of training.

P7 and P8 were aimed at identifying the most common risks for children. The first question (P7) concerns the risks experienced among children. The question was multiple choice and was pre-set with seven of the most common risks collected from the reviewed literature. A total of 61 participants (39%) reported that their children were not exposed to any of them or did not know if they were exposed. The rest, that is, 96 parents reported 187 cyber risks and crimes their children experienced. According to Table 4, of the 187 risk experiences, 57 of them were related to exposure to interpret content or pornography, which represents 36% of the participants. Suspicious online relationships with strangers were reported 33 times, followed by financial fraud and cyberbullying, with 26 for each. Phishing and hacking recorded lower numbers by 20 and 19 respectively, while the least reported risk was blackmail with only 6 selections. In P8 parents were asked which of the seven risks their children are most likely to face. We asked participants to select up to three from the list, resulting in a total of 353 selections received for this question. Their percentage is from the number of total selections, as illustrated in Table 4. Most parents consider exposure to interpreted content to be the most common risk for their children 31%, and relationships with strangers were the second threat (20%). Then, financial fraud and hacking with similar numbers (13%), and finally phishing, blackmail, and cyberbullying were the least chosen risks as the most likely risks to face their children online.

Using a comparison of the results of the two questions as illustrated in Table 4. In particular, experienced risks and the most likely ones drawing almost similar trends among them, interpret content, relationships with strangers, and financial fraud are duplicated in both results as the highest, while blackmail got the lowest percentage. This could effectively help us determine the most serious and common risks facing children currently in Bahrain.

3) PARENTAL MONITORING

Table 5 shows five questions (P9-P13) designed to measure the situational awareness of parents and applied control strategies on the use of their children. In P9, a total of 99 of the 157 surviving parents agreed that they are aware of the use and activities of their children on the Internet, representing the majority (62%). On the other hand, 18%

TABLE 4. Most commonly risks and likelihood of exposure.

	Q7- Have your children been exposed to any of the following online risks before?		Q8- I think my children are more likely to be exposed to these risks.	
Risks	Count	% of total participants	Count	% of total participants
Inappropriate/pornographic content	57	36%	109	69%
Financial fraud	26	17%	46	29%
Relations with stranger	33	21%	69	44%
Cyberbullying	26	17%	26	17%
Phishing	20	13%	32	20%
Hacking	19	12%	45	29%
Blackmailing	6	4%	26	17%
Total selections/choices	187		353	

TABLE 5. Parents' situational awareness and controlling level of their children.

Question		Strongly disagree	Disagree	Neutral	Agree	Strongly agree
P9	#	10	17	31	46	53
	%	7%	11%	20%	29%	33%
P10	#	6	13	21	42	75
	%	4%	8%	13%	27%	48%
P11	#	15	13	37	48	44
	%	10%	8%	24%	30%	28%
P12	#	11	10	25	36	75
	%	7%	6%	16%	23%	48%
P13	#	15	22	31	34	55
	%	10%	14%	20%	21%	35%

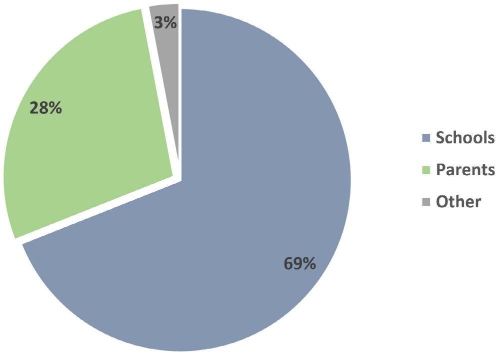


FIGURE 3. Parents' answers to the question: Who is the most responsible party for making children aware of cyber safety?

of them reported disagreeing. 20% remain neutral on this fact.

Knowledge and awareness of the risks surrounding children in cyberspace formed an upward curve in P10 similar to the previous question to approval, with a slight difference represented by strongly agreeing responses, which received 75 (48%) and 42 participants agreeing (27%), for a total of 75%. The remaining quarters were divided equally between neutral responses and disagreeing. This concluded that most parents are aware of their children's Internet use and the risks they face there. In terms of parental control methods on child use measured by P11, only 92 of 157 (58%) reported that they apply control and monitoring strategies on the use of their children. While 24% remained neutral and 18% stated that they do not apply such strategies.

In P12 was designed to measure the degree of concern of parents about their children's activities and threats they faced on the Internet. Of 157 parents, only 21 stated that they are not concerned. The vast majority of parents who reported being concerned reported a total of 111 (71%), and 16% of the parents chose neutrality. As a result, almost 3 out of each 4 parents are concerned about the presence of their children online. In P13, parents were asked in what way they agree with having the ability to handle the risks of the Internet if their children had been exposed to one of them. Only 56% of them agreed with the strong and normal agreement. Although 20% of them choose neutrality, almost a quarter do not think they are capable of handling online risks in their children. In general, most parents are aware and concerned about the use of the Internet by their children and the risks associated with it; however, not the same results are reported in terms of actual supervision and monitoring due to the fact that most disagree, and neutral responses were reported in P13 related to applied parental control strategies. Furthermore, 44% of parents do not believe they are capable of handling online risks.

4) CYBERSECURITY EDUCATION

P14 is designed for parents to find out their perspective on which of the main educational parties (parents and educational institutions) is more responsible for raising awareness and educating children about cybersecurity and internet safety concepts. The result revealed that most parents believe that educational institutions/schools are more responsible in 108 responses of 157 (69%); however, 44 parents believed that they are more responsible for that (Figure 3). The remaining five responses (3%) were about "other", including aspects such as cybersecurity authorities and self-learning.

In a similar approach, P15 declares the importance of awareness of cyber safety education and awareness among parents. On a four-level scale, most parents said it is of the utmost importance to involve cybersecurity awareness in the educational process, with 118 responses (75%), followed by moderate importance (20), while neutrality and unimportance recorded 19 votes only. For P16, the following three options were provided for this question: elementary, secondary, and high school, representing the main school stages in Bahrain. A total of 109 parents suggested that the dissemination of such education should start from the beginning, in the

TABLE 6. Parents' selections on the challenges facing the cybersecurity education process.

Challenges	Count	Percentage
Unprepared/unready educational institutions	121	34%
Lack of awareness among surrounding parties (i.e. teachers, parents)	118	33%
Delivering information to students	44	12%
Ineffectiveness process	43	12%
Student acceptance	21	6%
Other	8	2%
Total selections	355	100%

elementary stage. 42 parents chose secondary school, while high school received only 6 votes (Figure 4). According to the parents' perspective, the finding from the last three questions highlights the perceived importance and necessity of implementing educational programmes focused on cybersecurity and online safety in schools.

5) CHALLENGES

In Table 1, P17 aims to identify parents' opinions on the level of challenges facing cybersecurity education in schools. Almost half of parents (49%) believe that the educational process faces great and extremely great challenges. On the contrary, less than 20% said that it does not face any challenges or a few once, while 32% believes that there are normal challenges as with any other educational curriculum.

P18 is designed to identify the challenges / possible faced by the cybersecurity education process in Bahrain. Participants were asked to select up to three options from seven, which were refined from the reviewed literature and similar studies. There were a total of 355 selections illustrated in Table 6. According to it, the most reported challenges are unprepared educational institutions (34%) and lack of awareness of cybersecurity in the environment (33%). However, the difficulty in delivering this information to children and the lack of efficiency in this field scored 12% for each. Interestingly, only 6% of parents think that their children can accept the awareness programme, with only selections of 6%.

Finally, P19 seeks to identify the most appropriate mechanisms and strategies to teach children about concepts related to cybersecurity and safety on the Internet. Like in the approach of the previous question, we set nine instead of seven choices. The choices were mixed between strategies/methods and systems due to the frequency of education and cybersecurity professionalism among the participants. As Table 7 shows, a total of 410 selections were received. In particular, storytelling was the method most selected of 100 (24%). The parents then choose practical weekly workshops as the second (16%). Problem-solving, game-based and challenge-based strategies scored similar percentages with 13%, 12% and 1%, respectively. With 4% for each, practical homework and self-learning through interactive books were the least appropriate approaches from the parents' perspective.

