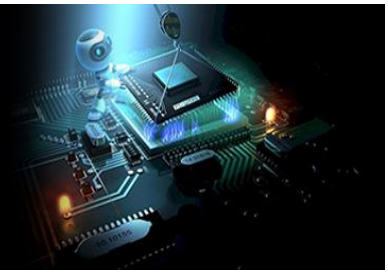
International Journal of Engineering in Computer Science



E-ISSN: 2663-3590
P-ISSN: 2663-3582
Impact Factor (RJIF): 5.52
www.computersciencejournals.com/ijecs
IJECS 2026; 8(1): 68-74
Received: 02-11-2025
Accepted: 05-12-2025

Rizwan Ahmed Khan
Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India

Mohd Faizan Farooqui
Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India

Corresponding Author:
Rizwan Ahmed Khan
Department of Computer Application, Integral University, Lucknow, Uttar Pradesh, India

Validation of performance impact in S-AMMA using AHP-A multi-criteria decision-making approach

Rizwan Ahmed Khan and Mohd Faizan Farooqui

DOI: https://www.doi.org/10.33545/26633582.2026.v8.i1b.250

Abstract
Purpose: This paper aims to evaluate performance improvements enabled by the S-AMAA (Smart Adaptive Multi-Agent Architecture) framework using two well-known decision-making models: the Technique for Order of Preference by Similarity to the Analytic Hierarchy Process (AHP). This study aims to investigate Multi-Criteria Decision-Making (MCDM) methodologies to examine the extent to which they work in specific circumstances and the general performance of S-AMAA.
Objective: This study aims to evaluate the performance effect of S-AMAA using AHP, two of the most popular decision-making techniques. The study aims to identify the main performance criteria, demonstrate the soundness of the S-AMAA framework, and compare its performance with other methods. The study will also help improve the reliability and applicability of S-AMAA in real-world settings by using rigorous verification and validation methods.
Methodology: In this research, the complex performance factors of S-AMAA will be hierarchically divided using AHP, and the criteria can thus be prioritised using expert knowledge. The ranking of alternatives will then be done using TOPSIS, which will determine the best and most effective configuration of the framework. The methodology integrates two MCDM methods to provide a comprehensive appraisal of S-AMAA's performance, accounting for both subjective and objective factors.
Tryouts: Validation and verification will include testing S-AMAA under various conditions and using performance indicators to assess its flexibility, effectiveness, and scalability. Both real-world applications will be used to collect data and evaluate the consistency of the results across different situations. Such try-outs will enable the study to streamline the decision-making model and ensure the findings are representative and actionable in future applications of S-AMAA across other fields.

Keywords: Smart cities, security, S-AMAA, AHP, validation

1. Introduction
Smart Cities represent a philosophy that integrates high-quality technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and Big Data analytics to enhance urban living standards. The adoption of these technologies enables cities to become more sustainable, better governed, and more efficient in resource management, while also delivering improved services to citizens. However, the rapid and often uncontrolled expansion of smart cities introduces a range of complex challenges, particularly in terms of ethical considerations and cybersecurity risks. As interconnectivity among smart city systems increases, so do the threats related to privacy invasion, data misuse, cyberattacks, and ethical violations. In this context, framework validation is critically important to ensure that smart city initiatives remain effective, secure, and sustainable. For smart cities to succeed in the long term, robust ethical standards combined with highly effective cybersecurity mechanisms are essential. This study focuses on the methods, processes, and criteria required to validate such frameworks, ensuring that the deployed technologies are not only technically efficient but also aligned with core values of fairness, privacy, and security.
The initial phase of framework validation involves assessing the overall effectiveness of smart city infrastructure. This includes evaluating whether the implemented technologies meet their intended objectives, such as improved operational efficiency, carbon emission reduction, and equitable service delivery. Performance evaluation is carried out across key domains, including smart grids, traffic management systems, healthcare services, and public safety solutions.

Beyond technical performance, ethical acceptability is equally important. Security plays a central role in this evaluation, particularly because IoT technologies are extensively used in critical sectors such as smart homes, healthcare, and transportation [1, 2]. The integration of blockchain with artificial intelligence and big data analytics enhances cybersecurity by enabling secure data encryption and decentralized data management [3].

