Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.043935

ARTICLE

Enhancing Cybersecurity Competency in the Kingdom of Saudi Arabia: A Fuzzy Decision-Making Approach

Wajdi Alhakami*

Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia

*Corresponding Author: Wajdi Alhakami. Email: whakami@tu.edu.sa

Received: 16 July 2023 Accepted: 21 November 2023 Published: 15 May 2024

ABSTRACT

The Kingdom of Saudi Arabia (KSA) has achieved significant milestones in cybersecurity. KSA has maintained solid regulatory mechanisms to prevent, trace, and punish offenders to protect the interests of both individual users and organizations from the online threats of data poaching and pilferage. The widespread usage of Information Technology (IT) and IT Enable Services (ITES) reinforces security measures. The constantly evolving cyber threats are a topic that is generating a lot of discussion. In this league, the present article enlists a broad perspective on how cybercrime is developing in KSA at present and also takes a look at some of the most significant attacks that have taken place in the region. The existing legislative framework and measures in the KSA are geared toward deterring criminal activity online. Different competency models have been devised to address the necessary cybercrime competencies in this context. The research specialists in this domain can benefit more by developing a master competency level for achieving optimum security. To address this research query, the present assessment uses the Fuzzy Decision-Making Trial and Evaluation Laboratory (Fuzzy-DMTAEL), Fuzzy Analytic Hierarchy Process (F.AHP), and Fuzzy TOPSIS methodology to achieve segment-wise competency development in cyber security policy. The similarities and differences between the three methods are also discussed. This cybersecurity analysis determined that the National Cyber Security Centre got the highest priority. The study concludes by perusing the challenges that still need to be examined and resolved in effectuating more credible and efficacious online security mechanisms to offer a more empowered ITES-driven economy for Saudi Arabia. Moreover, cybersecurity specialists and policymakers need to collate their efforts to protect the country's digital assets in the era of overt and covert cyber warfare.

KEYWORDS

Cyber security; fuzzy DMTAEL; security policy; cyber crime; MCDM

1 Introduction

Over the past few years, there has been a notable surge in smartphone and digital communication devices adoption. This observable shift is similarly evident in the Middle East, with a particular focus on the Kingdom of Saudi Arabia (KSA) [1]. Following a strategic directive from the Saudi Arabian government, the use of computers in business, education, health, and other daily life became

widespread in 2007 [2]. The Communication and Information Technology Commission of the KSA oversees technology and communication services in Saudi Arabia. It conducts annual surveys of all market segments, citing a marked increase in the use of computers and online services [3]. The use of computers by individuals and commercial organizations rose from 43% in 2007 to 51% in 2009 [4]. Information and communications technology grew into a goal in and of itself with the development of the internet, making communication access more straightforward, affordable, and smoother. The KSA in IT infrastructure and IT Enable Services (ITES) investments was to modernize the economy and establish the country as a leader in the digital economy. It uses computers, software, and other digital technologies to process, store, and transmit information. IT infrastructure refers to the hardware, software, and networks that support the use of IT in an organization or country. ITES relates to services delivered using IT, such as e-commerce, online banking, and telemedicine.

The investments made by Saudi Arabia in IT infrastructure and ITES are significant because they have the potential to transform the economy and create new opportunities for businesses and individuals. For example, e-commerce platforms can enable small businesses to reach a wider audience and compete with larger companies. Online banking can make financial services more accessible to people in remote areas. Telemedicine can improve access to healthcare for people who live far from medical facilities. The investments made by Saudi Arabia in IT infrastructure and ITES reflect a commitment to modernization and innovation. By embracing digital technologies, the country is positioning itself for success in the global economy [5–8]. These hypotheses were made to help the realm progress on the United Nations e-Government Development Index (UN EGDI) and e-Participation Index (EPI). Table 1 compares the Middle Eastern countries' standings on the UN EGDI during the last ten years.

Table 1: Comparison with the Middle Eastern Countries [6]

Country	EGDI rank 2012	EGDI rank 2022	Change +/−
KSA	70	58	22
IRAN	110	86	24
TURKEY	76	53	23
UAE	32	21	11
QATAR	45	51	6
OMAN	94	63	31
BAHRAIN	42	26	16
EGYPT	89	114	25

The most recent statistics demonstrate that internet users worldwide have consistently risen over the past few years. It is more than twice as many as the 2.53 billion users 2013 [9–11]. This report results in an average yearly growth rate over time, as shown in Fig. 1.

Cybersecurity is the planning, choice, and application of technologies, procedures, and techniques to safeguard private information in cyberspace from intruders and criminals who might harm or misdirect businesses. This means that only authorized personnel may access sensitive data, including software, hardware, information, and the structure of the internet. This is a correct explanation of cybersecurity management in education [5]. There is an urgent need to look at the potential cybersecurity dangers that firms may face, especially regarding sensitive data [6]. With today's digital

designs, hardware and software are not the only components. Systemic political, social, and economic concerns are also mentioned because they are so interwoven that it is nearly impossible to separate humans from IT systems [7]. Despite extensive documentation of the social aspect's impact on cyber operations in the existing literature, more needs to be known about how it pertains to cybersecurity.

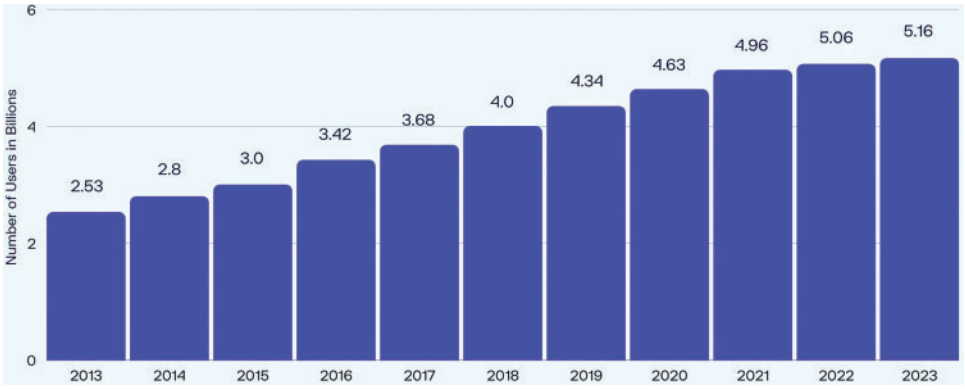

Figure 1: Number of Internet users worldwide 2013–2023 (Source: DataReportal)

Nonetheless, several dangers are impacting management's plan to keep cybersecurity effective. Public, medical, and educational institutions must cope with various cybersecurity problems affecting data management and heightening security risks. One sort of threat is cybercrime, which includes using the system as a target for financial gain. The second threat is political cyber-attacks that seek to collect information for personal advantage. The third is digital psychological warfare, which aims to undermine the electronic structure and instill fear in web users.

The cybersecurity policy and decision-making area in the Kingdom of Saudi Arabia has dramatically benefited from the research presented in this paper. Initially, it thoroughly studies how Saudi Arabia's cybercrime situation is currently developing, underlining the country's main obstacles and dangers regarding internet security. The study provides detailed cybersecurity knowledge by examining noteworthy cyber-attacks and evaluating the current legal system. Furthermore, the study presents and employs cutting-edge fuzzy decision-making methodologies, including the Fuzzy Analytic Hierarchy Process (F.AHP), the Fuzzy Technique for Order of Preference by Similarity to Ideal Solution (Fuzzy TOPSIS), and the Fuzzy Decision-Making Trial and Evaluation Laboratory (Fuzzy-DMTAEL). These techniques are consistently used to develop cybersecurity policy competency in segments. The study carefully examines the parallels and discrepancies between these approaches, offering insights into their relative merits and suitability for use in cybersecurity.

Additionally, focusing on the National Cyber Security Centre, the research determines and ranks important entities within Saudi Arabia's cybersecurity architecture. This prioritization emphasizes how crucial it is to reinforce key elements of the cybersecurity ecosystem to improve the country's defense against cyber threats. The study also offers doable policy suggestions to strengthen Saudi Arabia's cyber security defenses. These suggestions cover various topics, from raising public knowledge and comprehension of cybercrime laws to modernizing and harmonizing legislation to address growing cyber threats. The study emphasizes the need for sanctions for breaking security rules and calls for constructing digital forensics labs to improve the nation's capacity for criminal investigations.

The rest of this study has been organized as follows: Section 2 discusses the related works. Section 3 details the cyber security factors and security measures for cyber security in KSA; Section 4

explains the fuzzy DMATEL methodology and its estimation through the Python program. Section 5 tabulates the results of this analytical study about cyber security threats in KSA. Section 6 concludes the study.

2 Related Work

The related works section delves into earlier research pertinent to this study on cybersecurity and competency advancement in the KSA. By reviewing these publications, researcher can get insights into the existing knowledge landscape and identify research gaps, this study attempts to fill. The segments outline each study's significant contributions and findings, emphasizing their importance to this research on cybersecurity skill development in KSA.

2.1 Cyber Security Policy

At least two of Saudi Arabia's cities will be listed among the top 100 future intelligent cities. Thoughts concerning cyber security are still being raised by the everyday appearance of threats like phishing and denial of service, as well as by incorporating innovative technologies and more city connections. Hence, the need for a cybersecurity policy framework in Saudi Arabia to protect parties involved in smart cities from online dangers is becoming more imminent daily. A smart city is a city that uses technology to improve the quality of life for its citizens, such as through the use of sensors to monitor traffic or air quality. However, with the increased use of technology comes the risk of cyber-attacks, which can compromise the security and privacy of individuals and organizations. A cybersecurity policy framework is a set of guidelines and procedures that outline how to protect against cyber threats. It includes risk assessments, security controls, incident response plans, and employee training. By implementing a cybersecurity policy framework, Saudi Arabia can ensure that its intelligent cities are secure and that the parties involved are protected from online dangers [12–15]. This text emphasizes the importance of cybersecurity in smart cities and the need for a policy framework to protect against cyber threats effectively. One that uses all the connected data at their disposal is much more likely to understand, manage, and employ the resources at their disposal. Every effort to build a world-class city has at least one goal: making the most of the innovation and foundation already in place, delivering greener technologies while keeping an eye on environmental challenges, and not having pollution or traffic jams. Another critical goal is the moderate and cautious planning of metropolitan development. Unprecedented growth in unsustainable urbanization has been observed in recent years. They need more public infrastructure, adequate public transportation, renewable technologies, and relief from congestion. Cybersecurity issues are caused anxiety, worsened pressure, and psychological difficulties.

