processes

MDPI

Article

Computational Study of Security Risk Evaluation in Energy Management and Control Systems Based on a Fuzzy MCDM Method

Wajdi Alhakami

Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; whakami@tu.edu.sa

Abstract: Numerous cyberattacks on connected control systems are being reported every day. Such control systems are subject to hostile external attacks due to their communication system. Network security is vital because it protects sensitive information from cyber threats and preserves network operations and trustworthiness. Multiple safety solutions are implemented in strong and reliable network security plans to safeguard users and companies from spyware and cyber attacks, such as distributed denial of service attacks. A crucial component that must be conducted prior to any security implementation is a security analysis. Because cyberattack encounters in power control networks are currently limited, a comprehensive security evaluation approach for power control technology in communication networks is required. According to previous studies, the challenges of security evaluation include a power control process security assessment as well as the security level of every control phase. To address such issues, the fuzzy technique for order preference by similarity to ideal solution (TOPSIS) based on multiple criteria decision-making (MCDM) is presented for a security risk assessment of the communication networks of energy management and control systems (EMCS). The methodology focuses on quantifying the security extent in each control step; in order to value the security vulnerability variables derived by the protection analysis model, an MCDM strategy incorporated as a TOPSIS is presented. Ultimately, the example of six communication networks of a power management system is modelled to conduct the security evaluation. The outcome validates the utility of the security evaluation.

Keywords: communication network; security risk; multiple criteria decision-making; security evaluation; power control system

Citation: Alhakami, W. Computational Study of Security Risk Evaluation in Energy Management and Control Systems Based on a Fuzzy MCDM Method. *Processes* **2023**, *11*, 1366. https://doi.org/10.3390/pr11051366

Academic Editors: Radomir Gono, Tomáš Novák, Petr Kacor and Petr Moldřík

Received: 27 March 2023
Revised: 21 April 2023
Accepted: 24 April 2023
Published: 29 April 2023

1. Introduction

Energy tariffing as well as trading, transmission line planning, the control and automation grid interconnection of renewables and electric transportation, energy management, electrical safeguards, cyber security, and copious data-based implementations such as (forecasting) servicing are presently the primary application aspects of ICT in energy systems. Major research and development initiatives are underway in all of these domains. Energy is regarded as a vital development strategy in a country; however, in the current circumstances, energy usage is insufficient, and prices are rising. All of these aspects have a direct impression on the Kingdom of Saudi Arabia's progressive development. As a result, renewable energy resources must be implemented for future usage [1–3]. Furthermore, renewable energy, for example, solar energy, is not constantly available during the day. It is vital to offer a reliable power supply for the entire day when using renewable energy sources as a hybrid power system. The primary goal of energy management control systems (EMCS) is to ensure healthy as well as safe operating parameters for building occupants whilst also reducing the facility's energy and operational expenses. EMCS have been created to increase indoor quality while preserving more power, thanks to technologi-

cal advancements in the fields of electronics, computer systems, as well as sophisticated communications [4–7].

The EMCS architecture consists of various exterior sensors and services, such as fire alarms, surveillance cameras, badge viewers, illumination systems, etc. It additionally encompasses enabling power systems, such as microgrids and power backups, building air conditioning and heating systems, as well HVAC systems. The facility administrators who are in charge of the EMCS architecture that is under threat are among the new stakeholders that must participate as a result of the increased emphasis on securing EMCS. Those currently tasked with ensuring that EMCS have the necessary level of cyber security measures as a component of their crucial infrastructure risk management programs will find important considerations in this paper that can significantly benefit information security control guidelines. The fundamental structure of many of the elements used to provide numerous assistance services presents a significant barrier to protecting energy management control systems. The EMCS elements still in use today often have a long history. The concept of networked devices did not exist when component conception and delivery first began.

Earlier technologies used to manage building loads (including lighting and space conditioning) in the first half of the twentieth century were electromechanical timers that utilized a tiny motor connected to a gearbox to activate electrical connections in accordance with a predetermined timescale. As the output shaft of the gearbox spins, one or more pairings of electrical connections either open or close. Such electromechanical gadgets were simple and dependable, and they continue to be used in some houses to regulate lights and airflow. The main disadvantage of this kind of timer for light as well as ventilation systems was its lack of flexibility. Manual intervention is needed to adjust parameters, and the operating mode is practically without a response (open-loop controllers) because the regulated process's scheduling is not easily changed by the parameters [8–11].

In 2015, the business for energy management systems (EMS) in the United States was worth USD 7.97 billion. The increasing demand for dependable and effective information technology systems for managing, optimizing, and analyzing energy sources is likely to be a major factor driving market expansion. Investment plans in this area are expected to be driven by technological breakthroughs and the increased commercialization of novel products. An increased need for EMS in the industrial sector, particularly in manufacturing as well as power and energy sectors, for the assessment and real-time tracking of energy consumption patterns is expected to drive market expansion throughout the forecast timeframe [12–14]. The Figure 1 shows the market revenue for energy management systems (EMS) in the United States, by product, from 2014 to 2024 (USD Million) as per the market analysis report published by Grand View Research [13].

Connectivity with cloud-based systems, combined with a high degree of automation, has enabled the real-time surveillance of energy-consuming machinery such as HVAC. The stated reason is expected to boost the growth of the U.S. EMS industry within the next eight years. EMS monitors optimizes and saves energy for a variety of end-user segments in the domestic, industrial, as well as manufacturing industries, encompassing power and energy, telecommunications and IT, production, retail and businesses, and healthcare. These sectors identify fast-changing power consumption as well as efficiency potential patterns in the United States, which causes product demand to increase during the projection period. Considerations on minimizing carbon footprints and reusing waste heat in operations are projected to boost demands for cost-effective as well as elevated EMS components in the coming years. Rising R&D efforts to commercialize highly efficient technologies in the United States are expected to create enormous potential for industry participants.

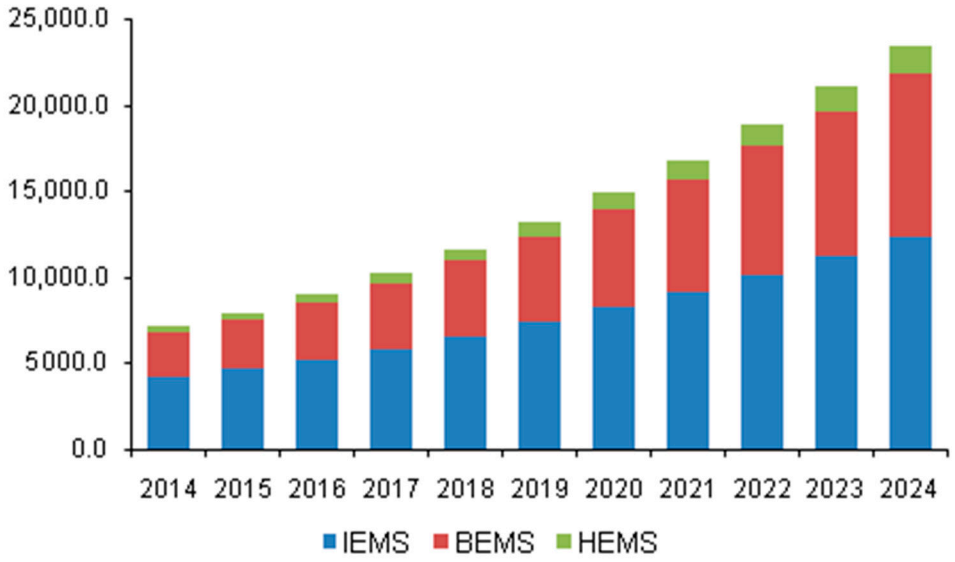

Figure 1. The U.S. energy management systems market size, share, and trends

In relation to cyber security, however, EMCS continues to be terribly lacking. By employing readily available networking technologies, a variety of modern and complex control systems have lately been created. Despite the fact that they are better understood from a cybersecurity standpoint, they still need a coordinated effort and participation from many stakeholders to be protected from malicious actors that intend to do them damage. Institutions that serve critical infrastructure have to guarantee that any operational technology installed is effectively safeguarded against compromise, irrespective of how old or new it is. Numerous regulating authorities frequently demand strong cyber security for all energy management control technologies. The implementation of a strong risk management system is crucial for an organization. In this study, the security risk of EMCS was assessed using the fuzzy TOPSIS approach. Additionally, for resolving collaborative decision-making issues in a fuzzy setting, the fuzzy TOPSIS technique was implemented. It is the recommended strategy for decision-making where the input criterion's details are unclear, yet the criteria themselves are equally significant.