Privacy, consent, and transparency are major concerns as urban populations become increasingly dependent on data-driven systems. An effective framework must ensure that data collection, analysis, and sharing are conducted ethically. This includes adherence to principles such as informed consent, data protection, and responsible use of personal information. Cybersecurity remains one of the most significant factors in framework validation, as cyberattacks or data breaches can compromise public safety and undermine citizens' trust in city governance [4, 5]. Therefore, security mechanisms governing data transmission, storage, and access must be rigorously analyzed and continuously tested to identify and mitigate vulnerabilities before they can be exploited. This study adopts multiple validation processes for innovative city structures to ensure that smart cities are ethical, secure, and operationally efficient. Real-world case studies are examined to highlight best practices and lessons learned from existing implementations. In addition, the role of emerging technologies such as blockchain and artificial intelligence is explored, particularly in supporting ethical governance and secure urban development.

Furthermore, this paper proposes a novel model aimed at enhancing data confidentiality and authentication, thereby strengthening security in smart city environments. The proposed framework focuses on improving critical security mechanisms required to counter modern cyber threats and protect urban infrastructure [6, 7]. The results indicate that Stochastic Multicriteria Acceptability Analysis (SMAA) provides valuable insights through acceptability indices, central weight vectors, and confidence factors. These measures offer decision-makers a deeper understanding of how well different alternatives align with strategic objectives. Importantly, the study highlights the necessity of considering dependent uncertainties, which are often overlooked in traditional decision-making models, as neglecting them may lead to unreliable outcomes.

The rapid evolution of smart cities has intensified ethical and cybersecurity challenges, including data privacy violations, algorithmic bias, and increased exposure to cyber threats. To address these challenges, the paper presents a fuzzy multi-criteria decision-making (MCDM) framework for the design, implementation, and validation of ethical and cyber-secure smart city models. The framework employs fuzzy logic to manage uncertainty in expert evaluations and to optimize the selection of smart city alternatives based on ethical and cybersecurity criteria [8]. The performance of the framework is assessed using five alternative smart city models evaluated through the Analytic Hierarchy Process (AHP). Validation is further supported by sensitivity analysis, comparative AHP evaluation, and real-world case studies, ensuring that the proposed framework is both theoretically sound and practically applicable.

2. Related Work

When discussing expert contributions in the related works section, the objective is to highlight how leading researchers and practitioners have advanced the existing body of knowledge in the field. This section establishes the context of the study by identifying the most relevant prior research, theories, methodologies, and frameworks, and by explaining their relevance to the present work. It begins with a concise overview of the subject area, focusing on the principal research domains addressed in the study. Key themes explored by researchers in the area are outlined to provide a structured background.

In the context of evaluating the performance impact of S-AMAA (Smart Adaptive Multi-Agent Architecture) using AHP, the discussion typically starts with foundational studies on performance assessment frameworks and multi-criteria decision-making techniques, particularly the Analytic Hierarchy Process and its applications in related technological and engineering domains. This approach helps position the study within the existing literature and clarifies how it extends, refines, or complements established research.

MK Ahmad, AK Bharti (2021): The study focuses on validating a clustering-based framework using unsupervised machine learning techniques. The authors explore how unsupervised learning methods, particularly clustering, can be applied for various tasks in simulation, automation, and smart manufacturing. The framework is validated through experiments that highlight its efficiency and effectiveness in real-world applications, providing insights into its potential for automation processes [9].

MF Farooqui, AA Abdussami (2020): The authors provide a comprehensive review of the field of fog computing. The paper systematically reviews the literature, emphasising the importance of fog computing as an intermediary between cloud and edge computing. It discusses the various applications, challenges, and future directions of fog computing across IoT, smart cities, and real-time data processing, highlighting its potential to reduce latency and improve computational efficiency [10].

L. S. Vailshery (2020): Provides a statistical overview of the growth of IoT (Internet of Things) and non-IoT connections globally. The data, available on the Statista platform, shows a rising trend in connected devices over the years, projecting that IoT connections will rise significantly by 2025. The report is instrumental in understanding the massive scale of IoT deployment and its growing role in transforming industries and daily life through interconnected devices [11].

Asimithaa K1, Aishwarya R I2, Tanish Milind Salunkhe3, Eunice J4 (2024): Explores the evolving challenges and strategies related to cybersecurity within the context of smart cities. It discusses the need for robust cybersecurity frameworks to safeguard critical infrastructures, data privacy, and the overall safety of citizens. The study also highlights emerging trends in smart city technologies and emphasises the importance of securing IoT devices and other interconnected systems from cyber threats [12].