2.2 Policy Challenges

Smart cities in the United States have faced sporadic cybersecurity vulnerabilities, such as when the Texas Health and Human Services Commission inadvertently disclosed sensitive information about 6,617 patients in Dallas. The hack happened when the old, secured public server was replaced. The organization was fined $1.6 million for violating HIPAA due to system and process flaws. The federal government's participation proved the importance of a centrally coordinated plan for creating and sustaining cyber security. Two more cases highlight the continuous cybersecurity concerns that intelligent cities in the United States confront. One such case was the hacking of Omni Hotels & Resorts in Dallas. Alarms were set off deliberately in another incident in Chicago. In response to these breaches, federal and state agencies launched a mix of cybersecurity operations and upgraded

database security measures. As a result, life became self-conscious, with increased pressure and mental health difficulties. The Office of Cyber and Infrastructure Analysis (OCIA) of the Department of Homeland Security (DHS) assesses the threats presented by cyberspace infrastructure. The OCIA provides a framework for risk assessment and mitigation in the country's expanding number of smart cities [16–19].

A report by OCIA examined how the nation's smart cities can handle the mounting dangers in the cyber-physical space [13–15]. In addition to the country's current cybercrime regulations, the OCIA has suggested a three-tiered strategy for addressing risks to cyber cities. The first is to provide safety at the revolving lines separating the rural and urban areas and between the current and future infrastructure. The spaces between systems are evolving as they get networked and improved. These modifications make it simpler for cyber poachers to invade systems and tamper with data. The OCIA suggests using this platform to detect and prevent assaults in smart cities [20–22]. The OCIA's second recommendation is to make better use of intelligent infrastructure overall. The organization asserts that the development of vital infrastructure will occur at varied rates and stages depending on user preferences, finance, and resource availability with OCIA. The organization worries that ecosystem inconsistencies will significantly complicate securing the intelligent city. Due to the blind spots created when the old and new systems overlap, cybercrime is made simpler. This problem arises naturally in many of the country's intelligent cities as new technology is integrated into the old infrastructure. Cities must have a uniform security policy for them to succeed. The organization also urges the automation of more procedures in intelligent cities [23–26].

There have been several cyber-attacks [27–30] reported in KSA during the last few years; some of the attacks are listed in Table 2.

Table 2: List of cyber security threat in KSA

Cyber security attack	Effect
Shamoon 2.0	This malware, which purports to delete data from a compromised computer, was the cause of a devastating attack on Saudi Aramco in 2012.
Operation PZChao	A cyber-espionage group allegedly located in China started an operation explicitly targeted at Saudi Arabia. The organization that stole a lot of data from numerous firms was known as APT10 or Stone Panda.
OilRig	A group of hackers believed to be connected to the Iranian government targeted Saudi Arabian institutions in June 2018, including government agencies and energy businesses. The organization, also known as OilRig or APT34, used malware and phishing emails, among other tactics, to carry out their attacks.
ZeroCleare	In November 2018, a fresh malware variant called ZeroCleare was found in Saudi Arabia. The Iranian government has been linked to this malware, which was made to attack critical infrastructure and industrial control systems.
Shamoon 3	Another variant of the Shamoon virus, known as Shamoon 3, was discovered in Saudi Arabia in December 2018 and January 2019. This malware, which is supposed to delete data from a system that has been hacked, was behind a terrible attack on Saudi Aramco in 2012.

(Continued)

Table 2 (continued)

Cyber security attack	Effect
OilRig 2.0	The cyber espionage outfit OilRig considered connected to the Iranian government, continued to target Saudi Arabian corporations in 2019. The organization used malware and spear-phishing emails, among other tactics, to carry out their attacks.
APT33	In 2019, the cyber espionage organization APT33, considered connected to the Iranian government, targeted several Saudi Arabian companies. The organization used malware and spear-phishing emails, among other tactics, to carry out their attacks.
Magecart	In July 2019, it was revealed that a group of hackers named Magecart had shut down several Saudi Arabian e-commerce websites and stolen cardholder data.
Hades	In August 2019, a fresh strain of malware known as Hades was found in Saudi Arabia. This malware targets crucial infrastructure and industrial control systems.
COVID-19	Attacks with motifs from COVID-19 Globally and in Saudi Arabia, cyberattacks intensified due to the COVID-19 outbreak. The attackers utilized phishing emails and malware with the COVID-19 theme to lure victims into downloading malware or divulging personal information.
OilRig 3.0	The suspected Iranian government-affiliated cyber espionage group OilRig continued to target Saudi Arabian organizations in 2020. The organization used malware and spear-phishing emails, among other tactics, to carry out their attacks.
Dustman	In August 2020, Saudi Arabia reported the discovery of a brand-new strain of malware known as "Dustman." This malware aims to steal data from compromised machines and exfiltrate it to a remote server.
Silence	In September 2020, it was revealed that a brand-new cybercriminal group named Silence had stolen substantial quantities of money from several Saudi Arabian banks.
Qbot	In December 2020, Saudi Arabia found a brand-new Qbot malware version. This malware aims to steal sensitive information and login credentials from compromised systems.
Hafnium	In March 2021, a brand-new cyber espionage group named Hafnium was identified, and it immediately started focusing on Microsoft Exchange servers worldwide, including those in Saudi Arabia. Because the gang could access email accounts and other private data, the government is believed to support them.
OilRig 4.0	The cyber espionage group OilRig, considered connected to the Iranian government, continues to target Saudi Arabian corporations in 2021. The organization used malware and spear-phishing emails, among other tactics, to carry out their attacks.

(Continued)

Table 2 (continued)

Cyber security attack	Effect
Ransomware threats	In 2021, Saudi Arabia was still at risk from ransomware attacks. Cybercriminals have encrypted sensitive data using this type of malware and demanded money in exchange for the decryption key.
Advanced persistent threats, or APT	APTs, which are long-term, targeted attacks done by enemies with many resources and knowledge, were still a problem in 2021. These attacks are usually hard to spot and could significantly affect the thing being attacked.
Ransomware threats	Ransomware assaults are rising, and Saudi Arabia is not the only country to see this trend. In these attacks, cybercriminals encrypt an organization's data and demand payment in exchange for the decryption key.
Phishing and social engineering attacks	Cybercriminals regularly use phishing and social engineering attacks to install malware or access sensitive data. These attacks typically succeed because they are frequently challenging to detect and depend on human error.
Internet of things (IoT) vulnerabilities	As the number of IoT devices in Saudi Arabia keeps increasing, cyberattacks on these devices are becoming more likely. Many IoT devices have security weaknesses that cybercriminals can exploit to access a network or data.
Risks associated with cloud security	New security vulnerabilities could develop as many Saudi Arabian companies shift their apps and data to the cloud. By taking advantage of cloud-related vulnerabilities, including improperly configured cloud services and insufficient access restrictions, cybercriminals can obtain unauthorized access to an organization's data.

Agrawal et al. [31] emphasized the importance of developing innovative web applications that ensure sustainable security for users. They highlighted the significance of security and sustainability attributes in achieving optimal outcomes. They proposed using the Fuzzy Analytic Hierarchy Process (Fuzzy AHP) to assess sustainability goals and long-term impacts. The study examined consecutive versions of two web applications to determine their symmetrical sustainability, and the findings provided valuable insights for enhancing web application sustainability.

Alhakami [32] addressed the challenges in security evaluation, particularly in the power control process security assessment and security levels of control phases. To overcome these challenges, the study introduced a fuzzy technique based on the TOPSIS method for security risk assessment in communication networks. By quantifying security extents and vulnerabilities, the approach demonstrated its utility in evaluating security and presented a methodology for security assessment.

Ahmad et al. [33] employed the critical success factors (CSFs) approach to identify a sustainable E-learning implementation model. Through literature review, expert opinions, and in-depth interviews, they identified fifteen CSFs. They modeled their interdependence using interpretive structural modeling and Matriced' Impacts Croise's Multiplication Appliquée a UN Classement (MICMAC) analysis. The study provided a quantitative analysis of the CSFs and their impact on E-learning sustainability and performance, offering valuable insights for stakeholders to prioritize resources.

Hijji et al. [34] proposed a CAT framework for cybersecurity awareness and training in organizations. The framework consisted of three levels and twenty-five core practices, aiming to help organizations effectively manage security-related challenges and protect critical information. The study conducted case studies to evaluate the framework's usefulness in real-world settings, demonstrating its capability to identify employees' cybersecurity capability levels and enhance their training.

Yeboah-Ofori et al. [35] utilized Cyber Threat Intelligence (CTI) and Machine Learning (ML) techniques to analyze and predict threats in cyber supply chains. They employed ML algorithms and CTI properties to identify vulnerabilities and indicators of compromise. The study focused on improving cyber supply chain security by identifying inherent vulnerabilities and recommending relevant controls.

Almalki et al. [36] proposed a logistics hubs (LHs) allocation model to optimize logistics infrastructure in Saudi Arabia. They integrated multi-logistical, infrastructural, and geographical information system (GIS) layers to identify feasible areas for LHs. The study employed integer linear programming (ILP) to maximize the number of allocated LHs and minimize overall distances, resulting in improved logistics performance.

Alholiby et al. [37] conducted a comparative analysis of the US and Saudi Public Comment (PC) experiences. They aimed to provide a better understanding of the PC concept in both countries and propose recommendations for effective PC implementation in Saudi Arabia. The study examined PC practices conducted by Saudi government agencies before and after PC adoption in the Kingdom.

El Khatib et al. [38] explored the implementation of Big Data Analytics (BDA) in cities in the UAE and other developed nations. They investigated the relationship between BDA success, innovation, technical expertise, and infrastructure quality. The study provided recommendations based on the results applicable to cities such as Dubai.

