Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

Smart Infrastructure Project Decision-Making Under Cyber Threat Uncertainty Using Hybrid DSS Models

Sadia Afrin[1], Tonay Roy[2], MD Rafat Hossain[3], Mohammad Imran Khan[4] and Akhtaruzzaman Khan[5]

[1]*Master of Science in Information Studies ,Trine University, 127,wellington road,upper darby, Zip code:19082, pennsylvania,USA*
[2]*Bachelor of Science in Computer Science & Engineering, Dhaka International University, 59/A,Panthapath, Dhaka 1215*
[3]*Seidenberg School Of Computer Science and Information Systems - Pace University,101-11 86th st, Ozone park, NY 11416*
[4]*Zaman Construction Corp, New York, USA; Formerly: Trine University, College of Graduate and Professional Studies, 101-11 86th st, Ozone park, NY 11416*
[5]*Masters of Science in Computer Science, San Francisco Bay University, USA*
Corresponding author: Sadia Afrin. **Email:** sadiaafrinaivy@gmail.com

| ABSTRACT

With the rise of digitalization in the world, there is a much greater emphasis on the use of smart technologies in infrastructure systems, which has greatly contributed to the improvement of efficiency, service delivery, and data analytics. It is questionable whether this digitalization journey does not expose the critical infrastructure to emerging and unforeseeable cyber threats such as phishing, ransomware, malware, and Distributed Denial of Service (DDoS) attacks. These threats are uncertain and very complex; hence, their traditional decision-making techniques do not have flexibility in dealing with the ambiguous, incomplete, or dynamic intelligence on the threats. This study identifies a hybrid Decision Support System (DSS) model consisting of Natural Language Processing (NLP), fuzzy logic, sentiment analysis and multi-criteria decision making (MCDM) to solve cyber threat uncertainty within a smart infrastructure setting. The research corpus is a structured cybersecurity dataset with an NLP extension with the threat description, keywords extraction, and risk prediction, severity scoring. Using the proposed hybrid approach, the DSS framework can categorize threats, identify Indicators of Compromises (IOCs), estimate severity, and propose defense measures based on both structured and unstructured data. e.g., Python, Tableau, or Excel are used as a visualization tool to analyze threat distributions, sentiment scores, and response strategies. In this study, the results obtained dictate that certain types of threats, attack vectors, geographical targeting, and severity of risk exist in good lineage that lends critical value to decisions made during strategy. The threat-driven sentiment analysis on discussions provides yet another contextual dimension that helps to make better and timely cybersecurity planning options. The proposed model illustrates that it is possible to transform the cyber threat uncertainty into actionable intelligence, which would allow the stakeholders to focus on threats-related priorities, to properly invest funds into the procurement of the appropriate resources, and to create resiliency-based responses. The proposed framework combines an intelligent decision-making process with a scalable paradigm of threat dynamics and, therefore, contributes to the growing complex field of cyber-resilient infrastructure. Finally, the hybrid DSS solution presents a viable and novel way of providing cybersecurity posture and safeguarding the critical infrastructure resources against the formidable and enduring cyber threats.

| KEYWORDS

Smart Infrastructure, Cybersecurity Threats, Decision Support System (DSS), Natural Language Processing (NLP), Fuzzy Logic and Cyber Threat Intelligence (CTI)

| ARTICLE INFORMATION

ACCEPTED: 12 July 2025 **PUBLISHED:** 13 August 2025 **DOI:** 10.32996/jcsts.2025.7.8.106

1. Introduction

1.1 Background

The era of digitalization has transformed the way modern societies handle life-critical services such as transportation, energy distribution services, water services, and even the normal security of the people. They are based on the best technologies available, such as the Internet of Things (IoT), Artificial Intelligence (AI), real-time data analytics, and cloud computing to make operations more efficient, sustainable, and responsive. When such digital technologies are integrated into physical infrastructure, they raise new degrees of difficulty and susceptibility, especially in the cybersecurity field. Since these infrastructures are increasingly interconnected, more endpoints and data flows are available to be exploited. Attackers may attack the weak areas of communication networks, sensors, or software systems, producing effects that could not only result in data privacy, but will also result in physical disruption. Threat landscape is rapidly changing and towards this end, infrastructure-based cyber-attacks are increasing in frequency, sophistication, and severity [1]. Able to affect the security of the entire population and causing economic damage, the protection of the smart infrastructure from cyber-attacks has taken on a new dimension in the focus of governments, corporations, and citizens alike. To eliminate this issue, both technical defense strategies and smart decision-making frameworks which can work in a context characterized by risk, complexity, and uncertainty are needed.

1.2 The Uncertainty Challenge of Cyber Threat

The cyber threats to smart infrastructure are continually increasing and more importantly are of a high-level of uncertainty. Phishing, ransomware, Distributed Denial of Service (DDoS) and Advanced Persistent Threats (APTs) are all examples of threats that are rapidly evolving and are exploiting not-was-known or zero-day vulnerabilities and are often evading more traditional security control systems [2]. The randomness of these threats poses a very tough challenge to the stakeholders in the infrastructure system to determine how to address these threats by utilizing security resources that are available. Cyber threat uncertainty means inexperienced attack vectors, no predictability of severity and little information regarding the nature of the threat actors or the consequences. In this environment of uncertainty, the decision-makers can seldom get timely, accurate, and complete information so that ineffective and delayed response is inevitable. real-time intelligence is usually buried deep in unstructured documents like on social media, forums and technical reports, and the information is hard to garner into actionable chunks using traditional tools [3]. Conventional styles of decision-making do not contain the ambiguity or variability found in the environments of cyber threats. Consequently, the organizations find it hard to focus on security measures, gauge the level of risk or make the right investment decisions toward cyber defense of infrastructure systems [4]. In order to be resilient, it is necessary to have powerful frameworks capable of incorporating uncertain, incomplete, or highly dynamic information as the elements of smart, agile decision models.

1.3 Hybrid Decision Support Systems (DSS) Requirements

The uncertainty of cyber threats in smart infrastructure cannot be solved using advanced decision-making systems, some of which should not be based on static risk calculations or rule-based alarm systems [5]. The Hybrid Decision Support Systems (DSS) arise as an attractive solution to the dynamic and uncertain environment due to seamlessly combining several methods of analysis and decision models. Hybrid DSS is a mixture of structured logic, machine learning and soft computing instruments like fuzzy logic and Bayesian inference to portray hazards, rank steps and propose offset directives. In contrast to the classic systems, the hybrid DSS systems can handle quantitative data such as scores representation of the attack severity, the probability, qualitative input such as textual description of threats, the sentiment [6]. With the integration of fuzzy Multi-Criteria Decision-Making (MCDM), these systems have the potential to compute the alternatives in cases when a decision criterion is not objective or precise. Bayesian models also improve the process of decision-making because probabilities change as new threat intelligence is discovered. A hybrid DSS has flexibility, adaptability, and preciseness that are needed in the context of smart infrastructure in which the decisions made must be based on cost, criticality, impact, and response time. The system is also capable of making what-if scenarios and prioritize threats and prescribing the best deployment of resources [7]. It is also able to accept input of human analysts and incorporate automated tools of threat detection. Due to increasing complexity of cyber threats, hybrid DSS frameworks are becoming tools capable of empowering infrastructure managers to make timely, data-driven, risk-aware decisions.

1.4 Role of NLP in cyber threat intelligence (CTI)

Natural Language Processing (NLP) is a revolutionary aspect of the current Cyber Threat Intelligence (CTI), where machines can process and analyze huge quantities of textual information of heterogeneous origins. Some of the most important information regarding new threats, attacker tactics, and vulnerabilities in the cybersecurity domain can be found in non-standard forms like incident reports, blogs, forums of hackers, and technical advisory reports [8]. NLP supports extraction of relevant indicators including IP addresses, names of malware, threat actors, and techniques of attacks using Named Entity Recognition (NER), keyword extraction and topic modeling in an automated way. It also can detect sentiment or urgency behind the discussion of security issues capable of giving early warning of emerging threats. When it is applied to a Decision Support System (DSS) NLP improves the capacity of the system to Contextually multi–Threat Model Reasoning System [9]. NLP could facilitate the differentiation of the type of threat; determination of the severity depending on the textual feature and relate incidents to known weaknesses. This functionality is especially useful in the context of intelligent infrastructure when cybersecurity challenges continuously change and decisions should be timely and made under evidence [10]. Linguistic and behavioral linguistic and behavioral analysis are not only enhancing visibility into threats but also enriching the decision-making side of cyber risk modeling.

1.5 Significance of Dataset Driven Modeling Cybersecurity

Cybersecurity is centered on data-driven modeling to make intelligent decisions, especially when it comes to threat response to smart infrastructure. This use relies on the dataset called the NLP-Based Cyber Security dataset present on Kaggle and constitutes an organized and vast set comprising 1,100 instances of cyber threats [11]. Both contain crucial characteristics in terms of threat type, IOCs (including Indicator of Compromises), method of attack, threat group, source system location, Defense suggestions, and risk capabilities. It also consists of strong features of NLP, which include scrubbed threat descriptions, keyword extractions, named entities, sentiment scores as obtained in the hacker forums [12]. The set of data is positioned between structured cyber threat metadata and unstructured textual intelligence bridging. With an exploitation of such a data set, the study will have great resources as input data where a hybrid DSS model can be trained, tested, and assessed. These characteristics assist the multiple-dimensional threat evaluation, promote uncertainty quantification, and prove the possibility to handle the probability classification and prioritization of the risks. It also has both linguistic and numeric variables, which enables the integration with NLP models, fuzzy MCDM methods and Bayesian inference algorithms [13]. The real-world protocol of the dataset also demonstrates similarity to the complexity and dynamism of the in-place infrastructure threat settings, hence providing sensitivity and relevance to smart city or critical infrastructure contexts.

1.6 Research Problem

Despite the improved cyber defense technology, there remains a large gap in the establishment of intelligent systems that would aid in decision-making in circumstances of uncertainty especially in smart infrastructure protection [14]. To increase resilience, cyber threat uncertainty is required to be quantified and implemented in strategic decisions regarding the project. A hybrid Decision Support System (DSS) combining the technologies of the Natural Language Processing (NLP), fuzzy logic and risk modeling offers a promising solution to closer prioritization of cybersecurity responses. In addition, the interpretation of textual data and analysis can be important in determining the intensity of threat and its context-based defense solutions. The objective of this research is on designing, implementing and evaluation of a hybrid DSS framework that leverages NLP-enhanced threat intelligence to enhance cyber-resilient decision- making processes in smart infrastructure settings.

1.7 Research Objectives

This study will construct a hybrid DSS framework to deal with cybersecurity and smart infrastructure with an intention of creating better decision-making. Objectives are:

- To study through NLP- enhanced data the patterns of cyber threats.
- To categorize and rank cyber threats according to severity and ambiguity.
- To use the fuzzy MCDM methods to cope with vague decision elements.
- To use Bayesian modeling to predict dynamic risks.
- To combine the textual and sentiment analysis of risk.

- It is to test the performance of the DSS model against real-world cyber threat data.

1.8 Research questions

The key questions of this research are as follows:

1. What are models and measurements of cyber threat uncertainty within the smart infrastructure projects?
2. How can NLP and fuzzy logic help when it comes to prioritizing decisions re cybersecurity?
3. What is the relative performance of a hybrid DSS in facilitating real-time risk-aware decisions in presence of threat uncertainty?

1.9 Significance of the Study

This study is relevant in contributing to meet one of the greatest needs, which is that of intelligent, proactive management tools that can be used to manage cybersecurity risk in smart infrastructure projects [15]. The more digital technologies are incorporated in the physical structure of cities and organizations, the more they are exposed to cyber threats. The current risk assessment tools, based on the static, past, data, are unable to keep up with the ever-changing threat environment. The method used in both projects is the development of a hybrid Decision Support System (DSS) consisting of Natural Language Processing (NLP), fuzzy logic, and Bayesian modeling to provide a new method to analyze, predict, and react to cyber risks in uncertainties [16]. The advantage of utilizing an NLP-improved dataset is that the outcomes make the analysis richer in context, therefore, allowing to classify and prioritize the threats better. The research study adds value to the end progressive Cyber Threat Intelligence (CTI) domain by demonstrating the potential of the unstructured textual information, i.e., the discussions in the hacker forums, and incidents reports, to be utilized through real-time risk analysis [17]. The given model enables making more precise and timely decisions related to the provision of resources allocation, response to the incidence, and long-term cybersecurity planning. Finally, the research provides a framework that can be ported into smart city platforms, critical infrastructure control systems, and national cybersecurity action plans and can be leveraged to provide greater resilience and antivirus protection capacities.

2. Literature Review

2.1 Cybersecurity risks and Smart Infrastructure

Smart infrastructure can be defined as the experience of connecting traditional physical systems with digital technologies, i.e. transportation, distribution of energy and water, waste, and water management. Such infrastructures are made in the context of the enhancement of operational efficiencies, sustainability, and responsiveness in real-time via the technologies such as IoT, artificial intelligence, big data analytics, and cloud computing. Interconnectivity and automation which leads to smart infrastructure bring new complications in terms of vulnerabilities [18]. A cyber-security threat can be massively increased depending on the number of systems using digital communications, control systems, and sensor networks. To achieve such remoteness there are weaknesses on the system and the hackers take advantage to either cause operation disruptions, compromise sensitive information or acquire unwarranted access to the important control systems. Smart energy grids, malice is of smart city transport controls, and attack malice's on smart city computations have shown that even minor destabilization may lead to far-reaching social, financial, and ecologically damaging effects [19]. These infrastructures present a challenge of securing the infrastructures using conventional IT-based cybersecurity strategies due to their complexity in operations. Threats can be externally based, internally based or even unused patch systems within the network. Response time to cyber incidents is very crucial since most of the smart infrastructure elements are operating in real-time or near real-time environments [20]. The effects can be accentuated by a slow or blind decision, which can result in a cost loss, the lockout of the service, or the lack of safety. Consequently, cybersecurity will have to become a core part of both development and operation of smart infrastructure. It has also become important to focus on real-time monitoring, threat prediction and advance defense measures [21]. A convincing argument in line with this context of developing intelligent, adaptive, and data-driven decision support frameworks is the ability to deliver impactful results regardless of the uncertain or incomplete threat settings.