TABLE 7. The most appropriate/effective strategies and systems to teach cyber safety and security to children.

Methods & Strategies	Count	Percentage
Storytelling	100	24%
Problem solving and challenges	40	13%
Online interactive systems/applications	52	10%
Game-based strategy	49	12%
Video-based strategy	50	12%
Self-learning through interactive books and systems	14	4%
Practical weekly/monthly workshops	65	16%
Traditional curriculum system	26	6%
Practical homework	14	4%
Total selections	410	100%

6) THEMATIC ANALYSIS OF OPEN-ENDED QUESTIONS

This section explores the themes identified from participants' responses to the following open-ended questions (see questions P17-18 and T5-T8 in Table 1):

- What is the level of challenges and obstacles facing cybersecurity / safety education in schools? [P17]
- What are the challenges facing Cs education in schools? [P18 and T5]
- Have you ever received or attended any of Cs education strategies and training? [T6]
- How do you feel about your trust in teaching Cs to students? [T7]
- I am interested in attending training courses regarding Cs education [T8]

To gain deeper insights into participants' experiences (both teachers and parents) regarding cybersecurity, we conducted a thematic analysis of their responses to the open-ended survey questions. This analysis allows us to identify patterns and recurring themes within the data, revealing the perspectives, opinions, and underlying meanings (latent semantics) expressed by participants. Themes were identified by grouping related codes based on connections and patterns aligned with the survey questions. The results of this analysis are presented in four tables (Tables 8, 9, 13, 14). Tables 8, 9 detail the themes identified in parent responses regarding encountered and common cybersecurity risks, and challenges, respectively. Similarly, Tables 13, 14 present themes identified in teacher responses for encountered/common risks and challenges.

a: PERCEPTION ABOUT IMPROVING AWARENESS OF ONLINE RISKS

Thematic analysis of parent responses regarding encountered online risks (Table 8) identified key areas for mitigation and awareness programs to protect children online. These include cyberbullying, inappropriate content, attempts to steal financial information, and suspicious online relationships. The analysis of teacher responses (Table 13) focused on how well-equipped institutions and teachers feel to tackle cybersecurity issues. Here are the main themes identified:

- Engaging teaching methods: Teachers emphasised the importance of using storytelling and relatable case studies to create student engagement in cybersecurity

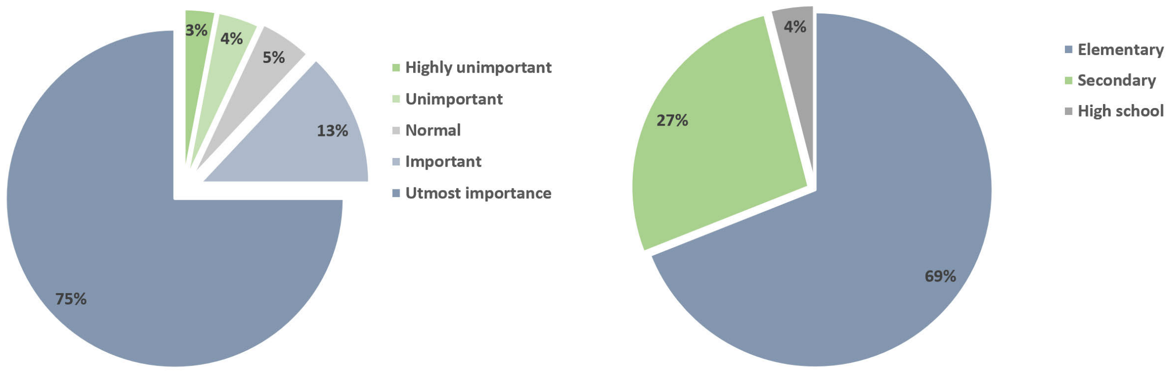


FIGURE 4. An illustration of the percentage distribution of the parent's perspective about the importance of cybersecurity education (Left) and at which school stage it should begin (Right).

education. Additionally, offering flexible learning options was seen as a way to further enhance student participation.

- Teacher training and resources: Also, teachers highlighted the need for more comprehensive training, access to modern interactive tools, and a centralised guide on cybersecurity best practices, all specifically designed for educators.

b: PERCEPTION ABOUT ONLINE RISKS AND MITIGATION CHALLENGES

Thematic analysis of parent responses (Table 9) revealed key challenges hindering awareness and cyber risk mitigation. Notably, some parents perceived a lack of effort from educational staff in preventing online risks.

We notice some discrepancy in the challenges identified by both groups (parents and teachers) and underscore the need for collaboration. This observation highlights a significant discrepancy between parental and teacher perspectives (Tables 9 and 14). This difference in viewpoints could hinder effective collaboration in addressing cyber risks. A unified approach, prioritising common areas of concern, is essential. Overall, parents expressed a strong desire for increased support from the government, schools, and teachers in protecting children online.

Analysis of teacher responses (Table 14) identified key challenges in implementing cybersecurity education:

- Unprepared educational institutions: Similar to parents, some teachers perceive a lack of preparedness within educational institutions to address evolving cyber threats.
- Enhancing student engagement: Teachers highlighted the need for strategies to improve student acceptance and participation, overcoming potential disinterest or pushback.
- Public awareness gap: Teachers also raised concerns about a general lack of public awareness regarding cyber risks and mitigation strategies.

Findings from thematic analysis suggest misplaced responsibility; there is a pattern where parents perceived a lack of teacher preparedness, while teachers attributed preparedness gaps to the educational institutions. Across both groups, some responses pointed to a need for increased government intervention in cybersecurity.

B. TEACHER RESULTS

In addition to the questions provided in Table 1, a teacher is asked to disclose their current or previous teaching experience (T1). We were able to obtain various responses from the different stages with a good distribution of a total of 103 selections (that is, 7-9% of the participants worked in multiple stages). A percentage of 37% and 36% of the teachers surveyed worked in elementary and high school, respectively. While 27% reported this for middle schools. Regarding other stages, such as kindergarten and general departments, the percentage of teachers was 21%. This draws a good distribution among the different stages, as we aspired in our study.

1) CYBERSECURITY AWARENESS

Question T2 resulted in the level of awareness about the concepts of cybersecurity and cyber risks among the teachers surveyed. This illustrates the background knowledge of the participants. Almost half of them (47%) said that they have a good awareness, while 18% do not have any idea. The rest are distributed between normal awareness and little of it, with 22% and 12%, respectively (Figure 5).

Similarly to parents, teachers were asked (T3) to vote on which party is more responsible for being aware and educating children about cyber safety. The results were almost similar as well; more than two-thirds of the teachers (64%) believe that the educational institutions are the party considered. On the other hand, 31% of them chose parents and 5% reported other parties.

2) CYBERSECURITY EDUCATION

T4 asked teachers how important it is to include cybersecurity and online safety education in educational institutions? As illustrated in Figure 6 the vast majority of teachers

TABLE 8. Some relevant themes in the online risks encountered by the participants under the 'Parents' category.

Theme	*cyberbullying and inappropriate content*
Remark	– Because cyberbullying can involve the use of offensive and harassing language, both cyberbullying and inappropriate content have been used interchangeably in the responses of participants.
Theme	*financial fraud*
Remark	– This entails attempts to steal financial information or money online; blackmailing, phishing scams, and hacking have been used quite often under this theme.
Theme	*suspicious relationship*
Remark	– This theme entails dubious or suspicious online interactions that could lead to manipulative and harmful relationships.
Theme	*online threats and security weaknesses*
Remark	– This theme highlights all the threats and vulnerabilities online known to the participants.

TABLE 9. Some relevant themes in the challenges identified by the participants under the 'Parents' category.