The relevant studies discussed in this part shed light on many areas of cybersecurity and offer helpful insights for improving cybersecurity expertise in the Kingdom of Saudi Arabia. The research investigations presented in this paper addressed critical issues such as web application sustainability, assessment of security methodologies, E-learning implementation scenarios, cybersecurity education and training frameworks, cyber security in supply chains, transportation infrastructure optimization, and Big Data Analytics deployment. Thus, the preventive steps to reduce the risk of cyber-attacks in Saudi Arabia call for more effective interventions. In this regard, multi-factor authentication and regular security audits are essential for governments and businesses to keep their IT infrastructure secure [30]. Furthermore, this study proposes a Fuzzy Decision-Making Trial and Evaluation Laboratory (Fuzzy-DMTAEL) methodology to develop segment-wise competency in cyber security policy. This research intends to establish a comprehensive fuzzy decision-making approach to improve cybersecurity expertise in Saudi Arabia by synthesizing the findings and recommendations from previous studies. By adopting these findings and recommendations, policymakers and cybersecurity experts may collaborate to defend the country's digital assets and protect its interests in the face of growing cyber threats.

3 Cyber Security Factors and Alternatives

The Kingdom of Saudi Arabia has consulted with various organizations in this area. These organizations have the expertise and knowledge to develop effective strategies and implement best practices for IT and cybersecurity. Consulting with external organizations provides several benefits, including access to the latest technologies, industry best practices, and insights into emerging threats

and vulnerabilities. By partnering with these organizations, Saudi Arabia can stay up-to-date with the latest developments in the field and ensure that its IT and cybersecurity practices are robust and productive. Saudi Arabia is taking a proactive approach to managing IT and cybersecurity. The country is leveraging the expertise of the best minds in the industry to develop and implement foolproof mechanisms that can help protect the country's information infrastructure from cyber threats. A thorough literature research and expert panel interviews are part of the systematic process that went into creating the Hierarchy of Cyber Security Factors and Alternatives. The starting point of the hierarchy is made using a thorough review of the literature that determines the essential elements and variables of cybersecurity. After that, organized interviews are used to tap into the knowledge and experience of security professionals, during which a panel of experts shares their insights, judgments, and prioritisations. A refined and well-structured hierarchy that includes crucial cybersecurity criteria and potential alternatives is produced by integrating literature findings and expert perspectives, strengthening the robustness and relevance of the decision-making framework. Fig. 2 shows the Hierarchy of Cyber Security Factors and Alternatives. In this context, the following actions have been taken by the Kingdom of Saudi Arabia to control different elements of the national information infrastructure.

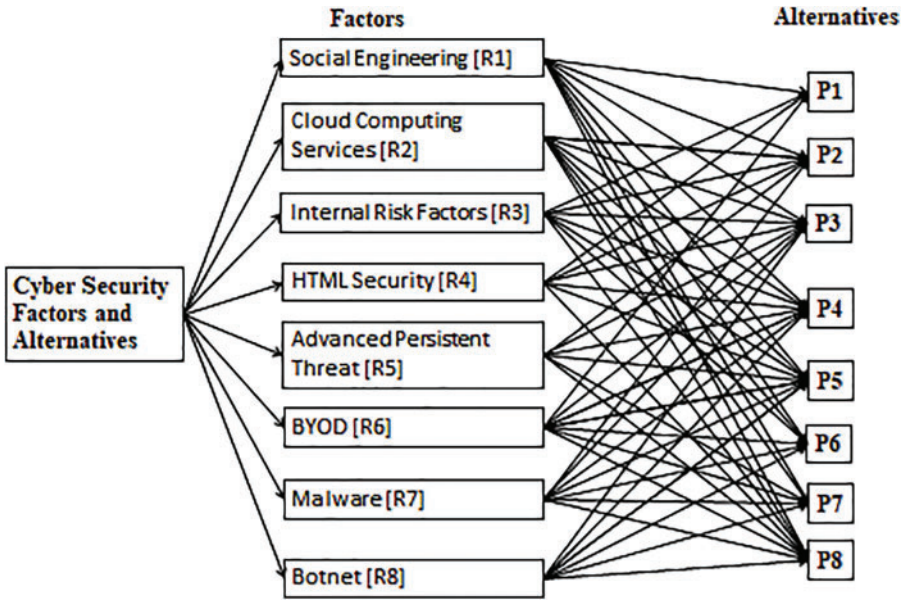

Figure 2: Hierarchy of cyber security factors and alternatives

3.1 Computer Emergency Response Team (CERT) [P1]

The CERT, a trusted source for information security, was formed by the CITC in 2006. The fact that the National Institute of Standards and Technology is the source of the following data must always be remembered. The main goal of the CERT's effort was to give the foundation the skills and information needed to identify and prevent digital incidents while also being able to prepare and train others. CERT offers a variety of services, such as giving businesses the equipment they need to deal with security risks, educating the public about cybersecurity through training campaigns, creating new cybersecurity curricula, enabling government agency programs through partnerships with universities, and disseminating knowledge about cyber incidents, vulnerabilities, and attacks [39,40].

3.2 Center of Excellence in Information Assurance [P2]

To assist the public, private, and academic sectors with developing cybersecurity solutions, implementing cybersecurity standards, consultations, and enablement, the King Saud University Centre of Excellence in Information Assurance (CoEIA) was founded as a non-profit organization in 2009. The CoEIA undertakes cybersecurity research and offers advisory services and is renowned for its patents, significant and avant-garde cybersecurity-related information, and awareness initiatives.

3.3 King Abdul-Aziz City for Science and Technology (KACST) [P3]

Research on application security, information security, network security, and security governance is done in-depth by C4C, a unit of the KACST. It was founded in that year. To utilize Saudi Arabia's people resources and serve as a catalyst for developing the framework for implementing KSA Vision 2030, the center will recruit qualified individuals with experience in cybersecurity research and application.

3.4 National Cyber Security Center (NCSC) [P4]

The NCSC has created a series of cybersecurity-compliant examinations since its founding in 2016 to help companies assess their degree of security and find security issues. This evaluation enables organizations to locate, validate, and examine technical vulnerabilities. It also offers a greater understanding of how to improve the security posture of the IT infrastructure. In light of the examination above, the NCSC gives specialized advice and warnings.

3.5 Saudi Arabian Federation for Cybersecurity, Programming, and Drones [P5]

The Saudi Arabian Federation for Cybersecurity, Programming, and Drones has operated as a national organization within the Saudi Arabian Olympic Committee since its inception in 2018. Its goal is to promote best practices and standards that are acknowledged globally for the growth of professional and national capacities in drone technology, programming, and cybersecurity. This will hasten the Kingdom of Saudi Arabia's rise among sophisticated nations regarding technical innovation.

3.6 National Cybersecurity Authority [P6]

A royal order to improve the state's cybersecurity and safeguard the country's infrastructure led to the establishment of the National Cybersecurity Authority, or NCSA, in 2017 [39,40]. In line with the KSA Vision 2030 and the National Transformation Programme that supports it, NCA seeks to promote the long-awaited technical renaissance (NTR) by enhancing national cyber capabilities. Following a series of ransomware attacks on Saudi Bedouin organizations in 2016, which targeted protected innovation and framework and had a significant impact on many government hubs, the public power of Saudi Arabia recognized the need to develop online security capabilities further and requested the general organization's wellbeing efforts and drives be overseen by a central expert.

3.7 MBS College for Advanced Technologies, Artificial Intelligence, and Cybersecurity [P7]

The Kingdom of Saudi Arabia's momentum administration has laid out scholar and examination joint efforts with driving organizations to improve skilled preparation and abilities in the crucial fields of online protection, computerized reasoning, and other cutting-edge advances. Through expanding scientific training and research activities, this project seeks to increase local human resources [40]. The events and competition are also assigned as an alternative to estimating cyber security threats [P8].

3.8 Factors

Over the past ten years, internet usage has expanded worldwide, and many companies now have an online presence. Because of this significant rise in private and business customers, the computerized environment is undoubtedly more complex, with more money involved in large web-based partnerships, and security bets are subsequently more moving and intricate. Concerning the illegal digital environment, the numbers display a steady expansion of assaults, breaks, and fruitful hacks. Several experts predict that a professional-heavy arms race will continue between system security experts and cyber attackers in the upcoming years. In the current digital world, the fight against cyber-attacks will continue to be led by IT departments and security experts, and their positions will only become more critical. The hierarchy of cyber security factors and alternatives is presented in the Fig. 2. The main threats to computer security that need to be considered when creating a secure and efficient system are listed below:

Social Engineering [R1]-The most significant threat is believed to be social engineering because of the abundance of social media websites and their recent increase in popularity. Due to the development of social networks like Facebook, Twitter, LinkedIn, and others, hackers now have almost limitless attack options. Social media may also be the finest breeding ground for future hackers if a user has an extensive network of friends and acquaintances who are similar to them, a compelling profile, and an unexpected friend request. These *wannabe social hackers* can take down even significant companies with weak security systems, allowing them to expand out of control.

Cloud Computing Services [R2]-The newest development in computer technology is cloud computing. More companies are using this efficient registration framework than at any other point in recent memory, and the amount of data facilitated on these cloud frameworks needs to be fixed. These systems are undoubtedly among the most alluring targets for contemporary hackers because even a modest security failure can have devastating effects. Organizations using this technology should constantly discuss and request the best security measures from their cloud specialist co-ops to avoid problems.

Internal Risk Factors [R3]-Experts and security-trained individuals know how the riskiest digital assaults begin. These attacks are harmful since a privileged user knows specific data to use or delete. Dangerous insiders are only uncovered 32 months after being first identified, according to a recent study funded by the US Secret Service and conducted by the Carnegie University Software Engineering Institute's CERT Insider Threat Centre. Banks and stock exchanges are among the financial institutions that are most at risk. Yet, ongoing staff review—already notoriously challenging—is a partnership's most robust line of defense against this threat.

HTML Security [R4]-It is likely that the framework's new implementation of the new HTML 5 norm will have security problems. The new protocol enables secure communication across technologies that might not function well together. So, programmers can carry out their nefarious deeds covertly. Despite improvements over the previous two years, HTML 5 is still a relatively young standard. As a result, many programmers keep making mistakes, and some professionals think cyber-attacks are getting worse.