The remaining part of the work is organized in the following manner. A thorough review of the literature on security risk assessment for communication networks of energy management and control systems is presented in Section 2. The prominent MCDM technique for security risk assessment problems with fuzzy TOPSIS is introduced in Section 3. The study's findings are demonstrated in Section 4 with a case including six different communication networks as alternatives. Moreover, Section 5 discusses the research investigation. Concluding thoughts, restrictions, and future work are presented in Section 6.

2. Related Works

Song et al. [15] reviewed the properties of nuclear power plant control and instrumentation technologies as well as the considerations required when performing cyber security risk evaluations in compliance with the instrumentation and control device service lifecycle. The actions and considerations required for cyber security risk evaluations of instrumentation and control systems throughout the design of the system or element development and device supply phase were outlined in the following six steps: (1) system characterization and cybersecurity modelling; (2) resource and impact assessment; (3) threat assessment; (4) vulnerability assessment; (5) security control architecture; and (6) penetration testing.

To tackle the complications of security assessment, Liu et al. [16] presented the attack scenarios as well as multiple criteria decision-making (MCDM). The total security evaluation was divided into two sections. The first is a security analytical method for power control systems centered on an attack graph, which comprises the description of

core ideas, the building algorithm, the vulnerability functionality of every control stage, as well as the computation of connectivity model-based system compromise. Another was centered on quantifying the security extent at every control step. In order to benefit the vulnerability considerations obtained by the security analysis concept, a hybrid MCDM strategy incorporated with an analytic hierarchy process (AHP) and a technique for order preference by similarity to ideal solution (TOPSIS) were also presented. Ultimately, an example communication network of a power management system was modeled to validate the security evaluation. The outcome demonstrated the utility of the security evaluation.

Pan et al. [17] investigated the information security of energy management systems (EMS). They started by expanding their analytic framework, which classifies data breaches as optimization challenges with goals stated as security metrics as well as constraints related to communication network aspects. Second, they created a co-simulation system by combining the energy system simulator DIgSILENT PowerFactory with the communications system simulator OMNeT++ as well as Matlab for EMS implementations. The framework was then utilized to run attack models for a power grid testing phase on the co-simulation-based infrastructure. The findings demonstrated how susceptible EMS is to data breaches and also how co-simulation might aid in vulnerability assessment.

Kim et al. [18] developed a paradigm for risk assessment that quantifies the potential of cyber exploitation as well as the effects of cyberattacks. The assessment of the possibility of cyber exploitation was motivated by a work on Bayesian attack graphs (BAGs), which enabled a probability assessment that takes into account the causal association among ICSs as well as multistage cyberattacks. They presented a way to determine how far an impact would travel and hence how many functionalities would be changed whenever an ICS is abused for cyberattack consequences estimation. ICS professionals used a methodology to identify and define functional connections and critical function goals across ICSs with which they are already aware and do not demand in-depth cybersecurity expertise. They presented the methods to use their framework to determine the dangers of a nuclear power reactor plant's protection systems, which are safety-grade digital systems. Their findings demonstrated that risk could be measured in more dimensions than as was presented in earlier studies, such as identifying that elements that were not previously deemed relevant had a high risk because of their functional connection.

Kim et al. [19] proposed a blockchain-based secure intelligent energy management solution. The blockchain is a decentralized data processing platform in which all network participants share and store information. Incorporating blockchain technology to the smart grid would allow for a more reliable management of energy information, as well as lead to the improvement of the modern intelligent energy sector.

Paridari et al. [20] suggested a revolutionary EMS cyber-physical-security system that employs security analytics to implement a resilient strategy whenever an assault is identified. Both the robust policy as well as the security assessment were driven through EMS data in this approach, where physical correlations among data points were detected to identify outliers, and the feedback control was closed through the use of an approximate value in place of the anomaly. A limited-order version of a real EMS site was used to evaluate the system.

Albakri et al. [21] established a security risk evaluation methodology that allows cloud vendors to evaluate security threats in the cloud computing systems while also allowing cloud customers to participate in risk evaluation. By taking into account cloud clients' judgement of security risk elements and minimizing the complexity which can occur from user involvement in the entire risk assessment process, the suggested methodology produced a more realistic and complete risk assessment output.

According to Woo and Kim [22], contemporary power infrastructure changes need security, and the construction of a cybersecurity infrastructure becomes critical. As a result, they investigated the operations of energy information control systems and calculated the danger level for every component using the security risk measurement criteria in the Korean smart grid security model.

Maziku et al. [23] provided a framework for assessing security vulnerabilities in an intelligent grid communication system with SDN. They specifically assessed the security concerns associated with DoS attacks on intelligent electronic devices (IEDs) as well as the IEC 61850 network. Their security score approach takes into account each IED's crucial role and assesses its impact on the broader smart grid network. They demonstrated how SDN eliminates traffic in the smart grid network as well as enhanced the timing efficiency of IEC 61850-type communications, rendering them time-compatible.

Supervisory control and data acquisition (SCADA) solutions are commonly employed to monitor and regulate industrial processes, as per Gao et al. [24]. They supplied critical capabilities for smart grid, that is a potential power distribution method for the coming years, such as real-time surveillance, logging/archiving, report production, as well as automation. Several SCADA designs, including hardware as well as software layout, have been developed and standardized on the foundation of such functionalities; however, the most open as well as rapidly increasing domains in the smart grid were the architecture-underlying solutions for SCADA communication as well as security. In their work, they discussed several published SCADA regulations, as well as its cutting-edge communication and security features.

Ralston et al. [25] offered a comprehensive overview of cybersecurity as well as risk evaluation for SCADA and DCS, along with an introduction to the major industrial organizations and government organizations involved in the project, and a thorough analysis of the literature to date. The primary principles associated with risk assessment methodologies were presented with references mentioned for extra information. Risk assessment approaches such as HHM, IIM, and RFRM were included in the techniques that have been effectively applied to SCADA systems with complex interdependencies and which have underlined the necessity for quantitative metrics. Probability risk analysis (PRA) is a broad phrase that encompasses approaches such as FTA, ETA, and FEMA. The study continues with a broad description of two recent methodologies (one focused on compromise graphs and another on augmented vulnerability trees) for quantitatively determining the likelihood of an attack, the consequence of the attack, as well as the risk reduction related to a particular form of defense.

Jokar et al. [26] concentrated on smart grid confidentiality and security considerations. Existing security methods created for conventional information technology systems could be leveraged to build smart grid security protocols. Furthermore, new approaches must be developed to fulfil the unique characteristics and requirements of the smart grid. Despite the challenges of building specific security measures for the futuristic smart grid, including such architectural uncertainty as well as a dearth of operational expertise with security assaults, some research have been conducted in this field in recent years. They reviewed the available literature on several elements of smart grid security as well as suggested future research options.