Theme	*educational staff not ready*
Remark	– This is the most frequent issue raised by the participants under the 'Parents' category. This suggests that the parents expect more to be done by the Government, school, and teachers to safeguard children against online harm.
Theme	*lack of required educational resources*
Remark	– This theme is related to the above theme because it points to the lack of adequate resources that are necessary to combat cyber risks and vulnerabilities.
Theme	*difficulty in evaluating mitigation strategies*
Remark	– This theme raised some concerns about how any mitigation strategy against cyber risks and vulnerabilities can be objectively measured.
Theme	*better ways to engage students for cybersecurity awareness*
Remark	– This theme alludes to the potential problems that involve students in an attempt to create awareness and relevant training about cybersecurity.

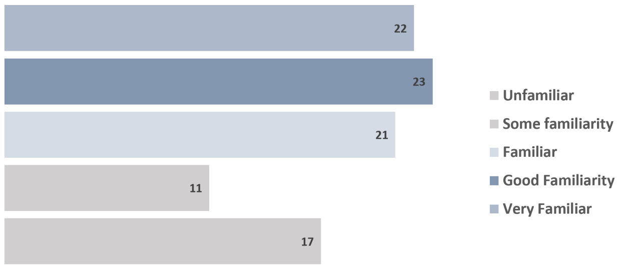


FIGURE 5. Level of familiarity with cybersecurity concepts and related crimes/threats.

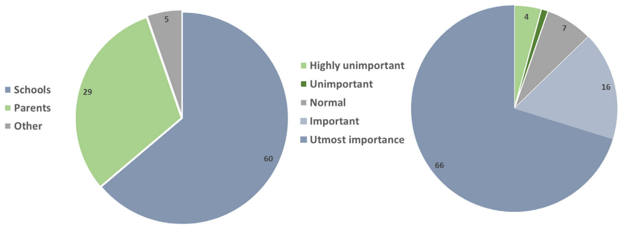


FIGURE 6. Count distribution of teachers' responses on which party is more responsible for educating children about cyber safety (Left) and how important is the inclusion of cybersecurity awareness in schools (Right).

(87%) stated that it is an essential/high priority to involve cybersecurity and safety in schools. In particular, that is even more than the parents' responses about the importance of this.

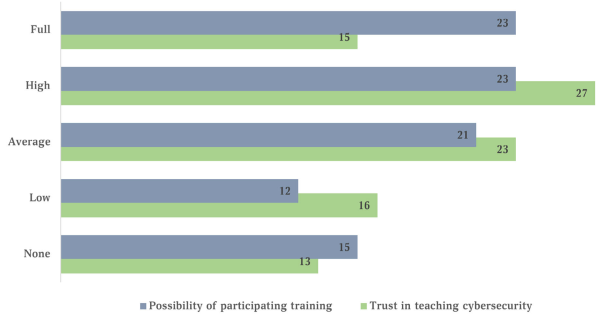


FIGURE 7. Count of teachers' responses to trust level regarding cybersecurity teaching in schools and how likely to participate in related training.

Both T6 and T7 These questions were established to measure the level of trust of teachers in teaching basic awareness of cybersecurity and safety and to determine how they could participate in related training courses to determine the cybersecurity education process. Figure 7 indicates that almost half of teachers (45%) are highly trusted. Average confidence was reported by (24%), while around a third (31%) feels little or no confidence.

In T9, teachers as parents have been asked to identify the most appropriate methods/strategies and systems to deliver information to children/students effectively. In a three-selection option, he received a total of 252 selections

TABLE 10. Teachers' responses to the most appropriate/effective strategies and systems to teach cyber safety and security to children.

Methods & Strategies	Count	Percentage
Storytelling (i.e., previous actual cases and stories, scenarios)	55	22%
Problem solving and challenges	35	14%
Online interactive systems/applications	22	8%
Game-based strategy	20	8%
Video-based strategy	24	10%
Self-learning through interactive books and systems	12	5%
Practical weekly/monthly workshops	49	19%
Traditional curriculum system	19	8%
Practical homework	16	6%
Total selections	252	100%

TABLE 11. The most significant challenges facing cybersecurity education are from teachers' perspectives.

Challenges & Obstacles	Count	Percentage
Lack of cybersecurity educators	44	18%
Outdated educational materials and curricula	40	17%
Difficulty in delivering information to students	35	15%
Challenges in assessing success	32	13%
Rapidly evolving field (keeping up with technological advancement	31	13%
Management and fundings/resources challenges	31	13%
Student acceptance	25	11%
Other	19	8%
Total selections	252	100%

from 94 teachers, as illustrated in Table 10. By 22%, the results show that teachers agree with parents in considering storytelling as the most effective method and periodic practical training as the most appropriate system for this education (19%). The following order sets the problem solving based on 14%, followed by the video based (10%). Unlike the perspective of parents, teachers voted less for the game-based method by 8% of the total choices. Interactive online applications and traditional systems received similar results (8%), while self-learning or homework practice received the least votes, the same as parents, by 6% and 5%, respectively.

T5 asked tech workers from their perspective what challenges are faced or could be met in the cybersecurity education process in schools? Teachers have been asked to choose from more detailed options than parents due to their specialisation and experience in the educational field. As illustrated in Table 11, the responses were distributed fairly closely; however, the lack of awareness among the educational parties was the most selected challenge of 18%, close to outdated educational materials and curricula (17%). Furthermore, teachers believe that providing this information to students (15%) is more challenging than other obstacles, including assessment methods that keep up with the challenges of rapidly evolving and funding. The least likely challenge is the acceptance of the students (8%), where teachers and parents agree.

TABLE 12. Teachers' responses to the most effective/important solutions and kinds of support regarding the cybersecurity education challenges.

Solutions	Count	% Of the total
Cybersecurity awareness programmes among teachers	53	21%
Training programmes regarding teaching cybersecurity	55	21%
Provide technical materials and interactive systems	60	23%
managing time and sources	30	12%
Involving related authorities (i.e., NCSA)	43	17%
Create and provide teacher guide	17	6%
Total selections	252	100%

T10 asks teachers what training needs or support would help overcome these challenges? Six options were established for teachers to choose up to three of the most important support means, as illustrated in Table 12. Of the 258 selections received, 21% of the selection were the training programmes on cybersecurity awareness and teaching strategies for each. The most important solution (23%) from the teacher's perspective is to provide technical and interactive materials. However, teachers do not believe that the teacher guide is as essential as the others for only 6% of the total selections. In addition, 30 other solutions were received that were mainly about managing enough time for the process, improving funding/resources, and conducting parents-children lectures.

VI. DISCUSSION

This section is dedicated to presenting our findings and results from the research questions. Specifically, each set of questions addresses one of the primary inquiries described in Table 1. Subsequently, we will provide a comprehensive overview of the key findings derived from the entire research paper.

Our research seeks to address the prevalent risks that children are susceptible to online and emphasises the importance of cybersecurity education to protect them from these potential threats. Recognising the gaps in our understanding, we are committed to conducting a comprehensive investigation into these issues of paramount importance. Our objective is to examine the various types of danger children can face online, assess the effectiveness of parental controls in reducing these risks, and explore the complexities of educating children about cybersecurity. Our research assumes added significance as reliable information in this field is currently scarce.

What are the main risks facing children on the Internet? To address this question, we thoroughly analyse the dangers related to the Internet to which children in Bahrain are exposed. Our findings reveal a troubling trend, with three out of four children accessing the Internet before age 10, while two of them gain access at or before age 7. Furthermore, 70% of the children spend three or more hours a day participating in online activities, which is half of their free time after school. In particular, this result is

TABLE 13. Some relevant themes in responses provided by the participants under the 'Teachers' category about the most appropriate method of teaching and creating awareness on cybersecurity and the expected support to be provided.

Theme	*content and delivery method*
Remark	– This theme is dominated by the use of storytelling and case studies to impart effective knowledge about cybersecurity. Some of the examples provided include game-based problem-solving activities. The participants also pointed out the need for flexible learning that students could choose from.
Theme	*support to be provided to educators*
Remark	– This theme summarises the support expected to be provided to educators to make them effective. There is a strong emphasis on the following: relevant teacher training, modern interactive tools, and comprehensive guide for teachers about cybersecurity.

TABLE 14. Some relevant themes in challenges identified by the participants under the 'Teachers' category about the issue of cybersecurity and awareness creation.