Advanced Persistent Threats [R5]-APTs, sometimes known as high-level diligent dangers, are targeted attacks on businesses or other associations to silently obtain and steal data. They frequently use social engineering to slowly undermine security precautions and receive access to an organization's internal network. APT assaults beneficial to servers can be challenging to identify since they take place at strange times and are lengthy. APTs are generally discernible when the system detects an abnormal change in traffic, even though the numbers can occasionally be challenging to read. The assaults are

aimed at information-rich files like Word and PDF documents. So, various vectors, such as implanted devices and cell phones, which are becoming increasingly common in offices, may need to be more effective. Due to this, it is essential to carefully safeguard all digital devices, including the tiniest and least used ones (such as mobile hard drives, tablets, and smartphones).

BYOD [R6]-It is getting tougher and tougher to control the modern phenomenon at work, so *bring your gadget*. Numerous new technologies in the office can link to the internet, which is the only thing it alludes to. In the office, several Android phones, iPhones, iPods, tablets, and other devices could be used as access points by competent hackers. Those who use these gadgets often need to be made aware of the dangers they and the office setting may face. These new gadgets feature a lot of installed apps, some of which have lax security settings and can covertly install dangerous add-on software. Every contemporary smartphone has high-definition cameras, audio recorders, sensitive microphones, and other surprising recording features. To a skilled hacker, these methods are perfect Windows security measures [30].

Malware [R7]-Malware has been a popular and efficient technique for many experienced hackers for a very long time. The new threat is posed by precision-focused malware, a brand-new malware attack. Their approach has been substantially enhanced, their targets have been more precisely defined, and they are created to target particular computer configurations and parts. Mobile devices, remote servers, social media platforms, and the accounts and groups connected to them are all weak points.

Botnet [R8]-Botnets are getting increasingly specialized, hazardous, and targeted like other cyber weapons. These tools are the cybercriminals' best assets; therefore, they will continue to invest a lot of time, money, and energy in them. They grow in popularity across various platforms and are easy to distribute on almost every system. Cybercriminals will eventually develop better spam and malware tools, and takedowns launched by major companies like Adobe or Microsoft will only be effective for a limited time. Essentially, they benefit from each stage and keep developing their hacking skills.

4 Methodology

The study aims to provide insightful information on the effectiveness of using fuzzy decision-making techniques to address complex policy issues. The research seeks to illustrate the relevance of fuzzy decision-making approaches and their potential to offer reliable solutions in situations where more than conventional crisp techniques might be needed. Investigating methods that enable group decision-making, thorough alternative appraisal, and insightful comparisons in conditions characterized by ambiguity and subjectivity becomes essential in fuzzy decision-making. Fuzzy decision-making strategies address circumstances where uncertainty predominates and require specialized techniques to produce reliable results. By utilizing particular Multiple Criteria Decision Making (MCDM) techniques, such as Fuzzy-DMTAEL, Fuzzy AHP, and Fuzzy TOPSIS, the present evaluation considerably contributes to this area. These techniques have clear advantages when assessing segment-wise competency development in cybersecurity policy. To enable stakeholders to make well-informed decisions in a fuzzy setting, the Fuzzy-DMTAEL technique develops an extensive framework for collaborative assessment and prioritization of alternatives.

In contrast, Fuzzy AHP offers a formal framework for complicated decision hierarchies by dissecting issues into smaller, more manageable parts and allocating priority weights using linguistic and hazy judgments. This allows for subjective evaluations, improving the assimilation of many aspects. Additionally, Fuzzy TOPSIS provides an organized way to evaluate options concerning the best choice by statistically comparing performance based on proximity. The assessment obtains a comprehensive toolkit for efficient collaboration, review, and comparison through integrating

different methodologies, aiding in developing robust and informed cybersecurity strategies. The results of this study may further knowledge of how fuzzy decision-making might improve policy analysis as well as decision-making procedures when addressing complex problems, consequently leading the way for more sensible and successful policy decisions.

4.1 Fuzzy Decision-Making Trial and Evaluation Laboratory (FDMTAEL) Methodology

The FDMATEL approach, which can aggregate involved components into a cause-and-effect group, is built on digraphs. Directed graphs, commonly referred to as digraphs, are preferable to directionless graphs because they may display the directed relationships that exist between subsystems. A dominant connection between people or a communication network is generally shown as a digraph. The mathematical relationship R is therefore expressed as a direct-relation matrix with entries from the set S acting as equal indices on both dimensions. Certain pair-wise relations are built to model a system with a collection of elements. If the entry is a positive integer, it signifies that (1) the ordered pair (1) is in the relation R and (2) there is some sort of relation about the number in the cell (i, j) unless it is zero. The digraph, in which the number denotes the strength of impact, communicates the essential concept of the contextual link between the system's constituent parts. As a result, the FDEMATEL technique is capable of constructing a comprehensible structural model of the system from the link between elements' causes and effects. To use the FDEMATEL approach seamlessly, researcher added key definitions and enhanced the version used in the process [21].

To methodically handle complex decision-making difficulties, the Fuzzy-DMTAEL procedure entails several essential components. Setting clear objectives and limitations for the decision-making process by properly defining the issue's scope and boundaries is the first and most important phase. The next step is to identify pertinent criteria and factors, which include both qualitative and quantitative elements important to the system under consideration. A crucial step in building the Fuzzy-DMTAEL model is developing a cause-and-effect connection matrix that encapsulates the connections and interdependencies among the selected criteria and components. This matrix is used to visualize and quantify the linkages, making it easier to fully comprehend how they interact. The effect and dependency values obtained from the Fuzzy-DMTAEL model are standardized, putting them on a common scale ensuring consistency and comparability. For relevant comparisons and correct evaluations of the criteria and components, this normalization procedure is essential. After normalization, the criteria and factors are arranged according to the levels of their combined influence and dependency. Greater relevance is denoted by larger values, which highlight important components within the dynamic decision-making cycle. The Fuzzy-DMTAEL technique culminates in making defensible assessments or evaluations of the system under consideration. This can apply to a variety of applications, including evaluating the effectiveness of the system as a whole or performing comparative studies of multiple-choice alternatives depending on how well they perform against predetermined criteria and parameters. The analysis's conclusions must be interpreted at the final step when information sharing and advice are crucial. The knowledge acquired from the Fuzzy-DMTAEL process aids in framework assessment, guiding navigation, as well as informed decision-making. Fuzzy-DMTAEL offers a solid strategy to address complex decision-making difficulties across several domains by methodically merging fuzzy logic and evaluative methodologies. The Fuzzy-DMTAEL workflow diagram is shown in Fig. 3.

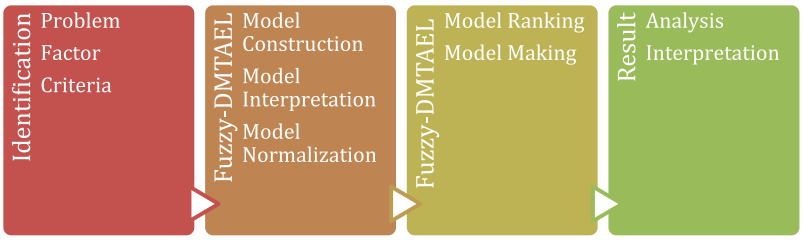

Figure 3: Fuzzy-DMTAEL process diagram

Step 1: The pair-wise comparison scale includes four levels, "No influence," "Little impact," "High influence," and "Very strong influence," with scores of 0, 1, 2, and 3.

Step 2: The initial direct-relation matrix Z, which is a $n \times n$ matrix with z_{ij} denoting the strength to which the criterion i affects the criterion j, or $\mathrm{Z} = [z_{ij}]$, $n \times n$, is produced via a pair-wise comparison of influences and directions between criteria.

Step 3: The initial direct-relation matrix X is a $n \times n$ matrix with z_{ij} denoting the strength of the influence of criterion i on criterion j, or $\mathrm{Z} = [z_{ij}]$, $n \times n$, and is obtained by pair-wise comparing Eqs. (1) and (2) directions between criteria. The principal diagonal elements are zero.

$$X = s.Z \tag{1}$$

$$s = \frac{1}{max_{1 \le i \le n} \sum_{j=1}^{n} z_{ij}}, i, j = 1, 2, 3, \ldots n \tag{2}$$

Step 4: The total-relation matrix T can be obtained using the Eq. (3), where I is referred to as the identity matrix.

$$T = X\,(I - X)^{-1} \tag{3}$$

Step 5: Inside the whole connection grid T, the number of lines and the number of sections are each independently denoted as D and R by the recipes (4)–(6).

$$T = t_{ij} \quad i, j = 1, 2, \ldots .n \tag{4}$$

$$D = \sum_{j=1}^{n} t_{ij} \tag{5}$$

$$R = \sum_{i=1}^{n} t_{ij} \tag{6}$$

The sum of the rows and columns is denoted by D and R, respectively.

Step 6: A causal diagram can be made by mapping the data to $(D + R, D - R)$, where the horizontal axis $(D + R)$ is made by adding D to R, and the vertical axis $(D - R)$ is made by removing D from R.

4.2 Fuzzy Analytic Hierarchy Process

The Analytic Hierarchy Process (AHP), created by Thomas L. Saaty, is still frequently used as a technique for making decisions based on a range of factors. Since its conception, the AHP has been

utilized by both researchers and decision-makers, making it one of the most popular techniques for making judgments based on a variety of factors. Despite the classic AHP's attempt to portray the expert's knowledge, it is still hard to precisely capture human thought processes. The disadvantage of the traditional AHP technique is that the decision-maker's sentiments towards various possibilities are quantified by an exact number. Because it uses an imbalanced scale of assessments and is unable to manage the inherent ambiguity and imprecision of the pair-wise comparison procedure, the AHP method is widely criticized. Fuzzy AHP was created to address all of these difficulties with the goal of addressing hierarchical problems. Decision-makers usually discover that interval evaluations are more accurate than fixed value judgments. This is due to the fact that due to the ambiguous nature of the comparison process. People often find it challenging to describe their choices in precise terms. The first study on fuzzy AHP is reported in [31], which contrasts triangular fuzzy numbers with fuzzy ratios. Buckley created trapezoidal fuzzy numbers to reflect how decision-makers assess choices in relation to each criterion. By using the extent analysis methodology for the synthetic extent values of the pair-wise comparisons and triangular fuzzy numbers for the pair-wise comparison scale, Chang developed a unique method for handling fuzzy AHP [30–33].

