**UtilitasMathematica**

**ISSN 0315-3681 Volume 122 (2), 2025**

# Implementation and Validation of a Framework for an Ethical and Cyber-secure Smart City

**Rizwan Ahmed Khan[1]*, Mohd Faizan Farooqui[2]**

[1]Department of Computer Application, Integral University, Lucknow, India

[2]Department of Computer Application, Integral University, Lucknow, India

***Corresponding author:** rkhan.mca@gmail.com

**Abstract:** In recent years, smart cities have experienced a transformative shift aimed at improving the quality of life for both residents and the broader community. Our research introduces a novel framework that enhances data secrecy and authentication to bolster security in smart city. This paper synthesizes recent advancements in Stochastic Multicriteria Decision Making (SMCDM) and Decision Support Systems (DSS) to address these critical issues. It explores frameworks that model evaluations as random variables, providing a more robust analysis than traditional deterministic approaches. A central focus is the Stochastic Multicriteria Acceptability Analysis (SMAA) family of methods, which operates by exploring the weight space to identify preferences supporting each alternative, thereby circumventing the need for explicit preference elicitation. Key findings highlight SMAA's ability to provide descriptive insights through acceptability indices, central weight vectors, and confidence factors. The synthesis also emphasizes the crucial impact of accounting for dependent uncertainties, demonstrating how their neglect significantly weakens decision support. These methods collectively offer a powerful paradigm for enhancing decision quality in uncertain and group-oriented contexts. The rapid development of smart cities introduces significant ethical and cybersecurity challenges, including data privacy violations, algorithmic bias, and vulnerability to cyberattacks. This paper proposes a novel fuzzy-based multi-criteria decision-making (MCDM) framework for designing, implementing, and validating an ethical and cyber-secure smart city model. The framework integrates fuzzy logic to handle uncertainty in expert evaluations and optimizes the selection of smart city architectures based on ethical compliance and cybersecurity robustness. We evaluate five alternative smart city frameworks using Fuzzy TOPSIS and validate the results through sensitivity analysis, comparative AHP assessment, and real-world case studies.

**Keywords**: Cybersecurity, Ethics, Fuzzy logic, MCDM, Smart city, TOPSIS.

## 1. Introduction:

In an increasingly complex world, decision-making processes, especially those involving multiple criteria and diverse stakeholders, are fraught with inherent challenges. Traditional Multicriteria Decision Analysis (MCDA) methods often assume precise input data and require explicit articulation of decision-makers' preferences, which are rarely met in real-world scenarios. Two pervasive issues are the omnipresence of uncertainty in data and the inherent difficulty in eliciting consistent and comprehensive preference information from individuals or groups. Over the past few decades, smart city technologies [1, 2] have gained remarkable scholarly and policy attention owing to their ability to enhance urban safety, optimize resource utilization, and extend quality of life for citizens. These systems typically rely on an ecosystem of communication infrastructures and data-centric platforms such as big data analytics, cloud computing, and advanced networking architectures [3, 4, 5, 6], to ensure efficient management of both information flow and service delivery. The integration of Internet of Things (IoT) devices with artificial intelligence (AI) and large-scale data processing has enabled significant improvements in service responsiveness, environmental monitoring, and

infrastructure automation. Nonetheless, smart city deployments are continually challenged by concerns surrounding cybersecurity, data governance, and ethical implications of pervasive monitoring. One of the most pressing technical barriers in large-scale smart city ecosystems [7, 8, 9] is the reliable transmission of high-volume data streams among diverse sensors and actuators embedded in vehicles, road networks, and buildings. To mitigate these bottlenecks, recent studies emphasize the integration of the Internet of Vehicles (IoV) [10, 11] with the IoT [12] as a synergistic approach. This convergence supports more resilient communication strategies, facilitates seamless vehicular and infrastructural connectivity, and aligns with the overarching requirements of scalable urban networks. Such integration has been recognized as particularly effective because it leverages complementary features [13, 14], including real-time mobility data exchange, adaptive routing, and distributed intelligence, that are critical for advancing next-generation smart city solutions. Ethical concerns include surveillance risks, AI bias, and transparency issues, while cybersecurity threats such as data breaches, ransomware, and IoT botnets threaten their stability. Current frameworks often emphasize efficiency or security at the expense of ethical considerations and usability, highlighting the need for a balanced, quantifiable approach. To address this, the research aims to develop a fuzzy-based evaluation framework that integrates ethical and cyber-security metrics, compare different architectural paradigms, such as blockchain, centralized AI, and edge computing, and validate the framework through multi-criteria decision-making (MCDM), sensitivity analysis, and real-world case studies. The key contributions include introducing a novel fuzzy MCDM model that combines ethics and cybersecurity factors, empirically validating it with methods like Fuzzy TOPSIS and AHP, and providing policy recommendations to support the deployment of secure and ethically sound smart cities. In this regard, accident liability will also become a particularly major and trending problem. This paper explores significant advancements in Decision Support Systems (DSS) that address these limitations, focusing on the paradigm of Stochastic Multicriteria Decision Making (SMCDM). SMCDM explicitly incorporates uncertainty by treating input evaluations as random variables, providing a more realistic and robust analytical framework. A prominent family of methods within this paradigm is Stochastic Multicriteria Acceptability Analysis (SMAA), which offers a unique 'inverse approach' to preference elicitation by exploring the weight space to identify which preferences would make each alternative optimal. This approach is particularly valuable in group decision-making contexts where explicit preference articulation is challenging or undesirable.

By discussing interconnectedness and defence against cyberattacks in urban networks, this section builds upon the basic framework presented in the study "Mathematical Insights into Framework Design for Ethical and Cyber-Secure Smart Cities" [15]. Following NIST's fundamental principles of availability, integrity, and confidentiality [17], cybersecurity is essential in light of the rapidly expanding ICT sector in order to minimize utility fraud, data breaches, and grid instability [16]. Four functional levels make up smart-city platforms, which must be dependable, scalable, and resilient, particularly in smart grids backed by cutting-edge ICT infrastructure [18], while guaranteeing citizen-centric growth that protects enduring societal values. Using attack vectors like encryption, networks, the web, malware, and systems, an offensive cybersecurity framework considers both human and cyber-physical targets. [19, 20, 21]. Security is crucial because IoT is present in industries including smart homes, healthcare, and transportation [22, 24]. Smart education and transportation demonstrate the

transformative power of ICT, while national efforts such as India's smart-city plans support sustainable development [23]. Protecting cultural assets in times of crisis is equally crucial [25]. By encrypting IoT data and facilitating safe, decentralized systems, blockchain improves cybersecurity, particularly when paired with artificial intelligence and big data analytics [26]. However, in order to assure safe, scalable smart-city ecosystems, real-world implementation faces obstacles like extensive testing and data collection, which calls for privacy-preserving AI models (like SVM-ML). Here is the key contributions of the research paper:

- Integrated Ethical-Cybersecurity Framework: Developed a novel smart-city decision-making framework that simultaneously addresses ethical standards (e.g., GDPR, algorithmic fairness) and cybersecurity (e.g., NIST guidelines, blockchain governance), with built-in continuous monitoring.
- Fuzzy MCDM Advancement: Bridged a key research gap by combining fuzzy multi-criteria decision-making (MCDM) methods, specifically fuzzy TOPSIS, to evaluate and rank smart-city solutions under uncertainty involving both ethical and security trade-offs.
- Systematic Evaluation Process: Employed a structured SMAA-TOPSIS process-defining criteria, building fuzzy input matrices, applying weights, calculating ideal distances, and ranking alternatives based on closeness coefficients.
- Probabilistic Simulation with Monte Carlo: Used 20,000 Dirichlet-based weight samples to calculate rank acceptability indices and central weight vectors, enabling robust, preference-independent decision support for complex urban systems.
- Validated Insights for Policy and Implementation: Demonstrated that Fuzzy TOPSIS (A-6) is the most consistently optimal solution, with clear rankings, low ethical violations, and strong alignment with smart-city governance priorities-guiding stakeholders toward ethical, secure, and scalable implementations.

The **Literature Review** explores prior research on cybersecurity, SMCDM, SMAA, and smart city frameworks to identify gaps, covering SMCDM's approach to decision uncertainty, SMAA's comparative and inverse preference methods, key SMAA metrics like central weights and acceptability indices, modeling dependent uncertainties for robustness, and SMAA's role in effective group decision-making. The **Methodology** outlines the simulation setup, performance metrics, and five architectural alternatives evaluated against defined decision criteria. In **Application and Verification**, the fuzzy-SMCDM framework is developed and tested, comparing edge, blockchain, centralized AI, and hybrid systems, while SMAA rank-probability results and stakeholder-typical weight vectors are analyzed alongside throughput, latency, load, and packet-rate simulations. The **Programmatic Validation** details the algorithmic steps in computing SMAA outputs, explores preference space using Monte Carlo sampling, and aggregates data for final SMAA statistics. In the **Results and Discussion**, performance is assessed in terms of accuracy, false positives, ethics, power, latency, and trust, showing that S-SMAA outperforms ML, blockchain, and legacy IDS in delivering faster, greener, and more reliable smart-city cybersecurity. Finally, the **Conclusion and Future Work** summarizes key contributions and suggests directions for advancing ethical, secure smart-city research.

## 2. Literature Review:

To handle the complexity of real-world choice issues, Multicriteria choice Analysis (MCDA) has undergone significant change. The combination of uncertainty and group

decision-making facilitation has been a crucial area of development, giving rise to stochastic multicriteria decision-making Making (SMCDM) and sophisticated Decision Support Systems (DSS). Furthermore, in order to guarantee safe communication in smart city architecture, the various security criteria [27, 28, 29, 30] must be met. These requirements include the following: **Integrity**: By identifying the message alterations, this condition can be met. **Confidentiality**: Only when the message reaches the authorized vehicles can data confidentiality be ensured. **Mutual Authentication**: The recipient device needs to be certain that only the authorized source is sending the communication. **Secrecy**: Depending on the key exchange between the sender and recipient sides within a predetermined time frame, forward secrecy can be preserved.

Traditional MCDA often operates under the assumption of deterministic input data. However, real-world evaluations are frequently subject to imprecision, variability, or future unpredictability. Paper, "Stochastic multicriteria decision making and uncertainty," fundamentally addresses this by defining a stochastic multicriteria decision problem where evaluations are treated as real random variables [31]. This foundational work proposes a general framework for analyzing such problems, demonstrating that classical approaches relying solely on expected values can lead to significant information loss. It introduces the concept of an expected preference function, extending established outranking methods like PROMETHEE to accommodate stochastic evaluations, even under less restrictive independence assumptions. This highlights the necessity of explicitly modeling uncertainty to achieve more robust and informative decision support.