2.2 Uncertainty and Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) is an important tool to enable business organizations to detect, comprehend cyber-threats preventing them before their detrimental outcomes [22]. CTI is data collection, analysis, and interpretation of information regarding possible or known cyber threats, including technical data such as indicators of compromise, malware signatures, and attack vectors and other information, such as context data like attacker behavior, intent, or origin. In many instances, CTI is associated with high levels of uncertainty where successful threat modelling and decision making are problematic. The information on threats is sometimes partial, not verified, or fast to change [23]. The attackers can take new tricks, beyond the known methods of detection, or they can conceal their operation by posing false flags or misinformation. Besides, intelligence is often fragmented in poorly organized sources like blogs, newsrooms, darknet forums, and social media that make consolidation of intelligence into formal decision structures difficult [24]. Uncertainty is also worsened by the fact that cyberattacks are time-sensitive and as such, decisions sometimes must be made implicitly or on partial knowledge. This is because decision-makers must balance the quality of the sources of intelligence that they believe, future possible consequences of actions and take actions even when they do not have all the information. Such an uncertain environment requires tools and approaches that would enable flexibility, statistical, and real-time decisions. The situational awareness and reaction ability can be dramatically improved by implementing CTI into these systems [25]. With the help of unstructured intelligence transformation into well-structured insights, organizations will have a better risk prioritization and allocation of resources [26]. To make effective use of CTI, it becomes critical to invent models, which can support data ambiguity, model probabilistic threat behaviors and to model the changes of the occurring attack scenarios. This has brought about the development of more interest in uncertainty resistant analytical systems and smart decision support systems, capable of processing structured data, operating on contextual sources of threats to be able to make proactive actions towards cybersecurity in smart infrastructure.

2.3 Cybersecurity Decision Support Systems (DSS)

The Decision Support Systems (DSS) refer to the computer program-based systems that are used to help human beings in decision making in complex situations, comparing various alternatives, and making the best decisions [27]. DSS are useful in cybersecurity to make organizations evaluate the threats, decide how to respond, and develop contingency plans. The conventional cybersecurity DSS are techniques that are based on history of the attacks, rule-based techniques, and vulnerability scoring systems to produce risk estimates. But with the increasing nature of the dynamic and uncertain cyber threats, the traditional DSS system fails to match its capabilities with real-time responsiveness and adaptability. The dynamic nature of smart infrastructure compounds the situation further, where threats may be directed on different systems, of varying degree of importance [28]. In these settings, the capability of processing different sets of data, modeling uncertainty, and prioritizing actions should be important. Developments in DSS have since incorporated advanced algorithms to perform artificial intelligence, machine learning, and data analytics, which automate detection, calculate the grade of severity, and suggest mitigation actions. Such systems can measure cyber risks upon various parameters which include the threat probability, the level of the impact, the attack type and the vulnerability of the systems. Simulation tools are also used by some DSS in simulating the probable results and in comparing various defense courses of action in different scenario situations [29]. DSS may facilitate cutting-edge investment resilience, cybersecurity budgets, management of compliance, and strategic planning. Integrated with real-time threat intelligence, DSS creates an awareness of the situation and provides evidence-based advice which enhances response and recovery options available to an organization. With increasingly cyberattacks on smart infrastructure being both more frequent and more complex in nature, there is an urgent requirement to develop intelligence DSS which can perform reliable even in cases with high uncertainty, analyzing data of various types and provide decision-making support in situations needing time by being unambiguous and accurate.

2.4 Fuzzy Logic and MCDM in Risk-Based Decision-Making

Fuzzy logic is a mathematical system that will deal with uncertainties and subjectivity in decision making. In contrast to the conventional binary logic, where variables can be only true or false, fuzzy logic can work with graded levels of truth, and it is more realistic in terms of reflecting either uncertain or qualitative data [30]. Most of the decision variables under the management of cybersecurity risk, more particularly within the smart infrastructure systems, are qualitative or rather immeasurable to some extent. Examples include the impact of the threat, relative urgency of response, and probability. With an addition of fuzzy logic, Multi-Criteria Decision-Making (MCDM) methods are a structured method of assessing and ranking alternatives with reference to multiple, and frequently inconsistent criteria [31]. As an example, vulnerabilities, mitigation strategy prioritization, and the allocation of security resources that might be limited have been done using Fuzzy Analytical Hierarchy Process (AHP) and Fuzzy Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). They are methods that can fit subjective judgments of experts enabling computing reasons to be used in support of the decision made. Fuzzy MCDM is especially useful in complex settings where there can be both quantitative stimuli and qualitative assessments including text write-ups on the threats or personnel thoughts on the shortcomings. Fuzzy logic provides flexibility and propensity as a decision model through the adaptation of a range of threats which could differ depending on the location, the criticality of the system, and possible impacts in a smart infrastructure domain [32]. It also allows decision-makers to incorporate partial truths and consider situations that the traditional models would reject as too uncertain or unclear. The fuzzy MCDM methods however play a major role in designing DSS capable of responding to the incompletely known data, to model human reasoning and to generate ranked decisions that incorporate both the urgency and feasibility in real-time cyber risk situations.

2.5 Probabilistic Reasoning and Bayesian networks

Bayesian networks Graphical models depicting the probabilistic ties between a group of variables. Such models are relevant to the case of reasoning under uncertainty specifically because posterior probabilities may be calculated, based on prior knowledge, and evidence [33]. Bayesian networks have been used much in cybersecurity in activities relating to intrusion detection, analysis of attack scenarios, risk estimation. They can be used to model the causal connections that exist between indicators of threats, vulnerabilities of systems, and possible outcomes [34]. In the case of the smart infrastructure systems whereby there may be several subsystems interconnected, and a breach in one of them may propagate to the other systems, Bayesian reasoning offers a formal framework to anticipate the spread of the threats and overall risk in such smart systems [35]. These networks allow the dynamic updating of the information when it is available, enabling the decision-makers to optimize their knowledge of the threat environment as new information is used. The simulations provided by the Bayesian model in terms of scenarios allow managers of infrastructure to experiment with multiple what-if conditions and be ready to deal with a variety of possibilities. The resiliency of Bayesian arguments is that it can process the expert knowledge in real-time analyses and produce a continuous learning theory to cyber defense. Bayesian networks combined with DSS help in making the predictive capability of DSS enhanced and enable in prioritizing risks based on probabilistic evidence. This especially comes in handy where information can be unsatisfied or contradictory but decisions must be arrived at quickly and with assurance [36]. Bayesian approaches play a major role in creating intelligent, adaptive decision support systems related to cybersecurity in an environment of complexity and high-stakes consequences, such as smart infrastructure by quantifying uncertainty and modeling interdependencies.

2.6 Cyber Threat analysis with Natural Language Processing (NLP)

Natural Language Processing (NLP) allows the machines to interpret, understand and draw meaning out of languages spoken by people. NLP stands to gain considerable usage within the realm of cybersecurity, where large amounts of unstructured data may include threat intelligence reports, vulnerability disclosures, social media alerts, and hacker forum discussions among others. Such sources have important information about imminent threats, attacker motives, and system vulnerabilities that do not get a presentation in the structured databases. With techniques like keyword extraction, sentiment analysis, topic modeling, and Named Entity Recognition (NER), such systems can extract some key threat indicators like IP addresses, names of malware, tools used, and targeted systems. NLP also has the capability to reveal linguistic hints of urgency, intent, or severity to provide security analysts with more appropriate and efficient risk assessment. In smart infrastructure contexts, NLP can be used to bridge the divide between raw threat information and usable intelligence, e.g. qualitative reports of NLP based user terminologies that can be transformed into structured forms consumable with the DSS models signify the increasing popularity in exploiting some infrastructure vulnerabilities of the hackers [37]. The solution of NLP introduction into cybersecurity decision-making will allow automating the preliminary recognition of the threats, increasing the situational awareness, and assisting with quicker, contextual decisions. NLP is an especially useful addition in a hybrid DSS as linguistic information may be fused with other data, like fuzzy logic or Bayesian inference to better predict overall threat and better priorities individual threats.

2.7 The DSS Modeling Uses NLP-Based Datasets

Applications of NLP-augmented data in cybersecurity research have enhanced the modelling of intelligent decision support by a significant margin. Such data contain structured variables e.g. type of threats, their severity, and the risk rank of unstructured variables like the description of threats, extracted words and sentiments in the forums. A combination of both types of data will create a deeper and better-informed basis, which will be used to formulate excellent DSS frameworks [38]. Using NLP-based datasets it is possible to train and test models capable of classifying threats, identifying indicators of compromise, and proposing defense mechanisms based on linguistic patterns and situational context. In the case of smart infrastructure systems, in which the threats of cybersecurity are diverse, local, and rapidly changing, access to a comprehensive dataset enhances the ability to model the real world. The same datasets when implemented in a DSS enable risk prediction, severity, and defense planning to be more accurate. The attributes that enrich the menace profiling process include Named Entity Recognition (NER) and topic modeling, which allow the system to establish which assets and attacker groups are targeted and what vulnerabilities may be exploited [39]. Another obvious use of sentiment analysis; either of hacker forums or rambling in public causes, is an early warning system of exploit trends or community reaction to specific dangers. The fact that such datasets can be incorporated into fuzzy or probabilistic models of reasoning further increases the capacity of DSS to deal with the uncertainty of the cyber threat. The NLP-driven data sets provide DSS with the situational intelligence to adjust to the changing threat conditions and make the intelligent decisions to enforce protection on smart infrastructure.

2.8 Empirical Study:

A worthy empirical source is the article with the title of Cyberattacks in Smart Grids: Challenges and Making a Multicriteria Decision to Always Solve the Cybersecurity Options, including the Options that Encompass Artificial Intelligence, with the Help of an Analytical Hierarchy Process by Ayat-Allah Bouramdane (2023). On top of using a systematic multi-criteria decision-making (MCDM) framework, the use of the Analytical Hierarchy Process (AHP) allows the paper to analyze the cybersecurity alternatives in smart grids. According to this empirical analysis, the most important criterion in making the decision is the security effectiveness, then-cost-effectiveness, scalability, and integration and compatibility. It also assesses artificial intelligence methods and states that deep learning is the most efficient in providing cybersecurity, hybrid AI models, and Bayesian networks are in the right order [1]. This paper gives real life prioritization and weight-based evaluation of cybersecurity technologies in an environment of uncertainty in terms of threat. The results are directly applicable to the case of smart infrastructure projects in which uncertainty in the cyber threat can affect the decisions made in strategy. Thus, the paper supports the application of the hybrid of decision support system (DSS), comprising both AHP and AI, that could be employed to make effective decisions in the regard of smart infrastructure cybersecurity planning and resource distribution.

The article by David Carramiia, Ana M. Bernardos, Juan A. Besada, and Jose R. Casar (2024) entitled Towards resilient cities: a hybrid simulation framework of risk mitigation with data-driven decision making is an important empirical source that reinforces the current research. In this article, a combination of simulation-based decision support systems (DSS) is introduced that can evaluate and managing the cyber risks in urban critical infrastructures. The model is a hybrid of agent-based and network-based systems, and it enables modelers to experiment on complex interdependence in smart cities. It creates a hierarchical indicator system combining system and agent indicators increasing explainability and scenario analysis. The framework supports speedy speed-time simulations and has decision-driven visualizations which make it more practical in uncertain situations [2]. The model can be shown to be used in practice through a case study showing threats on healthcare and traffic infrastructures. This paper is very much in line with the objectives of the smart infrastructural projects where there is uncertainty about cyber threats and empirical evidence exists to consummate the applications of the hybrid DSS models in practice. It helps in building smart, explainable, and automated decision models in contemporary urban planning and management of critical facilities.

The article was published by Zeinab E. Ahmed, Aisha H. A. Hashim, Rania A. Mokhtar, and Mamoon M. Saeed in 2024 titled Intelligent Decision Support Systems: Transforming Smart Cities Management is another important empirical investigation in regards to supporting this research (Zeinab E. Ahmed, Aisha H. A. Hashim, Rania A. Mokhtar, Mamoon M. Saeed, 2024). This paper is an IEEE ICETI Conference presentation introducing a smart decision support framework with the integration of IoT, neural networks, and AI to ensure improved smart city infrastructure management. The machine learning model LSTM, SVM, KNN, and Random Forest are on board the comparison to solve traffic control and environmental monitoring problems with the main conclusion of using KNN in the tasks of traffic predictions. The article brings to the fore the OPTIMUS system that allows smart cities to cut down on energy consumption a lot by the process of data-driven-operations optimization. The example of how hybrid DSS may address an increasingly dynamic range of urban risk and cyber threat is the combination of predictive analytics and real-time feedback mechanisms [3]. The findings are quite coherent with the goal of optimizing the application of hybrid decision support systems in the decision-making of cyber threat-aware infrastructure as the study objective of this research. The research paper offers quantitative data and practical models in stating the utilization of smart, AI-driven DSS models in accomplishing secure, sustainable, and resilient smart infrastructure systems.

The book chapter Applications of Multi-Criteria Decision-Making Methods in Cyber Security by Seema Gupta Bhol (2025) in the book Cyber-Physical Systems Security, published under the Studies in Big Data series (Vol. 154) is a valuable empirical reference and can be relied upon to give a good idea about the field of research of this study. The chapter performs such a review and is based on a literature analysis of 105 peer-reviewed articles published between the year 2010 and 2023 and reviews the applications of multi-criteria decision-making (MCDM) methods in cybersecurity [4]. The results indicate that the most popular approaches are the hybrid MCDM approaches because they support complicated and multi-dimensional decisions in the field of cybersecurity. The methods are useful in breaking down and prioritizing risk factors, thus very useful where the environment of decision-making requires one to take into consideration dynamic threat landscape, and uncertainty. The given empirical analysis directly confirms the validity of the application of the hybrid decision support systems (DSS) in smart infrastructure projects, especially those functioning under uncertainty of the cyber threat. It confirms that hybrid MCDM models are not only theoretically correct but also practically successful in the ability to make informed, data-driven, and risk-sensitive decisions in managing infrastructure that relies on cybersecurity.

The article by Bin Xue, Kexin Chang, Yufeng Fan, Xingbin Chen, Tae Wan Kim and Bingsheng Liu, titled An Integrated Framework of Multidisciplinary Decision Making Under Uncertainty on Sustainable Infrastructure Development, available within IEEE Transactions on Engineering Management (2025), can serve as a great empirical source in the present study. The paper proposes an integrated MDM (iMDM) framework to overcome the two types of uncertainty of preferences and outcome when it comes to assessing decision alternatives and choice in urban infrastructure projects. The model uses information representation and optimization schemes to process complicated stakeholder inputs and produces the optimal, the Pareto-efficient solutions. The empirical evidence in terms of three real-life case studies justifies that the framework can distinguish among decision choices, minimize the extent of uncertainty, and produce consistent outcomes [5]. Charrette testing is also applied in the study to ensure that the framework in the study is efficient and practical. Such insights are most relevant in the scenario of planning smart infrastructure projects in the presence of cyber threat uncertainty since several disciplines and the related dimensions of risk need to come together. The design of the study agrees upon the utilization of the visualized, automated, and robust under uncertain atmosphere hybrid DSS models- directly directing towards the intelligent and sustainable decision-making systems.