The system should be separated into several tiers for each index. The upper index also affects all other indices at the same level as the lower index. The hierarchical structure of the problem may then be modeled.

It is advised to look at the index linkages in the system. Most of the time, comparing an index to two indexes at the same level will reveal how important it is to the higher index. The comparing process may then be investigated using a comparison matrix.

The weight of each index may be determined using the rule-based comparison matrix, but its accuracy has to be verified. The weight of the indices may then be used to calculate the overall arrangement level of the system.

By contrasting it with the rule index at the top level, it is possible to estimate the weight of this index. When all index weights are at the same level, the AHP is utilized to determine the index weight using the hierarchical structure model.

To assess their relative contribution to the index at the upper level, researcher may compare the indices i and j at the same level. AHP advises using a ratio scale to assess an index's relevance. On a scale of 1 to 9, this article uses ratings. If there are n indexes at this level, the comparison matrix is C = (Cij), where Cij is the assignment that defines the index's relevance to index j. In Eq. (7), the weight calculation is displayed.

$$\tilde{p}_i = \left(\prod_{j=1}^{n} .\tilde{k}_{ij}\right)^{\frac{1}{n}}, i = 1, 2, 3 \ldots \mathrm{n} \tag{7}$$

The issue with weight calculation is solved by determining the comparison matrix's greatest eigenvalue and eigenvector. The value mi is generated by the comparison matrix entries in each row.

$$\tilde{w}_i = \tilde{p}_i \otimes \left(\tilde{p}_1 \oplus \tilde{p}_2 \oplus \tilde{p}_3 \ldots . \oplus \tilde{p}_n\right)^{-1} \tag{8}$$

Additionally, using equations to determine the average and normalized weight criteria.

$$M_i = \frac{\tilde{w}_1 \oplus \tilde{w}_2 \ldots .. \oplus \tilde{w}_n}{n} \tag{9}$$

$$Nr_i = \frac{M_i}{M_1 \oplus M_2 \oplus \ldots\ldots \oplus M_n} \tag{10}$$

The reliability of the similarity grids Examining networks reduces deliberative thinking to a series of numbers, but they must still be verified for consistency. The findings of various experts' assessments on the applicability of lists ought to be consistent. When using the AHP, the comparability of the comparison matrix should be assessed to make sure that the critical thinking of multiple experts is consistent. The consistency ratio CR may be used to assess the comparison matrix's consistency.

$$\text{CR} = \text{CI}/\text{RI} \tag{11}$$

C.I. is consistency index and C.I. = max−n/ n−1 (10)

The random index, or RI, value is shown in Table 3. If CR is 0.1, the comparison matrix is acceptable.

Table 3: Values of RI

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
RI	0	0	0.52	0.88	1.1	1.24	1.34	1.4	1.44	1.48	1.51	1.53	1.55	1.57	1.58

4.3 Fuzzy TOPSIS

To address ranking problems in the actual world, the TOPSIS is widely utilized. Despite its popularity and seeming simplicity, this approach is commonly criticized for failing to appropriately handle the inherent ambiguity and imprecision of mapping the decision-makers perspective to other values. Values are categorically identified as being subjective judgmentsjudgments using the conventional TOPSIS formula. Decision-makers may be reluctant or unable to assign exact values to comparison judgments because the human preference model is erroneous in many real-world scenarios. The obligation to employ crisp values is one of the challenging parts of the crisp evaluation procedure. This could be the case because decision-makers usually like using intervals over discrete numbers when expressing their judgments. Some factors are typically disregarded throughout the evaluation process because they are hard to quantify with precise numbers. Another justification is the use of crisp value-based mathematical models.

These methods fall short in dealing with decision-makers ambiguity, uncertainty, and vagueness, which cannot be overcome by establishing unambiguous values. By using fuzzy set theory 2 [31,32], the decision-makers are able to include information that is insufficient, unavailable, impossible to quantify, and only partially informed in the decision model. As a result, fuzzy TOPSIS and its extensions are used to handle ranking and justification concerns.

In order to determine how near an alternative is to the optimal answer, the fuzzy TOPSIS approach is used. Positive or negative distances can exist between the options. The approach establishes two values: the project's cost and the profit. These two values are known as the fuzzy positive ideal solution (FPIS) and fuzzy negative ideal solution (FNIS), respectively. The alternative that is closest to the ideal positive solution and farthest from the ideal negative solution is selected by the strategy. The fuzzy TOPSIS mathematical idea is explained as follows:

Step 1: For each criterion, there are definitions for the language variables, the weighting of the assessment criteria, and the membership functions. Each linguistic variable is given a set of membership functions, and the linguistic terms are used to determine the weights of the evaluation criteria and alternative ratings.

Step 2: Building the fuzzy decision matrix is necessary. The decision matrix is intimately tied to both the alternative criteria and the linguistic characteristics. The following matrix illustrates the fuzzy decision matrix, which has m rows and n columns and assumes n criteria and m projects. It must be graded using the defined standards. The score that option Ai earns in reference to criteria Cj is C1, C2, . . . , Cn, xij. The importance of the weighted values of the criteria in project evaluation also necessitates the need to aggregate.

$$\tilde{K} = \begin{array}{c} \\ A_1 \\ \dots \\ A_m \end{array} \begin{array}{c} \begin{array}{ccc} C_1 & \dots & C_n \end{array} \\ \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \dots & \ddots & \dots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \end{array} \tag{12}$$

where W is the weight vector containing the criteria's values.

where $\tilde{x}_{ij} = \frac{1}{D}\left(\tilde{x}_{ij}^{1} \cdots \oplus \tilde{x}_{ij}^{d} \oplus \cdots \tilde{x}_{ij}^{D}\right)$, and $\tilde{x}_{ij}^{d}$ is the d^{th} practitioner's estimation of the alternative A_i performance in relation to factor Cj and $\tilde{x}_{ij}^{d} = (l_{ij}^{d}, mi_{ij}^{d}, u_{ij}^{d})$.

Step 3: Normalising the fuzzy decision matrix is essential. The fuzzy decision matrix is normalized using the linear scale transformation. Calculations are done using Eq. (14).

$$\tilde{p}_{ij} = \left(\frac{l_{ij}}{u_j^+}, \frac{mi_{ij}}{u_j^+}, \frac{u_{ij}}{u_j^+}\right), \; u_j^+ = max\left\{u_{ij}, i = 1, 2, 3 \dots n\right\} \tag{13}$$

If researcher employ criteria in the cybersecurity quality evaluation whose value shows the advantage, researcher apply the Eq. (13) in such a case. Otherwise, the quality evaluation criteria that reflect expenses will be determined using the cost-benefit criteria.

Step 4: It is necessary to compute the weighted fuzzy decision matrix. The weighted normalized fuzzy decision matrix is produced by multiplying the weights (wj) of the evaluation criteria by the normalized value (rij) of the fuzzy decision matrix. The weighted normalized decision matrix is shown in the equation.

$$\sim \tilde{Q} = \left[\tilde{q}_{ij}\right]_{m \times n} i = 1, 2, \dots m; j = 1, 2, 3 \dots n \tag{14}$$

Step 5: The fuzzy positive-ideal solution (FPIS A+) and fuzzy negative-ideal solution (FNIS A-) must be distinguished. The positive and negative deviations from the ideal response are now calculated using the weighted normalized fuzzy decision matrix. The closed interval enclosing each of their ranges is 0,1. FPIS and FNIS are defined by the triplets (1,1,1) or (0,0,0), and their values are calculated using the following formula:

$$A^+ = \left(\tilde{q}_{1,\dots\dots}^{*} \tilde{q}_{j,\dots\dots}^{*} \tilde{q}_{n,}^{*}\right) \tag{15}$$

$$A^- = \left(\tilde{q}_{1,\dots\dots}^{*} \tilde{q}_{j,\dots\dots}^{*} \tilde{q}_{n,}^{*}\right) \tag{16}$$

Step 6: Calculate the separation between each option and FPIS and FNIS. The following formula may be used to calculate the distances (dj+ and dj) between each option A+ and A−:

$$\tilde{d}_i^+ = \sum_{j=1}^{n} .d\left(\tilde{q}_{ij}, \tilde{q}_{ij}^*\right) i = 1, 2, \ldots m; j = 1, 2, 3 \ldots n \tag{17}$$

$$\tilde{d}_i^- = \sum_{j=1}^{n} .d\left(\tilde{q}_{ij}, \tilde{q}_{ij}^*\right) i = 1, 2, \ldots m; j = 1, 2, 3 \ldots n \tag{18}$$

Step 7: To rank all of the alternatives in order of preference, get the closeness coefficient (CCi). The indicator CCi indicates the alternative's closeness to the FPIS (dj+) and separation from the FNIS (dj). The closeness coefficient for each assessed quality may be computed as:

$$C\tilde{C}_i = \frac{\tilde{k}_i^-}{\tilde{k}_i^+ + \tilde{k}_i^-} = 1 - \frac{\tilde{k}_i^+}{\tilde{k}_i^+ + k_i^-}, i = 1, 2, \ldots., m \tag{19}$$

Step 8: The options are sorted in preference order based on the computed proximity coefficients. The choice with the greatest coefficient is the most beneficial.

5 Results

A thorough discussion throughout the research is necessary due to the complicated nature of fuzzy decision-making models, especially when addressing multiple scenarios involving various criteria and decision factors. It is important to pay attention to how such complicated models are integrated into frameworks for policy analysis. Particularly, using fuzzy decision-making methodologies like the Fuzzy-DMTAEL, the Fuzzy AHP, and the Fuzzy TOPSIS necessitates a significant investment in computational power and specialized knowledge. It is crucial to examine the difficulties and factors to be taken into account when putting such models into practice in the setting of policy analysis. To enable a nuanced comprehension of the consequences and complexities of implementing fuzzy decision-making models into policy analysis frameworks, it is essential to handle computational demands, optimize algorithmic efficiency, and ensure robust interpretation of findings.