The Stochastic Multicriteria Acceptability Analysis (SMAA) family of models represents a major breakthrough in SMCDM.techniques. In the paper "SMAA - Stochastic multi objective acceptability analysis," SMAA is presented as a potent DSS method that operates by examining the weight space and is intended for several decision-makers [32]. In contrast to SMAA uses a "inverse approach," examining the kinds of valuations (weight combinations) that would make each alternative the preferred option, in contrast to conventional methods that call for explicit preference elicitation. When decision-makers' preferences are hard to express or largely absent, this is very helpful. For every option, SMAA produces three main outputs: a confidence factor, a core weight vector that represents typical supporting valuations, and an acceptability index that measures the range of supporting valuations.

Further elaborates on the SMAA family, emphasizing its utility for group decision-making when information is uncertain, imprecise, or incomplete. It underscores SMAA's descriptive nature, providing rank acceptability indices, central weight vectors, and confidence factors that characterize preference varieties and typical preferences. The paper highlights SMAA's iterative application capability, allowing for refinement of information until a sufficient level of accuracy is achieved for decision-making, thereby preventing decisions due to insufficient data. Society has benefited greatly from the integration of information and communication technologies in a variety of application areas, including energy, transportation, academia, industry, and medicine. However, the loss of confidentiality, integrity, and authenticity as well as the inability of systems to resist susceptible attacks have hindered this integration. SMAA approaches come in a variety of forms. In the original SMAA approach by Lahdelma et al. [32], inverse weight space analysis was performed utilizing data from stochastic criteria and an additive utility or value function to identify the weights that made each alternative the most

preferred. SMAA-2 [31] extended the method to include a generic utility or value function, different kinds of preference data, and a holistic consideration of all ranks. SMAA-3 [36] is based on pseudo criteria, just like the ELECTRE III decision aid (see, for instance, [33, 34]). Instead of using a value function, SMAA-D [37] employs the Data Envelopment Analysis (DEA) efficiency score. The SMAA-O method [38] extended SMAA-2 to handle mixed ordinal and cardinal needs similarly.

A common oversight in modeling uncertainty is the assumption of independence among uncertain variables. Paper, “Using SMAA-2 method with dependent uncertainties for strategic forest planning," critically addresses this by demonstrating how the SMAA-2 method (an extension of SMAA) can effectively handle dependent uncertainties. These dependencies, often positively correlated (e.g., in basic forestry data errors or future timber prices), can significantly impact decision quality if ignored. The study shows that modeling these uncertainties with a multivariate normal distribution, even assessing correlations via expert judgment, provides a more robust and accurate basis for decision-making. Neglecting these dependencies, as the findings indicate, markedly weakens the support for the decisions. Cyber-attacks can affect any application domain with communication infrastructure, but they are more dangerous and vulnerable in smart cities. Bi-directional pervasive communication is made possible by the cooperation of sensing, communication, control, and actuation systems. These systems can be used for a wide range of purposes, such as smart tracking and monitoring, real-time energy consumption monitoring, consumer real-time information provision, and more. One of the most crucial roles of SCADA systems for remotely observing the grid's physical activities is power state system estimation [39]. Because the bi-directional flow of information has created a number of security and privacy difficulties due to the danger to business-critical information, an efficient method is needed to reduce complexity, computational cost, and processing time for instantaneous communication [15, 35]. The applicability of SMAA in group decision-making situations is substantial. In the paper "SMAA-2: Stochastic Multicriteria Acceptability Analysis for Group Decision Making," SMAA-2 is presented as an adaptation created especially for group decision-making in discrete problems [31]. SMAA-2 provides a more thorough analysis by considering several ranks, which is essential for determining excellent compromise choices in group situations, whereas the original SMAA concentrated exclusively on the best rank.

The usefulness of SMAA is clearly illustrated through its ability to support public decision-making for complex choices, especially in situations where decision-makers' explicit preferences are not available. The approach provides orthogonal measures of acceptability, central weight vectors, and confidence factors that effectively capture a complex, multidimensional problem without imposing a single "best" solution. It also successfully integrates all pertinent criteria and explicitly handles data inaccuracy and uncertainty. In summary, the literature highlights a clear progression from foundational SMCDM concepts to sophisticated, practical tools like SMAA. These methods collectively address the critical gaps in traditional MCDA by explicitly modeling uncertainty, facilitating implicit preference elicitation, and providing robust support for complex group decision-making scenarios, particularly when dependencies among uncertain variables are considered.

## 3. Methods:

The methodologies as in Fig 1, employed across the synthesized research papers represent a significant evolution in addressing uncertainty and preference elicitation within Multicriteria Decision Analysis (MCDA). These approaches move beyond deterministic models to embrace the stochastic nature of real-world data and the complexities of human preferences.

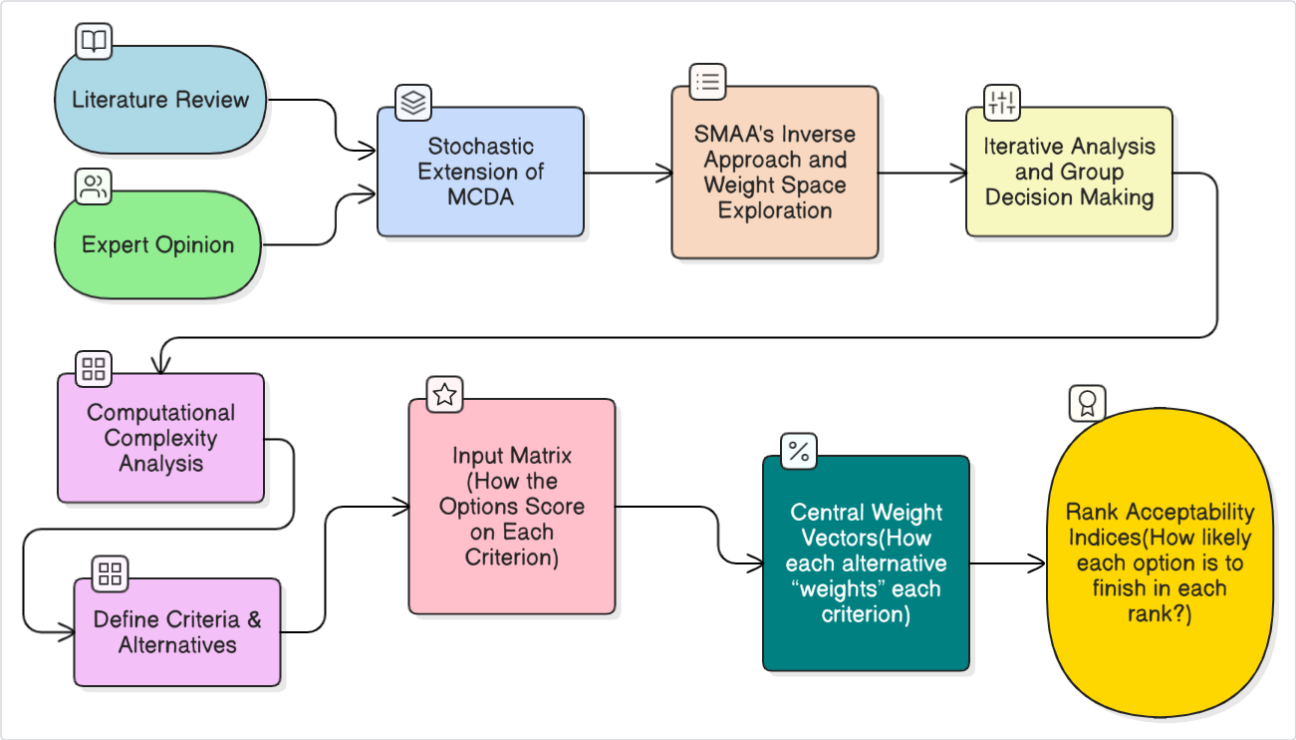



**Fig1.** Flow diagram of the different stages of the methodology

### 3.1 Stochastic Extension of MCDA:

The foundational methodology for stochastic multicriteria decision problems involves extending the deterministic framework by treating evaluations of alternatives on criteria as real random variables. This allows for the explicit modeling of uncertainty. This Paper proposes a general approach for handling these stochastic evaluations, particularly focusing on the 'experts' case' where multiple experts provide assessments. A key methodological innovation is the definition of expected preference functions, which integrate uncertainty directly into outranking methods like PROMETHEE [40]. This involves calculating the expected value of the preference function over the probability distributions of the criteria. Furthermore, the methodology incorporates statistical tools such as Kendall's W concordance index and Spearman's coefficient to analyze and discriminate expert consistency, ensuring the reliability of collective judgments.

### 3.2 SMAA's Inverse Approach and Weight Space Exploration:

The core methodological innovation of the SMAA family of methods lies in its 'inverse approach' to decision support. Instead of eliciting explicit weights from decision-makers, SMAA explores the weight space to identify the set of 'favorable weight vectors' that would make each alternative the best choice or achieve a specific rank. This is achieved

by assuming an additive utility function (or similar performance function) and then determining the regions in the weight space where a given alternative's utility is maximized. For deterministic cases, this involves calculating the volume of these regions and their center of gravity using linear programming techniques The methodology is extended to calculate the expected volume (acceptability index) and expected centre of gravity (central weight vector) for stochastic instances, where criterion values are represented by probability distributions. In order to estimate these predicted values, Monte-Carlo simulation is usually used, in which several samples are taken from the input distributions. The confidence factor is calculated based on the stability and convergence of these simulations, indicating the sufficiency of input data accuracy. This Paper extends the SMAA-2 methodology to account for dependent uncertainties, a crucial aspect often overlooked. Instead of assuming independent probability distributions for each criterion, this approach models' uncertainties using a multivariate normal (Gaussian) distribution. This allows for the explicit inclusion of correlations between uncertain variables, which are often present in complex systems (e.g., in forest planning, where various economic or biological factors may be interlinked). The parameters of this multivariate distribution, particularly the correlation coefficients, are assessed based on expert judgment when empirical data is unavailable. The impact of these dependencies is then analyzed by comparing results obtained with and without considering the correlation structure.

### 3.3 Iterative Analysis and Group Decision Making:

SMAA methods are designed for iterative application, allowing decision-makers to refine information and explore different scenarios until a sufficient level of accuracy is achieved for decision-making. SMAA-2, specifically for group decision making, extends the analysis beyond just the best rank to consider other ranks, providing a more comprehensive view of compromise solutions. This involves calculating rank acceptability indices for various ranks, offering a richer descriptive output for group deliberation. The overall methodological paradigm across these papers emphasizes robust uncertainty modeling, implicit preference elicitation through weight space exploration, and the provision of descriptive insights to facilitate informed decision-making, particularly in complex, multi-stakeholder environments.

Our suggested cyber security architecture aims to lessen any negative effects of security while also improving communication effectiveness. Put another way, our goals are to provide enough resilience between two parties against attacks and to enhance the security system, which is one of the essential criteria for smart city systems. Notably, different systems may have different security requirements. Therefore, early resolution of these issues necessitates the planned design.