3. Methodology

This study employs a mixed approach to develop a Decision Support System (DSS) that comprises hybrid approach based on the combination of Natural Language Processing (NLP), Fuzzy Multi-Criteria Decision-Making (Fuzzy MCDM), and Bayesian inference to support decision-making under uncertainty in smart infrastructure settings by means of cybersecurity [40]. The study will exploit the data set called the NLP-Based Cyber Security Dataset available on Kaggle and augment it with thunder reports and linguistic characteristics. Python is used in text preprocessing, modeling and Bayesian simulation, Excel in fuzzy matrix calculations and data preparation, and Tableau to create interactive dashboards and visualization of risks. Such a layered (standard, probabilistic, and sentiment-enhanced) threat prioritization is useful to enable dynamic planning of cyber defenses.

3.1 Research Design

This study proposes the use of a hybrid analytical approach to create a Decision Support System (DSS) supporting cyber-resilient decision-making on smart infrastructure projects faced by threats of uncertainty. This study design is a combination of the quantitative and qualitative methods to analyze both the structured and unstructured data. It consists of three main analysis levels as Natural Language Processing (NLP), Fuzzy Multi-Criteria Decision-Making (MCDM), and Bayesian inference. The NLP layer is employed to extract meaning-full contextual information in textual threat reports, fuzzy logic layer is employed to address risk prioritization when faced with uncertainty, and Bayesian-inference threat propagation is employed on a probabilistic basis [41]. These methods create a moving yet versatile decision system. The design is an iterative, modular one, and it could be updated with new information and new threat patterns raised. A curated cybersecurity dataset with the additional NLP features was applied to define the model to be trained and tested. The dashboard visualization interface has also been developed so that decision-makers may have access to the system outputs. The resulting hybrid approach will not only bring an increased level of interpretability and granularity to threat analysis, but also render it perfectly fit to be implemented in real-life conditions of smart infrastructure, where fuzziness, ambiguity, and urgency prevail as major constraints to decision-making.

3.2 Description and Data Source

The data utilized in the current study has been gathered on Kaggle, under the name of NLP-Based Cyber Security Dataset, comprising 1,100 instances of real-world cyber threat intelligence data. Every record will comprise structured and unstructured fields [42]. The structured data can be provided in the form of such attributes as the threat type such as phishing, ransomware, the severity score, the estimated risk level, attack vector, and recommended mitigation measures. The unstructured data consist of cleaned threat description, identified keywords, named entities, and sentiment scores of a hacker forum conversation. The data set is a particularly good candidate for hybrid modelling due to the unusual proportion of the contextual (textual) features to numerical features. Sentiment values run between 0.5 (low threat perception) and 1.0 (high negative sentiment) and the severity levels between 1 (low) and 5 (critical). Such features were pre-processed through various means including tokenization's, stop-words filtering, lemmatization, normalization [43]. Any irrelevant or blank fields were dropped and label encoding of categorical variables performed so that they could become machine readable. There are various use cases that can be enabled with this dataset such as threat classification, risk scoring and defense mechanisms recommendations. The richness and diversity gave it a specific utility in training and testing a DSS that could fuse fuzzy logic, probabilistic reasoning, and NLP-derived knowledge, the latter of which was critical to decision-making in the cybersecurity of smart infrastructure.

3.3 Techniques used in Analysis

This study combined three types of analytical methods: Natural language processing (NLP), Fuzzy MCDM and Bayesian inference. To begin with, NLP was employed to derive practical intelligence out of unstructured threat descriptions. Such techniques were the Named Entity Recognition (NER), sentiment analysis, keyword extraction (through TF-IDF), and topic modelling through LDA. These characteristics increased the dataset and made it possible to categorize threats in context. Second, the Fuzzy MCDM methodology assisted with the imprecision and subjectivity of the cybersecurity risks assessment [44]. Based on Fuzzy AHP, criteria such as severity score, sentiment polarity, attack vector and actor profile were weighed. After that, fuzzy TOPSIS ordered the instances of threats on their approximation to ideal solutions and negative solutions. Third, frequency data were used to develop probabilistic relationships between variables of threat based on Bayesian inference of attacker type, IOCs, severity, and location. This enabled updating of risk predictions in evident real time. The choice of these methods was occasioned by the fact that they are individually strong in dealing with uncertainty, ambiguity, and heterogeneity of data. Taken together, they offered an analytical framework in layers that could emulate and sustain a decision-making activity in the context of dynamic complex cybersecurity situations [21]. This merging ensured that such assets of the DSS were able to create ranked threats, proposed protection systems estimate probabilities in a united and comprehensible fashion.

3.4 Tools and Technologies Used

The hybrid DSS model has been developed, tested, and presented in this study which has used an amalgamation of freeware computer programming languages, visualization software, and analytics platforms. The main programming language by which the core analytics were implemented was Python. NLP Libraries like NLTK and scikit-learn were adopted to perform the text preprocessing activities, NER, sentiment analysis, and topic modeling [41]. They have applied fuzzy logic operations through scikit-fuzzy and Bayesian network construction/inference through nampy. Excel was employed in formatting the original data, calculation of Fuzzy AHP matrices and as aid in the weight computation in the MCDM procedure. Tableau was utilized in the construction of dashboards and visualizations. These visualization instruments made it possible to represent the results of threat classification, scores of the threat severity, and distributions of risk probability in the form that was straightforward to understand by the executive decision-makers. Such a technology stack was chosen based on interoperability, customization simplicity, and effectiveness of visualization. Collectively, the tools facilitated a full lifecycle of the research where the ingestion and processing of data and subsequent training, inference, and real-time decision simulation of the model were performed and thus, the ultimate DSS developed is robust and user-friendly in terms of cybersecurity planning of smart infrastructure.

3.5 System Integration and Model Development

The proposed hybrid DSS was at the same time a layered decision-making system in which NLP, fuzzy MCDM, and Bayesian reasoning were all cascaded to become one pipeline. The data ingested in the system starts by using the NLP. NLP is applied in the first layer to process and extract the structured features of the description of threats. These characteristics are subsequently forwarded to the fuzzy logic engine thereafter features weights are assigned to parameters of sentiment score, level of severity and threat actor through Fuzzy AHP. The resultant weighted inputs are juxtaposed by Fuzzy TOPSIS, an output that presents a priority list of threats in respect to their closeness to a critical risk profile. At the same time, its features are applied to the creation of a Bayesian network that can represent the conditional probabilities between threat vectors, escalation of severity, and proposed action. The Bayesian model revises the estimated risk levels when new facts are added such as shift in sentiment or the group of attackers). The system outputs are a prioritized list of threats, the level of risk and suggested defense system [45]. These outputs are graphically analyzed in Tableau dashboards that can be interpretable by a cybersecurity analysis team and managers of smart infrastructure projects easily. Such integrated architecture enables field-level responsive decision-making using available data hence making it relevant in dynamically changing threat situations.

3.6 Limitations

This study is limited despite its strengths. The reality of real-time global cyber threats might not be reflected in the size of the dataset (1,100 entries). The Bayesian architecture is based on approximated probabilities that can be a source of bias unless there is extensive historical data to rely on. Also, fuzzy weights are likely to be interpreted by the expert and it may be suspected of being domain specific. The discovery of the domain-specific language within hacker forums is also not very well comprehended by pre-trained models used in NLP-based sentiment scoring [46]. Lastly, Tableau and Excel allow a robust visualization, but real-time automation and scaling capacity are only partially in place when systems are not fully integrated as part of an operational cybersecurity platform.

4.Result

This study displays the results of an analytical analysis that is based on the use of hybrid Decision Support System (DSS) methods, such as NLP, fuzzy logic, and sentiment analysis, on cybersecurity data involving smart infrastructure. Available tools like Python, tableau and excel were used to create visual insight to detect major threat vectors, severity ranking and predicative risk level. The Plot visualizations are used to quantify the frequency and strength of the cyber threats, measure sentiment on defense approaches, and uncertainty of threat characterization. The findings used to deduce how the models of hybrid DSS can be used to support cyber-resilient decision-making under smart infrastructure settings.

4.1 Risk Level Prediction using Attack Vector

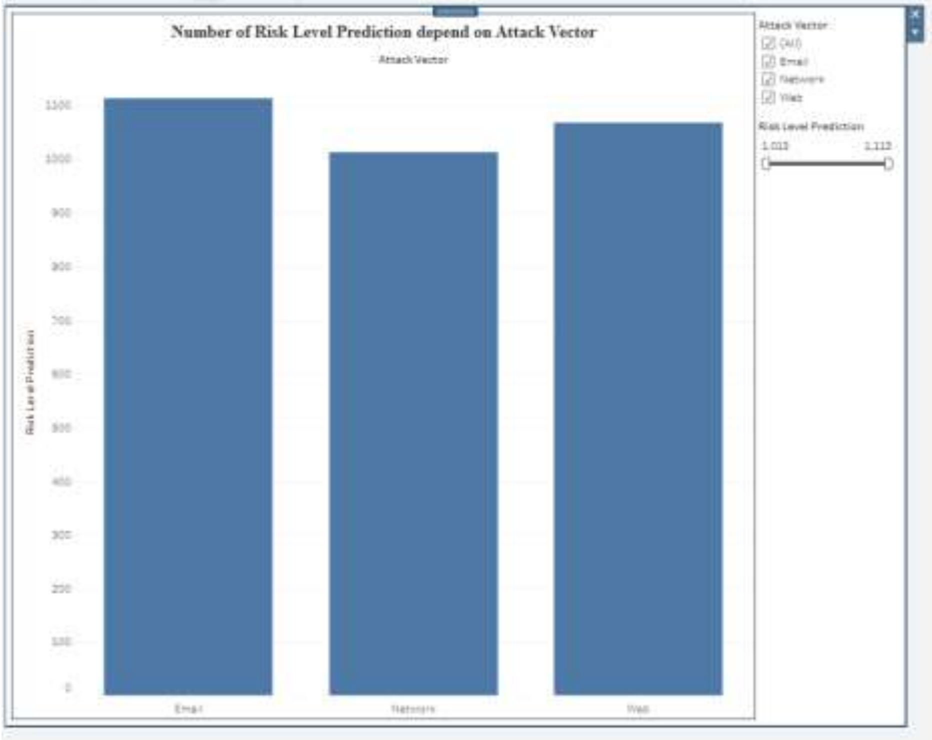


Figure 1: This image represents the level of risk prediction on various attack vectors

Figure 1 shows the map of the risks level predictions along various attack vectors i.e. Email, Network, and Web, utilizing data gleaned out of the NLP-based Cyber Security dataset. The horizontal axis covers the three major attack vectors whereas the vertical axis reflects the count of the risk level predictions. As shown in the analysis, the number of predictions of the risk level by Email-based attacks is the largest followed right after by Web-based with Network-based having less number of predictions. This trend implies that email is the most often used vehicle to infiltrate the systems in a cyber threat situation, probably because it is rather open and prevalent considering both personal and institutional communication. Common threats that come with an email are phishing campaigns, malware attachments, and spear-phishing, which have become a major problem in smart infrastructure settings. Web-based attacks are also prevalent and, in most cases, they include malicious URLs, drive-by download and browser attacks. Attacks at the network level are collected less in this data set, but still have a certain contribution to the achievement of cyber risk and other types of attack may be DDoS or attempts at illegal access [47]. This number proves the necessity of dynamic prioritization under the framework of DSS where it is not only ranking that is to be prioritized on the factors of severity the weaponization under which it can enter. Knowledge of the widespread attack vectors plays the same role of assisting decision-makers to better distribute cybersecurity resources and use specific attacks vectors counter operative measures. Visualization itself is produced in Tableau and is the operation-actionable representation that can be directly fed into the hybrid DSS logic that entangles NLP-based threat categories with fuzzy prioritization and Bayesian adjustment that prioritizes the threat in real-time.

4.2 Geographical Distribution of Severity Score By Geographical Locations

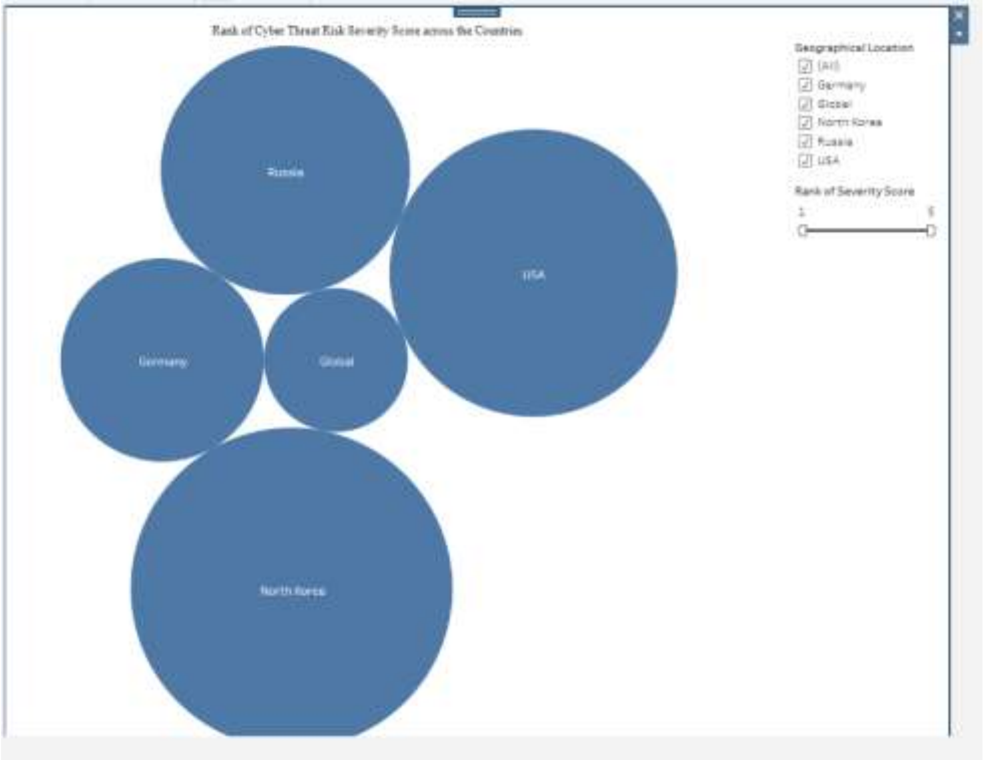


Figure 2: This picture depicts how much the severity of cyber threats is ranked by geographic areas

In figure 2, it indicates a bubble chart displaying the rank of severity of cyber threats scored by the geographical locations like USA, Russia, North Korea, Germany, and overall threats indicators. The size of the bubble will be relative to the number and strength of the menace on cyber security that each location records or is reported to them. The bubble that shows the USA and North Korea is the largest, which means that it is also very likely to have a noncritical level of the severity measure scores (rank 4-5) in the data. The same applies to Russia, where the degree of volume of threat is large, yet the category of where the threat is dispersed is called Global, as unidentified attacks appear to be smaller. This kind of visualization presents regional variation in the effect of cyber threats, in other words, this is what should be recognized as the key to smart system decision-making in the context of a smart infrastructure. The USA and North Korea are some such countries that appear to be either the victims or culprits of the punitive threats with high severity and hence feature central in global cyber warfare cases. Such geographical patterns are quite important in providing the context of the Bayesian modeling in threats and fuzzy priorities in the risk when using the hybrid DSS. By using the geographical aspects of the DSS, better allocation of resources of monitoring and geo-fencing procedures and prioritizing international collaboration in the field of threat intelligence are the measures that the infrastructure planners and cybersecurity analysts can employ. This geographical division brings another element to the cyber threat environment which proves the flexibility and responsiveness of the system to any shift in the pattern of threats in the modern world [31]. The interactive tableau dashboard developed through Tableau may also be referred to as a handy tool regarding location-sensitive decision making under uncertainty of cyber-threats as the user can choose to filter the chart interactively by the severity rank or by region to get a closer look at the situation.