Considering the intrinsic nature of fuzzy decision-making systems, which essentially entail subjective judgments and linguistic variables, tackling subjectivity and interpretability is a key aspect of this research. The study places emphasis on a strict and organized process for dealing with subjectivity, where professional judgments and insights are used to mold the main criteria and sub-criteria. The research attempts to reduce the possibility of bias linked to subjectivity and provide a thorough evaluation of diverse perspectives by merging existing literature with expert viewpoints. Additionally, using cutting-edge fuzzy decision-making approaches like the Fuzzy AHP, Fuzzy TOPSIS, and Fuzzy-DMTAEL aims to make results easier to understand. These approaches provide organized models that enable the conversion of linguistic factors into measurable quantities, aiding in the comprehension of the decision-making procedure. The research aims to establish a solid and credible framework for policy analysis in the area of cybersecurity skill upgrading by specifically addressing subjectivity and prioritizing interpretability.

The findings of this thorough analysis regarding the development of cybersecurity capability within the Kingdom of Saudi Arabia are presented and discussed in this section. Researcher examine the empirical results obtained through the use of advanced fuzzy decision-making approaches, such as Fuzzy AHP, Fuzzy TOPSIS, and Fuzzy-DMTAEL, building on the framework established in the preceding sections. The segment-wise creation of cybersecurity policies can be evaluated and prioritized using these techniques, which are effective instruments. Researcher uncover insights into

the relative significance of various aspects, entities, and alternatives by a thorough examination of the research data, which helps to further our grasp of the complexities surrounding efficient cybersecurity solutions and regulatory frameworks. The discussion that follows will reveal the precise specifics of the empirical results researcher obtained, leading to a thorough assessment of cybersecurity proficiency and useful policy recommendations.

5.1 Evaluation with Fuzzy-DMTAEL Methodology

The numerical analysis of the cyber security estimation in KSA is represented by the prominence relation diagram, and the security factors are arranged in quadrants II and IV. The quadrant values are assigned by the given details:

QUADRANT I has the Most Important Criteria (Prominence: High, Relation: High), QUADRANT II has Important Criteria that can be improved by Other Criteria (Prominence: Low, Relation: High), QUADRANT III has Criteria that are Not Important (Prominence: Low, Relation: Low), QUADRANT IV has Important Criteria that cannot be improved by Other Criteria (Prominence: High, Relation: Low) (g1: Quadrant II, g2: Quadrant II, g3: Quadrant II, g4: Quadrant IV, g5: Quadrant II, g6: Quadrant IV, g7: Quadrant IV, g7: Quadrant IV, g7: Quadrant IV, g7: Quadrant IV, g7: Quadrant IV, g7: Quadrant IV, g7: The values of prominence are shown in the resultant Table 4. The values are derived from the Python code. Table 5 shows the findings of the resultant relation. The final weights of the factors are represented in Table 6. Factor P4 has the highest priority of the factors, and factor P2 has the least. Fig. 4 shows the prominence relation diagram.

Table 4: Resultant prominence

Factors	Prominence
P4	4.503
P6	4.123
P8	4.015
P7	3.929
P1	3.561
P3	3.476
P5	3.371
P2	3.295

Table 5: Resultant relation

Factors	Relation
P5	2.026
P1	1.564
P3	0.484
P2	0.257
P6	−0.643

(Continued)

Table 5 (continued)	
Factors	Relation
P7	−1.137
P4	−1.233
P8	−1.318

Table 6: Criteria weight of the factors associated with the cyber security

Factors	Weight
P4	0.149
P6	0.136
P8	0.133
P7	0.13
P1	0.118
P3	0.115
P5	0.111
P2	0.109

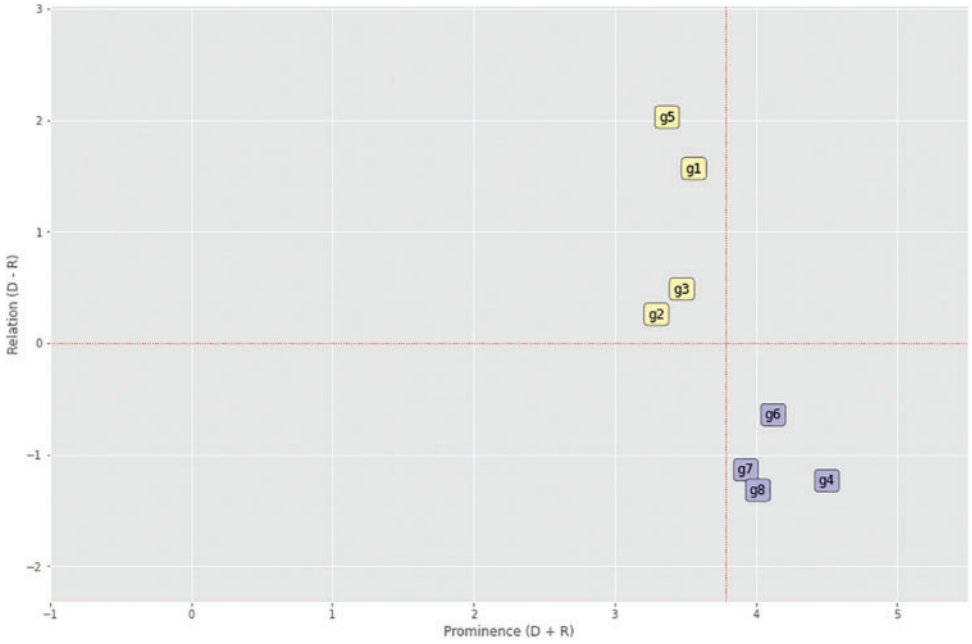

Figure 4: Prominence relation diagram

The prominence diagram shows the factors in two quadrants, IInd and IVth, and P1, P2, P3, and P5 have the second quadrant, which means they will be changed or improved with the proper alternate factors effect. The fourth quadrant has the P4, P6, P7, and P8 factors; it does not change its effect with the other factors or alternatives. The prominence and relation are shown in Tables 4 and 5. The results are represented in Table 6. The National Cyber Security Centre of Saudi Arabia has the highest preference over the security factors shown in Fig. 5.

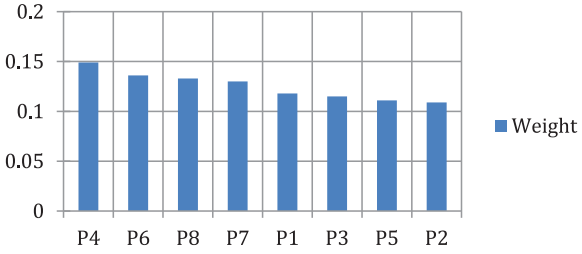

Figure 5: Graphical representation of the weight of the alternatives

As is the case with most of the thriving digital economies of the world, Saudi Arabia is also vulnerable to cybercrime. Saudi Arabia is a wealthy country with a high level of digitalization, which means that there is a significant amount of valuable data and resources that cybercriminals can target. This includes government agencies, financial institutions, and critical infrastructure such as oil and gas facilities. Saudi Arabia is located in a region that is particularly susceptible to cyber threats. The Middle East has been the target of numerous cyber-attacks in recent years, with state-sponsored actors and hacktivist groups launching attacks on government agencies and critical infrastructure [2]. Saudi Arabia is also a target for cybercriminals due to its geopolitical significance. The country's strategic location and importance in the global oil market make it an attractive target for cybercriminals seeking to disrupt the country's economy and political stability. While Saudi Arabia is taking steps to improve its cybersecurity posture, the present canvas of cyber-attacks enlists more concerted efforts to reinforce the initiatives taken in this direction. This study's empirical analysis will be a significant contribution to this research ambit.

The analytic study of cyber security in KSA resulted from the priorities listed in ascending order as P2<P5<P3<P1<P7<P8<P6<P4. Factor P4 got the top priority, and P2 got the least. Furthermore, the theoretical selection of factors and their estimation established NCSC as the most prioritized factor, CoEIA being the least one.

5.2 Evaluation with Fuzzy AHP Methodology

This section discusses utilizing the Fuzzy AHP technique to address the same problem—the policymaker's decision. Here, a Fuzzy AHP-based group choice was shown. Decision-makers evaluated pairs using the significance division approach after developing surveys and forms. Decision-makers employ the linguistic variables, which have been converted into triangular fuzzy numbers, to assess the alternatives in regard to each criterion. The triangular fuzzy numbers are used to compare pairs using fuzzy words with a range of 1 to 9. The ultimate weight of the submodels is computed based on the loads of the standards and submodels. The weights of the primary measures that correspond to such loads are then added to the sub-rules by big loads.

5.3 Evaluation with Fuzzy TOPSIS Methodology

The Fuzzy TOPSIS technique is suggested in this part as a solution to the problem of choosing IT infrastructure policymakers. The process utilized to assess the linguistic words and membership functions is as follows:

- The fuzzy decision matrix is produced by normalizing the linguistic variables and converting them into triangular fuzzy integers. Both the weighted normalized fuzzy decision matrix and the normalized decision matrix may be produced using equations.
- After the decision matrix has been normalized, the weighted fuzzy decision matrix is generated. The results of this surgery are assessed. Correct the FPIS and FNIS: It is known that both the fuzzy negative ideal solution (FNIS, A) and the fuzzy positive ideal solution (FPIS, A+) exist.
- Ranking any option is achievable once the closeness coefficient is known. This tactic enables the decision-makers to pick the best choice. The proximity coefficient of each choice is calculated using an equation.
- Based on the closeness coefficient of three of the options, P2>P5>P3>P1>P7>P8>P6>P4 represents the preferred order for the alternatives. The ideal choice is further from the FNIS but closer to the FPIS.

They have essentially accomplished the same outcome using Fuzzy AHP. The first alternative is P2. Both Fuzzy TOPSIS and Fuzzy AHP techniques can use the choice. These techniques do have benefits and drawbacks, though. In light of the problem, the best course of action should be adopted. The following is an overview of how this study's Fuzzy TOPSIS, Fuzzy-DMTAEL, and Fuzzy AHP approaches differ from one another and from one another.