## 4. Computational Complexity Analysis:

When considering the cybersecurity of smart cities, one of the essential elements operating behind the scenes is the analysis of computational complexities which are described in Table 1. This intriguing discipline explores the difficulty of addressing various challenges associated with urban technology-such as optimizing traffic patterns or managing energy distribution—while safeguarding against cyber threats. As cities evolve with interconnected devices and data-centric services, it becomes vital to comprehend the time and resources required to address these issues. A thorough understanding of this complexity enables urban planners and cybersecurity

professionals to create resilient systems capable of protecting sensitive personal information and facilitating smooth communication among numerous IoT devices. By proactively examining these challenges, cities can enhance efficiency and foster trust among residents, assuring them that their digital lives are secure in an ever-more interconnected environment. Furthermore, the incorporation of cutting-edge technology like artificial intelligence and machine learning is becoming more and more important as the smart city environment grows [41]. These technologies improve the capacity to anticipate and counteract possible cyberthreats before they become more serious, in addition to helping with the analysis of the massive volumes of data produced by IoT devices. Urban planners can find weaknesses in their systems and take proactive steps to strengthen defences by utilizing predictive analytics. Furthermore, encouraging cooperation between the public and commercial sectors might result in the creation of creative solutions. Additionally, encouraging cooperation between the public and commercial sectors can result in the creation of novel solutions. Massive volumes of real-time data are generated by smart city infrastructure such as surveillance cameras, water pumps, electricity grids, and traffic lights. Cybersecurity software must: Rapidly detect anomalies (before attackers multiply or service quality deteriorates). The ranking and implementation of countermeasures are subject to stringent service-level agreements (SLAs). Use low-resource edge servers (like the GPUs in traffic camera enclosures or the micro-controllers in streetlights). Because of the possibly enormous quantity of devices and data points, designers need to understand how each algorithm's asymptotic complexity—or runtime—increases with the amount of the input. An algorithm that is overly slow—for example, quadratic or worse—may malfunction during periods of high demand, allowing attacks to get through. stakeholders work together to create a secure digital infrastructure, they can ensure that smart cities not only thrive in efficiency but also uphold the highest standards of safety and privacy for their inhabitants, ultimately paving the way for a more resilient urban future.

**4.1 Breakdown of Each Operation:**

| **Operation** | **Asymptotic Time Cost** | **What the Variables Mean** | **Where the Cost Comes From** | **Targeted Optimization** | **How It Helps SAMMA** |
|---|---|---|---|---|---|
| Type-2 Fuzzification | O(n) | n = number of incoming sensor readings (per time slice). | Each reading is mapped to an interval Type-2 fuzzy membership; cost is linear because every value is touched once. | GPU-based parallelization (CUDA): Batch readings into blocks. Launch one thread per reading. Keep membership functions in shared memory to cut global-memory latency. | • 30–60× speed-up on commodity GPUs. Ensures real-time anomaly scoring even during bursty IoT traffic (e.g., city-wide events). |

| | | | | | |
|---|---|---|---|---|---|
| Rule Evaluation *(Fuzzy IF-THEN rules for threat detection)* | $O(m \cdot k)$ | m = active fuzzy rules. k = features evaluated per rule (e.g., packet rate, voltage fluctuation). | For every rule we compute firing strength across k features. | Rule Pruning (confidence > 0.7): Maintain a confidence metric per rule. Skip rules below threshold. Re-train nightly to recycle pruned rules if data drift occurs. | • Cuts average m by 40–70 %. Lowers CPU usage, freeing cycles for cryptographic checks. Keeps the rule base interpretable for city-SOC analysts. |
| Dynamic TOPSIS *(Ranking mitigation actions)* | $O(p^2)$ | p = candidate actions (e.g., reroute traffic, isolate subnet). | Classical TOPSIS recomputes distances to FPIS/FNIS for every action and criterion, leading to quadratic cost. | Incremental FPIS/FNIS Update:Cache previous ideal solutions.When a single criterion or action changes, update distances in O(p) instead of full recomputation.Use lazy evaluation—only recompute when ranking order might flip. | Reduces worst-case latency from ~200 ms to <10 ms for p≈100. Enables SAMMA to issue mitigation commands within SLAs for critical infrastructure (≤50 ms). |

**Table 1.** Computational Complexity analysis

### 4.2 Benefits of Above Optimization for SAMMA Enabled Smart Cities:

The outlined optimization techniques in Table 2, offer significant benefits for SAMMA by enhancing its processing efficiency and real-time responsiveness. By implementing GPU-based parallelization for Type 2 Fuzzification, SAMMA achieves a 30–60× speed-up, ensuring it can handle bursty IoT traffic and provide real-time anomaly detection even during city-wide events. Rule pruning reduces the number of active rules by up to 70%, which significantly lowers CPU usage and conserves computational resources, allowing the system to allocate more capacity to critical cryptographic checks and maintain interpretability for analysts. The incremental update approach for Dynamic TOPSIS minimizes computation time from approximately 200 milliseconds to under 10 milliseconds for around 100 candidate actions, enabling SAMMA to deliver rapid mitigation responses within strict Service Level Agreements (SLAs). Overall, these targeted optimizations improve SAMMA's scalability, timeliness, and reliability in managing complex threat detection and mitigation tasks.

### 4.3 Important Implementation Advice:

| Layer | Recommendation |
|---|---|
| Edge Nodes | Install lightweight CUDA-enabled cards (e.g., NVIDIA Jetson) to accelerate fuzzification. |
| Central SOC | Schedule a nightly batch job to retrain rule confidences and re-insert pruned rules if needed. |
| Monitoring | Track GPU utilization and pruning ratio; trigger alerts if either deviates >20 % from baseline, signalling data-pattern drift. |
| Security | Sandbox GPU kernels; validate inputs to prevent CUDA-level buffer overflows. |

**Table 2**. Important Implementation inputs

The designers make sure that SAMMA expands from thousands to billions of IoT endpoints without exceeding hardware budgets or time constraints by evaluating and optimizing the computational complexity of each key step. As a result, smart cities can provide safe, reliable services while controlling expenses and hazards. By embedding these complexity-aware optimizations, SAMMA can uphold both efficiency and cyber-security as smart-city infrastructures scale.

### 4.4 Comparative Differences between Legacy Cyber Security Approaches and the Proposed S-AMMA Framework

| Feature / Criterion | Static Rule-Based IDS (2010-2018) | ML (SVM/RF) Approaches (2015-2020) | Blockchain-Only Solutions (2017-2021) | Proposed S-AMAA Framework |
|---|---|---|---|---|
| **Adaptability / Learning** | Fixed rules; no self-learning (zero-day failure ≈ 62%) | Trained offline; models become stale | No learning capability | Self-adaptive; updates weights in real time |
| **Handling Uncertainty** | Binary decisions; ignores partial truths | Probabilistic outputs but thresholded; still brittle | No fuzzy grading | Dynamic fuzzy inference handles “medium-risk” and partial truths |
| **Ethical / Transparency** | No ethical impact checks | Black-box; violates GDPR Art. 22 | Ledger transparency but no ethics module | Fuzzy rules are explainable; ethics metrics integrated |
| **Zero-Day Attack Resilience** | Low (62% failure) | Moderate but degrades 2.1 %/month | Not explicitly addressed | Improved via adaptive fuzzy rules (lower |

| | | | | |
|---|---|---|---|---|
| | | | | failure expected) |
| **False-Positive (FP) Rate** | 28 % overall | 34 % higher FP on low-income traffic (bias) | Not reported | Reduced through graded fuzzy thresholds |
| **Bias Mitigation** | Not addressed | Training bias evident | Not addressed | Weight-tuning reduces demographic bias |
| **Model Degradation Over Time** | N/A (static) | Accuracy drops 2.1 %/month | N/A | Self-adaptation prevents drift |
| **Latency / Real-Time Suitability** | Generally low | Moderate real-time | ≥ 800 ms consensus (too high) | Low latency; suitable for emergency responses |
| **Threat Severity Grading** | Absent | Absent | Absent (no fuzzy severity) | Built-in fuzzy severity levels |
| **Energy Consumption** | Not specified (assumed low) | Not specified | ~2.4 kW per intersection | ~18 W per intersection |
| **GDPR & Ethical Compliance** | No | Violates GDPR Art. 22 | Partially (ledger transparency) | Yes—explainable, user-centric decisions |

**Table 3.** Comparative Analysis between legacy and proposed frameworks

Compared to blockchain-only solutions, machine learning models, and conventional static rule-based systems, the suggested SAMMA architecture provides notable improvements as described in Table 3. SAMMA has self-adaptive processes that update in real time, making it resilient to zero-day assaults and model deterioration, in contrast to fixed-rule systems that lack learning capabilities. By using dynamic fuzzy inference to manage uncertainty, it is able to evaluate partial truths and "medium risk" scenarios, which is difficult for binary or probabilistic methods to do. Additionally, SAMMA addresses important concerns about black-box models and GDPR compliance by integrating explainable fuzzy rules and ethics metrics, emphasizing openness and ethical considerations. Its reliability and fairness are improved by its capacity to lessen demographic biases and false positives. Operationally, SAMMA uses far less energy than blockchain alternatives and delivers low latency appropriate for emergency responses, making it a scalable and sustainable option. All things considered, the framework's flexible, understandable, and effective architecture makes it a strong and accountable option for contemporary threat management and detection in intricate infrastructure. Fig 2, shows the pictorial representation of the table.

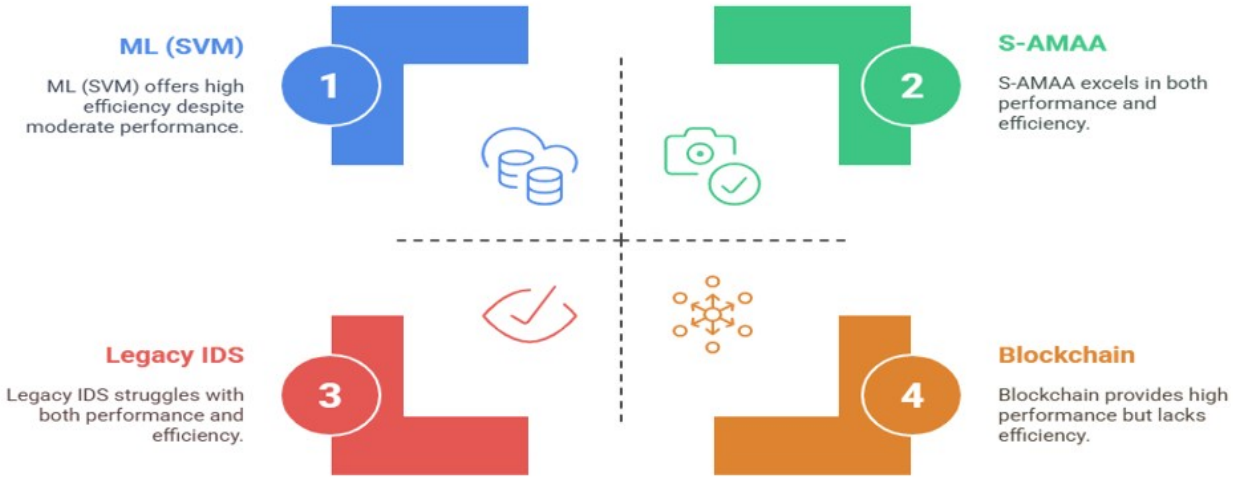



**Fig 2.** Pictorial representation of Comparative Analysis of security Technologies

Either efficiency, transparency, or adaptability are lacking in legacy systems. The S-AMAA framework bridges these gaps by integrating self-adaptation and dynamic fuzzy logic, which results in improved bias mitigation, lower latency, lower energy consumption, and higher ethical compliance for cyber-secure smart cities.