Cárdenas et al. [27] demonstrated how we can identify computer attacks that modify the behavior of the intended control system by combining knowledge about the physical process under control. They can concentrate on the eventual goal of the assault rather than the specific processes of how loopholes are attacked, and the attack is camouflaged by employing an understanding of the physical system. They investigated the consequences of stealthy assaults as well as ensure that automated attack–response systems do not force the system into an unsafe state to assess the safety and confidentiality of the processes. A secondary purpose of this work is to start a conversation among control and security professionals, two fields that have hitherto had minimal interaction.

Kuzlu et al. [28] assembled information on various communication network needs for various smart grid technologies, including those employed in a home area network (HAN), neighborhood area network (NAN), as well as wide-area network (WAN) (WAN). Communications systems that are being used to facilitate the deployment of chosen smart grid initiatives were also discussed. Their study was meant to provide a complete library

of technical needs and best practices for communication engineers to utilize when creating a smart grid system.

3. Materials and Methods

Multi-criteria decision-making (MCDM) is a methodical method for selecting the best choice among workable options. Choosing the optimal option while taking into account multiple factors is difficult in the majority of real-life challenges that decision-makers confront on a regular basis in industries, healthcare, and tertiary institutions, among many other fields. The use of several MCDM technologies, particularly fuzzy TOPSIS, is possible to resolve issues of this kind.

3.1. Factors Affecting the Security of Energy Management and Control System's Communication Networks

To assess the security risk for the communications systems of power management and control systems, the variables that contribute to such complications must first be determined. These would be known as generating variables, and they can be found by analyzing current research as well as the opinions of organizational experts [29]. Such discovered characteristics must be studied in order to assess the security risk appropriately. Numerous characteristics are gathered from the literature study in order to assess the security risk, as shown in Table 1. Table 1 also shows the correlations between the identified parameters and security risk. Following that, each of the discovered variables is simply summarized. Figure 2 illustrates the hierarchical structure for the security risk assessment.

Table 1. Different factors for assessing security risk.

Factors	Definition
Communication Protocol (C1)	A communication protocol is a set of guidelines that enables two or more individuals in a communication network to send information using any physical quantity change. The protocol specifies the communication procedures, syntax, semantics, as well as synchronization, in addition to potential error recovery mechanisms.
Node Security (C2)	A wireless sensor network (WSN) is composed of a group of sensor devices (nodes) that are typically supplied by batteries and linked together via radio links to ensure transmission of data, analysis, and reception. The goal of node security management is to enable sensor nodes to function indefinitely without being compromised by a security assault.
Network Monitoring (C3)	The technique of controlling and maintaining computer networks is known as network management. This field provides services such as fault detection, process improvement, network deployment, as well as quality of service maintenance.
Cryptography (C4)	Cryptography is a means of securing information and communications by using codes to ensure that only those who are supposed to comprehend and utilize the information have access to it.
Security Policy (C5)	A security policy is a generalized document that specifies computer network access restrictions, specifies how policies are implemented, as well as specifies some of the basic infrastructure of the enterprise security/network regulatory environment.

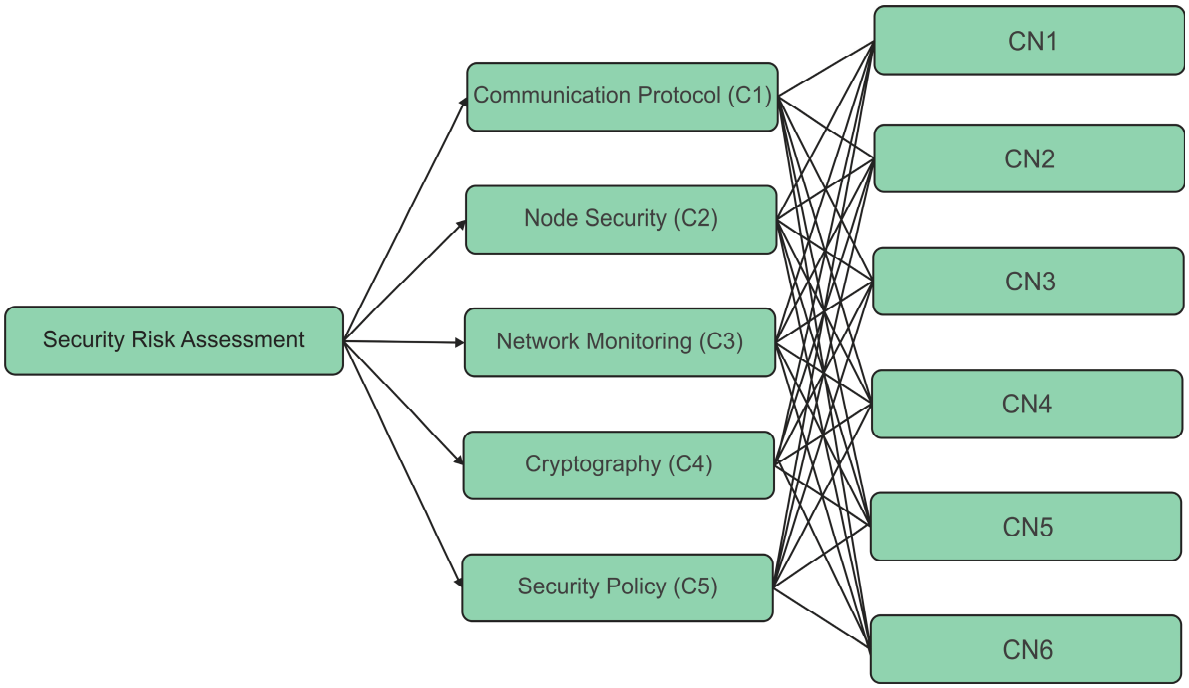

Figure 2. Hierarchical structure for the security risk assessment.

3.2. Fuzzy TOPSIS Methodology

In today's current technology arena, a security risk assessment is still a crucial business concern. This decision procedure involves far too many variables, including economical, technical, societal, as well as risk aspects. Security risk assessment focused on reducing uncontrollable factors and enhancing controllable factors is not a simple undertaking. The fuzzy technique can be a good benchmark to analyze security risk in this MCDM situation. Fuzzy TOPSIS is another multicriteria approach that has gained popularity due to its straightforward methodology as well as readily programmable computing procedure. Hwang and Yoon proposed the TOPSIS method in 1981 [30–32]. It was employed to select the top alternatives centered on many criteria. The TOPSIS method's prominence could be judged by its use in numerous fields to tackle MCDM problems [33–35]. TOPSIS is a form of MCDM techniques that employs fuzzy numbers to tackle the challenges involving human judgement and ambiguity. Numerous techniques which blend TOPSIS with fuzzy logic and can be successfully deployed for handling group decision-making challenges have been developed over the last two decades [36,37].