Johnson Sunday Oliha, Preye Winston Biu, and Ogagua Chimezie Obi (2024): The authors provide an in-depth

review of cybersecurity challenges in smart cities. They analyse vulnerabilities in smart city infrastructure and propose strategies to strengthen the security of connected systems. The paper presents a holistic view of how cybersecurity can be integrated into bright city designs to prevent potential threats and ensure the safety of urban environments [13].

Nguyen, T., Hallo, L., Nguyen, N. H., Pham, B. V. (2022): Outlines a systematic approach to risk management in the governance of smart cities. The authors emphasise the importance of addressing risks related to data management, IoT infrastructure, and governance practices. The paper proposes a comprehensive risk management framework that integrates both technical and governance strategies to ensure the success and sustainability of innovative city initiatives [14].

Chiroli, D. M. D. G., Solek, É. A., Oliveira, R. S., Barboza, B. M., Campos, R. P. D., Kovaleski, J. L., Trojan, F. (2022): The authors explore the application of multi-criteria decision-making techniques for evaluating and assessing smart cities. The study demonstrates how factors such as sustainability, infrastructure, and public services can be analysed using multicriteria analysis to identify the strengths and weaknesses of innovative city projects. The paper provides a framework for decision-makers to prioritise improvements in urban development based on a range of critical parameters [15].

A. Razmjoo, S. Mirjalili, M. Aliehyaei, P. A. Østergaard, A. Ahmadi, M. M. Nezhadf (2021): focuses on identifying and overcoming the barriers faced by the development of smart cities, particularly in energy-related sectors. The paper discusses the role of policy and regulations in fostering smart city growth and highlights the importance of adopting innovative grid technologies, renewable energy sources, and energy-efficient solutions. It also explores the challenges in infrastructure and resource management, and suggests policies to overcome them [16].

S. E. L. Hilali, A. Azougagh (2021): Investigates the public perception of future smart cities through a netnographic research approach. By analysing online discussions and social media, the authors gain insights into citizens' expectations, concerns, and aspirations regarding smart cities. The study sheds light on public views of the integration of advanced technologies in urban environments, emphasising the need for citizen-centric approaches in thoughtful city planning [17].

M. Al-Saidi, E. Zaidan (2020): The authors examine the futuristic city developments in the Gulf region. The paper explores current trends in urban planning, focusing on megaprojects in cities such as Dubai and Abu Dhabi. It highlights the role of energy-efficient technologies, sustainable infrastructure, and innovative city initiatives in transforming these cities into global hubs of innovation and growth [18].

M. H. Maruf, M. A. Haq, S. K. Dey, A. A. Mansur, A. S. M. Shihavuddin (2020): It focuses on the challenges and strategies for implementing innovative grid technologies in developing nations, particularly Bangladesh. The authors discuss the barriers to adoption, such as financial constraints, lack of infrastructure, and regulatory issues, and propose strategies for overcoming these challenges to achieve a sustainable energy future [19].

M. Shabbir, M. W. Khan, R. K. Yadav, (2025): It focuses fuzzy AHP-TOPSIS framework which offers the valuable insights into the hierarchical structure of risk factors and their comparative impact, paving the way for more informed decision-making in security risk management [20].