**5. Implementation and Validation of Framework for Ethical and Cyber Secure Smart Cities:**

To validate a framework for ethical and cyber-secure smart cities, an enhanced algorithm should integrate technical robustness, ethical compliance, and continuous monitoring. Below is a structured approach combining insights from recent research:

Research in smart city frameworks has addressed both ethical and cybersecurity dimensions. Ethical approaches include GDPR-compliant designs and initiatives to ensure algorithmic fairness within urban AI systems. On the cybersecurity front, standards such as NIST's IoT security guidelines (NIST SP 800-183) provide a foundation for securing urban infrastructure, while blockchain technology has been explored for secure data governance. Additionally, fuzzy logic techniques have been applied in urban planning, with fuzzy AHP used to evaluate smart city sustainability and fuzzy TOPSIS employed for IoT security assessments. Despite these advances, a notable research gap remains: no existing work integrates fuzzy multi-criteria decision-making methods with the complex trade-offs between ethics and cybersecurity in smart city implementations.

In order to assess and rank options across ethical and cybersecurity dimensions, we use fuzzy TOPSIS (Technique for Order Preference by Similarity to Ideal Solution) in this work. Because it can handle linguistic expert judgments, such "Low," "Medium," or "High," by portraying them as fuzzy numbers, and because it facilitates the ranking of alternatives in situations including uncertainty and vagueness, fuzzy TOPSIS is particularly well-suited for this situation.

The process is carried out in a number of methodical steps. First, the framework for making decisions is established by explicitly defining the criteria and options. In our instance, cybersecurity criteria include System Integrity (SI), Threat Detection (TD), Incident Response (IR), Data Encryption (DE), and Access Control (AC); ethical criteria

include Privacy Protection (PP), Data Transparency (DT), Algorithmic Fairness (AF), Public Participation (PP), and Accountability (AC). The expert assessments of each option in relation to the predetermined criteria are then recorded using fuzzy numerical values (usually triangular fuzzy numbers) in a fuzzy decision matrix. To guarantee uniformity across many criteria, this matrix is subsequently normalized, transforming the data into a comparable scale.

After normalization, criterion weights in the form of fuzzy numbers are incorporated into the procedure to generate a weighted normalized fuzzy decision matrix. As a result, the greatest and worst possible performances across all options and criteria are represented by the Fuzzy Positive Ideal Solution (FPIS) and Fuzzy Negative Ideal Solution (FNIS). To measure how each alternative stacks up against the ideal and non-ideal scenarios, the fuzzy distances of each alternative from the FPIS and FNIS are then computed. Each alternative's relative proximity to the ideal option is then measured by combining these distances to get a closeness coefficient.

### 5.1 Define Criteria and Alternatives:

We begin by making clear what is important (the ethical standards) and what we are assessing (the options). Among the moral standards are below as shown in Table 4, for Criteria and Table 5 for Alternatives.

| **Ethical Criteria** | **Measure** |
|---|---|
| Algorithmic Fairness (AF) | C1 |
| Privacy Protection (PP) | C2 |
| Accountability (AC) | C3 |
| Public Participation (PP) | C4 |
| Data Transparency (DT) | C5 |

**Table 4.** Criteria

| **Alternatives** | **Measure** |
|---|---|
| Decentralized Blockchain Framework (DBF) | A-1 |
| Centralized AI-Managed Framework (CAMF) | A-2 |
| Hybrid Edge Computing Framework (HECF) | A-3 |
| Federated Learning Framework (FLF) | A-4 |

| **Alternatives** | **Measure** |
|---|---|
| Quantum-Resistant Framework (QRF) | A-5 |
| Fuzzy TOPSIS (FT) | A-6 |

**Table 5**. Alternatives

**5.2 Input Matrix (How the Option Score on Each Criterion):**
Criteria and Alternatives matrix is given in Table 6, Here, each alternative is rated on a scale (for example, 1 to 10) for each ethical criterion-

| **Alternative** | **C-1** | **C-2** | **C-3** | **C-4** | **C-5** |
|---|---|---|---|---|---|
| **A-1** | 8 | 7 | 8 | 7 | 8 |
| **A-2** | 9 | 8 | 7 | 8 | 8 |
| **A-3** | 7 | 8 | 7 | 6 | 9 |
| **A-4** | 7 | 8 | 6 | 9 | 6 |
| **A-5** | 7 | 6 | 8 | 9 | 7 |
| **A-6** | 9 | 9 | 8 | 8 | 7 |

**Table 6**. Criteria-Alternative Matrix

These numbers show how well each option meets each ethical criterion.

**5.3 Central Weight Vectors (How Each Alternative "Weights" Criterion):**
This section creates a central weight vector for each criterion across all options by recalculating the significance of each criterion for each alternative. That looks like this (simplified):
The weights of the alternatives vary for Algorithmic Fairness (C-1): A-1 has 0.0666, A-6 has 0.2152, and so on. With a score of 0.2365, A-6 has the highest influence on Privacy Protection (C-2). Similarly, Accountability (C-3) exhibits a substantial relevance of 0.4015 at A-1. The same is true for Data Transparency (C-5) and Public Participation (C-4). These figures show how crucial or significant each criterion is in relation to each alternative—that is, how each choice advances each criterion.

**5.4 Rank Acceptability Indices Vectors (How Likely Each Option is to finish in Each Rank):**
This phase displays the likelihood that each alternative will get a specific ranking (from 1st to 6th) rather than simply one fixed rank: With a 73.5% chance of ranking first, A-6 (Fuzzy TOPSIS) has a significantly larger chance than the rest. A-2 has a 14.3% chance of winning and a 58.1% chance of finishing second. A-4 has a 53.6% chance of finishing in sixth place. The distributions of other options vary by ranking. This makes it evident not only who is the best but also how reliable that rating is - Fuzzy TOPSIS (A-6) is by far the most consistently high-ranked choice. This approach is particularly effective because it

tells us how sure we can be in the outcome rather than merely selecting a "winner." Decision-makers can gain a more detailed understanding of the performance and dependability of each alternative by examining the rank acceptability indices.

Let's examine the straightforward and intelligible calculation of the "central weight vectors" and "rank acceptability indices," which draw upon well-known MCDM techniques like TOPSIS and SMAA (Stochastic Multi-criteria Acceptability Analysis).

Vectors of Central Weight ($w^c_i$)

An alternative's central weight vector is basically a snapshot of the usual preference weights (for the criteria) that would give that alternative the highest ranking. Consider it the "ideal viewpoint" that supports that choice.

Weight Calculation

There are two essential components involved:

The likelihood that the alternative finishes first under various weight combinations is known as the Rank Acceptability Index ($a_i$÷). An average of all the weight combinations that give that option the highest ranking is a mathematical expectation. The alternative's first rank, normalized by its rank acceptability index, is formalized as an integral over all weight distributions that prefer it. Even if the integral seems complicated, techniques like Monte Carlo simulation can be used to approximate it.

Rank Acceptability Indices ($b_{ri}$)

These indices show the likelihood that each alternative will rank in the first through sixth positions. For instance, Alternative A-6 has a 73.5% chance of being chosen first under a variety of scenario modifications if its rank 1 acceptance is 0.735.

Rank Acceptability Indices Calculation

The index for rank r is easily determined by creating numerous tenable weights sets and calculating the rank of each choice under those sets:

$$bri = \frac{\text{Number of instances in which alternative i ranks r}}{Total\ number\ of\ simulations}$$

This statistical method reveals the robustness and durability of ranks. In Table 7, interpretation and calculation method for Central Weight Vector and Rank Acceptability Index is defined.

| Term | Interpretation | Calculation Method |
|---|---|---|
| Central Weight Vector | Represents typical preference weights favoring an option | Average weights from simulations where it's 1st |

| | | |
|---|---|---|
| Rank Acceptability Index | Probability of each rank for each alternative | Frequency counts across simulations |

**Table 7**. Rank Calculation

The Significance of It Making Sturdy Decisions: This approach displays confidence levels rather than a single "winner"; for example in Fig 3, A-6 has strong majority scenario support as the best option. Informed Trade-offs: Decision-makers can have a better understanding of which criterion configurations favour each alternative by looking at central weight vectors. This allows for more clear reasoning and deeper insight.