TOPSIS' basic principle is to choose an option depending on its proximity from the optimum answer. The disadvantage of a standard TOPSIS is that it utilizes the crisp value to choose the best option. Furthermore, there are numerous cases where clear facts are insufficient to mimic a real-life situation, particularly when human judgment is involved in the decision-making procedure. In such a case, the decision must be taken while keeping ambiguity and uncertainty in mind. As a result, rather than providing judgement in the form of a single crisp number, the decision-maker can assess the circumstance utilizing interval judgement and the linguistic phrase. Many TOPSIS researchers have utilized the fuzzy set concept, employing the language notion to cope with ambiguity and imprecise data. The decision-language maker's phrases are translated as triangular, trapezoidal, quadrilateral, as well as Gaussian fuzzy numbers [38–40]. The employment of a particular form of fuzzy number is determined by the nature as well as features of the recognized problems, as well as the eventual nature of their solutions. For example, the triangle membership function is the most basic and is commonly used to express linguistic words. There are several methods available for assessing and rating alternates with different criteria. Each method has benefits and difficulties over the others. Fuzzy TOPSIS is a

popular multicriteria decision-making method. Fuzzy TOPSIS has the benefit of being easy in its computational approach, easy to reflect human preferences, and allowing clear trade-offs between numerous criteria [41,42]. Additionally, the technique is classed as a co-operating approach, with the evidence that while no ideal situation exists, a system with optimal settings on all standards is attainable. As a consequence, fuzzy TOPSIS with a triangle membership function is employed in this work for the security risk assessment of the communication networks of energy management and control systems [43–47].

The sequential step-by-step method for weighting analysis and importance ranking with the use of fuzzy TOPSIS is as follows, as shown in Figure 3:

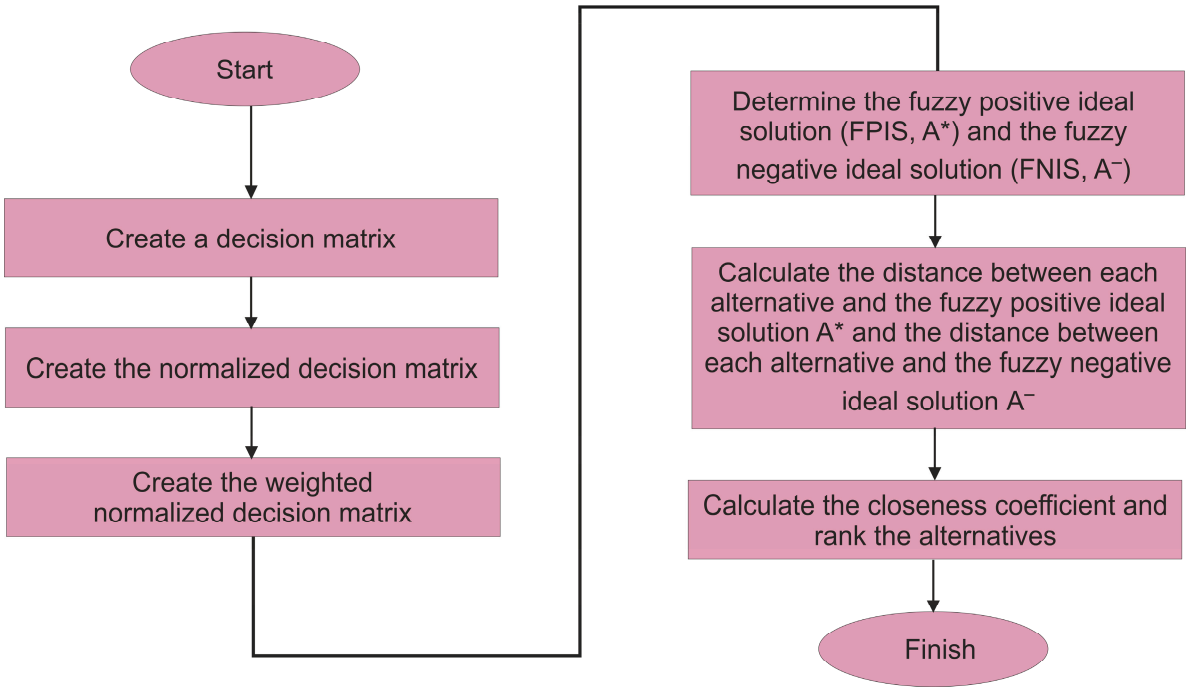

Figure 3. Flow diagram of fuzzy TOPSIS method.

Step 1: Generate a choice matrix for evaluation.

The fuzzy TOPSIS technique is used to assess 5 criteria as well as 6 possible alternatives in this research study. Table 2 shows the criterion classification which is positive for all criteria as well as the weight assigned to each criterion.

Table 2. Characteristics of criteria.

	Criteria	Category	Weight
1	C1	+	(0.200,0.200,0.200)
2	C2	+	(0.200,0.200,0.200)
3	C3	+	(0.200,0.200,0.200)
4	C4	+	(0.200,0.200,0.200)
5	C5	+	(0.200,0.200,0.200)

We assume that our decision-making team consists of K participants. The kth decision-maker's subjective assessment of the alternative A_i with respect to criterion C_j is indicated by $\check{x}_{ij}^{k} = \left(a_{ij}^{k}, b_{ij}^{k}, c_{ij}^{k}\right)$, and the weight of criterion C_j is correspondingly indicated by $\check{w}_{j}^{k} = \left(w_{j1}^{k}, w_{j2}^{k}, w_{j3}^{k}\right)$.

The fuzzy rating scale was developed to account for the fuzziness of individual experiences and perception while assessing attitudes in several areas of psychological research. This scale's adaptability and expressiveness enable us to adequately represent the results of numerous inquiries concerning psychological assessment. The fuzzy scale used in the analysis is illustrated in Table 3.

Table 3. Fuzzy scale.

Linguistic Terms	L	M	U
Very low	1	1	3
Low	1	3	5
Medium	3	5	7
High	5	7	9
Very high	7	9	9

Step 2: Start generating the normalized choice matrix.

A normalized choice matrix can be created by applying the following relation to both positive and negative ideal possibilities:

$$\tilde{r}_{ij} = \left(\frac{a_{ij}}{c_j^*}, \frac{b_{ij}}{c_j^*}, \frac{c_{ij}}{c_j^*} \right); \; c_j^* = \max_i c_{ij}; \text{positive ideal solution} \tag{1}$$

$$\tilde{r}_{ij} = \left(\frac{a_j^-}{c_{ij}}, \frac{a_j^-}{b_{ij}}, \frac{a_j^-}{a_{ij}} \right); \; a_j^- = \min_i a_{ij}; \text{negative ideal solution} \tag{2}$$

Step 3: Develop a weighted normalized decision matrix.

The weighted standardized decision matrix can be created by multiplying each criterion's weight in the normalized fuzzy decision matrix with the help of the following equation, keeping in mind the variable weights of each criterion:

$$\tilde{v}_{ij} = \tilde{r}_{ij}.\tilde{w}_{ij} \tag{3}$$

where $\tilde{w}_{ij}$ indicates weight of criterion c_j.

Step 4: Estimate the fuzzy positive ideal solution (FPIS, A*) as well as the fuzzy negative ideal solution (FNIS, A^-).

The FPIS and FNIS of the alternative solutions can be well characterized using Equation (4) as well as (5):

$$A^* = \left\{ \tilde{v}_1^*, \tilde{v}_2^*, \ldots, \tilde{v}_n^* \right\} = \left\{ \left(\max_j v_{ij} | i \in B \right), \left(\min_j v_{ij} | i \in C \right) \right\} \tag{4}$$

$$A^- = \left\{ \tilde{v}_1^-, \tilde{v}_2^-, \ldots, \tilde{v}_n^- \right\} = \left\{ \left(\min_j v_{ij} | i \in B \right), \left(\max_j v_{ij} | i \in C \right) \right\} \tag{5}$$

within which $\tilde{v}_i^*$ represents the highest proportion of i across all choices, whereas $\tilde{v}_1^-$ represents the least quantity of i across all alternatives. B and C represent the positive as well as negative ideal solutions, respectively.

Step 5: Measure the difference amongst each alternative and also the fuzzy positive ideal alternative A*, in addition to the range amongst each acceptable compromise as well as the fuzzy negative ideal alternative A^-.