Fuzzy AHP, Fuzzy-DMTAEL, and Fuzzy TOPSIS demand more complicated calculations when these methods are contrasted in terms of the number of computations needed. As opposed to Fuzzy TOPSIS, Fuzzy AHP compares criteria, sub-criterion, and alternatives pair-wise depending on how close they are to positive and negative ideal solutions. One of the more effective methods for addressing the rank reversal problem, which happens when a less-than-ideal alternative is introduced to the list of choices, is Fuzzy-DMTAEL. In the extent analysis of Fuzzy AHP, priority weights for the criteria or alternative might be set to zero. This alternative or criterion is not taken into account in this situation. This is one of the shortcomings of this strategy. Both Fuzzy TOPSIS and Fuzzy AHP allow for the inclusion of linguistic variables. The rankings for the Fuzzy AHP, Fuzzy-DMTAEL, and Fuzzy TOPSIS are essentially the same. This demonstrates that the positioning outcomes will be the same when the chiefs are trustworthy with them in picking the information and two tactics at their discretion.

6 Comparisons

When several approaches are applied, the same data yields various outputs, and various procedures are used to assess the validity and efficacy of the methodology. In this study, researcher applied the Fuzzy AHP, Fuzzy-DMTAEL, and Fuzzy TOPSIS methods to evaluate the effectiveness and precision of the outcomes. In AHP, DMTAEL, and TOPSIS, the methods for data collection and estimate are all the same. As a result, values for typical F-AHP, F-DMTAEL, and F-TOPSIS are obtained in real number form. The conventional techniques' findings are correlated with each other using a Pearson correlation value of 0.999176. In terms of dependability and efficiency, Fuzzy-DMTAEL is better than the other multiple-criteria decision analysis (MCDA) approaches. The following Table 7 and Fig. 6 show the representation of comparison.

Table 7: Comparison of cybersecurity alternatives by Fuzzy-AHP, Fuzzy-TOPSIS and Fuzzy-DMTAEL method

Methods/Alternatives	P1	P2	P3	P4	P5	P6	P7	P8
Fuzzy-AHP	0.117	0.108	0.111	0.153	0.100	0.132	0.139	0.133
Fuzzy-TOPSIS	0.116	0.114	0.118	0.148	0.110	0.137	0.128	0.131
Fuzzy-DMTAEL	0.118	0.109	0.115	0.149	0.111	0.136	0.13	0.133

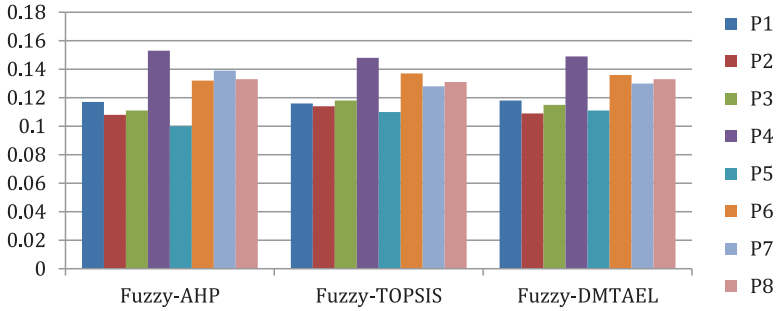

Figure 6: Graphical representation of comparison

7 Suggestions

Comparing the cybersecurity policy framework of Saudi Arabia to that of other countries finds both commonalities and differences. Similarities can often be seen in fundamental ideas, such as the creation of national cybersecurity organizations, legislative frameworks, and regulatory agencies to protect key digital infrastructure. However, differences show themselves in the focus placed on policies, methods for international cooperation, and the incorporation of cutting-edge technologies. The present system should be enhanced using a number of ways in order to improve cybersecurity proficiency in the Kingdom. The efficiency of the policy ecosystem can be increased through increasing cross-sector cooperation, public-private partnerships, as well as international information sharing. Additionally, Saudi Arabia's cyber defenses can be strengthened by ongoing adaptation to changing cyber threats through frequent policy reviews, dynamic risk evaluations, as well as the incorporation of artificial intelligence and machine learning. Equally crucial is the development of a strong cybersecurity culture through improved public awareness and education activities. Saudi Arabia can establish itself as a formidable force in the field of cybersecurity and make a significant contribution to the landscape of worldwide digital security by carefully aligning the framework with international best practices and utilizing technical breakthroughs.

A multifaceted strategy is required to improve the security climate in Saudi Arabia's private and public sectors. In order to strengthen cybersecurity, it may be necessary to mandate strong authentication systems, ensure the fast installation of security upgrades and patches, and provide thorough training and awareness programs for personnel. The use of encryption techniques, facilitation of information sharing between organizations, and implementation of strict access controls are also essential. Resilience is improved by adopting a risk-based approach that customizes security solutions to particular industry needs, as well as by performing routine cybersecurity audits and evaluations. A strong foundation to attain a higher level of cybersecurity competence throughout sectors, protecting against cyber threats and guaranteeing the protection of crucial digital assets, can be established by

adopting internationally recognized cybersecurity norms and frameworks, including ISO 27001, NIST Cybersecurity Framework, as well as CIS Controls.

The various cyber-attacks Saudi Arabia has experienced have made issues with cybersecurity and cyber defense more urgent. Defense against cyber-attacks is an ongoing management concern for cybersecurity organizations in the country. Digital information is used more often in daily life, which makes people more susceptible to assault. The effectiveness of the Saudi Arabian judicial system in preventing cybercrime and its capacity to deal with the growing threat of computer-related crimes are the foundation of this study. In addition, the following measures will supplement the existing online security infrastructure in the country:

- Sharing cybercrime cases with the public can help raise awareness about the legal frameworks currently in place for addressing cybercrime. Establishing a clear rule about the release of incident reports and cases can be a positive initial step toward improving digital safety and security.
- Increasing awareness about the existing rules can help reduce cybercrime. It can also improve law-abiding individuals' understanding of their rights and responsibilities, which may encourage more people to report cybercrimes.
- Updating the current laws to include the latest cybercrime developments, their unique features, and different scenarios.
- Currently, many countries have laws in place to address cybercrimes, but these laws often only focus on specific aspects of a single type of cybercrime [38,39]. This can create inconsistencies in the legal system and make it difficult to prosecute cybercriminals for their actions. To address this issue, some experts suggest creating sub-laws that cover related or similar cybercrimes and all of their relevant rules in a single document. It can provide a clear and consistent legal framework that enables them to take effective action against cybercrime. Overall, having a single document that covers all the relevant rules for related or similar cybercrimes can help to create a more coherent and effective legal system for addressing cybercrime.
- Penalties can refer to punishments such as fines, legal action, or other forms of enforcement. The statement suggests that in Saudi organizations, there should be penalties applied for not adhering to security guidelines and best practices. The purpose of applying penalties in this context is to encourage organizations to take cybersecurity seriously and to follow established best practices to protect against cyber threats. By implementing penalties, organizations will have a greater incentive to invest in their cybersecurity defenses and to ensure that they are meeting industry standards for protecting their data and systems.
- Forensic investigation is a critical science in the field of information security [40]. It involves analyzing digital data to identify and collect evidence of cybercrime or other digital activities that may be relevant in a legal or investigative context. Given the rise in cyber attacks globally, computer forensics has become an essential tool for demonstrating and establishing strong evidence that implicates a person in a digital crime. This is because cybercriminals often leave a trail of digital evidence that can be analyzed and used to identify them and build a case against them.
- Digital forensics labs are facilities equipped with specialized tools and software used by professionals to analyze and process digital evidence. These labs are essential in the field of digital forensics, as they provide a controlled environment for the collection, preservation, and analysis of digital data. Digital forensics labs are necessary because they allow professionals to gather and organize digital evidence in a way that is admissible in a court of law. The use of digital forensics labs is essential in criminal investigations, corporate litigation, and other legal

and investigative contexts. By providing a controlled environment for the collection and analysis of digital evidence, these labs help to ensure the integrity and admissibility of evidence in legal proceedings.

8 Conclusions

The strong cybersecurity framework offers a comprehensive approach to monitoring network safety in various e-government contexts. Monitoring potential threats to network security is a crucial function of the cybersecurity framework. In this paper, the author finds the most promising cyber security factors by using Fuzzy DMTEAL, AHP, and Fuzzy TOPSIS, and the authors observed that everyone achieves the same results. However, the performance of the DMTEAL method is too good in comparison to the Fuzzy AHP and TOPSIS methods. The Fuzzy TOPSIS method performs better than Fuzzy AHP because it does not need a pair-wise comparison in TOPSIS same as Fuzzy DMTEAL performs well in comparison to Fuzzy TOPSIS because this method does not check the FPIS and FNIS value, which takes more time to calculate the results. The Saudi Arabian government has established a comprehensive cybersecurity framework that outlines policies, procedures, and guidelines to protect the country's critical information infrastructure from cyber threats. In addition to its cybersecurity framework, the Saudi Arabian government has launched several initiatives to promote cybersecurity awareness and education among the public and private sectors. These initiatives include training programs, awareness campaigns, and conferences and events focused on cybersecurity. Overall, the cybersecurity framework in Saudi Arabia is comprehensive and reflects the government's commitment to protecting its critical information infrastructure from cyber threats. By establishing strong cybersecurity measures and promoting cybersecurity awareness, the country is better prepared to defend against cyber attacks and safeguard its national security and economic interests. It consists of exercises that are paired with a myriad of network protection programs and come in many forms. These programs are flexible and can be changed to address any concerns that may arise within the protective framework. One of the many areas that still needs improvement is the systematic building of capacity across all work groups functioning at all levels of government. This is only one of the many areas that still need to be improved. The government of Saudi Arabia has made substantial progress toward protecting the country's online infrastructure. The country has made significant progress in developing its digital infrastructure and capabilities. Saudi Arabia's digital future ensures that the country can realize the full potential of digital technologies to drive economic growth, improve social outcomes, and enhance national security. In the future, the author can use other decision-making methods with machine learning algorithms.

Acknowledgement: The author extends his appreciation to Taif University, Saudi Arabia, for supporting this work through Project Number (TU-DSPP-2024-121).

Funding Statement: This research was funded by Taif University, Taif, Saudi Arabia, project No. (TUDSPP- 2024-121).