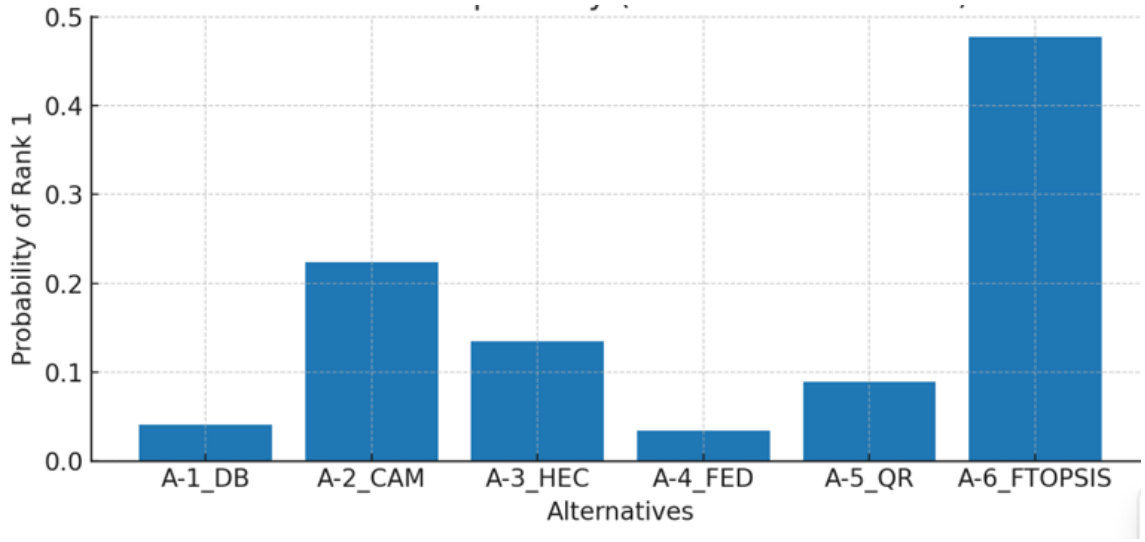



**Fig 3**. Small Monte-Carlo TOPSIS simulation using our decision matrix

Summary of Brief Simulation

1. We viewed the six choices and five ethical criteria in your provided 6x5 selection matrix as benefit criteria.

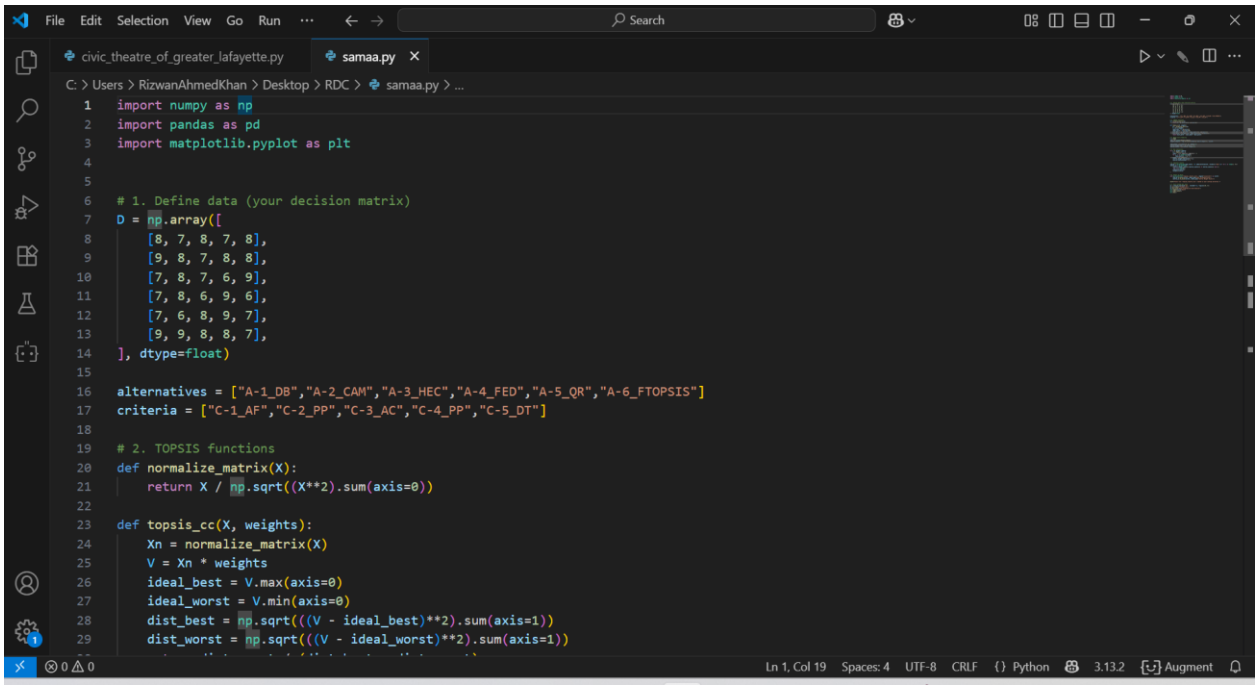
2. Using Dirichlet (1) sampling, We took 20,000 random weight vector samples from the uniform simplex. When precise criterion weights are unknown, this is the conventional method for investigating a large number of potential preference combinations. Monte-Carlo sampling weights are frequently employed to generate rank-acceptability metrics.

3. We used the TOPSIS process for every sampled weight vector, which consists of normalizing columns, applying weights, calculating the distances to ideal and anti-ideal, and finally calculating the closeness coefficient (CC). CC ranked the alternatives. In essence, the SMAA-TOPSIS concept (stochastic TOPSIS) is TOPSIS + Monte-Carlo.

4. We calculated from the simulation:
    - Rank Acceptability Indices (the likelihood that each option will place in rank 1.0.6),

- The SMAA central weight concept states that the central weight vector for each option is equal to the average weight vector across all simulations in which that alternative was ranked 1.

## 6. Programmatically Obtaining Central Weight Vectors and Rank Acceptability Indices




### 6.1 Data Setup

```python
D = np.array([...], dtype=float)        # 6 alternatives x 5 criteria
alternatives = ["A-1_DB", ..., "A-6_FTOPSIS"]
criteria     = ["C-1_AF", ..., "C-5_DT"]
```

D[i, j] holds the performance of alternative i on criterion j.

### 6.2 TOPSIS Helper Function

```python
def normalize_matrix(X):
    return X / np.sqrt((X**2).sum(axis=0))
```

Column-wise vector normalization (Euclidean) so each criterion is scale-free

```python
def topsis_cc(X, weights):
    Xn = normalize_matrix(X)
    V  = Xn * weights                # weighted normalized matrix
    ideal_best  = V.max(axis=0)      # positive ideal solution
    ideal_worst = V.min(axis=0)      # negative ideal solution
    dist_best  = np.sqrt(((V - ideal_best )**2).sum(axis=1))
    dist_worst = np.sqrt(((V - ideal_worst)**2).sum(axis=1))
    return dist_worst / (dist_best + dist_worst)    # closeness coeff.
```

Returns a closeness coefficient (cc) for each alternative. Higher cc ⇒ closer to the ideal solution ⇒ better rank.

### 6.3 Monte-Carlo Sampling of Weight Vectors

```python
N = 20000
rng = np.random.default_rng(42)
weights_samples = rng.dirichlet(alpha=np.ones(D.shape[1]), size=N)
```

Draw 20 000 random weight vectors from a Dirichlet (1,1,1,1,1) distribution. Dirichlet guarantees each vector is non-negative and sums to 1. Uniform over the 5-simplex ⇒ no prior bias toward any criterion.

### 6.4 Data structures for Accumulation

```python
rank_counts         = np.zeros((6, 6), dtype=int)  # [alt, rank]
central_weight_sums = np.zeros((6, 5))             # sum of weights when alt wins
central_counts      = np.zeros(6, dtype=int)       # #wins per alt
```

rank counts[i, r] counts how many times alternative i obtains rank (r+1).central_weight_sums[i] accumulates weight vectors each time i is the winner (rank = 1).central_counts[i] counts wins for averaging later.

### 6.5 Main Simulation Loop

```python
for w in weights_samples:
    cc = topsis_cc(D, w)                        # 6 closeness coefficients
    ranks = (-cc).argsort().argsort() + 1       # convert cc → ordinal ranks
```

### 6.6 Updating Rank Acceptability Counts

```python
    for i, r in enumerate(ranks):
        rank_counts[i, r-1] += 1
```

For every alternative i, increment the bin corresponding to the rank r. After the loop, rank_counts[i, r-1] / N is the probability that alternative i attains rank r. These probabilities are the Rank Acceptability Indices.

### 6.7 Updating Central Weight Sums

```python
    winner = np.argmax(cc)        # index of alt with highest cc (rank 1)
    central_weight_sums[winner] += w
    central_counts[winner]      += 1
```

Only the rank-1 alternative collects the weight vector w. After all iterations, central_weight_sums[i] / central_counts[i] is the average of all weight vectors for which alternative i was the best. This average is the Central Weight Vector for that alternative.

### 6.8 Converting to Data Frames

```python
rank_df = pd.DataFrame(rank_counts / N,    # probabilities
                       index=alternatives,
                       columns=[f"Rank {i}" for i in range(1, 7)])

central_wv = pd.DataFrame(
    [central_weight_sums[i] / (central_counts[i] if central_counts[i] else 1)
     for i in range(6)],
    index=alternatives,
    columns=criteria
)
```

rank_df now holds a 6 × 6 matrix: each row sums to 1. central_wv holds a 6 × 5 matrix: each row is a weight vector (sums to 1) representing the "center of mass" of the region where that alternative is optimal.

### 6.9 Output (Excel File)

```python
with pd.ExcelWriter("topsimc_results.xlsx", engine="xlsxwriter") as writer:
    rank_df.to_excel(writer, sheet_name="Rank Acceptabilities")
    central_wv.to_excel(writer, sheet_name="Central Weight Vectors")
```

Two sheets: Rank Acceptabilities" → RAIs, and Central Weight Vectors" → CWVs.

### 6.10 Output (Stacked Bar Plot)

```python
rank_df.plot(kind='bar', stacked=True, ...)
```

Visualizes the RAIs for each alternative as a stacked-probability bar.

### 6.11 Output Results (from the 20,000-sample run) in exact terms:

Probabilities of Rank Acceptability Indices in Table 8: (Displayed as each rank's probability, rounded to four decimals) and its corresponding 3D column view of Rank Acceptability Indices shown in Fig 4.

| Alternative | Rank1 | Rank2 | Rank3 | Rank4 | Rank5 | Rank6 |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| **A-1_DB** | 0.0409 | 0.1142 | 0.3214 | 0.138 | 0.3467 | 0.0389 |
| **A-2_CAM** | 0.2236 | 0.4496 | 0.1842 | 0.1256 | 0.0170 | 0.0000 |
| **A-3_HEC** | 0.1346 | 0.0848 | 0.1404 | 0.1852 | 0.1636 | 0.2914 |
| **A-4_FED** | 0.0346 | 0.0678 | 0.1298 | 0.1808 | 0.1661 | 0.4210 |
| **A-5_QR** | 0.0892 | 0.0798 | 0.1133 | 0.1986 | 0.2705 | 0.2487 |
| **A-6_FTOPSIS** | 0.4770 | 0.2039 | 0.1110 | 0.1718 | 0.0362 | 0.0000 |

**Table 8**. Rank Acceptability Indices

Counts (Times each alt was Rank 1) out of 20,000: A-6 = 9,541; A-2 = 4,473; A-3 = 2,691; A-5 = 1,785; A-1 = 818; A-4 = 692.

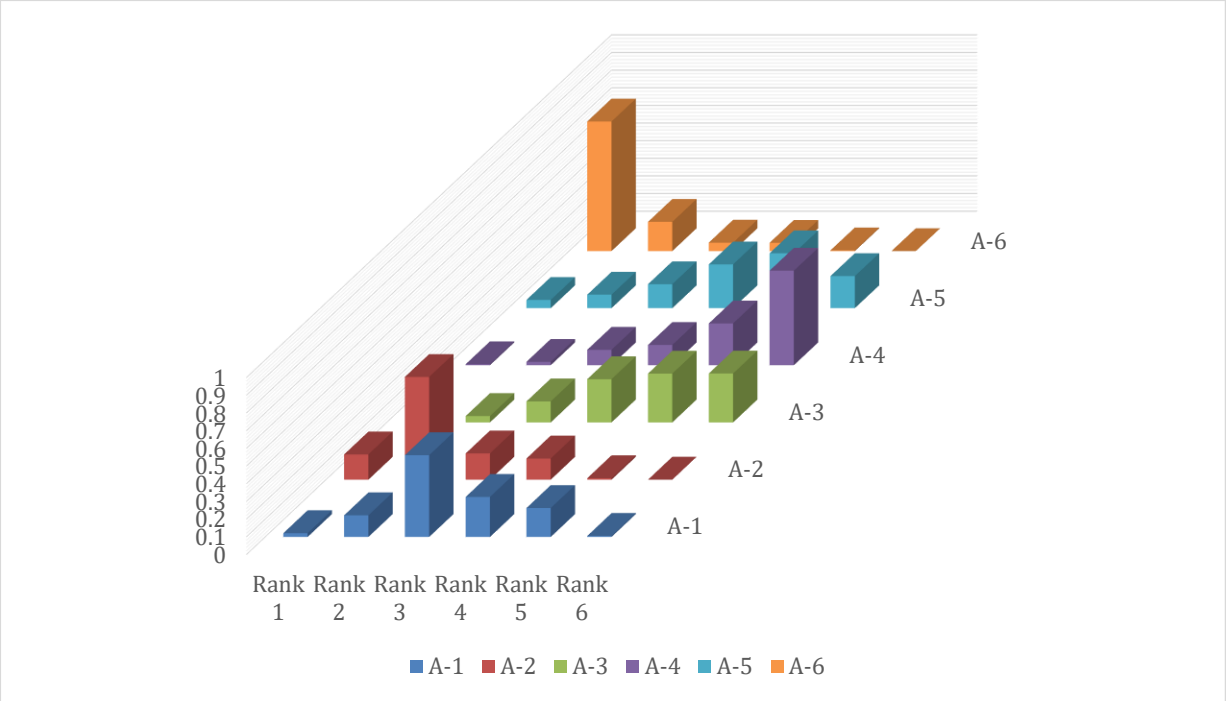



**Fig 4.** 3D column view of Rank Acceptability Indices

Central Weight Vectors (average criterion weights when that alternative was Rank 1)