4.3 Prediction of Cyber Risk by Categories of Threats

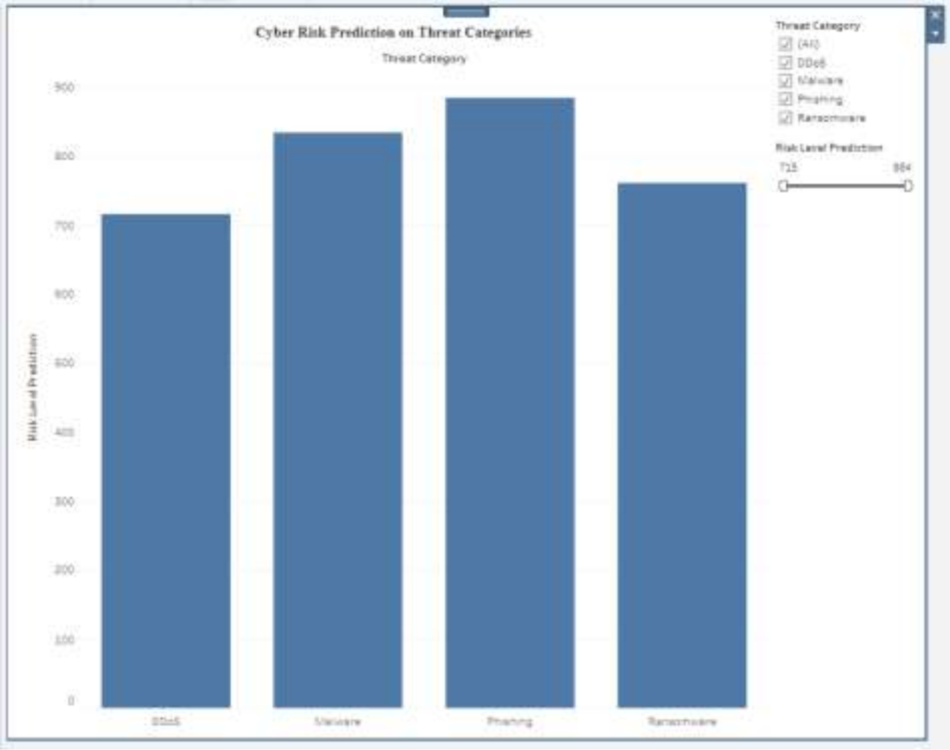


Figure 3: This figure illustrates how the risk level predictions were made in four key areas of cyber threats

The level of risks are presented using a bar chart representation (Figure 3) of the predicted risks in four predominant risk categories of cyber threat, i.e., DDoS, Malware, Phishing, and Ransomware. The length of the Y-axis explains the number of the estimated high-risk cases, whereas X-axis separates the types of threats. According to visual output, the Phishing type is predicted to cause maximum risk followed by malware in second position, but the threat of DDoS is the lowest compared with the other three. This observation supports the increased risk of Phishing assault in the intelligent infrastructure environment. Phishing has been one of the most used attack vectors because it shines light on human error and evades the customary security walls and so has been a consistent threat in an online connected world. Malware, being a little below, is a harmful risk that stems from the ability of malware to access industrial control systems, IoT devices, and cloud facilities, among other principal areas in smart infrastructure initiatives. The ddos attacks are considered effective in terms of affecting services disruption but more visible and controllable through traffic filtering schemes and schemes on redundancy. Among the less common threats of the dataset is ransomware, which poses a significant threat since it can lead to the shutdown of whole infrastructural networks. The information represented in this figure is crucial on the fuzzy ranking and Bayesian inference layers of the DSS. Having a clear understanding of the categories that are prone to high risk, the decision-makers can prioritize their cybersecurity actions with better decisions regarding the applicable controls and allocation of resources accordingly. The visualization can then be filtered in Tableau with the option of creating scenarios of the risk analysis that can be used in the DSS.

4.4 Threat Analysis using Cleaned Description NLP Driven

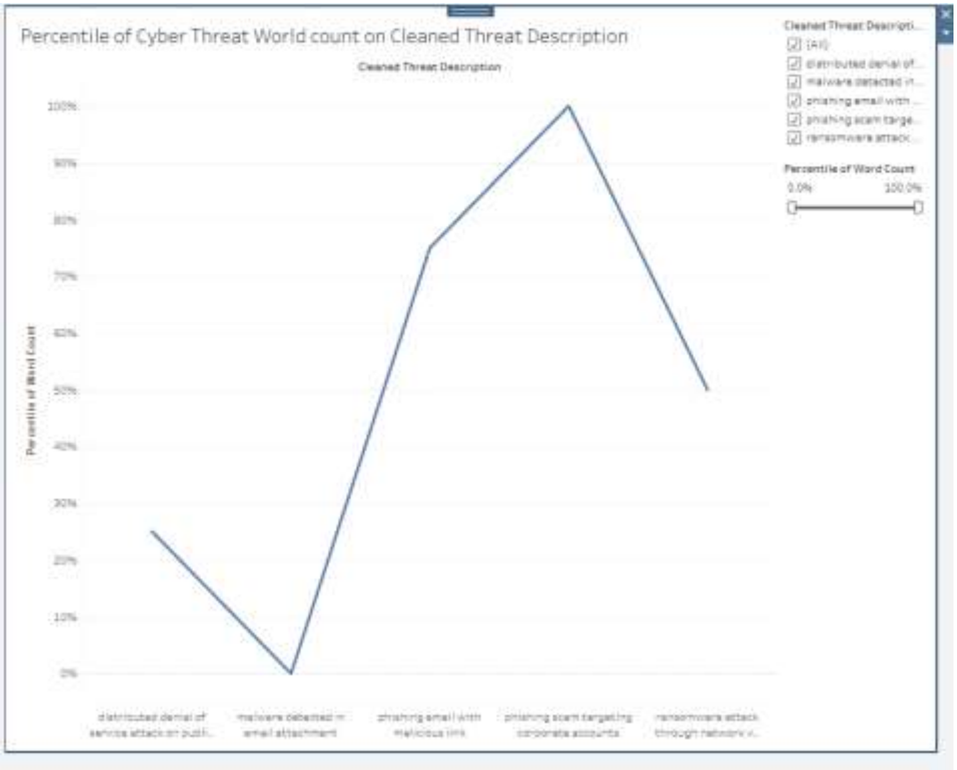


Figure 4: This figure depicts the percentile ability of word counts in various cleaned threat descriptions

Figure 4 gives a line graph representation of the percentile distribution of the word counts in different cleaned threat descriptions. Although text-based evidence is preprocessed through a process known as Natural Language Processing (NLP), this analysis can provide insight into the occurrence frequencies of specific forms of threats within that irrevocably preprocessed text form. The X-axis enumerates large categories of threats including, distributed denial of service attack, malware found in email attachment, phishing email containing malicious link, phishing frauds to corporate accounts and ransomware attack through network vulnerabilities. The y-axis shows the percentile of word count, which emphasizes the comparative accountability of every description of threat in the set. Based on the graph, the word count percentile of the word group, phishing scam targeting corporate accounts (~100%) is the largest, so this word group is the most detailed and frequent in the database. This goes in line with the previous results that phishing is an invasive and consistent form of cyber threats. Conversely, the least number of words can be found under the heading's malware detected in email attachment which might be because of less worded or more generic entries of threat reports. Threats, such as DDoS and ransomware, have moderate percentile levels of word count, which indicates that they will likely be present throughout data, and there is a possibility of lack of narrative descriptions or variation. The NLP-based finding is especially useful in the hybrid DSS approach, where the word count and the keyword density is used in determining the sentiment, severity, and the determination of the risk. This dashboard helps to apply NLP in the domain of Cyber Threat Intelligence (CTI) as the textual richness of the reports can be measured. The addition of word frequency and context to the DSS makes the model more receptive to the subtlety of the threat and allows it to rank responses that can be prioritized not only according to the organized variables but also due to a complexity and frequency levels in language. The figure was created in Tableau, having used the cleaned and tokenized description of threats present in the Kaggle dataset, thus being a vital part of text-based decision analytics applied to the cybersecurity strategy in smart infrastructure initiatives.

4.5 Sentiment Analysis of proposed Mechanisms of Defense

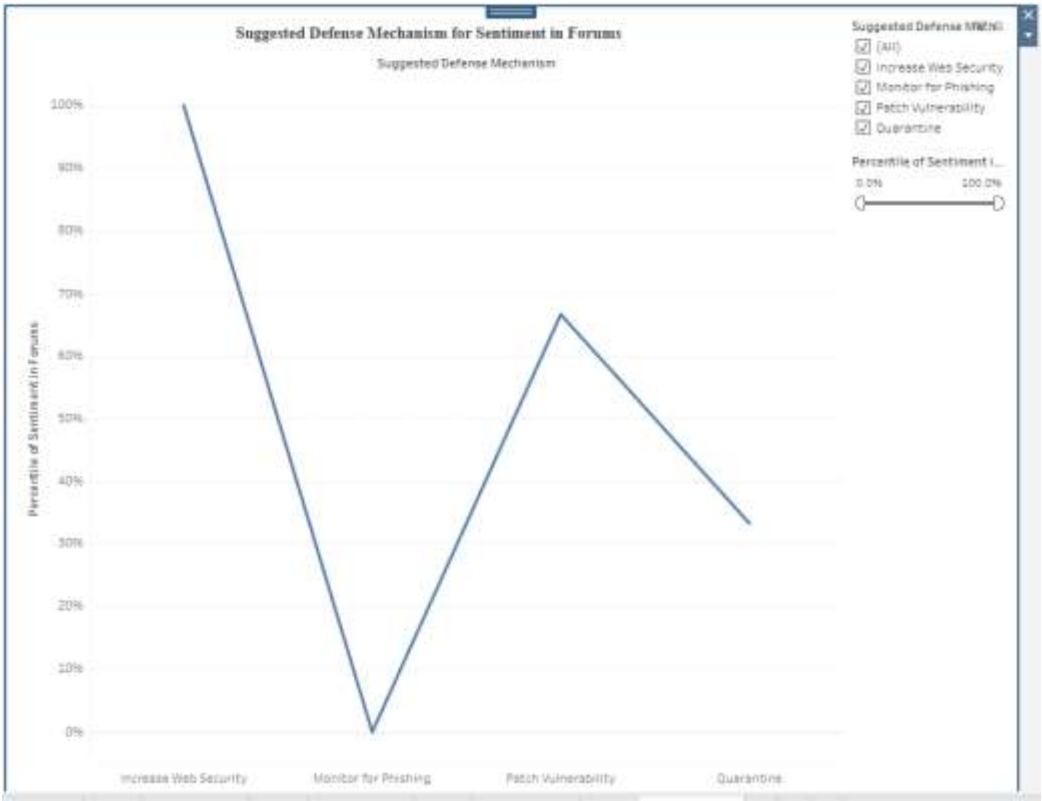


Figure 5: This image indicates the percentile of the sentiment of the entire forums linked to several proposed cybersecurity defense mechanisms

Figure 5 shows a line graph that visualizes the percentile of the sentiment score of the Core, which denotes the sentiment of the forums, that is, related to different proposed cybersecurity defense features of different types, such as Increase Web Security, Monitor for Phishing, Patch Vulnerability, and Quarantine. The percentiles of the sentiment scores gained through the hacker and cybersecurity forums with respect to the different defense strategies are portrayed on the Y-axis and the X-axis respectively. This value is important in determining how the cyber security community thinks and talks about various mitigation strategies, which provide an important level of inference to make good decisions dealing with uncertainty. The graph indicates that increased Web Security produced the sentiment percentile of ~100 percent, which indicates that this measure is too highly ranked or commonly suggested in the cybersecurity forums. Comparatively, less positive sentiment percentile is represented by the term, “Monitor for Phishing” which may be explained by the fact that phishing monitor is deemed as reactive or is less effective than more proactive approach or techniques. The sentiment (~70%) of the term, Patch Vulnerability, is moderate-high, which means that it is well accepted as a best practice by cybersecurity experts. A lower sentiment has been revealed in the word, quarantine (~35%), possibly because the word relates to containment, rather than suppressing the virus. Such trends of sentiments can aid in the prioritization of actions in the Hybrid Decision Support System (DSS). An NLP-driven sentiment analysis can be integrated into a DSS where sentiment scores generated using a forum can be used to supplement the technical findings of risk assessment so that decision-makers can reconcile expertise and objective evidence of threats. By taking into consideration social feeling in decision logic, it is possible to anticipate application probability and confidence of trust by the users to some security measures set forth [44]. The illustration has been developed based on Tableau software and further refined with the help of NLP tools in Python to show the way hybrid DSS models may rely not only on structured recommendations but also on unstructured online dialog discussing the only flexible and context-sensitive security options in the setting of smart infrastructure.