Theme	*unprepared educational institutions*
Remark	– This is a recurring theme that suggests that educational institutions need to be well prepared and equipped to deal to evolving cyber threats.
Theme	*acceptance and engagement from students*
Remark	– This theme points to the potential of pushback and lack of interest from the student. Thus, designing and implementing engaging content is key here. Similar theme (*better ways to engage students in cybersecurity awareness*) appeared in the participants' response under the 'Parents' category.
Theme	*sensitisation program to create wider awareness*
Remark	– This theme raised some concerns about insufficient awareness among the public and the need to make the public fully aware about cyber risks and mitigation strategies.

perfectly consistent with the findings of TRA [15]. Therefore, such early and frequent use of the Internet puts children at risk of various threats, including phishing, cyberbullying, exposure to inappropriate content, hacking, blackmailing, and financial fraud, as seen in many previously published studies [52], [53]. The results of our survey indicate that the most common risks facing Bahraini children are exposure to inappropriate content, such as pornography and interactions with strangers, as well as financial fraud. This differs from previous research, such as the study by [15] and [64], which found that cyberbullying and downloading unwanted materials are a primary threat; however, it agrees with the first in terms of inappropriate content as the main risk. Furthermore, our survey revealed that while parents consider hacking a significant risk, they do not view cyberbullying or blackmailing as likely to occur. Therefore, as the world of cybercrime evolves, the threats children face also evolve. It is crucial to continuously update our knowledge of the most common hazards and educate children about them, whether through parental guidance or school programmes, to ensure their continued safety.

What is the level of awareness of cybersecurity among parents and teachers? In Bahrain and other countries, it is common for parents to take care of their children's Internet usage. However, our research reveals that 77% of parents in Bahrain lack sufficient awareness or training on cybersecurity. This knowledge gap poses a serious concern for parents and their children who rely on their guidance. Furthermore, when we asked parents to evaluate their understanding of Internet safety, the results were highly diverse on the scale; approximately a third of them did not attend or receive any cybersecurity awareness programme similar to the study [19]. In today's digital world, it is imperative for individuals, including parents, to enhance their awareness of online security. They must recognise the criticality of online safety, just as they do in the physical world, to safeguard their children's welfare.

Our results have brought to light the concerning fact that many parents are not taking sufficient measures to ensure their children's safety online. Although almost three-quarters (71%) of parents have expressed serious concerns about their children's online behaviours and usage and 75% are aware of the risks involved, almost half need to effectively regulate, monitor, and supervise their children's Internet activities. This is surprising, since many popular platforms and devices have made it easier for parents to monitor and protect their children's online activities. Furthermore, only 52% of the parents say that they know what their children are doing online. The study also found that 24% of parents feel ill equipped to handle threats online, while only 35% feel confident in their ability to solve the problem. These findings suggest that around half of all children may need more adequate supervision to protect them from the dangers of the Internet. This lack of supervision could be attributed to children's independence today and a belief among some parents that prevention isn't as important as fixing a problem after it arises. We must find additional ways to ensure children's online safety. One potential solution is to introduce cybersecurity education in schools, as we will examine further in the following question.

What is the extent of parental control and its effectiveness in influencing their children's Internet usage?

What are the challenges associated with it? Due to the numerous risks children are exposed to in the online world, educational institutions must be responsible for educating and raising awareness of cybersecurity and online safety. The limited supervision provided by parents, combined with the complex and ever-changing nature of online threats, makes it necessary for schools to play a proactive role in safeguarding students' online activities. Our research has revealed that parents and teachers recognise the crucial role of integrating cybersecurity education into the educational process. An overwhelming 87% of the participants agreed on the importance of this education.

Furthermore, most of the participants believe that schools and educational institutions should lead in providing this education to students, and 69% parents and 60% teachers share this sentiment. It is clear that cybersecurity education should begin early. Our research indicates that three out of four children in Bahrain have accessed the Internet during their primary school years. Additionally, half of them spend more than four hours online daily. Given these statistics, online safety and cybersecurity education must be integrated into the curriculum early. As the online world becomes an increasingly integral part of our daily lives, children must be equipped with the necessary skills to navigate it safely and responsibly. Educational institutions have a crucial role to play in ensuring that students are educated about the potential risks and dangers of the online world and equipped with the tools to protect themselves. By integrating cybersecurity education into the curriculum, schools can play an essential and proactive role in protecting students' online activities.

Our study reveals that a significant proportion of children lack awareness or cybersecurity education, 75% do not receive any specialised or effective instruction and 67% not receiving any cybersecurity education whatsoever. This presents a major hurdle for cybersecurity education, as children's initial exposure to information poses a challenge compared to those with prior knowledge. Furthermore, no similar studies were found that measured the same conclusions. Previous studies have indicated that the challenges facing the cybersecurity educational process are diverse and change based on factors such as geographical scope and age classification [25], [85]. Therefore, it is crucial to establish a foundation for cybersecurity education in Bahrain by promoting prior awareness among parents and teachers. Our results indicate that 75% of parents and 47% of teachers agree with this notion. In light of these findings, it is imperative to address the urgent need for a comprehensive cybersecurity education programme that targets the educational environment surrounding the child, particularly parents and teachers.

Teachers are recognised as the foundation of the educational process in schools and play a crucial role in promoting effective education delivery. However, their challenges are often viewed as potential challenges in the educational process. A study conducted among teachers in various schools reveals that more than half of them (55%) do not know about cybersecurity and common cybercrimes in full. This highlights the need to improve the level of cyber culture and awareness, which poses a significant challenge in terms of the training aspect. It also supports the assertion made by teachers and parents that the lack of awareness and general knowledge related to cybersecurity is one of the main obstacles that must be overcome primarily.

Furthermore, the study reveals that 29% of teachers experience low levels of confidence in teaching cybersecurity. However, most teachers show moderate to high acceptance and readiness to teach these concepts to students, which is a positive indicator of overcoming the challenges mentioned above. The study also indicates that the currently available technological and educational means pose significant obstacles. This was expressed through challenges such as the inefficiency of available facilities/educational resources and the lack of current support provided by the administrations for related materials, as parents indicated at a rate of 77%. Additionally, simplified communication of this information to students is considered a challenge, especially for early-stage students. Furthermore, the effectiveness of the educational programme and the difficulty of measuring it are challenges that need to be addressed. This aligns with what [89] mentioned: The success of the cybersecurity educational process is reflected primarily in the success of the students in the evaluation operations. In general, the study results align with the challenge of lack of teacher awareness [87] and partially with logistical challenges [85].

What are the most suitable and effective methods for raising and improving awareness of cybersecurity? The educational process is a complex system that can be carried out through various methods, strategies and systems, with the aim of teaching and raising awareness of different concepts for students. This is also applicable to cybersecurity awareness. Several studies have evaluated the effectiveness of various methodologies and strategies used to teach cybersecurity to children and students. Various methods and strategies including video game / story telling, ebooks, challenge-based and simulation tools were discussed by ([76], [81]; [79], [80]; [32], [72], respectively. However, some methods have not been discussed or evaluated before. The effective delivery of cybersecurity concepts to students, especially in the early stages of education, can be challenging. However, appropriate approaches can be adopted and evaluated for their effectiveness. From the common and evaluated methods, the narrative system, which includes stories, real-life problems or scenarios, emerged as the most effective approach, according to 64% and 58% of parents and teachers, respectively, supported by a study conducted by [79]. Furthermore, the problem solving strategy was also highlighted as an effective method, particularly from the perspective of teachers, followed by the visual /

video-based approach of both parties, where the last was found to be effective according to [76]. However, the game-based approach was not appropriate from the point of view of teachers and parents. Regarding the systems (i.e. educational frameworks), it became evident that the interval-based learning system, or the periodic system, whether monthly or weekly, is preferred by both teachers and parents. However, the current education system (curricula and exams) and self-learning through books, interactive systems, or homework assignments were not considered effective methodologies, based on an average selection rate of 18% and 11% for the two methods, respectively.