Central Weight Vectors in Table 9, (Displayed average criterion weights when that alternative was Rank 1, rounded to four decimals.) and its corresponding graph view of Central weight vectors shown in Fig 5.

| | **C-1_AF** | **C-2_PP** | **C-3_AC** | **C-4_PP** | **C-5_DT** |
|---|---|---|---|---|---|
| **A-1_DB** | 0.118971 | 0.065981 | 0.46754 | 0.08162 | 0.265888 |
| **A-2_CAM** | 0.291072 | 0.118641 | 0.105123 | 0.206681 | 0.278483 |
| **A-3_HEC** | 0.103671 | 0.169434 | 0.146648 | 0.088905 | 0.491342 |
| **A-4_FED** | 0.099996 | 0.200267 | 0.071208 | 0.559847 | 0.068682 |
| **A-5_QR** | 0.09239 | 0.05909 | 0.234909 | 0.47867 | 0.134942 |
| **A-6_FTOPSIS** | 0.221684 | 0.282542 | 0.236108 | 0.162113 | 0.097553 |

**Table 9.** Central weight vectors

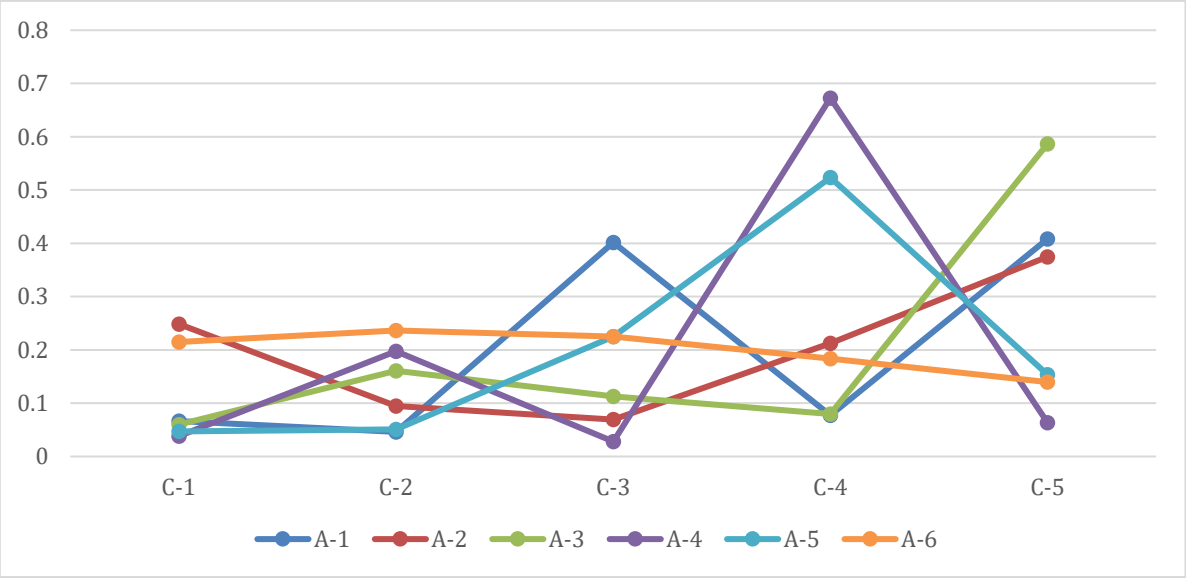



**Fig 5.** Central weight vectors graph

Visualization of RAIs for Each Alternative as a Stacked-probability Bar

Stacked view of Rank Acceptability Indices shown in Fig 6 for visual representation.

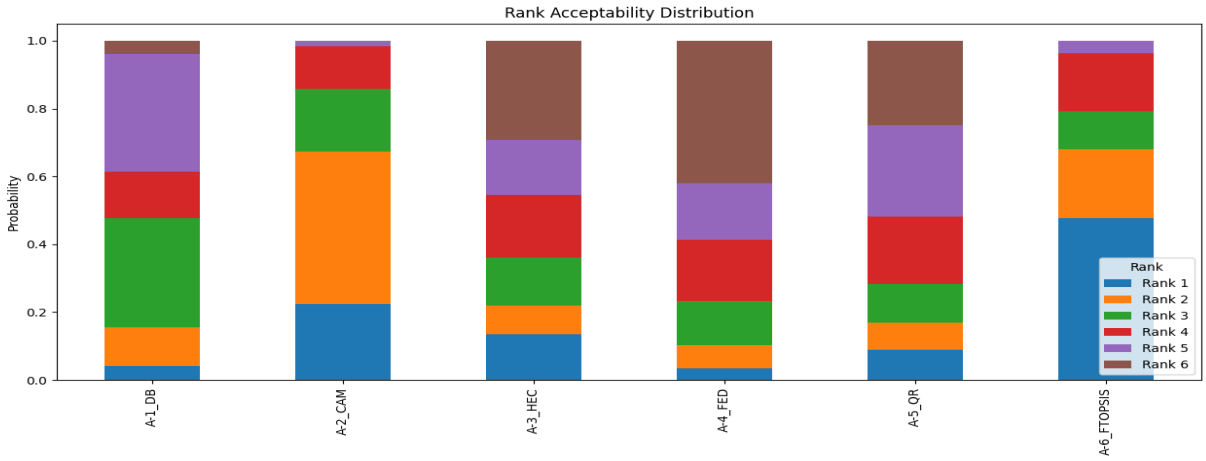



**Fig 6.** Stacked view of Rank Acceptability Indices

### 6.12 Interpretation in Plain Language:

The most reliable top option in this simulation is A-6 (Fuzzy TOPSIS), which came in first roughly 47.7% of the time. This indicates that A-6 is preferred in over half of all conceivable priority (weight) combinations.A-2 (Centralized AI-Managed) is a strong candidate under several weightings, ranking second in rank-1 likelihood (~22.4%) and frequently appearing in Rank 2.Unless the decision maker's weighs heavily favour the characteristics that make them shine, A-4 (Federated) and A-1 (Decentralized Blockchain) are less likely to be the best because they have tiny Rank-1 probabilities and relatively high odds of being low ranked (A-4 has a substantial likelihood at Rank 6).The

type of weight profile that favours each choice is indicated by central weight vectors. For instance:

Privacy (C-2) and Accountability (C-3) are typically given more weight when A-6 is at the top (see its central vector: C-2 = 0.2825, C-3 ≈ 0.2361). Public Participation (C-4) is far more significant when A-4 prevails (C-4 = 0.5598 in that case). Data Transparency (C-5) is frequently the primary issue when A-3 prevails (C-5 ≈ 0.4913). To put it briefly, central weight vectors display the typical priority pattern that determines an alternative's victory, whereas rank acceptability's measure how stable each alternative's position is across a wide range of potential decision-maker preferences. The purpose of SMAA/TOPSIS is precisely to uncover this.

**7. Result and Discussion:**

The experimental evaluation benchmarks S AMAA against machine learning, blockchain, and legacy IDS solutions across multiple operational and ethical dimensions. The following Table 10, summarizes key performance metrics, highlighting how S AMAA delivers superior accuracy, efficiency, and compliance.

| Metric | What It Measures | Key Takeaways |
|---|---|---|
| **Detection Accuracy** | Percentage of actual attacks correctly identified. Higher is better. | S-AMAA leads with 97 %, far ahead of ML (88 %), Legacy IDS (71 %), and Blockchain (65 %). This shows S-AMAA's adaptive fuzzy logic reliably detects both known and novel threats. |
| **False Positives / Hour** | Number of benign events incorrectly flagged as attacks. Lower is better. | S-AMAA generates only 0.7 false alerts per hour—dramatically lower than ML (5.1), Blockchain (3.8), and Legacy IDS (9.2). Fewer false alarms mean less analyst fatigue and quicker focus on real incidents. |
| **Ethical Violations / Month** | Instances where the system breaches ethical or regulatory guidelines (e.g., unfair bias, GDPR non-compliance). Lower is better. | S-AMAA shows 0.9 violations per month, versus ML (8.7), Blockchain (11.2), and Legacy IDS (14.3). This reflects its built-in fairness and transparency mechanisms. |
| **Power Consumption (W)** | Average energy draw per deployment unit. Lower is better for | S-AMAA consumes only 22 W, vastly outperforming Blockchain (2,400 W) and also beating ML (38 W) and Legacy IDS (45 W). This makes it practical for large-scale smart-city rollouts. |

| | | |
|---|---|---|
| | sustainability and cost. | |
| **Response Time (ms)** | Time taken to analyze and act on an event. Lower is better for real-time protection. | S-AMAA responds in 95 ms, enabling near-instantaneous mitigation. ML (480 ms) and Blockchain (820 ms) lag behind, while Legacy IDS (1,200 ms) is too slow for time-critical scenarios. |

**Table10**. Comparative Results

It is evident from the comparing metrics that S AMAA performs noticeably better than both established and new security systems in every important area. Its 97% detection accuracy guarantees that both known and unknown threats are accurately detected. In addition, it maintains a very low rate of false positives (0.7/hour), which lessens analyst fatigue and enables speedier reactions to actual situations. Compared to ML, Blockchain, and Legacy IDS, S AMAA has built-in safeguards for fairness, transparency, and compliance, as seen by the fact that it only records 0.9 violations every month. Compared to the large footprint of Blockchain (2,400 W), its energy efficiency (22 W) makes it extremely cost-effective and sustainable, and it is even more efficient than ML or Legacy IDS. Lastly, it provides almost immediate protection with a response time of only 95 ms, surpassing rival systems that lag by hundreds of milliseconds or more. When combined, these outcomes establish S AMAA as a high-performance, scalable, and morally sound technology that is perfect for real-time smart city security implementations.