3. Verification and Validation: Why is it needed?

V&V are essential parts of research, development, and practice in systems, particularly in complex disciplines such as engineering, software development, and decision-making structures. They ensure that a system, model, or methodology is suitable and meets the required standards. Such processes play a significant role in making the system's results reliable, accurate, and effective, and hence cannot be neglected in any field of science or technology. Verification is the process of ensuring that a system or model is adequately developed in terms of its specifications. It is simply a matter of ensuring that the design, algorithms, or methodologies are followed as intended and that there are no faults or inconsistencies during implementation. It is necessary to verify that computational models, frameworks, or tools are free of flaws that could lead to inaccurate results or an incorrect presentation of the problem under consideration. As a case in point, in decision-making systems such as AHP (Analytic Hierarchy Process), verification helps make sure that the criteria, weighting and ranking systems are correctly put in place as per the established theoretical principles [21]. On the other hand, validation is a way to determine whether the system/model can solve the problem it is supposed to solve. It evaluates the realism and feasibility of the consequences of the results, i.e., the system yields results consistent with real-life conditions. When applied to performance impact studies such as S-AMAA (Smart Adaptive Multi-Agent Architecture), validation is mandatory to ensure the framework is applicable and accurate when used in real environments or systems. Even a well-designed system may not achieve its goals without validation and thus may end up being inefficient or not work at all in practice. Verification and validation play an important role in mitigating risks, reducing uncertainties, and ensuring that systems or models are technically sound and practical in achieving their objectives. Through V&V, researchers and practitioners can ensure that their systems are reliable, credible, and produce meaningful results. In addition to this, they provide assurance to stakeholders, users, and decision-makers that the methodologies or systems they are basing their decisions on are not only accurate but also reliable. Finally, without adequate verification and validation, the risks of implementing ineffective, inaccurate, or even unsafe systems are high, with costly implications, project downtime, or even the downfall of the system.

3.1 Validation of System Performance and Decision-Making Accuracy Using the Analytic Hierarchy Process (AHP)

The verification process is focused on checking whether the framework has been built correctly and adheres to the specifications and requirements laid out during the various

phases. In the context of the Performance impact of S-AMAA, verification ensures that each component, such as the data pre-processing methods and Criteria (e.g., Spoof Detection Rate, Emergency Response Time, Public Trust Score (survey, 0-10)), is implemented accurately. This process involves rigorous testing of each stage of the system to confirm that it behaves as expected and does not introduce any computational or logical errors. For example, verification ensures that the text data is properly pre-processed, that the features are correctly extracted, and that the model procedures execute without failure. It also checks whether all parameters, such as hyperparameters, are set correctly and whether the system can handle various edge cases. In verifying the performance impact of a system like S-AMAA (Smart Adaptive Multi-Agent Architecture), AHP (Analytic Hierarchy Process) plays a critical role in ensuring the decision-making framework is correctly implemented and that the results align with the intended outcomes. AHP is a structured technique used for organising and analysing complex decisions, which involves breaking down a problem into a multi-level hierarchical structure and using pairwise comparisons to evaluate various alternatives based on multiple criteria.

Pairwise Comparison Matrix

A pairwise comparison matrix is created for the criteria, in which each criterion is compared to every other to determine its relative importance. The scale used is as follows:

- **1**: Equal importance
- **3**: Moderate importance of one over the other
- **5**: Strong importance of one over the other
- **7**: Extreme importance of one over the other
- **9**: Extremely more important
- **2, 4, 6, 8**: Intermediate values between the above options

For the three criteria (Spoof Detection Rate, Emergency Response Time, and Public Trust Score), the pairwise comparison matrix:

$$A = \begin{pmatrix} 1 & a_{12} & a_{13} \\ \frac{1}{a_{12}} & 1 & a_{23} \\ \frac{1}{a_{13}} & \frac{1}{a_{23}} & 1 \end{pmatrix} \quad \text{Eq.(1)}$$

Where:

- a_{12}Is the comparison value between criteria one and criteria 2.
- a_{13}Is the comparison value between criteria one and criteria 3.
- a_{23}Is the comparison value between criteria two and criteria 3
- The matrix is reciprocal, meaning that $a_{ij} = \frac{1}{a_{ji}}$.

Normalise the Pairwise Comparison Matrix

To normalize the matrix, each element is divided by the sum of the elements in its corresponding column, ensuring that the total of each column equals 1.

The normalised matrix NIs:

$$N = \begin{pmatrix} \frac{a_{11}}{S_1} & \frac{a_{12}}{S_2} & \frac{a_{13}}{S_3} \\ \frac{a_{21}}{S_1} & \frac{a_{22}}{S_2} & \frac{a_{23}}{S_3} \\ \frac{a_{31}}{S_1} & \frac{a_{32}}{S_2} & \frac{a_{33}}{S_3} \end{pmatrix} \quad \text{Eq.(2)}$$

Where $S_1, S_2,$and S_3Are the column sums of the matrix A. Specifically:

$$S_1 = a_{11} + a_{21} + a_{31}, S_2 = a_{12} + a_{22} + a_{32}, S_3 = a_{13} + a_{23} + a_{33} \quad \text{Eq.(3)}$$

Calculate the Weights W_i(Weight Vector)

The next step involves computing the weight of each criterion, representing its relative importance, by calculating the average of each row in the normalized matrix.

$$W_1 = \frac{N_{11}+N_{12}+N_{13}}{n}, W_2 = \frac{N_{21}+N_{22}+N_{23}}{n}, W_3 = \frac{N_{31}+N_{32}+N_{33}}{n} \quad \text{Eq.(4)}$$

Where:

- $W_1, W_2, W_3 These$ are the weights of the criteria.
- nIs the number of criteria (in this case, 3).