The cybersecurity education process in Bahrain has been found to be challenged by multiple challenges. To determine the nature of solutions that can serve as remedies for these challenges, teachers were asked to choose the most appropriate and important solutions. The survey revealed that the creation of awareness among the surrounding parties and especially teachers, the teaching of training to simplify cybersecurity concepts for students, and the provision of appropriate technological means such as computers are the three most effective solutions. Furthermore, these findings suggest that the establishment of pretraining and logistic support can help overcome the challenges identified in the study. Therefore, it is crucial to adopt proactive measures to improve the cybersecurity education process in Bahrain.

A. SUMMARY OF KEY ACTIONS

Based on the findings of this work, the following priority actions are presented against the four main findings of the study.

1) COMMON RISKS AND CHALLENGES

- Develop age-appropriate educational materials (videos, games, interactive activities) that address exposure to inappropriate content, online predators, and financial scams.
- Conduct regular studies to identify the most common cyber threats to children in order to tailor awareness and educational materials accordingly.
- Evaluate the effectiveness of educational materials and assess their impact on reducing threats and crimes against the target group.

2) INTERNET ACCESS BY CHILDREN

- Advocate for mandatory inclusion of age-appropriate cybersecurity education in the national curriculum, starting in primary school.
- Activate the parental and educational oversight role by organising ongoing workshops for parents to explain the consequences of early internet access for children.
- Establish cooperative teams between relevant cyber entities and parents to clarify available tools and means of supervision and control over children's Internet usage as a proactive measure.

3) AWARENESS AMONG PARENTS AND TEACHERS

- Launch public awareness campaigns (TV, radio, social media) highlighting the importance of cybersecurity education for children.
- Activate continuous and periodic awareness and training courses among teachers related to cyber safety and addressing cyber threats against children or committed crimes. This can also be implemented through the design of a teacher's guide.
- Design and implement home-based curricula targeting parents alongside children to increase regular home activities that promote awareness for both parties.

4) DEVELOPMENT OF CYBERSECURITY AWARENESS FOR CHILDREN

- Develop a library of engaging video content (animated stories, live-action scenarios) that addresses common cyber threats in a relatable way for children.
- Direct awareness and educational programmes and content to the most common internet platforms among children, such as some social media platforms, through advertising and partnerships with local influencers.
- Conduct an annual assessment of children's awareness levels through surveys or interactive tests to measure the progression of awareness and the level and quantity of threats tested during that period.

B. LIMITATIONS AND FURTHER WORK

As with most studies, the design of the current study is subject to limitations. In this text, we present the main limitations. A) During our analysis of the results, we identified the potential benefits of incorporating a qualitative approach alongside the primary quantitative method. This would be particularly useful for addressing challenges and providing more descriptive and objective themes. It should be noted that our data analysis mechanisms were limited due to differences in the data. This was intentional because we wanted to avoid leading-questions formats. However, this did result in missing out on some advanced analysis that would have been possible with numerical scales to study correlations and calculate average values. B) Sample size obtained: Generally, it was somewhat smaller than expected, which may occur because Bahrain's population is generally low. Relatively, it should be mentioned that the result of this study includes a specific group that was chosen as randomly as possible; therefore, the results may differ if the sample size was larger. C) The scope of this research is limited to parents of children who are currently enroled in public schools. It is important to note that parents who raise teenagers or students attending private schools are not included in this study. The motivation for not including private schools is because curriculum is standardised in all government schools in the Kingdom of Bahrain, unlike private schools. Therefore, by choosing government schools, we can avoid non-uniformity and variations in the criteria used for assessment. We also wanted to focus on the larger group of students, which constitutes government schools.[1] D) Insufficient research: It was observed that there are certain gaps in this crucial topic, specifically studies conducted on a regional level, which were found to be scarce, which ultimately resulted in an improvement in the comparison and evaluation section. It is also important that, in the future, a longitudinal study is performed to understand how awareness and practices evolve. We also acknowledge the importance of including other stakeholders such as children, administrators, and cybersecurity experts. Future research could expand on our findings by incorporating their perspectives for a more holistic understanding. Although there are limitations inherent to this survey research, the study design aimed to mitigate this by having clear questions and anonymity. Additionally, the strength of our study lies in the good coverage of the teacher and parent population. These factors contribute valuable insights despite the limitations of self-reported data.

Therefore, to obtain a comprehensive understanding of the challenges and methods of cybersecurity education, we propose to conduct a multi method study throughout the education semester involving both students and teachers and aims to provide tested results and effective assessments. We also intend to explore the correlations between the types of risk and effective teaching methods, determining whether specific methods are required for each risk to achieve prevention goals. While a full qualitative analysis is beyond the scope of this paper, the quantitative findings point toward interesting areas for further exploration. Future research could delve deeper into the nuances of responses using qualitative methods such as interviews or focus groups.

VII. CONCLUSION

The rise of the Internet has caused significant changes in the lives of children around the world. Consequently, it is imperative to consider the security implications of this change. Our research examined the importance of integrating cybersecurity in schools, including its causes, motivations, challenges, and appropriate approaches. To this end, we surveyed parents and teachers in Bahrain, which revealed a unanimous agreement on the significance of this issue. The need to initiate cybersecurity education at the earliest possible stages was also highlighted. This is due to the substantial time children spend online and the increasing variety and the accelerating pace of cyberthreats targeting them. Our review of related works identified several research gaps in various aspects of this topic, which we intend to investigate to fill these gaps. The discussion revealed that this topic is dynamic and depends on the geographical context, as the learning process can heavily rely on the nature of cyber threats that undoubtedly vary from one location to another. Furthermore, the capabilities of countries and governments, in addition to the social awareness of cybersecurity and its importance, play a crucial role.

In general, our study emphasises the importance of cybersecurity education in schools, highlighting its importance in protecting children from the growing threat of cybercrime. It also underscores the need for further research and investigation to identify the most effective approaches to cybersecurity education and to raise awareness of this critical issue.

In conclusion, our belief in the importance of our research lies in the establishment of foundations and preconceptions related to cybersecurity education in educational institutions, which Bahrain and many other countries have been striving for in recent years, coinciding with the increase in the rate of cybercrimes. Before concluding, on the basis of the results and conclusions of our study, we would like to present the following recommendations and suggestions:

Inclusion of educational security in schools is a priority. Educational institutions should initiate practical steps to allow evaluative studies, discussions of methodologies, challenges, and the enhancement of their effectiveness over the years, with the aim of developing a conscious society of children capable of addressing the cyber threats targeting them.

However, extensive training for teaching staff, in terms of raising awareness of the subject or teaching methods, is a prerequisite for the educational process. In addition, it is essential to promote a culture and awareness of cybersecurity in the child's surrounding environment, including parents, teachers, and others. This will help overcome the obstacles faced in the educational process. We also recommend studying the relationship between different types of cybercrime and threats and teaching methods in terms of their impact and effectiveness. Consequently, this knowledge can be applied to address the most prevalent risks among children and students in an educational setting.

REFERENCES

[1] A. Yang, C. Lu, J. Li, X. Huang, T. Ji, X. Li, and Y. Sheng, "Application of meta-learning in cyberspace security: A survey," *Digit. Commun. Netw.*, vol. 9, no. 1, pp. 67–78, Feb. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864822000281

[2] K. S. Kurniasanti, P. Assandi, R. I. Ismail, M. W. S. Nasrun, and T. Wiguna, "Internet addiction: A new addiction?" *Med. J. Indonesia*, vol. 28, no. 1, pp. 82–91, 2019.

[3] OECD, *PISA 2015 Results (Volume III): Students' Well-Being, PISA*. Paris, France: OECD Publishing, 2017, doi: 10.1787/9789264273856-en.

[4] J. H. Graafland, "New technologies and 21st century children: Recent trends and outcomes," Org. Econ. Co-Oper. Develop., Paris, France, Tech. Rep. EDU/WKP(2018)15, 2018.

[5] L. Hopkins, F. Brookes, and J. Green, "Books, bytes and brains: The implications of new knowledge for children's early literacy learning," *Australas. J. Early Childhood*, vol. 38, no. 1, pp. 23–28, Mar. 2013.