The distance between every alternative as well as FPIS, in addition to that between every alternative and FNIS, is calculated with the help of Equations (6) and (7), respectively:

$$S_i^* = \sum_{j=1}^{n} d\left(\tilde{v}_{ij}, \tilde{v}_j^*\right) \quad i = 1, 2 \ldots, m \tag{6}$$

$$S_i^- = \sum_{j=1}^{n} d\left(\tilde{v}_{ij}, \tilde{v}_j^-\right) \quad i = 1, 2 \ldots, m \tag{7}$$

Formula (8) can be employed to measure the separation between two triangular fuzzy integers (a1,b1,c1) and (a2,b2,c2), where d is the separation between the two.

$$d_v\left(\tilde{M}_1, \tilde{M}_2\right) = \sqrt{\frac{1}{3}\left[(a_1 - a_2)^2 + (b_1 - b_2)^2 + (c_1 - c_2)^2\right]} \tag{8}$$

Note that $d\left(\tilde{v}_{ij}, \tilde{v}_j^*\right)$ and $d\left(\tilde{v}_{ij}, \tilde{v}_j^-\right)$ are crisp numbers.

Step 6: Calculate the closeness coefficient and order the choices.

The closeness coefficient of each choice can now be determined using the formula below:

$$CC_i = \frac{S_i^-}{S_i^+ + S_i^-} \tag{9}$$

4. Results

4.1. Statistical Outcomes

In accordance with specific decision criteria, a panel of thirty-five decision-makers was utilized in this study to estimate the security risk for communication networks of energy management and control systems from among six alternatives (CN1, CN2, CN3, CN4, CN5, and CN6). Communication protocol (C1), node security (C2), network monitoring (C3), cryptography (C4), and security policy (C5) are the various criteria. To gather information for the fuzzy TOPSIS study, thirty-five decision-makers were surveyed to assess the relevance of alternative communication networks, utilizing the linguistic variable scale shown in Table 3. The data were determined by the researchers through using regular fuzzy scale (given in Table 3) as well as Equations (1)–(9). The answers are evaluated using a variety of criteria, and the decision matrix results are provided in the following table. The arithmetic mean of all 35 specialist judgements is provided by the choice matrix in Table 4. The normalized decision matrix is shown in Table 5. The weighted normalized decision matrix is also displayed in Table 6. The optimal solutions, both positive and negative, are shown in Table 7. Table 8 also displays the separation between the ideal solutions that are positive and negative. The closeness coefficient of several alternatives is shown in Table 9 as well as Figure 4, respectively.

Table 4. Decision matrix.

	C1	C2	C3	C4	C5
CN1	(4.143,6.143,8.143)	(4.257,6.257,7.743)	(4.600,6.600,7.914)	(3.971,5.971,7.457)	(3.343,5.286,7.000)
CN2	(3.457,5.400,7.171)	(3.686,5.686,7.286)	(3.400,5.400,7.000)	(3.571,5.571,7.229)	(3.171,5.171,7.000)
CN3	(3.400,5.343,7.343)	(3.686,5.686,7.457)	(3.343,5.229,7.057)	(3.514,5.514,7.171)	(3.400,5.343,7.114)
CN4	(3.743,5.686,7.514)	(4.086,6.086,7.743)	(4.086,6.086,7.686)	(3.857,5.857,7.571)	(3.971,5.971,7.743)
CN5	(3.971,5.971,7.686)	(4.371,6.371,7.743)	(4.314,6.314,7.914)	(4.143,6.143,7.629)	(4.486,6.486,8.200)
CN6	(5.629,7.629,8.829)	(5.629,7.629,8.714)	(6.086,8.086,8.771)	(6.086,8.086,8.886)	(6.029,8.029,8.886)

Table 5. A normalized decision matrix.

	C1	C2	C3	C4	C5
CN1	(0.469,0.696,0.922)	(0.489,0.718,0.889)	(0.524,0.752,0.902)	(0.447,0.672,0.839)	(0.376,0.595,0.788)
CN2	(0.392,0.612,0.812)	(0.423,0.653,0.836)	(0.388,0.616,0.798)	(0.402,0.627,0.814)	(0.357,0.582,0.788)
CN3	(0.385,0.605,0.832)	(0.423,0.653,0.856)	(0.381,0.596,0.805)	(0.395,0.621,0.807)	(0.383,0.601,0.801)
CN4	(0.424,0.644,0.851)	(0.469,0.698,0.889)	(0.466,0.694,0.876)	(0.434,0.659,0.852)	(0.447,0.672,0.871)
CN5	(0.450,0.676,0.871)	(0.502,0.731,0.889)	(0.492,0.720,0.902)	(0.466,0.691,0.859)	(0.505,0.730,0.923)
CN6	(0.638,0.864,1.000)	(0.646,0.875,1.000)	(0.694,0.922,1.000)	(0.685,0.910,1.000)	(0.678,0.904,1.000)

Table 6. The weighted normalized decision matrix.

	C1	C2	C3	C4	C5
CN1	(0.094,0.139,0.184)	(0.098,0.144,0.178)	(0.105,0.150,0.180)	(0.089,0.134,0.168)	(0.075,0.119,0.158)
CN2	(0.078,0.122,0.162)	(0.085,0.131,0.167)	(0.078,0.123,0.160)	(0.080,0.125,0.163)	(0.071,0.116,0.158)
CN3	(0.077,0.121,0.166)	(0.085,0.131,0.171)	(0.076,0.119,0.161)	(0.079,0.124,0.161)	(0.077,0.120,0.160)
CN4	(0.085,0.129,0.170)	(0.094,0.140,0.178)	(0.093,0.139,0.175)	(0.087,0.132,0.170)	(0.089,0.134,0.174)
CN5	(0.090,0.135,0.174)	(0.100,0.146,0.178)	(0.098,0.144,0.180)	(0.093,0.138,0.172)	(0.101,0.146,0.185)
CN6	(0.128,0.173,0.200)	(0.129,0.175,0.200)	(0.139,0.184,0.200)	(0.137,0.182,0.200)	(0.136,0.181,0.200)

Table 7. The positive and negative ideal solutions.

	Positive Ideal	Negative Ideal
C1	(0.128,0.173,0.200)	(0.077,0.121,0.162)
C2	(0.129,0.175,0.200)	(0.085,0.131,0.167)
C3	(0.139,0.184,0.200)	(0.076,0.119,0.160)
C4	(0.137,0.182,0.200)	(0.079,0.124,0.161)
C5	(0.136,0.181,0.200)	(0.071,0.116,0.158)

Table 8. Distance from positive and negative ideal solutions.

	Distance from Positive Ideal	Distance from Negative Ideal
CN1	0.186	0.071
CN2	0.251	0.005
CN3	0.249	0.009
CN4	0.196	0.061
CN5	0.165	0.092
CN6	0	0.255

Table 9. Closeness coefficient.