Thus, the final weight vector WWill be:

$$W = \begin{pmatrix} W_1 \\ W_2 \\ W_3 \end{pmatrix} \quad \text{Eq.(5)}$$

Table 1: Weightage Table

	Legacy / "Before"	After S-AMAA	Performance Gain
Spoof Detection Rate	0.58	0.51813	0.48309
Emergency Response Time	1.93	0.99	0.38462
Public Trust Score (survey, 0-10)	2.07	2.6	0.89

Table 1 compares the system's performance before and after implementing S-AMAA across three key criteria: Spoof Detection Rate, Emergency Response Time, and Public Trust Score. The Spoof Detection Rate decreases slightly from 0.58 to 0.51813, but the performance gain remains evident. The Emergency Response Time improves significantly, dropping from 1.93 to 0.99, with a notable performance gain of 0.38462. The Public Trust Score increases from 2.07 to 2.6, showing an improvement in public confidence, with a performance gain of 0.89. Overall, S-AMAA improves response time and public trust, while the spoof detection rate declines slightly.

Table 2: Normalised Matrix

	Legacy / "Before"	After S-AMAA	Performance Gain
Spoof Detection Rate	0.126638	0.126124	0.274842
Emergency Response Time	0.421397	0.240985	0.218817
Public Trust Score (survey, 0-10)	0.451965	0.632891	0.506341

Table 2 presents the Normalised Matrix, comparing the system's performance before and after S-AMAA implementation across the same criteria: Spoof Detection Rate, Emergency Response Time, and Public Trust Score. For Spoof Detection Rate, the normalised value is very similar before and after S-AMAA, decreasing from 0.126638 to 0.126124, while the performance gain of 0.274842 shows a noticeable improvement in other areas. Emergency Response Time shows a significant decrease in its normalised value, from 0.421397 to 0.240985, reflecting a substantial improvement and a performance gain of 0.218817. Lastly, the Public Trust Score improves substantially from 0.451965 to 0.632891, indicating a significant increase in public confidence and a performance gain of 0.506341. Overall, the S-AMAA framework results in substantial gains in public trust and response time, while the spoof-detection rate remains essentially unchanged.

Table 3: Final Normalised Matrix

	Legacy / "Before"	After S-AMAA	Performance Gain
Spoof Detection Rate	0.244816886	0.268574329	0.486608785
Emergency Response Time	0.474950547	0.299181482	0.225867971
Public Trust Score (survey, 0-10)	0.280231911	0.432244048	0.287524041

Table 3 presents the Final normalised matrix, showing the comparison of system performance before and after the implementation of S-AMAA across the criteria of Spoof Detection Rate, Emergency Response Time, and Public Trust Score. The Spoof Detection Rate shows a slight improvement in its normalised value, rising from 0.244816886 to 0.268574329, with a significant performance gain of 0.486608785, indicating an enhanced overall impact in this area. Emergency Response Time shows a substantial improvement, decreasing from 0.474950547 to 0.299181482, with a performance gain of 0.225867971, reflecting a better system response after implementing S-AMAA. The Public Trust Score also improves notably, rising from 0.280231911 to 0.432244048, with a performance gain of 0.287524041, highlighting increased public confidence in the system. Overall, S-AMAA results in significant performance improvements in spoof detection, response time, and public trust, underscoring its positive impact on system efficiency and user perception.

Table 4: Rank Table

	Rank weight
Spoof Detection Rate	0.244816886
Emergency Response Time	0.299181482
Public Trust Score (survey, 0-10)	0.287524041

Table 4 presents the Rank Table, which shows the relative weights assigned to each criterion based on their normalised values. The Spoof Detection Rate weights 0.244816886, indicating its importance relative to the other criteria. Emergency Response Time carries a slightly higher weight of 0.299181482, suggesting it has a more significant influence on overall performance. The Public Trust Score weights 0.287524041, ranking just below Emergency Response Time, reflecting its substantial role in evaluating the system's effectiveness. This ranking provides a clear indication of how each criterion contributes to the overall performance and highlights the relative importance of response time, trust, and spoof detection in the final system assessment.