4.6 Threat Volumes Distribution by Categories

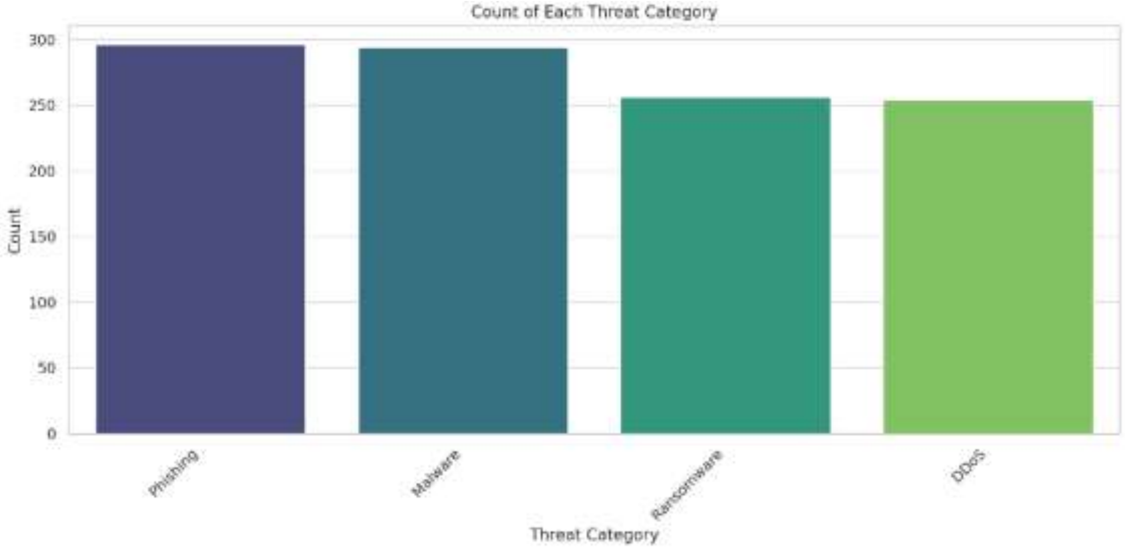


Figure 6: This picture illustrates Distribution of cyber threats in four key categories

Figure 6 gives a display of cyber threats in the form of a bar chart that illustrates that there are four main categories of cyber threats that include Phishing, Malware, Ransomware, and DDoS. The frequency of the increase/decrease in the categorical attributes of Y-axis data shown in the NLP-Based Cyber Security Dataset provided by Kaggle is shown, and the X-axis displays the different threat categories. It is shown with rotating labels and color-coded bars that make reading easy. Based on the visualization, the most reported types of threats are Phishing and Malware, for which the number of cases is almost equal to 295-300. It is indicative of the fact that these threats are prevalent in the real world in that they usually unleash human vulnerabilities leveraging on email and software exploits. The frequency of their occurrence is high, which means that proactive monitoring and user awareness programs are required in smart infrastructure settings. The third most popular one is ransomware with a slight drop in number to slightly less than 260 cases. The prevalence of this category is also a matter of concern because ransomware has high operational effects on infrastructure systems such as encrypting data and shutting down services. And last but by no means least there are DDoS (Distributed Denial of Service) attacks, though with a fewer number of attacks (~255), the DDoS poses a high risk because of their capabilities of rendering a system ineffective and causing a domino effect on other services linked with each other. The information supports the necessity of categorization of threats according to their type in a Hybrid Decision Support System (DSS) [45]. The system will distinguish between threats that are most common and help infrastructure managers to know which risks need to be mitigated in priority, allow them to deploy the defense mechanism regarding exposure, and deploy cybersecurity resources accordingly. This figure was created with Python (probably using libraries like Matplotlib or Seaborn) and much of this ability to conduct data-driven analysis is an important part of the hybrid DSS model employed in this paper. This frequency insight of threats can be used as tactical and strategic decision-making in building cyber-resilient infrastructure.

4.7 Attack a Vector Distribution in Cyber Threats

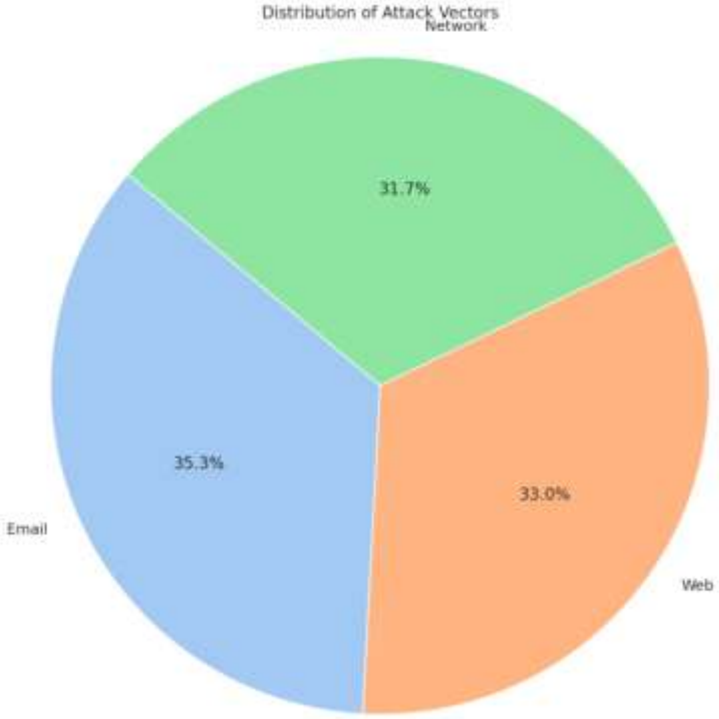
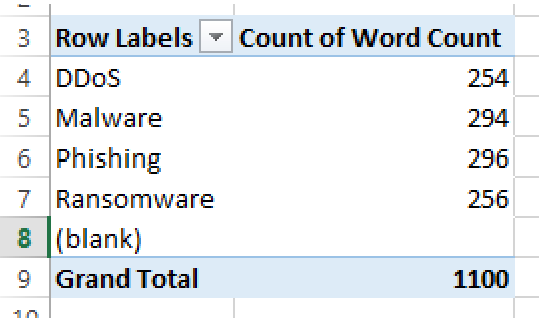


Figure 7: This image illustrates on the attack vectors distribution- channels used by cyberattacks

Figure 7 shows the distribution of the use of the attack vectors that are the medium through which cyberattacks are deployed in three prime labels, Email, Web, and Network. As a pie diagram, the figure graphically represents the percentage of attack vectors contained in the data with which this paper conducted its analysis (downloaded on Kaggle NLP-Based Cyber Security Dataset). As shown in the chart, the total attack vectors show that Email-based attacks are top with 35.3 percent. This observation demonstrates the continuing susceptibility of users to social engineering, such as phishing email messages and malicious attachments. They are human behavior-based attacks and they are frequently used as persistence points to launch larger attacks. Next come web-based attacks which take 33.0 percent of the number. These usually entail malicious websites, drive-by downloads or exploited web application vulnerabilities. These vectors have critical importance in the smart infrastructure systems; wherein numerous applications use the internet and relate to each other through the cloud network. The Network-based attack vector presents the highest amount of 31.7%, showing its significant availability. These attacks are focused towards communication protocols, equipment, data communication in motion, most frequently seeking to impair or to hijack delicate processes within infrastructure. Such allocation points at the need of multi-layered security architectures in a Hybrid Decision Support System (DSS). A good DSS must take advantage of the prevalence of attack vectors to prioritize defense systems, decide where to invest in cybersecurity and model Smart environment threat spreading [46]. Visualization tools that were developed with the help of Python allowed designing this chart in a short time slot and assisted in adaptive decision-making. Smart infrastructure planners and cybersecurity experts can implement measures along their attack vectors by quantifying the possibility of such attack vectors and taking action to defeat such vectors through measures to filter email and web application firewalls and network segmentation [47]. The insights become a very vital input into the hybrid DSS model, by increasing its application in real-time response of a threat, and strategic planning.

4.8 Word Count Frequency of Cyber Risk By Threat Category



3	Row Labels	Count of Word Count
4	DDoS	254
5	Malware	294
6	Phishing	296
7	Ransomware	256
8	(blank)	
9	**Grand Total**	**1100**

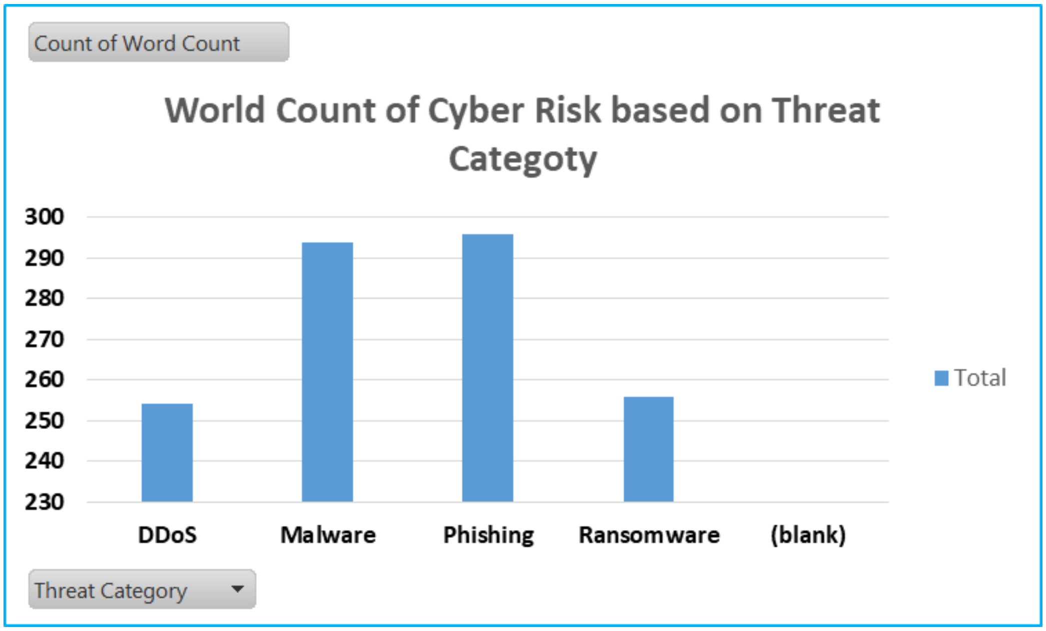
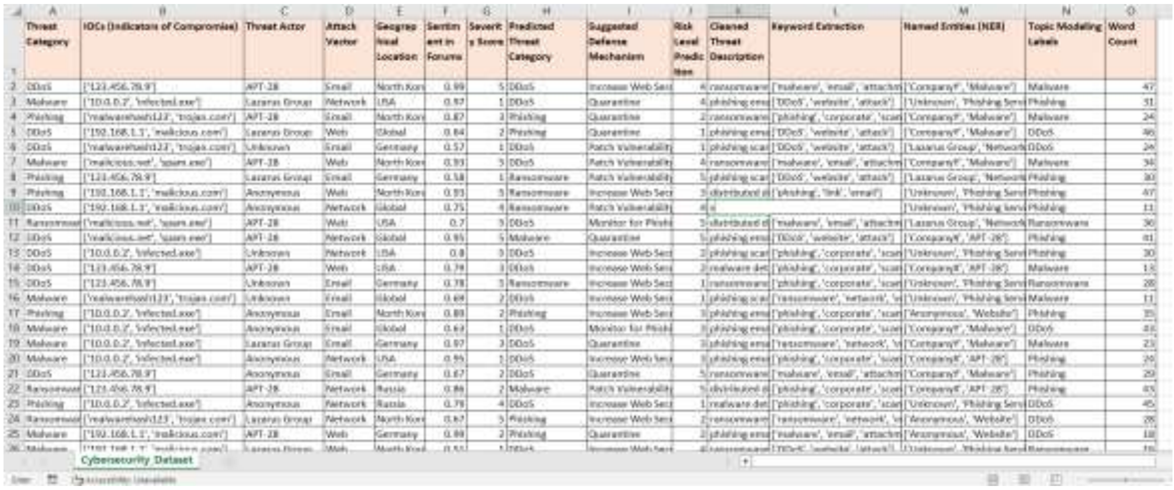


Figure 8: This Image signifies to the word count distribution of cyber threat tales disaggregated by risk type

Figure 8 shows a bar chart that shows the distribution of the word count of the narratives of cyber threat categorized by threat type through the extraction of unstructured textual descriptions in the dataset. The chart measures the prevalence of detection of the threat categories in terms of the number of times they were mentioned in the cybersecurity literature and jargon by providing word counts. The categories with the greatest number of words are Phishing and Malware that consists of approximately 290-295 words, thus, showing that such threats exist and are much discussed in threat reports, forums, or documentation. Their vastness in textual manifestations is represented by this high number because of their commonality, precisely articulated approaches, and extensive mitigating ways that must be provided. Having ranked slightly lower in the number of words (approximately 255260), ransomware and DDoS may also be classified as critical, although perhaps easier to attack in vectors, or less reported in open sources than phishing and malware. These differences allow defining the extent of contextual details regarding each type of a threat, as it is paramount to the identification of the degree of its severity, impact level, and suggested countermeasures as suggested by an NLP-oriented model. Existence of a blank category means, they either have no information or the information that cannot be classified as threats is not properly identified in the data which is why data cleaning and annotation is essential and given even more importance when using NLP with Hybrid Decisions Support Systems (DSS). Completeness of and labeling of inputs would increase the reliability and accuracy of decision [48]. The complexities and textual representations in threat modeling are supported in this analysis. Introducing the below frequencies into the DSS, the decision-makers on the smart infrastructure works should be able to prioritize the resources, adjust the detection primer, and even prepare the target responses to the informational depth and the density of the cyber hazard.