	Ci	Rank
CN1	0.275	3
CN2	0.018	6
CN3	0.036	5
CN4	0.236	4
CN5	0.357	2
CN6	1	1

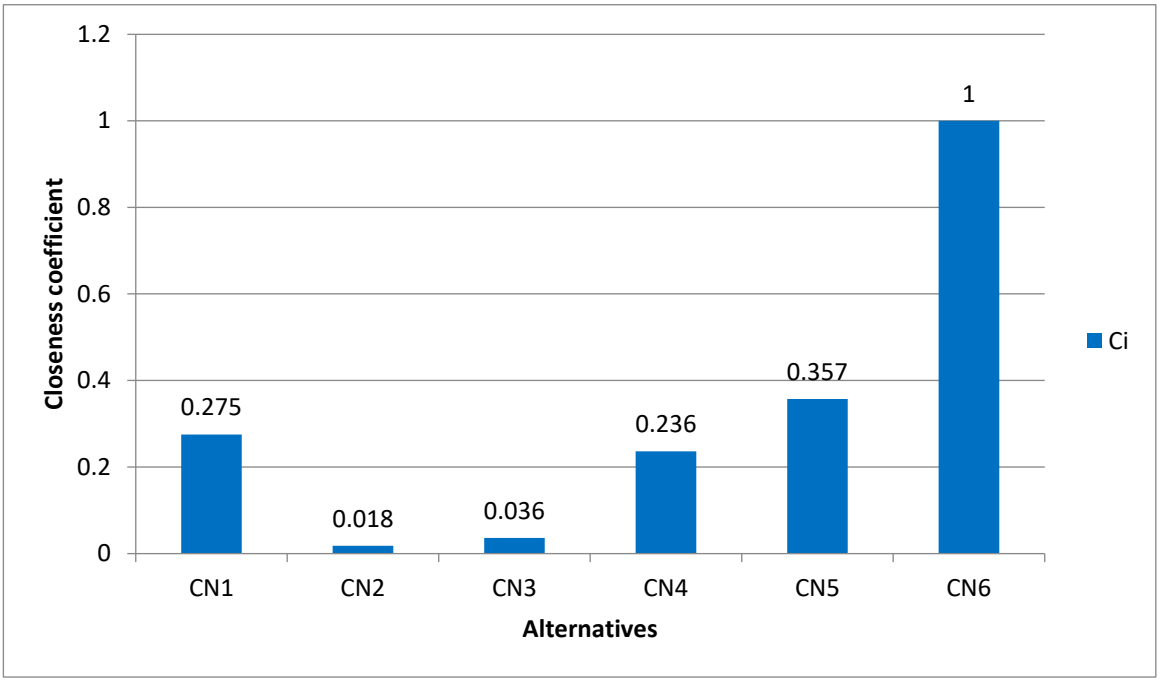

Figure 4. Graphical illustration of closeness coefficient (Ci).

Every alternative's proximity coefficient is displayed in the graphical diagram below.

Ultimately, the findings of the calculations for the proximity coefficient are displayed in Table 9. The various communication networks of energy management and control systems as alternatives are ranked based on closeness coefficient values and the rankings are also illustrated in Figure 4. From Table 9 and Figure 4, the alternative with the ranking of 1 is the communication network 6 (CN6), hence it is the optimal secure communication network for the energy management and control systems. The least secure communication network for the energy management and control systems is communication network 2 (CN2) ranking at number 6 among all alternative communication networks. The competence of the decision-makers and the weight given to various decision criteria are two variables that affect the outcome of the fuzzy TOPSIS assessment.

4.2. Comparative Findings of the Fuzzy TOPSIS and TOPSIS Analysis

Advanced configurable technologies with a dynamic network architecture and cognitive management layer are replacing basic point-to-point static solutions that are configured as well as controlled as silos in communications infrastructure. The network's physical component is moving toward an ultrahigh performance, long-reach optical connectivity, backed through sliceable bandwidth variable transmitters and different modulation formats deployed through a flexible spectrum segment. As a result of software defined networking (SDN), which enables the opening up of the connected devices through programmable ports, the control plane becomes separated from the data layer and is centralized. As the network moves toward scattered cloud environments, connectivity as well as traffic conditions also shift. Enterprises shift their storage and computing assets to dispersed large data centers for cloud platforms, and they are more concerned with access to resources that must meet a rigid set of performance requirements than they are with connectivity to specific sites. As a result, any one of the datacenters which serves the content may be chosen as the destination network of a special request, changing the unicast connection among an origin of a request and a particular, recognized destination which hosts the required material into an anycast connection. Furthermore, the virtualized applications can be moved across several physical servers that are housed in the same or separate datacenters, resulting in altered traffic patterns. Many malicious attack strategies can be created to target various network segments. Many attacks target the physical layer, taking advantage of the security

flaws in important optical components to obstruct services or record traffic. Intruders are also interested in the centralized SDN controller because taking control of it would give them access to a large portion of the network. Because of multitenancy as well as service movement, new security risks appear in cloud computing environments. Many of the attack techniques have traits with breakdown elements that may be avoided using current techniques, especially those that take large-scale network failures into account. Table 10 uses the TOPSIS and fuzzy TOPSIS methodologies to generate the security risk evaluation ranking of the EMCS communication networks as various scenarios. It is evident that CN6 will be chosen using any strategy, making EMCS CN6 the most effective and reliable communication network. Every method has a different preference, with the exception of CN6. The rankings produced by the fuzzy TOPSIS are CN6 > CN5 > CN1 > CN4 > CN3 > CN2, but the rankings produced by the TOPSIS method are CN6 > CN1 > CN5 > CN4 > CN2 > CN3. An optimal situation might not be possible given the MCDM features of the proposed problem, but a thorough study of the MCDM challenge might reduce the possibility of selecting a quality service that is insufficient. When reliable performance scores are provided, the TOPSIS strategy is regarded as a good answer to the security risk evaluation ranking of communication networks of a challenging EMCS task. Ambiguous or imprecise performance assessments are permissible when utilizing fuzzy TOPSIS to tackle the targeted service reliability concern.

Table 10. Comparison table.

Ranking Order	1	2	3	4	5	6
TOPSIS	CN6	CN1	CN5	CN4	CN2	CN3
Fuzzy TOPSIS	CN6	CN5	CN1	CN4	CN3	CN2

The proposed study compares TOPSIS with fuzzy TOPSIS in order to present a systematic evaluation process for selecting the most dependable and secure EMCS communication network. By limiting the amount of possibilities, the proposed methodology makes decision-making easier. In the end, the fuzzy TOPSIS method has some shortcomings. The degree of natural language representation membership is influenced by the decision-managerial maker's viewpoint. The decision-maker is required to be at a strategic position in the organization in order to evaluate the relevance and trends of all the various aspects, which include communication protocol (C1), node security (C2), network monitoring (C3), cryptography (C4), and security policy (C5), to analyze various communication networks of EMCS as alternative solutions.

5. Discussion

Machine learning and AI were hardly addressed in the expert interviews despite the fact that the most recent research indicates that approaches for detecting false data injection (FDI) assaults are actively being investigated using artificial intelligence (AI) techniques. This difference could be the result of two factors. One explanation could be that the interviewees' areas of specialization were primarily energy systems rather than, for example, computer science. An additional consideration might be the academic study's forward-looking nature (as all academic research ought to be). As a result, the use of AI in attack vectors may increase in the coming years. This shift might be consistent with the growing (noncriminal) use of AI across a range of fields and daily applications [48–53]. The novel approach described in this article was created to evaluate the security risks associated with various communication networks of energy management and control system infrastructures. As previously mentioned, any malfunction in the information infrastructure, particularly in the critical connectivity, can have far-reaching effects, such as significant reductions in public safety for a prolonged period of time, irrecoverable harmful damage of the architecture, or large-scale financial loss. The dangers connected with such technologies increase due to the potential for such infrastructure interruption. The presence

of security risks thus necessitates the development of efficient techniques for security risk assessment. The prevention of incidents and the stopping of operations at CII is a crucial concern for any nation. An assessment of the most likely and dangerous threats is the first step in implementing appropriate precautions. The risk management approach does not, therefore, begin with risk identification. To begin reducing the most hazardous threats, it is vital to assess the significance of each risk and its likelihood. Implementing scientific and computational procedures that need a significant amount of data and calculations will produce the most appropriate solutions to the problem. Experts can verbally provide the initial data using analogous group decision-making techniques. Every specialist has a unique perspective on the assessment criteria. The fuzzy TOPSIS rating system is then used to determine the significance of expert judgments. Additionally, because the prediction model may be used in different situations, it outperforms traditional approaches. As a result, it is an effective tool for handling such issues.