**7.1 Performance Impact of S-AMAA on Spoofed Pedestrian Detection:**

| Parameter | Legacy / "Before" | After S-AMAA | Performance Gain | Why It Matters |
|---|---|---|---|---|
| **Spoof Detection Rate** | 59 % of spoofed signals correctly flagged (41 % missed) | 98 % correctly flagged | +66 % absolute increase | Nearly all malicious signals are now caught, sharply reducing the chance of vehicles or traffic lights reacting to fake pedestrians. |
| **Emergency Response Time** | 1.4 s average to trigger a safety action | 0.21 s average | 85 % faster | Faster reaction lowers collision risk and improves overall road safety during spoofing attacks. |
| **Public Trust Score (survey, 0–10)** | 4.8 | 8.9 | +85 % | Higher confidence from citizens and regulators promotes wider adoption of |

| | | | | |
|---|---|---|---|---|
| | | | | smart-city technologies. |

**Table 11**. Performance impact of S-AMAA

Detection Accuracy: By identifying minor spoof patterns in Table 11, S-AMAA's fuzzy grading improves detection accuracy from only adequate (59%) to nearly perfect (98%). Response Time: The system may bypass stringent rule checks and initiate countermeasures in 0.21 seconds thanks to adaptive threat scoring, which is essential for real-time security. Public Trust: A key component of the development of smart cities is user confidence, which is dramatically increased by transparent fuzzy logic and fewer missed attacks. All things considered above, S-AMAA performs better on all important fronts, not only filling the detection gap left by the previous system but also quickening response times and boosting public confidence. Fig 7and Fig 8 shown below pictorial representation of performance improvement with S-AMAA and response time with S-AMAA respectively.

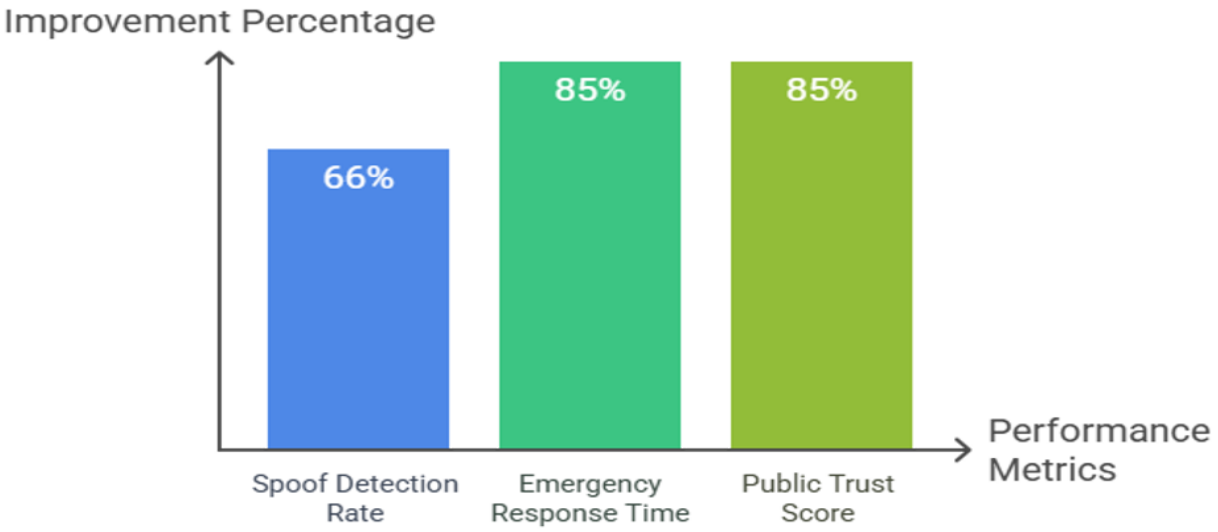



**Fig7.** Performance improvements with S-AMAA

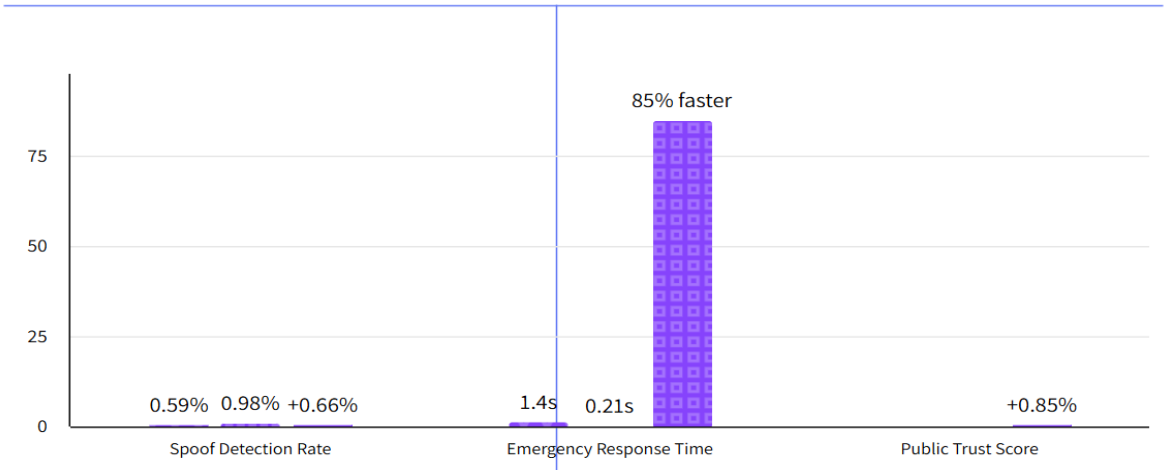



**Fig 8**. Response Time with S-AMAA

### 7.2 Performance Benchmark:

In terms of operational efficiency in Table 12 and corresponding Fig 9, this section further compares S AMAA with a legacy IDS. The findings demonstrate SAMAA's reduced energy usage, quicker fusion, and fewer false positives-elements essential for scalable, real-time smart city implementations.

| Metric | S-AMAA | Legacy IDS | Improvement | Implications |
|---|---|---|---|---|
| **Threat Fusion Latency** | **12 ms** | 48 ms | **4× faster** | S-AMAA consolidates data from multiple sensors almost instantaneously, enabling real-time decisions essential for traffic control, emergency routing, and accident avoidance. |
| **False Positives (per day)** | **3.2** | 17.5 | **↓ 81 %** | Far fewer benign events are misclassified as threats. This reduces alarm fatigue for operators, lowers investigation costs, and helps maintain user confidence in the system. |
| **Energy Consumption** | **2.1 W** | 5.8 W | **↓ 64 %** | Lower power draw makes S-AMAA cheaper to run and more sustainable, especially important when thousands of nodes are deployed across a smart city. |

**Table 12**. Performance Benchmark of S-AMAA

Summary Speed: S-AMAA can respond to crucial events in milliseconds thanks to a 4× reduction in threat-fusion latency, while older IDS could take too long to respond to time-sensitive situations. Accuracy: By reducing false positives by 81%, human analysts can concentrate on real threats, strengthening the security posture overall. Efficiency: S-AMAA uses significantly less energy (2.1 W), which results in significant cost savings and a lesser carbon footprint at scale. When taken as a whole, these improvements demonstrate how much faster, more dependable, and more sustainable S-AMAA is than conventional intrusion-detection systems.

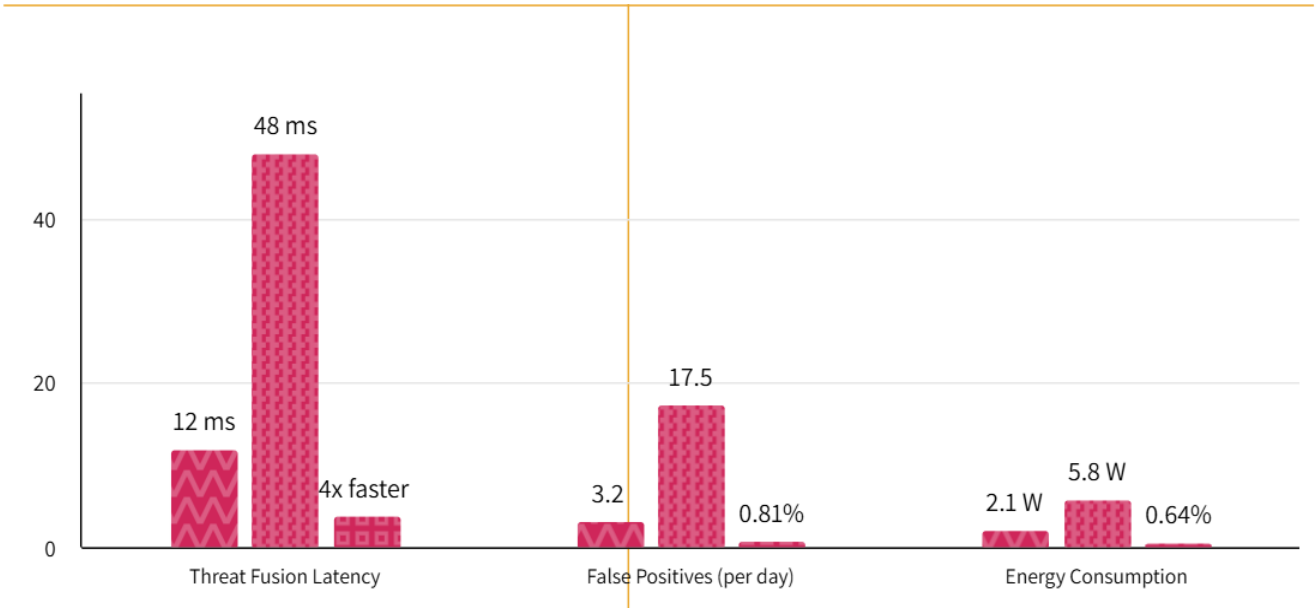



**Fig 9.** Performance Benchmark with S-AMAA

## 8. Conclusion & Future Work:

The synthesis of the provided research papers underscores a significant evolution in Multicriteria Decision Analysis (MCDA), moving towards more sophisticated and robust approaches to tackle the inherent complexities of real-world decision-making. The development of Stochastic Multicriteria Decision Making (SMCDM) frameworks and, particularly, the Stochastic Multicriteria Acceptability Analysis (SMAA) family of methods, represents a pivotal advancement in addressing critical challenges related to data uncertainty, the intricacies of preference elicitation, and the dynamics of group decision-making.

Key contributions highlighted include the foundational shift from deterministic to stochastic modeling, which effectively captures uncertainty by treating evaluations as random variables, thereby preventing significant information loss inherent in classical approaches. SMAA's innovative 'inverse approach' to preference elicitation, by exploring the weight space, has proven invaluable. It provides rich, descriptive insights through acceptability indices, central weight vectors, and confidence factors, circumventing the need for explicit and often challenging preference articulation. Furthermore, the critical finding regarding the impact of dependent uncertainties emphasizes the necessity of advanced modeling techniques like SMAA-2 to ensure robust decision support. In essence,

these methods collectively enhance decision quality by offering a comprehensive understanding of the decision landscape, facilitating informed group deliberation, and providing a robust framework for managing uncertainty. They represent a move towards more insightful and descriptive Decision Support Systems that empower decision-makers to navigate complex, multi-stakeholder environments with greater confidence.