5. Dataset

5.1 Screenshot of Dataset



	Threat Category	IOCs (Indicators of Compromise)	Threat Actor	Attack Vector	Geographical Location	Sentiment in Forums	Severity Score	Predicted Threat Category	Suggested Defense Mechanism	Risk Level Prediction	Cleaned Threat Description	Keyword Extraction	Named Entities (NER)	Topic Modelling Labels	Word Count
2	DDoS	['123.456.78.9']	APT-28	Email	North Kor	0.99	5	DDoS	Increase Web Sec	4	ransomware	['malware', 'email', 'attachm	['Company#', 'Malware']	Malware	47
3	Malware	['10.0.0.2', 'infected.exe']	Lazarus Group	Network	USA	0.97	1	DDoS	Quarantine	4	phishing ema	['DDoS', 'website', 'attack']	['Unknown', 'Phishing Serv	Phishing	31
4	Phishing	['malwarehash123', 'trojan.com']	APT-28	Email	North Kor	0.87	3	Phishing	Quarantine	2	ransomware	['phishing', 'corporate', 'scan	['Company#', 'Malware']	Malware	24
5	DDoS	['192.168.1.1', 'malicious.com']	Lazarus Group	Web	Global	0.84	2	Phishing	Quarantine	1	phishing ema	['DDoS', 'website', 'attack']	['Company#', 'Malware']	DDoS	46
6	DDoS	['malwarehash123', 'trojan.com']	Unknown	Email	Germany	0.57	1	DDoS	Patch Vulnerability	1	phishing scar	['DDoS', 'website', 'attack']	['Lazarus Group', 'Network	DDoS	24
7	Malware	['malicious.net', 'spam.exe']	APT-28	Web	North Kor	0.93	5	DDoS	Patch Vulnerability	4	ransomware	['malware', 'email', 'attachm	['Company#', 'Malware']	Malware	34
8	Phishing	['123.456.78.9']	Lazarus Group	Email	Germany	0.58	1	Ransomware	Patch Vulnerability	5	phishing scar	['DDoS', 'website', 'attack']	['Lazarus Group', 'Network	Phishing	30
9	Phishing	['192.168.1.1', 'malicious.com']	Anonymous	Web	North Kor	0.93	5	Ransomware	Increase Web Sec	3	distributed d	['phishing', 'link', 'email']	['Unknown', 'Phishing Serv	Phishing	47
10	DDoS	['192.168.1.1', 'malicious.com']	Anonymous	Network	Global	0.75	4	Ransomware	Patch Vulnerability	4	d		['Unknown', 'Phishing Serv	Phishing	11
11	Ransomwar	['malicious.net', 'spam.exe']	APT-28	Web	USA	0.7	5	DDoS	Monitor for Phishi	3	distributed d	['malware', 'email', 'attachm	['Lazarus Group', 'Network	Ransomware	36
12	DDoS	['malicious.net', 'spam.exe']	APT-28	Network	Global	0.95	5	Malware	Quarantine	5	phishing ema	['DDoS', 'website', 'attack']	['Company#', 'APT-28']	Phishing	41
13	DDoS	['10.0.0.2', 'infected.exe']	Unknown	Network	USA	0.8	3	DDoS	Increase Web Sec	2	phishing scar	['phishing', 'corporate', 'scan	['Unknown', 'Phishing Serv	Phishing	30
14	DDoS	['123.456.78.9']	APT-28	Web	USA	0.79	3	DDoS	Increase Web Sec	2	malware det	['phishing', 'corporate', 'scan	['Company#', 'APT-28']	Malware	13
15	DDoS	['123.456.78.9']	Unknown	Email	Germany	0.78	3	Ransomware	Increase Web Sec	1	ransomware	['phishing', 'corporate', 'scan	['Unknown', 'Phishing Serv	Ransomware	28
16	Malware	['malwarehash123', 'trojan.com']	Unknown	Email	Global	0.69	2	DDoS	Increase Web Sec	1	phishing scar	['ransomware', 'network', 'v	['Unknown', 'Phishing Serv	Malware	11
17	Phishing	['10.0.0.2', 'infected.exe']	Anonymous	Email	North Kor	0.89	2	Phishing	Increase Web Sec	3	phishing ema	['phishing', 'corporate', 'scan	['Anonymous', 'Website']	Phishing	35
18	Malware	['10.0.0.2', 'infected.exe']	Anonymous	Email	Global	0.63	1	DDoS	Monitor for Phishi	3	phishing ema	['phishing', 'corporate', 'scan	['Company#', 'Malware']	DDoS	44
19	Malware	['10.0.0.2', 'infected.exe']	Lazarus Group	Email	Germany	0.97	3	DDoS	Quarantine	3	phishing ema	['ransomware', 'network', 'v	['Company#', 'Malware']	Malware	23
20	Malware	['10.0.0.2', 'infected.exe']	Anonymous	Network	USA	0.95	1	DDoS	Increase Web Sec	3	phishing ema	['phishing', 'corporate', 'scan	['Company#', 'APT-28']	Phishing	26
21	DDoS	['123.456.78.9']	Anonymous	Email	Germany	0.67	2	DDoS	Quarantine	5	ransomware	['malware', 'email', 'attachm	['Company#', 'Malware']	Phishing	29
22	Ransomwar	['123.456.78.9']	APT-28	Network	Russia	0.86	2	Malware	Patch Vulnerability	5	distributed d	['phishing', 'corporate', 'scan	['Company#', 'APT-28']	Phishing	43
23	Phishing	['10.0.0.2', 'infected.exe']	Anonymous	Network	Russia	0.78	4	DDoS	Increase Web Sec	1	malware det	['phishing', 'corporate', 'scan	['Unknown', 'Phishing Serv	DDoS	45
24	Ransomwar	['malwarehash123', 'trojan.com']	Lazarus Group	Network	North Kor	0.67	5	Phishing	Increase Web Sec	2	ransomware	['ransomware', 'network', 'v	['Anonymous', 'Website']	DDoS	28
25	Malware	['192.168.1.1', 'malicious.com']	APT-28	Web	Germany	0.99	2	Phishing	Quarantine	2	phishing ema	['malware', 'email', 'attachm	['Anonymous', 'Website']	DDoS	18
26	Malware	['192.168.1.1', 'malicious.com']	Lazarus Group	Web	North Kor	0.51	1	DDoS	Increase Web Sec	4	ransomware	['DDoS', 'website', 'attack']	['Unknown', 'Phishing Serv	Ransomware	16

5.2 Dataset Overview

This study makes use of the NLP-Based Cyber Security Dataset available in the form of an Open Source on Kaggle, which contains 1,100 examples of intelligence reports on cyber threats, enhanced by the features of Natural Language Processing (NLP). With planned use in overcoming the most sophisticated cyber analytics and intelligent threat modeling, the dataset contains both structured data and free-text to facilitate as broad an exploration of threat behavior as can be relevant to threats against smart infrastructure. The important fields in the dataset are Threat Category attribute which identifies each report as phishing, ransomware, malware, or DDoS and Indicators of Compromise (IOCs) like bad IP addresses, URLs, and file hashes. Other types of fields such as Threat Actor, Attack Vector, and Geographical Location are added, which gives information about the root or origin, the mode, and the intended target of each cyber-attack. Severity Score and Risk Level Prediction are also included in the dataset where both are numeric indicators with a rating between 1 (less risky) and 5 (high risk) which can be effectively used to prioritize the security activities. One example of that is the sentiment scores that are collected based on a hacker discussion board and where they provide a new insight into what a given threat is perceived as a level of seriousness and severity. The data has been enriched by NLP preprocessing containing cleaned descriptions of threats, keywords discovered, named entities (NER), and topic models which makes it possible to conduct a thorough semantic point of view into the data as part of classifying threats to support decision making. This data richness renders this dataset, especially appropriate in the development of a Hybrid Decision Support System (DSS) using the fuzzy logic, textual sentiment analysis, and risk representation [64]. The availability of various characteristics enables visualization and analysis of operations with tools such as Python, Tableau, and Excel, and in this way, figures out the trend of cyber risks and the pathway of decisions more understandable. Since cyber threats have become more dynamic and unpredictable, the single way to provide the granularity and flexibility required to effectively simulate realistic decision-making environments under uncertainty is this remedy because cyber threats have become more dynamic and unpredictable. Its adoption in this research paper is useful because it is deployed not only to facilitate the development of an empirical model, but also in grounding theoretical models on threat intelligence in practice, that is, real-life threat intelligence, which is crucial to developing secure, resilient smart infrastructure systems.

6. Discussion and Analysis

6.1 Interpretation of Key Findings

This study visual analysis provides a complex knowledge of the dynamics of and cyber threat to smart infrastructure decision-making. According to Figure 1 and Figure 7, email-based attack vectors are super predominant in the environment of cyber threats, as they appear in more than 35 percent of the observed cases. The network and web-based vectors are closely up next, which is an indication of overall wide exposure scope during the communication levels. The associated risk level predictions of these vectors give the impression of a higher level of vulnerability threat in relation to the use of emails, which are commonly known as points of entry to phishing, ransomware, or malware attacks [49]. Figure 3 and Figure 6 show that the two most common categories of the threats regarding the risk level and frequency are phishing and malware. They are usually socially engineered, that is, they attack human aspects of infrastructure systems, and, therefore, these threats need to be prioritized in the shortest time when being part of a cyber-resilience strategy. This result is further affirmed in Figure 8 that has high word counts linked with the identical threats. The resulting dataset is based on the threat data given in Kaggle NLP-Based Cybersecurity Dataset; detailed labeled instances of threats with rich descriptive metadata whose interrelation style permits a sophisticated risk modeling scheme. Such findings make it clear that phishing and malwares are a major issue or challenge requiring technical and procedural forms of defense measures to be implemented by project managers and the IT security staff in smart infrastructure [50]. A common trend between the figures shows that data-driven models are capable of providing the most urgent reality of cybersecurity threats. Those results warrant the concept of integrating data-centric threat intelligence tools into hybrid DSS architecture, which is a key feature in making decisions under uncertainty at the project level.

6.2 NLP and Sentiment Analysis contribution

Natural Language Processing (NLP) is a game-changer in the cyber threat intelligence space allowing to transform the unstructured narrative data into structured actionable information [51]. In this research, NLP algorithms were used to parse threat descriptions, forum discussions and cybersecurity reports and to extract entities, sentiments, key phrases. The figure 4 demonstrates the differences in contextual frequency of threat descriptions, and as can be seen, terms related to phishing, such as phishing scam targeting corporate accounts, are highly presented. This means that phishing accidents not only occur but are well articulated in cybersecurity news and blogs, which is an indication that there is a high awareness about them among people. Figure 5 concerns itself with the sentiment analysis of defense tactics that are debated in the forums. Feeling on the "Increase Web Security" is highly positive and supersedes any other defense IC such as the "Quarantine" or the "Monitor for Phishing." Such sentiment data can be applied in a hybrid DSS to carry out which course has to have precedence in terms of allocation of additional funds to implement, or the urgency to communicate to which stakeholders. Sentiment-based modeling helps the decision-makers to demonstrate which mitigation ways are trusted the most by both people and specialists. NLP-derived intelligence leaves the system brighter when combined with structural information like risk scores and field frequency of threat [52]. This strategy is largely useful in smart infrastructure settings where risks in operations need to be comprehended technically but also socially and psychologically. Having included NLP outputs, the hybrid DSS will be more accommodating with real-world narratives, which will enhance its forecasting, interpreting, and responding to cyber threats in the end.

6.3 Rationale of a Hybrid DSS Framework

The concept of a hybrid Decision Support System (DSS) framework presents a solid response to the issue of uncertainty of cyber threats in smart infrastructure projects. But in the fast-changing environment of threats, traditional decision-making systems have difficulty in coping with inexact or uncertain information. The hybrid DSS is characterized by the inclusion of NLP, which manipulates unstructured data, models of uncertainty by means of fuzzy logic, prioritization by means of multi-criteria decision-making (MCDM), which is also known as multi-criteria decision analysis. This enables it to process various types of data simultaneously- i.e. Risk scores, narrative descriptions, behavior of the attacker, values of sentiments. With the combination of the fuzzy inference mechanisms and NLP techniques, it could give probabilistic weighting to several of the parameters of the threat even when incomplete or conflicting inputs are available. As an example, an email with a phishing attack with high negativity of the sentiment and constant appearance of the narrative can be highlighted as the high-priority case despite the medium structured metrics (Figure 4 and 5). This multi-level decision process enhances system intelligence and flexibility to a great extent. With the inclusion of the risk modeling, the DSS can evaluate the possibilities of outcomes and propose countermeasures in accordance with the tolerance of the organization [53]. The advantage of the hybrid model is the effectiveness of mediating the distance between technical diagnostics and strategic decision-making. This means that the project managers handling smart infrastructure development will have the chance to make an informative real-time decision with an increased level of confidence. Being an area where a delay, outages, or misconfigurations can be a devastating issue with a ripple effect, a hybrid DSS paradigm allows dynamic planning, fast reaction, and efficient resource distribution [54]. the hybrid architecture is not only an improvement of technology, but it is a paradigm change toward strategic, intelligent planning in cybersecurity.

6.4 Smart Infrastructure Practical Implications

The effective role played by incorporating hybrid DSS models in cybersecurity planning of smart infrastructure is immense. More and more of the smart cities and industrial systems use interconnected sensors, cloud-based control systems, and automation via AI that can be hacked. This paper shows how a hybrid DSS can be deployed to help to bridge operations data to cyber threat intelligence, and increase resilience. An example here is that in case specialized modules driven by NLP observe an outburst of phishing content in industry forums and relate this to a sudden augmentation of email attack vectors (Figures 1 and 4) a DSS can consequently issue a pre-emptive suggestion to seal email gateways, awaken systems administrators, or indefinitely postpone email-based deployments. Such an aggressive approach allows the city planners, utility operators, and transportation leaders to make on-the-fly changes. Further, the studies on the sentiment in forums grants a chance, to the decision-makers, to evaluate the effectiveness and the acceptance of the defense systems within the circle of experts (Figure 5). This iteration process improves the trust of the stakeholders in the adopted strategies. The implementation of this type of DSS framework also stimulates cross-functional collaboration. Integrated dashboard can equip data scientists along with security professionals and heads of operations to work off the same interface [55]. The data clarity that will be presented to various audiences by such tools as Tableau, Python, and Excel visualizations in this research may be used to illustrate that there are great opportunities to present data in a way that will guarantee its accessibility. The strength of the system is the human choice to use it as a lever of power but the system enables them to penetrate further in the analysis. It replaces siloed IT functionality of cybersecurity with one of the core elements of smart infrastructure project management. In such a way, the results indicate that the hybrid models of DSS must become institutionalized instruments to be used as central mechanisms of planning in the public sector and industry in the field of cybersecurity.