By utilizing efficient MCDM techniques, risks can be regularly checked in order to avoid repercussions which might shut down or harm the system. The basis for a risk assessment must be due to expert understanding, which enables the prediction of future breakdowns in the communication networks of energy management and control systems by determining the frequency of malfunctions and their effects. Since erroneous information can result in significant losses, it is important to accurately gather information regarding the risks realized and the accidents that have happened. As a result, it is a subject that is of great importance and relevance to any nation.

6. Conclusions

Sustainable energy systems have evolved into hybrid systems that are tightly connected to information and communication networks. Information technology utilization enhances power system management and functioning, but it also raises the possibility of cybersecurity flaws. As a result, the protection of information and communication systems has steadily emerged as one of the key elements affecting the security of the energy system. By employing the fuzzy TOPSIS-based MCDM technique, the suggested model aims to tackle the problem of determining the risks of the communication networks of energy management and control system infrastructures. Communication protocol (C1), node security (C2), network monitoring (C3), cryptography (C4), and security policy (C5) are the six essential criteria (C5). According to the assessment, this particular order of criteria results in the most significant and secure communication network: CN6 > CN5 > CN1 > CN4 > CN3 > CN2. The model described in this paper is useful for analyzing the likelihood of risk and its consequences as well as for assessing the weighting of criteria in multicriteria utility functions. It is suggested that this model be expanded upon to estimate the risks associated with crucial information networks. Future research might concentrate on expanding communication network security with some more influencing criteria. A simulation theorem with additional effective MCDM techniques in a fuzzy environment might be proposed in a subsequent study. To create a more suitable approach for a network security risk assessment, future studies may examine such type of network security problems.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Jayachandran, M.; Reddy, C.R.; Padmanaban, S.; Milyani, A.H. Operational planning steps in smart electric power delivery system. *Sci. Rep.* **2021**, *11*, 17250. [CrossRef] [PubMed]
2. Liu, J.; Xiao, Y.; Li, S.; Liang, W.; Chen, C.P. Cyber security and privacy issues in smart grids. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 981–997. [CrossRef]

3. Wolsink, M. The research agenda on social acceptance of distributed generation in smart grids: Renewable as common pool resources. *Renew. Sustain. Energy Rev.* **2012**, *16*, 822–835. [CrossRef]
4. Hossain, E.; Khan, I.; Un-Noor, F.; Sikander, S.S.; Sunny MS, H. Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access* **2019**, *7*, 13960–13988. [CrossRef]
5. Huang, W.Z.; Zaheeruddin, M.; Cho, S.H. Dynamic simulation of energy management control functions for HVAC systems in buildings. *Energy Convers. Manag.* **2006**, *47*, 926–943. [CrossRef]
6. Papantoniou, S.; Kolokotsa, D.; Kalaitzakis, K. Building optimization and control algorithms implemented in existing BEMS using a web based energy management and control system. *Energy Build.* **2015**, *98*, 45–55. [CrossRef]
7. Yigit, M.; Gungor, V.C.; Tuna, G.; Rangoussi, M.; Fadel, E. Power line communication technologies for smart grid applications: A review of advances and challenges. *Comput. Netw.* **2014**, *70*, 366–383. [CrossRef]
8. Marzband, M.; Sumper, A.; Ruiz-Álvarez, A.; Domínguez-García, J.L.; Tomoiagă, B. Experimental evaluation of a real time energy management system for stand-alone microgrids in day-ahead markets. *Appl. Energy* **2013**, *106*, 365–376. [CrossRef]
9. So, A.T.P.; Chan, W.L. *Intelligent Building Systems*; Springer Science & Business Media: Berlin, Germany, 1999; Volume 5.
10. Ali, A.S.; Coté, C.; Heidarinejad, M.; Stephens, B. Elemental: An open-source wireless hardware and software platform for building energy and indoor environmental monitoring and control. *Sensors* **2019**, *19*, 4017. [CrossRef]
11. Alzahrani, F.A.; Ahmad, M.; Ansari MT, J. Towards design and development of security assessment framework for internet of medical things. *Appl. Sci.* **2022**, *12*, 8148. [CrossRef]
12. Gladence, L.M.; Sangeetha, K.K.; Soundharya, S.; Selvan, M.P. Smart Home Monitoring System and Prediction of Power Consumption. In Proceedings of the 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 29–31 March 2022; pp. 1–7.
13. U.S. Energy Management Systems Market Size Report, 2024. Available online: https://www.grandviewresearch.com/industry-analysis/us-energy-management-systems-ems-market (accessed on 1 February 2023).
14. Seh, A.H.; Al-Amri, J.F.; Subahi, A.F.; Ansari MT, J.; Kumar, R.; Bokhari, M.U.; Khan, R.A. Hybrid computational modeling for web application security assessment. *CMC-Comput. Mater. Contin.* **2022**, *70*, 469–489.
15. Song, J.G.; Lee, J.W.; Lee, C.K.; Kwon, K.C.; Lee, D.Y. A cyber security risk assessment for the design of I&C systems in nuclear power plants. *Nucl. Eng. Technol.* **2012**, *44*, 919–928.
16. Liu, N.; Zhang, J.; Zhang, H.; Liu, W. Security assessment for communication networks of power control systems using attack graph and MCDM. *IEEE Trans. Power Deliv.* **2010**, *25*, 1492–1500. [CrossRef]
17. Pan, K.; Teixeira, A.; López, C.D.; Palensky, P. Co-simulation for cyber security analysis: Data attacks against energy management system. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 253–258.
18. Kim, A.; Oh, J.; Kwon, K.; Lee, K. Consider the consequences: A risk assessment approach for industrial control systems. *Secur. Commun. Netw.* **2022**, *2022*, 3455647. [CrossRef]
19. Kim, S.M.; Lee, T.; Kim, S.; Park, L.W.; Park, S. Security issues on smart grid and blockchain-based secure smart energy management system. In *MATEC Web of Conferences*; EDP Sciences: Les Ulis, France, 2019; Volume 260, p. 01001.
20. Paridari, K.; Mady, A.E.D.; La Porta, S.; Chabukswar, R.; Blanco, J.; Teixeira, A.; Sandrberg, H.; Boubekeur, M. Cyber-physical-security framework for building energy management system. In Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS), Vienna, Austria, 11–14 April 2016; pp. 1–9.
21. Albakri, S.H.; Shanmugam, B.; Samy, G.N.; Idris, N.B.; Ahmed, A. Security risk assessment framework for cloud computing environments. *Secur. Commun. Netw.* **2014**, *7*, 2114–2124. [CrossRef]
22. Woo, P.S.; Kim, B.H. Risk analysis of power information control system based on smart grid security standardization. *Int. J. Smart Grid Clean Energy* **2019**, *8*, 140–148. [CrossRef]
23. Maziku, H.; Shetty, S.; Nicol, D.M. Security risk assessment for SDN-enabled smart grids. *Comput. Commun.* **2019**, *133*, 1–11. [CrossRef]
24. Gao, J.; Liu, J.; Rajan, B.; Nori, R.; Fu, B.; Xiao, Y.; Liang, W.; Philip Chen, C.L. SCADA communication and security issues. *Secur. Commun. Netw.* **2014**, *7*, 175–194. [CrossRef]
25. Ralston, P.A.; Graham, J.H.; Hieb, J.L. Cyber security risk assessment for SCADA and DCS networks. *ISA Trans.* **2007**, *46*, 583–594. [CrossRef]
26. Jokar, P.; Arianpoo, N.; Leung, V.C. A survey on security issues in smart grids. *Secur. Commun. Netw.* **2016**, *9*, 262–273. [CrossRef]
27. Cárdenas, A.A.; Amin, S.; Lin, Z.S.; Huang, Y.L.; Huang, C.Y.; Sastry, S. Attacks against process control systems: Risk assessment, detection, and response. In Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 22–24 March 2011; pp. 355–366.
28. Kuzlu, M.; Pipattanasomporn, M.; Rahman, S. Communication network requirements for major smart grid applications in HAN, NAN and WAN. *Comput. Netw.* **2014**, *67*, 74–88. [CrossRef]
29. Piya, S.; Shamsuzzoha, A.; Azizuddin, M.; Al-Hinai, N.; Erdebilli, B. Integrated fuzzy AHP-TOPSIS method to analyze green management practice in hospitality industry in the sultanate of Oman. *Sustainability* **2022**, *14*, 1118. [CrossRef]
30. Hwang, C.L.; Yoon, K.; Hwang, C.L.; Yoon, K. Methods for multiple attribute decision making. In *Multiple Attribute Decision Making: Methods and Applications a State-of-the-Art Survey*; Springer: Berlin/Heidelberg, Germany, 1981; pp. 58–191.