[6] (2022). *Why Children Are Unsafe in Cyberspace*. Accessed: Nov. 13, 2023. [Online]. Available: https://www.bcg.com/publications/2022/why-children-are-unsafe-in-cyberspace

[7] FBO Investigation. (2015). *Tnternet Crimes Report (2015–2022)*. Accessed: Nov. 14, 2023. [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

[1] According to the latest statistics from the Ministry of Education, more than two-thirds of students (68.01%) attend government schools. The same percentage applies to the number of government schools compared to the total number of schools (66.67%). Further information about published statistics are available online[2]

[8] K. Kopecký, "Online blackmail of Czech children focused on so-called 'sextortion'(analysis of culprit and victim behaviors)," *Telematics Informat.*, vol. 34, no. 1, pp. 11–19, 2017.

[9] H. Lahiani and M. S. Al-Khaza'leh, "Cybercrime and harassment: The impact of blackmailing on Jordanian society as a case study," *J. Intercultural Commun.*, vol. 23, no. 3, pp. 117–123, 2023, doi: 10.36923/jicc.v23i3.99.

[10] S. Livingstone, L. Kirwil, C. Ponte, and E. Staksrud, "In their own words: What bothers children online?" *Eur. J. Commun.*, vol. 29, no. 3, pp. 271–288, Jun. 2014.

[11] I. Kwan, K. Dickson, M. Richardson, W. MacDowall, H. Burchett, C. Stansfield, G. Brunton, K. Sutcliffe, and J. Thomas, "Cyberbullying and children and young people's mental health: A systematic map of systematic reviews," *Cyberpsychol., Behav., Social Netw.*, vol. 23, no. 2, pp. 72–82, Feb. 2020.

[12] V. Chang, L. Golightly, Q. A. Xu, T. Boonmee, and B. S. Liu, "Cybersecurity for children: An investigation into the application of social media," *Enterprise Inf. Syst.*, vol. 17, no. 11, Nov. 2023, Art. no. 2188122.

[13] G. Hornor, "Child and adolescent pornography exposure," *J. Pediatric Health Care*, vol. 34, no. 2, pp. 191–199, Mar. 2020.

[14] J. Zhao, G. Wang, C. Dally, P. Slovak, J. Edbrooke-Childs, M. Van Kleek, and N. Shadbolt, "'I make up a silly name': Understanding children's perception of privacy risks online," in *Proc. CHI Conf. Human Factors Comput. Syst.*, May 2019, pp. 1–13.

[15] J. Davidson and E. Martellozzo. (2015). *Kingdon of Bahrai: National Internet Safety Review*. Accessed: Nov. 13, 2023. [Online]. Available: https://www.tra.org.bh/Media/Awareness-Campaigns/nisr/NISR_report_English1.pdf

[16] M. Al-Mannai. (2015). *Child Online Protection Kingdom of Bahrain*. Accessed: Nov. 13, 2023. [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/ArabStates/Documents/events/2015/COP/Presentations/SessionI/Bahrain_COP%20Bahrain.pdf

[17] Y. Chen and S. S. Gau, "Sleep problems and internet addiction among children and adolescents: A longitudinal study," *J. Sleep Res.*, vol. 25, no. 4, pp. 458–465, Aug. 2016.

[18] N. B. Alotaibi and M. Mukred, "Factors affecting the cyber violence behavior among Saudi youth and its relation with the suiciding: A descriptive study on university students in Riyadh city of KSA," *Technol. Soc.*, vol. 68, Feb. 2022, Art. no. 101863.

[19] N. Ahmad, U. A. Mokhtar, W. F. P. Fauzi, Z. A. Othman, Y. H. Yeop, and S. N. Huda Sheikh Abdullah, "Cyber security situational awareness among parents," in *Proc. Cyber Resilience Conf. (CRC)*, Nov. 2018, pp. 1–3.

[20] N. Alqahtani, S. Furnell, S. Atkinson, and I. Stengel, "Internet risks for children: Parents' perceptions and attitudes: An investigative study of the Saudi context," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2017, pp. 98–103.

[21] T. Abdullah, A. U. Haq, and A. W. Qureshi, "Assessing the role of teachers & parents in developing strategies against social media misuse among students," *Gomal Univ. J. Res.*, vol. 39, no. 3, pp. 341–354, Sep. 2023.

[22] D. Ktoridou, N. Eteokleous, and A. Zahariadou, "Exploring parents' and children's awareness on internet threats in relation to internet safety," *Campus-Wide Inf. Syst.*, vol. 29, no. 3, pp. 133–143, Jun. 2012.

[23] NCS Centre. (2023). *National Cyber Security Alliance Survey Reveals the Complex Digital Lives of American Teens and Parents*. Accessed: Nov. 13, 2023. [Online]. Available: https://staysafeonline.org/News-Press/Survey-Reveals-Complex-Digital-Lives/

[24] F. A. Aloul, "Information security awareness in UAE: A survey paper," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, Nov. 2010, pp. 1–6.

[25] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi, and F. Khalid, "The importance of cybersecurity education in school," *Int. J. Inf. Educ. Technol.*, vol. 10, no. 5, pp. 378–382, 2020.

[26] L. Ilomäki, M. Lakkala, V. Kallunki, D. Mundy, M. Romero, T. Romeu, and A. Gouseti, "Critical digital literacies at school level: A systematic review," *Rev. Educ.*, vol. 11, no. 3, p. e3425, Dec. 2023.

[27] CMRPI. (2023). *CMRPI Prevention Plan—Childmolestation prevention.org*. Accessed: Nov. 13, 2023. [Online]. Available: https://www.childmolestationprevention.org/cmrpi-prevention-plan

[28] W. H. Organisation. (2022). *Child Maltreatment*. Accessed: Nov. 13, 2023. [Online]. Available: Https://Www.Who.Int/News-Room/Fact-Sheets/Detail/Child-Maltreatment

[29] A. M. Magarey, T. L. Pettman, A. Wilson, and N. Mastersson, "Changes in primary school children's behaviour, knowledge, attitudes, and environments related to nutrition and physical activity," *Int. Scholarly Res. Notices*, vol. 2013, p. 10, 2013, Art. no. 752081, doi: 10.1155/2013/752081.

[30] A. Patterson, L. Ryckman, and C. Guerra, "A systematic review of the education and awareness interventions to prevent online child sexual abuse," *J. Child Adolescent Trauma*, vol. 15, no. 3, pp. 857–867, Sep. 2022.

[31] A. A. Al Shamsi, "Effectiveness of cyber security awareness program for young children: A case study in UAE," *Int. J. Inf. Technol. Lang. Stud.*, vol. 3, no. 2, pp. 8–29, 2019.

[32] H. R. Schugar, C. A. Smith, and J. T. Schugar, "Teaching with interactive picture e-books in grades K–6," *Reading Teacher*, vol. 66, no. 8, pp. 615–624, May 2013.

[33] D. Ondrušková and R. Pospíšil, "The good practices for implementation of cyber security education for school children," *Contemp. Educ. Technol.*, vol. 15, no. 3, p. ep435, Jul. 2023.

[34] A. W. Fazil, M. Hakimi, S. Sajid, M. M. Quchi, and K. Q. Khaliqyar, "Enhancing internet safety and cybersecurity awareness among secondary and high school students in afghanistan: A case study of badakhshan province," *Amer. J. Educ. Technol.*, vol. 2, no. 4, pp. 50–61, Nov. 2023.

[35] D. Craigen, N. Diakun-Thibault, and R. Purse, "Technology innovation management review defining cybersecurity," Technol. Innov. Manage. Rev., Ottawa, ON, Canada, 2014.

[36] E. Luiijf, K. Besseling, and P. D. Graaf, "Nineteen national cyber security strategies," *Int. J. Crit. Infrastructures*, vol. 9, no. 1, pp. 3–31, 2013.

[37] S. Yusif, A. Hafeez-Baig, and C. Anachanser, "Internet governance and cyber-security: A systematic literature review," *Inf. Secur. J., A Global Perspective*, vol. 33, no. 2, pp. 158–171, Mar. 2024.