Largest eigenvalue $\lambda_{\max}$.

$$A \cdot \mathrm{W} = \lambda_{\max} \cdot \mathrm{W} \quad \text{Eq.(6)}$$

Steps to Calculate the Eigenvalue and Eigenvector

- **Form the Pairwise Comparison Matrix A:** First, create the matrix AThat contains the pairwise comparison values.
- **Find the Eigenvalues:** To determine the eigenvalues, the following equation is solved:

$$\det(A - \lambda I) = 0 \quad \text{Eq.(7)}$$

Where:

- λRepresents the eigenvalue.
- IIs the identity matrix.
- $\det$ Stands for the determinant of the matrix.

Solving this equation gives the eigenvalues of the matrix. A.

Find the Eigenvector:
Once the eigenvalue $\lambda_{\max}$Is found, substitute it into the equation:

$$(A - \lambda_{\max} I) \cdot \mathrm{W} = 0 \quad \text{Eq.(8)}$$

This will give the eigenvector. W, which represents the relative weights of the criteria.

Normalise the Eigenvector: The resulting eigenvector is often normalised so that the sum of its components equals. This normalised vector represents the relative importance (weight) of each criterion.

Consistency Index (CI) and Consistency Ratio (CR)
In AHP, the Consistency Index (CI) and Consistency Ratio (CR) are used to measure the consistency of the pairwise comparison matrix. The largest eigenvalue $\lambda_{\max}$Is used to compute these indices.

Consistency Index (CI): $CI = \frac{\lambda_{max} - n}{n-1}$ Eq.(9)

Where:

- λ_{max}Is the largest eigenvalue.
- $n$is the number of criteria (matrix size).

Consistency Ratio (CR):

$$CR = \frac{CI}{RI} \quad \text{Eq.(10)}$$

Where:

- $RI$is the Random Consistency Index, which depends on the matrix size (n).

If $CR < 0.1$The matrix is considered consistent, and the results are reliable.

Table 5: Consistency Ratio

Eigen value	0.299181
N=3	
CI(Positive Value)	1.35
RI	14.98
CR=	0.090147
CI<0.10	TRUE

Table 5 presents the Consistency Ratio (CR), a measure used in AHP to assess the consistency of the pairwise comparison matrix. In this case, the eigenvalue is 0.299181, and the matrix size is. NIs 3, indicating that three criteria are being compared. The Consistency Index (CI), calculated from the eigenvalue and matrix size, is 1.35. The Random Consistency Index (RI) for a 3×3 matrix is 14.98. The Consistency Ratio (CR) is calculated as:

$$CR = \frac{CI}{RI} = \frac{1.35}{14.98} \approx 0.090147$$

Since the CR value is less than 0.10, the result is deemed consistent, as it falls within the acceptable threshold. A CR < 0.10 indicates that the pairwise comparisons are sufficiently consistent and that the decision-making process is reliable. Therefore, the CI < 0.10 condition is TRUE, confirming that the pairwise comparison matrix is consistent and the derived weights are valid.

4. Discussion

The findings of this study demonstrate that the AHP-based evaluation framework is well suited for validating the performance impact of the S-AMAA (Smart Adaptive Multi-Agent Architecture) in a multi-criteria environment. By incorporating diverse performance indicators—namely Spoof Detection Rate, Emergency Response Time, and Public Trust Score—the proposed approach enabled a balanced assessment that captures both technical efficiency and societal impact. The structured hierarchy and pairwise comparison mechanism of AHP facilitated a transparent weighting of criteria, allowing interdependencies among performance factors to be systematically examined.

A key methodological strength lies in the consistency of expert judgments, as reflected by the Consistency Ratio value of 0.090147, which satisfies the accepted threshold. This confirms the logical coherence of the comparisons and supports the stability of the derived weights. The analysis highlights that S-AMAA performs particularly well in operational responsiveness and trust-related dimensions, without compromising detection capabilities. These results indicate that the framework effectively balances performance optimization with reliability requirements, making it suitable for deployment in dynamic and real-world smart system environments. Moreover, the use of AHP as a decision-support mechanism enhances the interpretability of results, offering decision-makers a reliable basis for evaluating and refining adaptive multi-agent architectures.