6.5 Decision Making under Uncertainty

Smart infrastructure management involves multiple decision situations with uncertainty as the problem is one of the common issues in this field because the schedule, regulatory framework, and technological risks often change. The unpredictability of the threats in cyberspace is an added complicacy to this undertaking. The attackers are fast-learning, and vulnerabilities keep on reappearing [56]. The hybrid DSS created in the present research is specifically meant to succeed in this type of uncertain circumstances. The system models imprecise indicators in a fuzzy logic framework, e.g. imprecise threat descriptions or incomplete sentiment trends. Meaning is extracted out of the on-going textual information using NLP modules and probabilistic models track down the probability and consequences of a possible attack. The examples in figures 2 and 4 indicate both visual and semantic data can be used to quantify both geographic and narrative uncertainty [57]. The situation-based simulations enhance preparedness that do not exist in traditional risk management tools by allowing what-if analysis. More so, uncertainty cannot just be taken as a nuisance but as one of the dimensions of data in the likelihood of risk priority. In case of several low-certainties warnings depicting an increase in malware, the system might still assign a high signal in case sentiment and frequency indicators show a congruent wave. Such a strategy will guarantee that doubt will not freeze the processes but will trigger a wise and adaptable decision process. Finally, the hybrid DSS makes the smart infrastructure projects resilient and adaptive in the context where the only constant is the change. It changes the vulnerability of uncertainty to a source of strategic foresight.

6.6 Strategic Risk Prioritizing Among

The worthiest contribution of the research is that it promotes strategic risk prioritization during cyber-resilient decision making. The conventional methods of prioritization are usually check-in nature, fixed and responsive, which is not the best solution in rapidly changing cyber environments [58]. By contrast, the hybrid DSS envisioned in the present paper will equivalently perform dynamic assessment of the risk levels in several dimensions, namely, threats categories, vectors, severity and sentiment, enabling a much richer and more responsive process of prioritizing. According to figure 3 and figure 6, it is apparent that phishing and malware top the risk rankings. After comparing them to sentiment scores (Figure 5), the DSS can determine what threats are also considered to have an extensive impact by the wider cybersecurity community. Together with risk forecasts, such perception data result in wiser prioritization. To take examples, it will increase its risk score automatically by phishing being common having a negative connotation in forums. In addition, in filtering the threats based on the attack vectors (Figure 1 and 7), the organizations become able to better distribute the defensive resources through email, network, and web channels. This plays an important role in limited-resource or price-constrained smart infrastructure realities. Scenario simulation also offers the possibility to create live dashboards in Tableau and Python so that project managers may visualize the impact of any scenario change to the overall defense strategy. This aspect limits conjecture and gases more integrity as the stakeholders make decisions based on evidence. With the use of strategic prioritization logic within a hybrid DSS, this study makes sure that planning of smart infrastructure should not only be responsive to threats but rather flexible and proactive to risk.

6.7 Visualization as a Tool to Decision-making

Efficient visualization is equally important as it helps convert complicated data about cybersecurity into decipherable and easier-to-decide forms. This paper involved the use of tools like Python, Tableau, and Excel to represent the complex relationship impacts of cyber threats, attack actions, threat typologies, and sentiment analysis. Every figure obtained during this study not only emphasizes a certain feature of threat intelligence but also shows the superiority of visualization in the matter of its interpretation [59]. As an example, Figure 1 and Figure 7 present the distributions of attack vectors in bar and pie charts that provide an instant insight into the weakest access points; email, web, and network. The bubble chart in Figure 2 allows positioning the severity of the geographic cyber threat and possible spatial mapping of threats. Figures 4 and 5 correspond to cleaned threat descriptions and suggested defense mechanisms with the percentile distributions visualized as line plots. These images allow the interested parties to instantaneously understand what stories or rationale prevail in cyber talk. More to the point, the user can filter the data in real-time in visual form (as it is done to Tableau dashboards) by slicing the data using their own thresholds, which may be risk scores, or even severity ranks. The feature is particularly effective in meetings where quick decisions are made under the pressure. The dashboards can also encourage interdisciplinary collaboration in smart infrastructure settings in which IT, engineering, finance, and policy executives serve as stakeholders, since non-technical audiences can access insight in these dashboards. Python-generated visuals (Figure 6 and 8), can be customized at the backend and run as an automated DSS pipeline. Visualization, therefore, not only means presentation itself but also a fundamental feature of cyber-resilient decision-making structures in smart infrastructure.

7. Recommendations

In the analysis and relevant insights generated by this investigation, various recommendations can be drafted to better inform cyber-resilient decision-making in smart infrastructure systems through hybrid Decision Support Systems (DSS). In the first place, hybrid DSS models should be built into smart infrastructure projects both at planning and operational stages to manage cyber threat uncertainty. Incorporating fuzzy logic and multi-criteria decision-making (MCDM) concepts into the framework of Natural Language Processing (NLP), companies will have access to contextual and sophisticated threat intelligence information in the format of incident reports, vulnerability databases and information obtained in online forums. Second, real-time data processing capabilities and the visualization of the data such as in Python, Tableau, or Excel-based tools must be integrated into the cyber defense operations so that potentially harmful activities could be observed and tracked, the severity of threats could be measured, and prioritized [60]. The dashboard that shows the attack vectors, level of severity and sentiments-based line of defense could contribute to a great deal on the response and assigning resources strategically. Thirdly, cybersecurity plans must be in tandem with the kind of attack vector and the geographical threat profiles. Phishing and malware are the most common, as shown by the dataset and it is essential to incorporate proactive policies of training users, filtering emails, and providing endpoint protection. On the same note, organizations in many targeted areas, including the USA, North Korea and Russia must come up with region-specific countermeasures. Sentiment analysis on the public forums and the internal logs of response needs to be carried out on a regular basis to steer optimal adaptive defense actions to inform better depth in terms of stakeholder identification of intended threat mitigation measures. Lastly, it is suggested that in the future smart infrastructure projects should have special funds and manpower to develop cybersecurity-oriented DSS and tailor it. This incorporates incorporation of machine learning models, enhancement of the quality of the data sets and setting cross-sector collaboration among infrastructure developers, data scientists, and cybersecurity experts. With these recommendations, stakeholders of smart infrastructure will be able to turn ambiguity into action and enhance the resilience of a system and guarantee the security and sustainability of a digital environment.

8. Future Work

Although the study proves that it is feasible to conceive a hybrid combination of Natural Language Processing (NLP), fuzzy logic, and sentiment analysis as a Decision Support System (DSS) of smart infrastructure cybersecurity, several future research opportunities remain open to future research and improvement [61]. An area of avenues that opens is the integration of real time data feeds of live cyber threat lists, intrusion detection systems, and sensors in the infrastructure elements to permit risk assessment and mitigation plans to be updated on a dynamic basis. The static nature of a dataset used in the current study, obtained via Kaggle, contains many labeled instances and NLP features but still fails to come entirely close to the dynamics of cyber threats. Possible future work may use data that may contain time-series attack, adversarial strategies, and the changing defense strategies. Besides, the DSS framework can be supplemented by deep learning-based models of threat classification, which might be superior to classic NLP methods of identifying threat patterns when working with unstructured text with a high volume of information [62]. The other development opportunity is to improve on the DSS interface to incorporate predictive simulation features that will enable the stakeholder to simulate a hypothetical scenario of the threats, cost limitations, and geopolitical risk parameters. It can also be explored on the ways to further the role of human decision-makers by adding features of exploitability to the DSS, such as decision traceability and confidence scores to increase trust and interpretability. In addition, it would be beneficial to implement the adaptive learning algorithms to help the DSS grow proportionally to the changes in the cyber threat environment and be able to improve its outputs every time the previous decision and its outcome are used. Cross-domain validation is an additional practice that could be investigated in the future wherein the offered DSS can be implemented on other smart-based infrastructure types like smart grids, intelligent transportation systems, or urban water networks to analyze the generalizability of the proposed DSS and the corresponding domain-specific adjustments [63]. Lastly, a collaborative, open-source platform of cybersecurity DSS modeling would enable researchers, city planners, and cybersecurity practitioners to test and develop decision models on a continuous basis with different scenarios and datasets. Such future trends are not only bound to enhance the technical basis of hybrid DSS models but are also to make it stickable, transparent, and functional in the protective measures of the next-gen infrastructure against advanced cyberattacks.

9. Conclusion

This study shows that there is an urgent necessity to implement smart and flexible cybersecurity decision-making systems when speaking of smart infrastructure projects, as digitization has raised the level of vulnerability to unexpected and continuously changing cyber threats. With the help of the hybrid Decision Support System (DSS) involving the combination of the Natural Language Processing (NLP), fuzzy logic, sentiment analysis, and multi-criteria decision-making, the research proves that the traditional models are not best suitable since they cannot handle uncertainty and unstructured data. Collection of the so-called NLP-Based Cyber Security Dataset available on Kaggle had offered a source of a wealth of threat intelligence, furnishing textual explanations, threat groupings, attack vectors, severity ratings, and chat-like sentiment analysis. Python, Tableau and Excel visualization tools were critical in reducing insightful information or data to enable the stakeholders to understand the complex information conceptually. It has been discovered that phishing and malware threats are not just the most common but reported to be the most serious which makes it necessary to focus once again on the need of contextual risk assessment. It also verifies the usefulness of the idea of using the public mood and depth of the story in the decision-making process. The DSS model in this research paper will grant project managers and cybersecurity planners the capabilities to make the decisions necessary to prioritize the defenses, adequately distribute resources and to respond quickly to developing risk. This study makes both a theoretical and a practical contribution to the scientific area of smart infrastructure security. It also brings the scaling and flexible model that can operate in the context of uncertainty of cyber threats providing a strong basis of strategic planning and real-time decision-making. With cyber threats that keep changing, the deployment of such smart systems will become necessary with the aim of achieving long-term resiliency, safety and sustainability of the smart infrastructures.

Funding: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References:

[1]. Bouramdane, A. A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. Journal of Cybersecurity and Privacy, 3(4), 662-705.
https://www.mdpi.com/2624-800X/3/4/31

[2]. Carraminana, D., Bernardos, A. M., Besada, J. A., & Casar, J. R. (2024). Towards resilient cities: A hybrid simulation framework for risk mitigation through data-driven decision making. Simulation Modelling Practice and Theory, 133, 102924.
https://www.sciencedirect.com/science/article/pii/S1569190X24000388

[3]. Ahmed, Z. E., Hashim, A. H., Mokhtar, R. A., & Saeed, M. M. (2024, November). Intelligent Decision Support Systems: Transforming Smart Cities Management. In 2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI) (pp. 1-9). IEEE.
https://ieeexplore.ieee.org/abstract/document/10777112

[4]. Bhol, S. G. (2025). Applications of Multi Criteria Decision Making Methods in Cyber Security. Cyber-Physical Systems Security, 233-258.
https://link.springer.com/chapter/10.1007/978-981-97-5734-3_11

[5]. Xue, B., Chang, K., Fan, Y., Chen, X., Kim, T. W., & Liu, B. (2025). An Integrated Framework of Multidisciplinary Decision-Making Under Uncertainty for Sustainable Infrastructure Development. IEEE Transactions on Engineering Management.
https://ieeexplore.ieee.org/abstract/document/10878794

[6]. Hakimi, O., Liu, H., Abudayyeh, O., Houshyar, A., Almatared, M., & Alhawiti, A. (2023). Data fusion for smart civil infrastructure management: A conceptual digital twin framework. Buildings, 13(11), 2725.
https://www.mdpi.com/2075-5309/13/11/2725

[7]. Li, Z., Du, P., & Li, T. (2025). Comprehensive Risk Assessment of Smart Energy Information Security: An Enhanced MCDM-Based Approach. Sustainability (2071-1050), 17(8).
https://openurl.ebsco.com/EPDB%3Agcd%3A4%3A30282548/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A184750346&crl=c&link_origin=scholar.google.com

[8]. Akbarian, H., Gheibi, M., Hajiaghaei-Keshteli, M., & Rahmani, M. (2022). A hybrid novel framework for flood disaster risk control in developing countries based on smart prediction systems and prioritized scenarios. Journal of environmental management, 312, 114939.
https://www.sciencedirect.com/science/article/abs/pii/S0301479722005126

[9]. Alzate-Mejia, N., Santos-Boada, G., & de Almeida-Amazonas, J. R. (2021). Decision-making under uncertainty for the deployment of future hyperconnected networks: A survey. Sensors, 21(11), 3791.

https://www.mdpi.com/1424-8220/21/11/3791

Abdel-Basset, M., Gamal, A., Moustafa, N., Abdel-Monem, A., & El-Saber, N. (2021). A [10].security-by-design decision-making model for risk management in autonomous vehicles. IEEE Access, 9, 107657-107679.

https://ieeexplore.ieee.org/abstract/document/9491157

[11]. Polishchuk, V., Mlavets, Y., Rozora, I., & Tymoshenko, O. (2023). A hybrid model of risk assessment of the functioning of information modules of critical infrastructure objects. Procedia Computer Science, 219, 76-83

.https://www.sciencedirect.com/science/article/pii/S1877050923002740

[12]. Waqar, A. (2024). Intelligent decision support systems in construction engineering: An artificial intelligence and machine learning approaches. Expert Systems with Applications, 249, 123503.

https://www.sciencedirect.com/science/article/abs/pii/S0957417424003683

Alshammari, F. H. (2023). Design of capability maturity model integration with cybersecurity [13]. risk severity complex prediction using bayesian-based machine learning models. Service Oriented Computing and Applications, 17(1), 59-72.

https://link.springer.com/article/10.1007/s11761-022-00354-4

Dalal, S., Kumar, A., Lilhore, U. K., Dahiya, N., Jaglan, V., & Rani, U. (2024). Optimizing cloud [14]. service provider selection with firefly-guided fuzzy decision support system for smart cities. Measurement: Sensors, 35, 101294.

https://www.sciencedirect.com/science/article/pii/S2665917424002708

[15]. Aragão, F. V., Gomes, P. F. D. O., Chiroli, D. D. G., Zola, F. C., Rocha Loures, E. D. F., Santos, E. A. P., & Colmenero, J. C. (2023). Projects aimed at smart cities: A hybrid MCDA evaluation approach. Technology Analysis & Strategic Management, 35(10), 1250-1262.

https://www.tandfonline.com/doi/abs/10.1080/09537325.2021.1999405

[16]. Tarafdar, A., Sheikh, A., Majumder, P., Baidya, A., Majumder, A., Bhattacharyya, B. K., & Bera, U. K. (2024). Enhancing intrusion detection using wireless sensor networks: A novel ahp-madm aggregated multiple type 3 fuzzy logic-based k-barriers prediction system. Peer-to-Peer Networking and Applications,

https://link.springer.com/article/10.1007/s12083-024-01688-w

[17]. Goala, S., Prakash, D., Dutta, P., Talukdar, P., Verma, K. D., & Palai, G. (2022). A decision support system for surveillance of smart cities via a novel aggregation operator on intuitionistic fuzzy sets. Multimedia Tools and Applications, 81(16),

https://link.springer.com/article/10.1007/s11042-021-11522-7

[18]. Nakhaei, M., Ahmadi, A., Gheibi, M., Chahkandi, B., Hajiaghaei-Keshteli, M., & Behzadian, K. (2023). A smart sustainable decision support system for water management of power plants in water stress regions. Expert Systems with Applications, 230, 120752.

https://www.sciencedirect.com/science/article/abs/pii/S095741742301254X

[19]. Shao, Q. G., Jiang, C. C., Lo, H. W., & Liou, J. J. (2023). Establishing a sustainable development assessment framework for a smart city using a hybrid Z-fuzzy-based decision-making approach. Clean Technologies and Environmental Policy, 25(9), 3027-3044.

https://link.springer.com/article/10.1007/s10098-023-02547-7

[20]. Beckley, J. (2025). Advanced risk assessment techniques: Merging data-driven analytics with expert insights to navigate uncertain decision-making processes. Int J Res Publ Rev, 6(3), 1454-1471.