[38] N. C. S. Centre. (2023). *What is Cyber Security?* Accessed: Nov. 11, 2023. [Online]. Available: https://www.ncsc.gov.uk/Section/about-Ncsc/What-Is-Cyber-Security#

[39] L. Blanc, "Défense et sécurité nationale," République Francaise, Tech. Rep., 2013.

[40] G-India. *Ministry of Electronics & Information Technology*. Accessed: Nov. 11, 2023. [Online]. Available: https://www.meity.gov.in/sites/upload_files/dit/files/compilation_comments_NCSPwebv2_18112011.pdf

[41] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[42] N. Liu, A. Nikitas, and S. Parkinson, "Exploring expert perceptions about the cyber security and privacy of connected and autonomous vehicles: A thematic analysis approach," *Transp. Res. F, Traffic Psychol. Behaviour*, vol. 75, pp. 66–86, Nov. 2020.

[43] A. Nikitas, S. Parkinson, and M. Vallati, "The deceitful connected and autonomous vehicle: Defining the concept, contextualising its dimensions and proposing mitigation policies," *Transp. Policy*, vol. 122, pp. 1–10, Jun. 2022.

[44] R. Mubarak, T. Alsboui, O. Alshaikh, I. Inuwa-Dutse, S. Khan, and S. Parkinson, "A survey on the detection and impacts of deepfakes in visual, audio, and textual formats," *IEEE Access*, vol. 11, pp. 144497–144529, 2023.

[45] 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, Apr. 2024, Art. no. 103694.

[46] S. Khan, S. Parkinson, L. Grant, N. Liu, and S. Mcguire, "Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security," *ACM Comput. Surveys*, vol. 53, no. 4, pp. 1–29, Jul. 2021.

[47] S. Parkinson, S. Khan, A. Badea, A. Crampton, N. Liu, and Q. Xu, "An empirical analysis of keystroke dynamics in passwords: A longitudinal study," *IET Biometrics*, vol. 12, no. 1, pp. 25–37, Jan. 2023.

[48] S. Parkinson and S. Khan, "A survey on empirical security analysis of access-control systems: A real-world perspective," *ACM Comput. Surv.*, vol. 55, no. 6, pp. 1–28, Jul. 2023.

[49] G. Cohen Zilka, "Awareness of eSafety and potential online dangers among children and teenagers," *J. Inf. Technol. Educ., Res.*, vol. 16, pp. 319–338, Jan. 2017.

[50] D. Greyson, C. Chabot, C. Mniszak, and J. A. Shoveller, "Social media and online safety practices of young parents," *J. Inf. Sci.*, vol. 49, no. 5, pp. 1344–1357, Oct. 2023.

[51] S. Livingstone, J. Davidson, J. Bryce, S. Batool, C. Haughton, and A. Nandi, "Children's online activities, risks and safety: A literature review by the UKCCIS evidence group," LSE Consulting, London, U.K., Tech. Rep., 2017. [Online]. Available: https://eprints.lse.ac.uk/84956/1/Literature%20Review%20Final%20October%202017.pdf

[52] U. Hasebrink, S. Livingstone, L. Haddon, and K. Ólafsson, "Comparing children's online opportunities and risks across Europe: Cross-national comparisons for EU Kids Online," EU Kids Online, Deliverable D3.2, 2nd ed., LSE, London, U.K., 2009.

[53] S. Livingstone, *Children and the Internet: Great Expectations, Challenging Realities*. Polity Press, 2008.

[54] V. Slavtcheva-Petkova, V. J. Nash, and M. Bulger, "Evidence on the extent of harms experienced by children as a result of online risks: Implications for policy and research," *Inf., Commun. Soc.*, vol. 18, no. 1, pp. 48–62, Jan. 2015.

[55] A. Farrukh, R. Sadwick, and J. Villasenor, "Youth internet safety: Risks, responses, and research recommendations," 2014. Accessed: Jun. 2024. [Online]. Available: http://www.brookings.edu/~/media/research/files/papers/2014/10/21-youth-internet-safety-farrukh-sadwick-villasenor/youth-internet-safety_v07.pdf

[56] K. J. Mitchell, J. Wolak, and D. Finkelhor, "Trends in youth reports of sexual solicitations, harassment and unwanted exposure to pornography on the internet," *J. Adolescent Health*, vol. 40, no. 2, pp. 116–126, Feb. 2007.

[57] T. B. Q. Li, "Cyber-harassment: A study of a new method for an old behavior," *J. Educ. Comput. Res.*, vol. 32, no. 3, pp. 265–277, Apr. 2005.

[58] F. Pereira, B. H. Spitzberg, and M. Matos, "Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents," *Comput. Hum. Behav.*, vol. 62, pp. 136–146, Sep. 2016.

[59] R. Slonje, P. K. Smith, and A. Frisén, "The nature of cyberbullying, and strategies for prevention," *Comput. Hum. Behav.*, vol. 29, no. 1, pp. 26–32, Jan. 2013.

[60] R. A. Sabella, J. W. Patchin, and S. Hinduja, "Cyberbullying myths and realities," *Comput. Hum. Behav.*, vol. 29, no. 6, pp. 2703–2711, Nov. 2013.

[61] M. Madden, S. Cortesi, U. Gasser, A. Lenhart, and M. Duggan, "Parents, teens, and online privacy," 2012. Accessed: Jun. 18, 2024. [Online]. Available: https://www.pewinternet.org/2012/11/20/parents-teens-and-online-privacy/

[62] S. Livingstone, L. Haddon, and A. Görzig, *Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective*. Bristol, U.K.: Policy Press, 2012.

[63] F. Annansingh and T. Veli, "An investigation into risks awareness and e-safety needs of children on the internet: A study of devon, UK," *Interact. Technol. Smart Educ.*, vol. 13, no. 2, pp. 147–165, Jun. 2016.

[64] A. E. Al-Naser, A. Bushager, and H. Al-Junaid, "Parents' awareness and readiness for smart devices' cybersecurity," in *Proc. 2nd Smart Cities Symp. (SCS)*, Mar. 2019, pp. 1–7.

[65] A. K. Alsaiari. *Overcoming Cultural Taboos: Protecting Children Online in Saudi Arabia*. Accessed: Nov. 13, 2023. [Online]. Available: https://blogs.lse.ac.uk/Parenting4digitalfuture/2019/06/12/Overcoming-Cultural-Taboos-Protecting-Children-Online-in-Saudi-Arabia/

[66] A. Sarri, P. Kyranoudi, A. Thirriot, F. Charelli, and Y. Dominique. (2023). *National Capabilities Assessment Framework*. Accessed: Nov. 13, 2023. [Online]. Available: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

[67] R. Shillair, P. Esteve-González, W. H. Dutton, S. Creese, E. Nagyfejeo, and B. von Solms, "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise," *Comput. Secur.*, vol. 119, Aug. 2022, Art. no. 102756.

[68] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Comput. Secur.*, vol. 119, Aug. 2022, Art. no. 102754.

[69] W. Cassidy, K. Brown, and M. Jackson, "'Making kind cool': Parents' suggestions for preventing cyber bullying and fostering cyber kindness," *J. Educ. Comput. Res.*, vol. 46, no. 4, pp. 415–436, 2012.

[70] L. Plowman, J. McPake, and C. Stephen, "The technologisation of childhood? Young children and technology in the home," *Children Soc.*, vol. 24, no. 1, pp. 63–74, Jan. 2010.

[71] H. Hammami and H. U. Khan, "Measuring internet addiction in Europe-based knowledge societies: A case study of France," *Int. J. Bus. Inf. Syst.*, vol. 32, no. 2, pp. 199–218, 2019.

[72] I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's,'" *Heliyon*, vol. 5, no. 12, pp. 1–8, 2019.

[73] N. Wager, B. Gallagher, R. Armitage, M. Rogerson, K. Christmann, S. Parkinson, C. Reeves, M. Ioannou, and J. Synnott, "Rapid evidence assessment: Quantifying online facilitated child sexual abuse: Report for the independent inquiry into child sexual abuse," Univ. Huddersfield, Huddersfield, U.K., Tech. Rep., 2018.