Author Contributions: Study conception and design: W. Alhakami; data collection: W. Alhakami; analysis and interpretation of results: W. Alhakami; draft manuscript preparation: W. Alhakami. The author reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The author confirms that the data supporting the findings of this study are available within the article.

Conflicts of Interest: The author declares that he has no conflicts of interest to report regarding the present study.

References

[1] A. Ali *et al.*, "Renewable portfolio standard development assessment in the Kingdom of Saudi Arabia from the perspective of policy networks theory," *Processes*, vol. 9, no. 7, pp. 1123, 2021. doi: 10.3390/pr9071123.

[2] A. Aljaber, "E-learning policy in Saudi Arabia: Challenges and successes," *Res. Comp. Int. Educ.*, vol. 13, no. 1, pp. 176–194, 2018. doi: 10.1177/1745499918764147.

[3] I. Almomani, M. Ahmed, and L. Maglaras, "Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia," *PeerJ Comput. Sci.*, vol. 7, no. 1, pp. 703–721, 2021. doi: 10.7717/peerj-cs.703.

[4] M. T. J. Ansari, D. Pandey, and M. Alenezi, "STORE: Security threat oriented requirements engineering methodology," *J. King Saud Univ.—Comput. Inf. Sci.*, vol. 34, no. 2, pp. 191–203, 2022. doi: 10.1016/j.jksuci.2018.12.005.

[5] S. Nifakos *et al.*, "Influence of human factors on cyber security within healthcare organisations: A systematic review," *Sens.*, vol. 21, no. 15, pp. 5119, 2021. doi: 10.3390/s21155119.

[6] M. M. Alkhusaili and Z. M. Aljazzaf, "The evolution of E-government project in GCC countries," in *Proc. Int. Conf. Ind. Eng. Oper. Manag.*, Detroit, Michigan, USA, 2020, pp. 2001–2012.

[7] R. Brindha *et al.*, "Intelligent deep learning based cybersecurity phishing email detection and classification," *Comput. Mater. Contin.*, vol. 74, no. 3, pp. 5901–5914, 2023.

[8] I. Chaudhry, "Arab revolutions: Breaking fear| #Hashtags for change: Can Twitter generate social progress in Saudi Arabia," *Int. J. Commun.*, vol. 8, no. 1, pp. 19–31, 2014.

[9] T. Alqudsi-ghabra, T. Al-Bannai, and M. A. Bahrani, "The internet in the arab gulf cooperation council (AGCC): Vehicle of change," *Int. J. Internet Sci.*, vol. 6, no. 1, pp. 44–67, 2011.

[10] R. Alqurashi, M. AlZain, B. Soh, and J. A. Amri, "Cyber attacks and impacts: A case study in saudi arabia," *Int. J.*, vol. 9, no. 1, pp. 217–224, 2020.

[11] J. Gaubys, "How many people use the internet in 2023?," Oberlo. Accessed: August 12, 2023. [Online]. Available: https://www.oberlo.com/statistics/how-many-people-use-internet

[12] Y. A. Aina, "Achieving smart sustainable cities with GeoICT support: The Saudi evolving smart cities," *Cities*, vol. 71, no. 1, pp. 49–58, 2017. doi: 10.1016/j.cities.2017.07.007.

[13] N. Alhalafi and P. Veeraraghavan, "Cybersecurity policy framework in Saudi Arabia: Literature review," *Front. Comput. Sci.*, vol. 3, no. 1, pp. 736874, 2021. doi: 10.3389/fcomp.2021.736874.

[14] A. A. Aridi, "Disparity between current legal frameworks and digital transformation development in GCC states," in *Proc. 6th Int. Conf. PhD Students Young Researchers*, Vilnius, Lithuania, Vilnius University, 2018, pp. 1–18.

[15] P. Diotte, "The big four and cyber espionage: How China, Russia, Iran and North Korea spy online," *Can. Mil. J.*, vol. 1, no. 1, pp. 1–18, 2017.

[16] G. H. Alshammri, A. K. Samha, E. El-Din Hemdan, M. Amoon, and W. El-Shafai, "An efficient intrusion detection framework in software-defined networking for cybersecurity applications," *Comput. Mater. Contin.*, vol. 72, no. 2, pp. 3529–3548, 2022. doi: 10.32604/cmc.2022.025262.

[17] T. D. Hunt, "The internet of buildings: Insurance of cyber risks for commercial real estate," *Oklahoma Law Rev.*, vol. 71, no. 1, pp. 397, 2018.

[18] N. Keller and A. Rosemarin, "Mind the middle layer: The HADES design strategy revisited," *Lect. Notes Comput. Sci.*, vol. 12697, no. 1, pp. 35–63, 2021. doi: 10.1007/978-3-030-77886-6.

[19] S. S. Aljameel *et al.*, "A sentiment analysis approach to predict an individual's awareness of the precautionary procedures to prevent COVID19 outbreaks in Saudi Arabia," *Int. J. Environ. Res. Public Health*, vol. 18, no. 1, pp. 218–240, 2021. doi: 10.3390/ijerph18010218.

[20] A. Alzahrani, "Coronavirus social engineering attacks: Issues and recommendations," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, pp. 1–21, 2020. doi: 10.14569/issn.2156-5570.

[21] I. G. Sahebi, A. Mosayebi, B. Masoomi, and F. Marandi, "Modeling the enablers for blockchain technology adoption in renewable energy supply chain," *Technol. Soc.*, vol. 68, no. 1, pp. 101871, 2022. doi: 10.1016/j.techsoc.2022.101871.
[22] R. A. Al-Mulhim, L. A. Al-Zamil, and F. M. Al-Dossary, "Cyber-attacks on Saudi Arabia environment," *Int. J. Comput. Netw. Commun. Secur.*, vol. 8, no. 3, pp. 26–31, 2020. doi: 10.47277/IJCNCS.
[23] M. A. Ahad, S. Paiva, G. Tripathi, and N. Feroz, "Enabling technologies and sustainable smart cities," *Sustain. Cities Soc.*, vol. 61, no. 1, pp. 102301, 2020. doi: 10.1016/j.scs.2020.102301.
[24] C. S. Lai *et al.*, "A review of technical standards for smart cities," *Clean Technol.*, vol. 2, no. 3, pp. 290–310, 2020. doi: 10.3390/cleantechnol2030019.
[25] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia," *Heliyon*, vol. 7, no. 1, pp. 1–13, 2021. doi: 10.1016/j.heliyon.2021.e06016.
[26] A. M. Talib, F. O. Alomary, H. F. Alwadi, and R. R. Albusayli, "Ontology-based cyber security policy implementation in Saudi Arabia," *J. Inf. Secur.*, vol. 9, no. 4, pp. 315–333, 2018. doi: 10.4236/jis.2018.94021.
[27] S. Alelyani and G. R. H. Kumar, "Overview of cyberattack on saudi organizations," *J. Inf. Secur. Cybercr. Res.*, vol. 1, no. 1, pp. 32–39, 2018. doi: 10.26735/16587790.2018.004.
[28] S. Vishnu, S. R. J. Ramson, and R. Jegan, "Internet of medical things (IoMT)—An overview," in *Proc. 5th Int. Conf. Devices, Circ. Syst. (ICDCS)*, Coimbatore, India, 2020, pp. 101–104.
[29] M. H. Alsulami *et al.*, "Measuring awareness of social engineering in the educational sector in the Kingdom of Saudi Arabia," *Information*, vol. 12, no. 5, pp. 208–228, 2021. doi: 10.3390/info12050208.
[30] K. Almarhabi, A. Bahaddad, and A. M. Alghamdi, "Security management of BYOD and cloud environment in Saudi Arabia," *Alex. Eng. J.*, vol. 63, no. 1, pp. 103–114, 2022. doi: 10.1016/j.aej.2022.07.031.
[31] A. Agrawal, M. Alenezi, R. Kumara, and R. A. Khan, "A unified fuzzy-based symmetrical multi-criteria decision-making method for evaluating sustainable-security of web applications," *Symmetry*, vol. 12, no. 3, pp. 448, 2020. doi: 10.3390/sym12030448.
[32] W. Alhakami, "Computational study of security risk evaluation in energy management and control systems based on a fuzzy MCDM method," *Processes*, vol. 11, no. 5, pp. 1366, 2023. doi: 10.3390/pr11051366.
[33] N. Ahmad, N. N. Quadri, M. R. N. Qureshi, and M. M. Alam, "Relationship modeling of critical success factors for enhancing sustainability and performance in e-learning," *Sustainability*, vol. 10, no. 12, pp. 4776, 2018. doi: 10.3390/su10124776.
[34] M. Hijji and G. Alam, "Cybersecurity awareness and training (CAT) framework for remote working employees," *Sensors*, vol. 22, no. 22, pp. 8663, 2022. doi: 10.3390/s22228663.
[35] A. Yeboah-Ofori *et al.*, "Cyber threat predictive analytics for improving cyber supply chain security," *IEEE Access*, vol. 9, pp. 94318–94337, 2021. doi: 10.1109/ACCESS.2021.3087109.
[36] M. Almalki and M. Alkahtani, "Allocation of regional logistics hubs and assessing their contribution to Saudi Arabia's logistics performance index ranking," *Sustainability*, vol. 14, no. 12, pp. 7474, 2022. doi: 10.3390/su14127474.
[37] S. M. Alholiby and Z. A. Almulhim, "From the lack to the requirement: The public consultation reform in Saudi Arabia," *UCLA J. Islamic Near Eastern Law, Forthcoming*, vol. 20, no. 1, pp. 21–72, 2021.
[38] M. M. El Khatib *et al.*, "Digital transformation and SMART-The analytics factor," in *Proc. Int. Conf. Bus. Anal. Technol. Secur. (ICBATS)*, Dubai, United Arab Emirates, IEEE, 2022, pp. 1–11.
[39] M. Robinson, K. Jones, H. Janicke, and L. Maglaras, "Developing cyber peacekeeping: Observation, monitoring and reporting," *Gov. Inf. Q.*, vol. 36, no. 2, pp. 276–293, 2019. doi: 10.1016/j.giq.2018.12.001.
[40] Q. Amanullah and M. K. Khan, "Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, present and future," *Glob. Found. Cyber Stud. Res.*, vol. 1, no. 1, pp. 1–18, 2019.