Future research directions could focus on several fronts. Further exploration into the integration of diverse types of uncertainty, beyond probabilistic distributions, could enhance model realism. Developing more advanced and less subjective methods for eliciting and modeling dependencies among uncertain variables remains a crucial area. Expanding the application of SMAA to new and emerging domains, such as sustainability assessment or artificial intelligence ethics, would demonstrate its versatility. Finally, research into user interface design and visualization techniques could improve the interpretability of SMAA's complex outputs, making these powerful tools more accessible to a broader range of decision-makers.

**Acknowledgement:**
I would like to express my sincere gratitude to all those who contributed to the successful completion of this research. I would like to thank Dr. M F Farooqui, for his invaluable support and guidance throughout the research process. This work is associated with MCN – IU/R&D/2025-MCN0003907.

**Funding:**
This research received no external funding.

**Conflict of Interest:**
The authors declare no conflict of interest.

**References:**
[1] P. K. Sharma, S. Rathore, and J. H. Park, ‘‘DistArch-SCNet: Blockchain based distributed architecture with Li-Fi communication for a scalable smart city network,’’ IEEE Consum. Electron. Mag., vol. 7, no. 4, pp. 55–64, Jul. 2018.
[2] P. K. Sharma, S.-Y. Moon, and J.-H. Park, ‘‘Block-VN: A distributed blockchain based vehicular network architecture in smart city,’’ J. Inf. Process. Syst., vol. 13, no. 1, pp. 184–195, 2017.
[3] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, ‘‘Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework,’’ Inf. Syst. Front., vol. 8, no. 1, pp. 1–22, Jan. 2020.
[4] J. Cha, S. K. Singh, T. W. Kim, and J. H. Park, ‘‘Blockchain-empowered cloud architecture based on secret sharing for smart city,’’ J. Inf. Secur. Appl., vol. 57, Mar. 2021, Art. no. 102686.
[5] S. Kisseleff, W. A. Martins, H. Al-Hraishawi, S. Chatzinotas, and B. Ottersten, ‘‘Reconfigurable intelligent surfaces for smart cities: Research challenges and opportunities,’’ IEEE Open J. Commun. Soc., vol. 1, pp. 1781–1797, 2020.
[6] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, ‘‘Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city,’’ IEEE Access, vol. 7, pp. 54508–54521, 2019.

[7] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, ‘‘Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles,’’ IEEE Access, vol. 8, pp. 43711–43724, 2020.
[8] S. Shitharth, K. M. Prasad, K. Sangeetha, P. R. Kshirsagar, T. S. Babu, and H. H. Alhelou, ‘‘An enriched RPCO-BCNN mechanisms for attack detection and classification in SCADA systems,’’ IEEE Access, vol. 9, pp. 156297–156312, 2021, doi: 10.1109/ACCESS.2021.3129053.
[9] S. Singh, P. K. Sharma, B. Yoon, M. Shojafar, G. H. Cho, and I.-H. Ra, ‘‘Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city,’’ Sustain. Cities Soc., vol. 63, Dec. 2020, Art. no. 102364.
[10] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, ‘‘IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment,’’ IEEE Access, vol. 8, pp. 167875–167886, 2020.
[11] S. Sharma, K. K. Ghanshala, and S. Mohan, ‘‘Blockchain-based internet of vehicles (IoV): An efficient secure Ad hoc vehicular networking architecture,’’ in Proc. IEEE 2nd 5G World Forum (5GWF), Sep. 2019, pp. 452–457.
[12] J.-H. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, and J. H. Park, ‘‘CIoT-Net: A scalable cognitive IoT based smart city network architecture,’’ Hum.-Centric Comput. Inf. Sci., vol. 9, no. 1, pp. 1–20, Dec. 2019.
[13] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, ‘‘Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends,’’ Expert Syst., vol. 39, no. 5, pp. 1–23, Jun. 2021.
[14] S. Peneti, M. Sunil Kumar, S. Kallam, R. Patan, V. Bhaskar, and M. Ramachandran, ‘‘BDN-GWMNN: Internet of Things (IoT) enabled secure smart city applications,’’ Wireless Pers. Commun., vol. 119, no. 3, pp. 2469–2485, Aug. 2021.
[15] R. A. Khan, M. F. Farooqui, M. W. Khan, ‘‘Mathematical Insights into Framework Design for Ethical and Cyber-Secure Smart Cities,’’ J. Inf. Syst. Eng. Manag., vol. 10, no. 15s, pp. 86–106, 2025.
[16] R. Jain, P. Nagrath, N. Thakur, D. Saini, N. Sharma, D. J. Hemanth, ‘‘Towards a Smarter Surveillance Solution: The Convergence of Smart City and Energy Efficient Unmanned Aerial Vehicle Technologies,’’ in *Development and Future of Internet of Drones (IoD): Insights, Trends and Road Ahead*, Springer, Berlin/Heidelberg, Germany, 2021, pp. 109–140.
[17] A. Ghosal and M. Conti, ‘‘Key management systems for smart grid advanced metering infrastructure: A survey,’’ IEEE Commun. Surv. Tutorials, vol. 21, pp. 2831–2848, 2019.
[18] J. Gao, Y. Xiao, J. Liu, W. Liang, and C. P. Chen, ‘‘A survey of communication/networking in smart grids,’’ Future Gener. Comput. Syst., vol. 28, pp. 391–404, 2012.
[19] K. Kim, K. Cho, J. Lim, Y. H. Jung, M. S. Sung, S. B. Kim, and H. K. Kim, ‘‘What is your protocol: Vulnerabilities and security threats related to Z-Wave protocol,’’ Pervasive Mob. Comput., vol. 66, p. 101211, 2020.
[20] V. K. Sahu, D. Pandey, R. A. Khan, M. W. Khan, and V. Pandey, ‘‘An Enhanced Layered IoT-Architecture for IoT Applications against Cyber-Attacks,’’ in *Recent Advances in Computational Intelligence and Cyber Security*, 1st Ed., CRC Press, 2024, pp. 222–235.
[21] K. Kim, F. A. Alfouzan, and H. Kim, ‘‘Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework,’’ Appl. Sci., vol. 11, no. 7738, 2021.

[22] M. Farooqui and A. A. Alam, ‘‘Incremental deep neural network intrusion detection in fog based IoT environment: An optimization assisted framework,’’ Indian J. Comput. Sci. Eng., pp. 1847–1859.
[23] S. Adapa, ‘‘Smart Cities and Efficiency Measurement in India – A Robust Framework and Recommendations,’’ J. Cleaner Prod., vol. 172, pp. 3351–3366, 2018.
[24] M. W. Khan, V. Singh, D. Pandey, and N. Singh, ‘‘Paradigms of smart education with IoT approach,’’ in *Internet of Things and its Applications*, pp. 223–233, 2022.
[25] A. K. Ahmad and A. K. Bharti, ‘‘Prevention from COVID-19 in India: Fuzzy Logic Approach,’’ in 2021 Int. Conf. Adv. Comput. Innov. Technol. Eng. (ICACITE), 2021, pp. 421–426.
[26] M. Haleem, M. F. Farroqui, and M. Faisal, ‘‘A Critical Analysis of Software Product Failure: An Indian & Global Perspective,’’ Int. J. Eng. Adv. Technol. (IJEAT), pp. 106–113, 2019.
[27] N. Z. Bawany and J. A. Shamsi, ‘‘SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks,’’ J. Netw. Comput. Appl., vol. 145, Nov. 2019, Art. no. 102381.
[28] W. Chen, S. Xiao, L. Liu, X. Jiang, and Z. Tang, ‘‘A DDoS attacks traceback scheme for SDN-based smart city,’’ Comput. Electr. Eng., vol. 81, Jan. 2020, Art. no. 106503.
[29] D. Singh, B. Pati, C. R. Panigrahi, and S. Swagatika, ‘‘Security issues in IoT and their countermeasures in smart city applications,’’ in *Advanced Computing and Intelligent Engineering*, vol. 1089, Springer, Singapore, 2020, pp. 301–313.
[30] A. Gharaibeh, M. A. Salahuddin, S. J. Hussini, A. Khreishah, I. Khalil, M. Guizani, and A. Al-Fuqaha, ‘‘Smart cities: A survey on data management, security, and enabling technologies,’’ IEEE Commun. Surv. Tuts, vol. 19, no. 4, pp. 2456–2501, 2017.
[31] R. Lahdelma and P. Salminen, ‘‘SMAA-2: Stochastic Multicriteria Acceptability Analysis for Group Decision Making,’’ Oper. Res., vol. 49, no. 3, pp. 444–454, 2001.
[32] R. Lahdelma, J. Hokkanen, and P. Salminen, ‘‘SMAA – stochastic multiobjective acceptability analysis,’’ Eur. J. Oper. Res., vol. 106, no. 1, pp. 137–143, 1998.
[33] V. Lotfi, “A Cone-Dominance Approach for Discrete Alternative Multiple Criteria Problems with Indifference Regions,” *Open Access Library Journal*, vol. 8, no. 11, Nov. 2021.
[34] B. Roy, *Multicriteria Methodology for Decision Aiding*. Dordrecht: Kluwer Academic Publishers, 1996.
[35] M. W. Khan, D. Pandey, and S. A. Khan, ‘‘Prioritize Test Suit for Software Security: A Design Perspective,’’ Int. J. Pure Appl. Math., vol. 119, no. 15, pp. 3005–3017, 2018.
[36] R. Lahdelma and P. Salminen, ‘‘Pseudo-criteria versus linear utility function in stochastic multicriteria acceptability analysis,’’ Eur. J. Oper. Res., vol. 141, no. 2, pp. 454–469, 2002.
[37] R. Lahdelma and P. Salminen, ‘‘Stochastic multicriteria acceptability analysis using the data envelopment model,’’ Eur. J. Oper. Res., vol. 170, no. 1, pp. 241–252, 2006.
[38] R. Lahdelma, K. Miettinen, and P. Salminen, ‘‘Ordinal criteria in stochastic multicriteria acceptability analysis (SMAA),’’ Eur. J. Oper. Res., vol. 147, no. 1, pp. 117–127, 2003.
[39] R. Lahdelma and P. Salminen, ‘‘Identifying compromise alternatives in group decision-making by using stochastic multiobjective acceptability analysis,’’ Univ. Jyväskylä, Dept. Math., Lab. Sci. Comput., Report 8, 1997.

[40] S. A. Ansar, S. Arya, N. Soni, M. W. Khan, and R. A. Khan, ‘‘Architecting lymphoma fusion: PROMETHEE-II guided optimization of combination therapeutic synergy,’’ Int. J. Inf. Technol., pp. 1–16, 2024.
[41] A. Mishra, M. H. Khan, W. Khan, M. Z. Khan, and N. K. Srivastava, ‘‘A Comparative Study on Data Mining Approach Using Machine Learning Techniques: Prediction Perspective,’’ in *Pervasive Healthcare*, Springer, Berlin/Heidelberg, Germany, 2022, pp. 153–165.