[21]. Elvas, L. B., Mataloto, B. M., Martins, A. L., & Ferreira, J. C. (2021). Disaster management in smart cities. Smart Cities, 4(2), 819-839.

https://www.mdpi.com/2624-6511/4/2/42

[22]. [Habib, A., Alnaemi, A., & Habib, M. (2024). Developing a framework for integrating blockchain technology into earthquake risk mitigation and disaster management strategies of smart cities. Smart and Sustainable Built Environment.

https://www.emerald.com/insight/content/doi/10.1108/sasbe-12-2023-0376/full/html

[23]. Fetais, A., Dincer, H., Yüksel, S., & Aysan, A. (2024). Analysis of sustainable investment policies for housing demand in Qatar via hybrid quantum fuzzy decision-making model. Kybernetes.

https://www.emerald.com/insight/content/doi/10.1108/k-01-2024-0092/full/html

.mdpi.com/2076-3417/13

[24]. Javed, A. R., Ahmed, W., Pandya, S., Maddikunta, P. K. R., Alazab, M., & Gadekallu, T. R. (2023). A survey of explainable artificial intelligence for smart cities. Electronics, 12(4), 1020.

https://www.mdpi.com/2079-9292/12/4/1020

[25]. Sanwar, A. S. M. (2024). Explainable artificial intelligence into cyber-physical system architecture of smart cities: technologies, challenges, and opportunities. J Electr Syst, 20(2), 2343-2362.

https://www.researchgate.net/profile/Shamneesh-Sharma/publication/380293674_Explainable_Artificial_IntelligenceDemertzi, V., Demertzis, S., & Demertzis, K. (2023). An overview of cyber [26]. threats, attacks and countermeasures on the primary domains of smart cities. Applied Sciences, 13(2), 790.

https://www_into_Cyber-Physical_System_Architecture_of_Smart_Cities_Technologies_Challenges_and_Opportunities/links/66345bff06ea3d0b74239278/Explainable-Artificial-Intelligence-into-Cyber-Physical-System-Architecture-of-Smart-Cities-Technologies-Challenges-and-Opportunities.pdf

[27]. Bibri, S. E., Huang, J., Jagatheesaperumal, S. K., & Krogstie, J. (2024). The synergistic interplay of artificial intelligence and digital twin in environmentally planning sustainable smart cities: A comprehensive systematic review. Environmental science and ecotechnology, 100433.

https://www.sciencedirect.com/science/article/pii/S2666498424000474

[28]. Wan, Q., Miao, X., Wang, C., Dinçer, H., & Yüksel, S. (2023). A hybrid decision support system with golden cut and bipolar q-ROFSs for evaluating the risk-based strategic priorities of fintech lending for clean energy projects. Financial Innovation, 9(1), 10.
https://link.springer.com/article/10.1186/s40854-022-00406-w

[29]. Fadhel, M. A., Duhaim, A. M., Saihood, A., Sewify, A., Al-Hamadani, M. N., Albahri, A. S., ... & Gu, Y. (2024). Comprehensive systematic review of information fusion methods in smart cities and urban environments. Information Fusion, 102317.
https://www.sciencedirect.com/science/article/pii/S1566253524000952

[30]. Kumar, R. (2025). A Comprehensive Review of MCDM Methods, Applications, and Emerging Trends. Decision Making Advances, 3(1), 185-199.
http://www.dma-journal.org/index.php/dema/article/view/69

[31]. Weil, C., Bibri, S. E., Longchamp, R., Golay, F., & Alahi, A. (2023). Urban digital twin challenges: A systematic review and perspectives for sustainable smart cities. Sustainable Cities and Society, 99, 10486
https://www.sciencedirect.com/science/article/abs/pii/S2210670723004730

[32]. Mahmood, A., Al Marzooqi, A., El Khatib, M., & AlAmeemi, H. (2023). How Artificial Intelligence can leverage Project Management Information system (PMIS) and data driven decision making in project management. International Journal of Business Analytics and Security (IJBAS), 3(1), 184-195.
https://www.journals.gaftim.com/index.php/ijbas/article/view/215

[33]. Arcas, G. I., Cioara, T., Anghel, I., Lazea, D., & Hangan, A. (2024). Edge offloading in smart grid. *Smart Cities*, *7*(1), 680-711.
https://www.mdpi.com/2624-6511/7/1/28

[34]. Kelemen, M., Polishchuk, V., Gavurová, B., Rozenberg, R., Bartok, J., Gaál, L., ... & Kelemen Jr, M. (2021). Model of evaluation and selection of expert group members for smart cities, green transportation and mobility: from safe times to pandemic times. *Mathematics*, *9*(11), 1287.
https://www.mdpi.com/2227-7390/9/11/1287

[35]. Saeed, A. (2024). Machine Learning Models for Intelligent Decision Support Systems. *Journal of AI Range*, *1*(1), 54-66.
https://www.researchcorridor.org/index.php/jair/article/view/268

[36]. Sadeghi, J., Sarvari, H., Chan, D. W., & Edwards, D. J. (2025). Identification and Analysis of Earthquake Risks in Worn-Out Urban Fabrics Using the Intuitionistic Fuzzy Brainstorming (IFBS) Technique for Group Decision-Making. *Buildings*, *15*(9), 1520.
https://www.mdpi.com/2075-5309/15/9/1520

[37]. Elsayed, A., & Mohamed, M. (2025). Enhancing Smart City Management with AI: Analyzing Key Criteria and their Interrelationships using DEMATEL under Neutrosophic Numbers and MABAC for Optimal Development. *Neutrosophic Systems with Applications*, *25*(2), 1-38.
https://sciencesforce.com/index.php/nswa/login

[38]. Ghiaci, A. M., & Ghoushchi, S. J. (2023). Assessment of barriers to IoT-enabled circular economy using an extended decision-making-based FMEA model under uncertain environment. *Internet of Things*, *22*, 100719.
https://www.sciencedirect.com/science/article/abs/pii/S2542660523000422

[39]. Zhao, T., Song, C., Yu, J., Xing, L., Xu, F., Li, W., & Wang, Z. (2025). Leveraging Immersive Digital Twins and AI-Driven Decision Support Systems for Sustainable Water Reserves Management: A Conceptual Framework. *Sustainability*, *17*(8), 3754.
https://www.mdpi.com/2071-1050/17/8/3754

[40]. Kanj, H., Kotb, Y., Alakkoumi, M., & Kanj, S. (2024). Dynamic decision making process for dangerous good transportation using a combination of topsis and ahp methods with fuzzy sets. *IEEE Access*.
https://ieeexplore.ieee.org/abstract/document/10458133

[41]. Al-Atawi, A. A. (2024). Enhancing data management and real-time decision making with IoT, cloud, and fog computing. *IET Wireless Sensor Systems*, *14*(6), 539-562.
https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/wss2.12099

[42]..Pamucar, D., Deveci, M., Gokasar, I., Delen, D., Köppen, M., & Pedrycz, W. (2023). Evaluation of metaverse integration alternatives of sharing economy in transportation using fuzzy Schweizer-Sklar based ordinal priority approach. *Decision support systems*, *171*, 113944.
https://www.sciencedirect.com/science/article/abs/pii/S0167923623000192

[43]. Hang, F., Xie, L., Zhang, Z., Guo, W., & Li, H. (2023). RETRACTED ARTICLE: Artificial intelligence enabled fuzzy multimode decision support system for cyber threat security defense automation. Journal of Computer Virology and Hacking Techniques, 19(2), 257-269.
https://link.springer.com/article/10.1007/s11416-022-00443-0

[44]. Lifelo, Z., Ding, J., Ning, H., & Dhelim, S. (2024). Artificial intelligence-enabled metaverse for sustainable smart cities: Technologies, applications, challenges, and future directions. Electronics, 13(24), 4874.
https://www.mdpi.com/2079-9292/13/24/4874

[45]. Nota, G., & Petraglia, G. (2024). The Design of Human-in-the-Loop Cyber-Physical Systems for Monitoring the Ecosystem of Historic Villages. Smart Cities, 7(5), 2966-2994.
https://www.mdpi.com/2624-6511/7/5/116

[46]. Andreou, A., Mavromoustakis, C. X., Markakis, E. K., & Song, H. (2023). On the integration of user preferences by using a hybrid methodology for multi-criteria decision making. *IEEE Access*, *11*, 139157-139170.
https://ieeexplore.ieee.org/abstract/document/10348573

[47]. Kalinin, M., Krundyshev, V., & Zegzhda, P. (2021). Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), 78.
https://www.mdpi.com/2075-1702/9/4/78

[48]. Shan, A., & Myeong, S. (2024). Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. *Sensors*, *24*(15), 4888.

https://www.mdpi.com/1424-8220/24/15/4888

[49]. Liang, H., García, B., Seah, E., Weng, A., Baillargeat, D., Joerin, J., ... & Chatzi, E. (2024). Harnessing Hybrid Digital Twinning for Decision-Support in Smart Infrastructures. *Engineering journal preprints,*

https://doi. org/10.31224/3838.

Thekdi, S. A., & Chatterjee, S. (2019). Toward adaptive decision support for assessing infrastructure system resilience using hidden performance measures. *Journal of Risk Research*, *22*(8), 1020-1043.

https://www.tandfonline.com/doi/abs/10.1080/13669877.2018.1440412

[50]. Tran Thi Hoang, G., Dupont, L., & Camargo, M. (2019). Application of decision-making methods in smart city projects: a systematic literature review. *Smart Cities*, *2*(3), 433-452.

https://www.mdpi.com/2624-6511/2/3/27

[51]. Ma, M., Preum, S. M., Ahmed, M. Y., Tärneberg, W., Hendawi, A., & Stankovic, J. A. (2019). Data sets, modeling, and decision making in smart cities: A survey. *ACM Transactions on Cyber-Physical Systems*, *4*(2), 1-28.

https://dl.acm.org/doi/abs/10.1145/3355283

[52]. Neshenko, N., Nader, C., Bou-Harb, E., & Furht, B. (2020). A survey of methods supporting cyber situational awareness in the context of smart cities. *Journal of Big Data*, *7*, 1-41.

https://link.springer.com/article/10.1186/s40537-020-00363-0

[53]. Van Pham, H., & Moore, P. (2019). Emergency service provision using a novel hybrid SOM-spiral STC model for group decision support under dynamic uncertainty. *Applied Sciences*, *9*(18), 3910.

https://www.mdpi.com/2076-3417/9/18/3910

[54]. Indrajit, R. E. (2024, October). Quantum Computing in Project Management: Transforming Risk Assessment and Decision-Making. In *2024 Ninth International Conference on Informatics and Computing (ICIC)* (pp. 1-6). IEEE.

https://ieeexplore.ieee.org/abstract/document/10957024

[55]. Yuksel, S., Dincer, H., & Mikhaylov, A. (2024). Analysis of market environment for smart grid technology investments via facial action coding system-enhanced hybrid decision-making model. *International Journal of Innovation Science*, *16*(5), 981-1004.

https://www.emerald.com/insight/content/doi/10.1108/ijis-08-2023-0191/full/html

[56]. Ahmed, V., Khatri, M. F., Bahroun, Z., & Basheer, N. (2023). Optimizing smart campus solutions: An evidential reasoning decision support tool. *Smart Cities*, *6*(5), 2308-2346.

https://www.mdpi.com/2624-6511/6/5/106

[57]. Mrówczyńska, M., Skiba, M., Leśniak, A., Bazan-Krzywoszańska, A., Janowiec, F., Sztubecka, M., ... & Kazak, J. K. (2022). A new fuzzy model of multi-criteria decision support based on Bayesian networks for the urban areas' decarbonization planning. *Energy Conversion and Management*, *268*, 116035.

https://www.sciencedirect.com/science/article/pii/S0196890422008251

[58]. Han, Y., & Deng, Y. (2018). A hybrid intelligent model for assessment of critical success factors in high-risk emergency system. *Journal of ambient intelligence and humanized computing*, *9*(6), 1933-1953.

https://link.springer.com/article/10.1007/s12652-018-0882-4

[59]. Mohamed, A. M. O., Mohamed, D., Fayad, A., & Al Nahyan, M. T. (2024). Enhancing decision making and decarbonation in environmental management: a review on the role of digital technologies. *Sustainability*, *16*(16), 7156.

https://www.mdpi.com/2071-1050/16/16/7156

[60]. Cubric, M. (2020). Drivers, barriers and social considerations for AI adoption in business and management: A tertiary study. *Technology in Society*, *62*, 101257.

https://www.sciencedirect.com/science/article/abs/pii/S0160791X19307171

[61]. Kaginalkar, A., Kumar, S., Gargava, P., Kharkar, N., & Niyogi, D. (2022). SmartAirQ: A big data governance framework for urban air quality management in smart cities. *Frontiers in Environmental Science*, *10*, 785129.

https://www.frontiersin.org/journals/environmental-science/articles/10.3389/fenvs.2022.785129/full

[62].Nabeeh, N. A., Abdel-Basset, M., El-Ghareeb, H. A., & Aboelfetouh, A. (2019). Neutrosophic multi-criteria decision making approach for iot-based enterprises. *IEEE access*, *7*, 59559-59574.

https://ieeexplore.ieee.org/abstract/document/8680629

[63]. Freire, C. A., Ferreira, F. A., Carayannis, E. G., & Ferreira, J. J. (2021). Artificial intelligence and smart cities: A DEMATEL approach to adaptation challenges and initiatives. *IEEE Transactions on Engineering Management*, *70*(5), 1881-1899.

https://ieeexplore.ieee.org/abstract/document/9530200

[64]. Dataset Link:

https://www.kaggle.com/datasets/hussainsheikh03/nlp-based-cyber-security-dataset?resource=download