31. Alassery, F.; Alzahrani, A.; Khan, A.I.; Khan, A.; Nadeem, M.; Ansari, T.J. Quantitative Evaluation of Mental-Health in Type-2 Diabetes Patients Through Computational Model. *Intell. Autom. Soft Comput.* **2022**, *32*, 1701–1715. [CrossRef]
32. Sun, Q.; Li, R. Stable and optimal adaptive fuzzy control of complex systems using fuzzy dynamic model. *Fuzzy Sets Syst.* **2003**, *133*, 1–17. [CrossRef]
33. Coban, A.; Ertis, I.F.; Cavdaroglu, N.A. Municipal solid waste management via multi-criteria decision making methods: A case study in Istanbul, Turkey. *J. Clean. Prod.* **2018**, *180*, 159–167. [CrossRef]
34. Parhi, M.; Acharya, B.M. A Flexible tool for Discovery and Selection of Sensor Web Registry Services with Extended SOA Framework. *Int. J. Comput. Appl.* **2012**, *975*, 8887. [CrossRef]
35. De Brito, M.M.; Evers, M. Multi-criteria decision-making for flood risk management:<? xmltex\newline?> a survey of the current state of the art. *Nat. Hazards Earth Syst. Sci.* **2016**, *16*, 1019–1033.
36. Mardani, A.; Zavadskas, E.K.; Khalifah, Z.; Zakuan, N.; Jusoh, A.; Nor, K.M.; Khoshnoudi, M. A review of multi-criteria decision-making applications to solve energy management problems: Two decades from 1995 to 2015. *Renew. Sustain. Energy Rev.* **2017**, *71*, 216–256. [CrossRef]
37. Agrawal, A.; Khan, R.A.; Ansari MT, J. Empowering Indian citizens through the secure e-governance: The digital India initiative context. In *Emerging Technologies in Data Mining and Information Security: Proceedings of IEMIS 2022*; Springer Nature Singapore: Singapore, 2022; Volume 3, pp. 3–11.
38. Feldman, J. Bias toward regular form in mental shape spaces. *J. Exp. Psychol. Hum. Percept. Perform.* **2000**, *26*, 152. [CrossRef]
39. Ibrahim, A.A.; Zhou, H.B.; Zhang, C.L.; Duan, J.A. Analysis of the Footprint of Uncertainty of a Parallelogram Membership Function. *Int. J. Artif. Intell. Math. Sci.* **2022**, *1*, 1–14. [CrossRef]
40. Pramanik, R.; Baidya, D.K.; Dhang, N. Reliability analysis for bearing capacity of surface strip footing using fuzzy finite element method. *Geomech. Geoengin.* **2020**, *15*, 29–41. [CrossRef]
41. Kannan, D.; Khodaverdi, R.; Olfat, L.; Jafarian, A.; Diabat, A. Integrated fuzzy multi criteria decision making method and multi-objective programming approach for supplier selection and order allocation in a green supply chain. *J. Clean. Prod.* **2013**, *47*, 355–367. [CrossRef]
42. Abdel-malak, F.F.; Issa, U.H.; Miky, Y.H.; Osman, E.A. Applying decision-making techniques to Civil Engineering Projects. *Beni-Suef Univ. J. Basic Appl. Sci.* **2017**, *6*, 326–331. [CrossRef]
43. Alshahrani, H.M.; Alotaibi, S.S.; Ansari MT, J.; Asiri, M.M.; Agrawal, A.; Khan, R.A.; Mohsen, H.; Hilal, A.M. Analysis and Ranking of IT Risk Factors Using Fuzzy TOPSIS-Based Approach. *Appl. Sci.* **2022**, *12*, 5911. [CrossRef]
44. Ansari, M.T.J.; Pandey, D.; Alenezi, M. STORE: Security threat oriented requirements engineering methodology. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 191–203. [CrossRef]
45. Ansari MT, J.; Al-Zahrani, F.A.; Pandey, D.; Agrawal, A. A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 236. [CrossRef]
46. Khodadadi-Karimvand, M.; Shirouyehzad, H. Well drilling fuzzy risk assessment using fuzzy FMEA and fuzzy TOPSIS. *J. Fuzzy Ext. Appl.* **2021**, *2*, 144–155.
47. Tiwari, S.; Rosak-Szyrocka, J.; Żywiołek, J. Internet of things as a sustainable energy management solution at tourism destinations in India. *Energies* **2022**, *15*, 2433. [CrossRef]
48. Al Sumarmad, K.A.; Sulaiman, N.; Wahab, N.I.A.; Hizam, H. Energy management and voltage control in microgrids using artificial neural networks, PID, and fuzzy logic controllers. *Energies* **2022**, *15*, 303. [CrossRef]
49. Muqeet, H.A.; Javed, H.; Akhter, M.N.; Shahzad, M.; Munir, H.M.; Nadeem, M.U.; Bukhari, S.S.H.; Huba, M. Sustainable Solutions for Advanced Energy Management System of Campus Microgrids: Model Opportunities and Future Challenges. *Sensors* **2022**, *22*, 2345. [CrossRef]
50. Kelm, P.; Wasiak, I.; Mieński, R.; Wędzik, A.; Szypowski, M.; Pawełek, R.; Szaniawski, K. Hardware-in-the-loop validation of an energy management system for LV distribution networks with renewable energy sources. *Energies* **2022**, *15*, 2561. [CrossRef]
51. Alanen, J.; Linnosmaa, J.; Malm, T.; Papakonstantinou, N.; Ahonen, T.; Heikkilä, E.; Tiusanen, R. Hybrid ontology for safety, security, and dependability risk assessments and Security Threat Analysis (STA) method for industrial control systems. *Reliab. Eng. Syst. Saf.* **2022**, *220*, 108270. [CrossRef]
52. Borenius, S.; Gopalakrishnan, P.; Bertling Tjernberg, L.; Kantola, R. Expert-Guided Security Risk Assessment of Evolving Power Grids. *Energies* **2022**, *15*, 3237. [CrossRef]
53. Yang, Y.S.; Lee, S.H.; Chen, W.C.; Yang, C.S.; Huang, Y.M.; Hou, T.W. Securing SCADA Energy Management System under DDos attacks using token verification approach. *Appl. Sci.* **2022**, *12*, 530. [CrossRef]