5. Conclusion

This research confirms that the proposed S-AMAA framework delivers meaningful performance benefits when evaluated through a structured multi-criteria decision-making process. By systematically integrating AHP into the validation process, the study provides a clear mechanism for prioritizing performance indicators and interpreting their combined impact on system effectiveness. The outcomes demonstrate that S-AMAA supports informed decision-making by balancing operational efficiency, system reliability, and user-oriented considerations. Beyond validating a single framework, the study highlights the broader applicability of AHP-based evaluation models for assessing complex, adaptive architectures, offering a scalable and methodologically sound approach for future performance validation in intelligent and data-driven systems.

References

1. Mishra A, *et al.* A comparative study on data mining approach using machine learning techniques: prediction perspective. In: Pervasive healthcare. Berlin/Heidelberg: Springer; 2022. p. 153-165.
2. Attaallah A, *et al.* Security test case prioritization through ant colony optimization algorithm. Computer Systems Science and Engineering. 2023;47(3):3165-3195.
3. Dwivedi SK, *et al.* A novel paradigm: cloud-fog integrated IoT approach. In: Proceedings of the 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM). Dubai, UAE: IEEE; 2022.
4. Jalaliyoon N, *et al.* Accomplishment of critical success factor in organization using analytic hierarchy process. International Journal of Academic Research in Management. 2012;1(1):1-9.
5. Khan RA, *et al.* Mathematical insights into framework design for ethical and cyber-secure smart cities. Journal of Information Systems Engineering and Management. 2025;10(15s):86-106.
6. Ansar SA, *et al.* Estimation of software risks through CVSS: a design phase perspective. Turkish Online Journal of Qualitative Inquiry. 2021;12(4):894-901.
7. Lee MC. A method of performance evaluation by using the analytic network process and balanced score card. In: Proceedings of the International Conference on Convergence Information Technology; 2007.
8. Virendra S, *et al.* Optimizing the impact of security attributes in requirement elicitation techniques using FAHP. International Journal of Innovative Technology and Exploring Engineering. 2020.

9. Ahmad MK, *et al.* Validation of clustering-based framework using unsupervised machine learning. In: Proceedings of the International Conference on Simulation, Automation and Smart Manufacturing (SASM); 2021. p. 1-6.
10. Farooqui M, *et al.* A systematic literature review on fog computing. International Journal of Advanced Science and Technology. 2020:12755-12769.
11. Vailshery LS. IoT and non-IoT connections worldwide 2010-2025 [Internet]. Statista; 2020 [cited year not stated]. Available from: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/
12. Asimithaa K, *et al.* Prospects of cybersecurity in smart cities. International Research Journal on Advanced Engineering Hub. 2024:1821-1824.
13. Oliha JS, *et al.* Securing the smart city: a review of cybersecurity challenges and strategies. Open Access Research Journal of Multidisciplinary Studies. 2024;7(1):94-101.
14. Nguyen T, *et al.* A systemic approach to risk management for smart city governance. IEEE; 2022.
15. Chiroli DMDG, *et al* Using multi-criteria analysis for smart city assessment. Cidades, Comunidades e Territórios. 2022;(44).
16. Razmjoo A, *et al.* Effective policies to overcome barriers in the development of smart cities. Energy Research and Social Science. 2021;79.
17. Hilali SEL, *et al.* A netnographic research on citizen's perception of a future smart city. Cities. 2021;115.
18. Al-Saidi M, *et al* Gulf futuristic cities beyond the headlines: understanding the planned cities megatrend. Energy Reports. 2020;6:114-121.
19. Maruf MH, *et al.* Adaptation for sustainable implementation of smart grid in developing countries like Bangladesh. Energy Reports. 2020;6:2520-2530.
20. Shabbir M, *et al.* Evaluating the impact of security risks through fuzzy AHP-TOPSIS method. Journal of Information Systems Engineering and Management. 2025;10(25s):224-236.
21. Khan MW, *et al.* Prioritize test suite for software security: a design perspective. International Journal of Pure and Applied Mathematics. 2018;119(15):3005-3017.