[74] S. Khan, S. Parkinson, M. Roopak, R. Armitage, and A. Barlow, "Automated planning to prioritise digital forensics investigation cases containing indecent images of children," in *Proc. Int. Conf. Automated Planning Scheduling*, 2023, vol. 33, no. 1, pp. 500–508.

[75] M. Roopak, S. Khan, S. Parkinson, and R. Armitage, "Comparison of deep learning classification models for facial image age estimation in digital forensic investigations," *Forensic Sci. Int., Digit. Invest.*, vol. 47, Dec. 2023, Art. no. 301637.

[76] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour Inf. Technol.*, vol. 33, no. 3, pp. 237–248, Mar. 2014.

[77] M. J. Boulton, L. Boulton, E. Camerone, J. Down, J. Hughes, C. Kirkbride, R. Kirkham, P. Macaulay, and J. Sanders, "Enhancing primary school children's knowledge of online safety and risks with the CATZ cooperative cross-age teaching intervention: Results from a pilot study," *Cyberpsychol., Behav., Social Netw.*, vol. 19, no. 10, pp. 609–614, Oct. 2016.

[78] L. Zhang-Kennedy, Y. Abdelaziz, and S. Chiasson, "Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy," *Int. J. Child-Comput. Interact.*, vol. 13, pp. 10–18, Jul. 2017.

[79] E. Lastdrager, I. C. Gallardo, P. Hartel, and M. Junger, "How effective is anti-phishing training for children?" in *Proc. 13th Symp. Usable Privacy Secur.*, 2017, pp. 229–239.

[80] K. E. Waldock, V. Miller, S. Li, and V. N. L. Franqueira, "Pre-university cyber security education: A report on developing cyber skills amongst children and young people," Global Forum Cyber Expertise, 2022, p. 159. [Online]. Available: https://kar.kent.ac.uk/96040/1/GFCE-report-20220731.pdf

[81] F. V. Binder, M. Nichols, S. Reinehr, and A. Malucelli, "Challenge based learning applied to mobile software development teaching," in *Proc. 30th IEEE Conf. Softw. Eng. Educ. Training (CSEE)*, Savannah, GA, USA, 2017.

[82] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber security behaviour among higher education students in Malaysia," *J. Inf. Assurance Cybersecurity*, vol. 2017, pp. 1–13, Feb. 2017.

[83] P. Pusey and W. Sadera, "Preservice teacher concerns about teaching cyberethics, cybersafety, and cybersecurity: A focus group study," in *Proc. Soc. Inf. Technol. Teacher Educ. Int. Conf.*, 2012, pp. 3415–3419.

[84] V. Pastor, G. Díaz, and M. Castro, "State-of-the-art simulation systems for information security education, training and awareness," in *Proc. IEEE EDUCON Conf.*, Apr. 2010, pp. 1907–1916.

[85] K. Salamzada, Z. Shukur, and M. Abu Bakar, "A framework for cybersecurity strategy for developing countries: Case study of Afghanistan," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 4, no. 1, pp. 1–10, Jun. 2015.

[86] D. Miles, "Youth protection: Digital citizenship—Principles & new resources," in *Proc. 2nd Worldwide Cybersecurity Summit (WCS)*, Jun. 2011, pp. 1–3.

[87] S. Al-Janabi and I. Al-Shourbaji, "A study of cyber security awareness in educational environment in the middle east," *J. Inf. Knowl. Manage.*, vol. 15, no. 1, Mar. 2016, Art. no. 1650007.

[88] A. L. Zepf and Z. Peterson, *Cyber-Security Curricula for Basic Users*. Monterey, CA, USA: Naval Postgraduate School, 2013.

[89] Wm. A. Conklin, R. E. Cline, and T. Roosa, "Re-engineering cybersecurity education in the US: An analysis of the critical factors," in *Proc. 47th Hawaii Int. Conf. Syst. Sci.*, Jan. 2014, pp. 2006–2014.

[90] A. E. McDaniel, "Securing the information and communications technology global supply chain from exploitation: Developing a strategy for education, training, and awareness," *Issues Informing Sci. Inf. Technol.*, vol. 10, no. 2012, pp. 313–324, 2013, doi: 10.28945/1813.

[91] S. H. Kim, K. H. Yang, and S. Park, "An integrative behavioral model of information security policy compliance," *Scientific World J.*, vol. 2014, pp. 1–12, Jan. 2014.

[92] A. Banga and S. Jaswal, "Parent-teacher perception of early childhood education," *J. Hum. Ecol.*, vol. 12, no. 6, pp. 449–455, 2001.

[93] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, Sep. 1951.

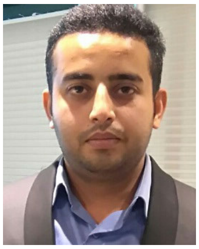
[94] G. Murazvu, S. Parkinson, S. Khan, N. Liu, and G. Allen, "A survey on factors preventing the adoption of automated software testing: A principal component analysis approach," *Software*, vol. 3, pp. 1–27, 2024, doi: 10.3390/software3010001.

MOHAMED AYYASH received the master's degree in cybersecurity and digital forensics from the University of Huddersfield, where he conducted this research supporting the degree requirements. He is currently a Police Officer at the Ministry of Interior, Bahrain. Alongside his duties as an Operation and IT Officer, he is engaged in the Ministry's strategic plans to integrate digital tools and technologies into their operational framework, while simultaneously promoting cybersecurity awareness within the community.

TARIQ ALSBOUI received the B.Sc. degree in internet computing from Manchester Metropolitan University, U.K., in 2010, and the Ph.D. degree in computer science from the University of Huddersfield, U.K., in 2021. He is currently a Lecturer in computing with the School of Computing and Engineering, University of Huddersfield. He has authored several peer-reviewed international journals and conference papers. He is a fellow of the Higher Education Academy (FHEA). He is a Reviewer of high-impact-factor journals, such as IEEE Access and IEEE Internet of Things Journal.

OMAR ALSHAIKH received the M.Sc. degree in operations management to obtain the core knowledge in strategy, planning and operations management. He is currently pursuing the Ph.D. degree with the University of Huddersfield. He is also a Police Officer at the Ministry of Interior, Bahrain. He is an artificial intelligence and leadership enthusiast; one of his roles in his career as a member of Bahrain law enforcement is to integrate cutting-edge technology to enhance the pedagogical methods in police sciences by carrying out simulations of virtual reality to meet the renewed security challenges. He is a fellow of the Higher Education Academy, U.K.

ISA INUWA-DUTSE received the first degree from Bayero University Kano, Nigeria, the M.Sc. degree from The University of Manchester, and the Ph.D. degree in computer science from Edge Hill University, U.K. He is currently a Lecturer with the University of Huddersfield. His previous roles include a Graduate Teaching Assistant with Edge Hill University, U.K.; and a full-time Lecturer with the Department of Computer Science, Federal University Dutse; and the Department of Statistics and Computer Science, Kano State Polytechnic. His research interests include artificial intelligence, text mining, and social network analysis and modeling. Some of his research publications appeared in major academic conferences and journals. He is a fellow of the Advance Higher Education, U.K. (formerly HEA). He holds a full membership of the British Computer Society, the Computer Professional Council of Nigeria, and the Royal Statistical Society, U.K. He contributes to various conferences and journals as a reviewer.



SAAD KHAN is currently a Senior Lecturer with the School of Computing and Engineering, University of Huddersfield, and a part of the Centre for Cybersecurity. His research interests include developing and utilizing artificial intelligence and machine learning techniques for cybersecurity in various domains, such as SIEM systems, vulnerability and anomaly detection, learning domain knowledge, mitigation planning, and access control.

SIMON PARKINSON is currently a Professor with the Department of Computer Science, University of Huddersfield, where he is also leading the Centre for Cybersecurity. His research interests include computer security and artificial intelligence. This includes undertaking research in biometric authentication systems and access control policy analysis. He has authored numerous papers on these topics as well as other cross-discipline applications of artificial intelligence, where he has a special interest in automated planning.