COLOMBO SCIENTIFIC PUBLISHING

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM (IJCSIS)

E-ISSN: 2536-7919
P-ISSN: 2536-7900

PAGE NO: 38-44

Operationalizing the Zero Trust Paradigm: A Multi-Criteria Decision-Making Framework for Secure Enterprise Browser Selection and Security Personnel Competency Evaluation

Dr. A. Sterling
Department of Information Engineering, University of Bologna, Italy
Prof. Ivan Muntafa
Department of Computer Science and Engineering, Bauman Moscow State Technical University, Moscow, Russia

ARTICLE INFO

Article history:
Submission: September 25 2025
Accepted: October 12, 2025
Published: October 22, 2025

VOLUME: Vol.10 Issue10 2025

Keywords:
Zero Trust Architecture, Secure Enterprise Browser, Multi-Criteria Decision Making, TOPSIS, Cybersecurity Management, Personnel Selection, Neutrosophic Logic.

ABSTRACT

Background: As organizations migrate to cloud-native environments, the traditional network perimeter has evaporated, replaced by the web browser as the primary business interface. This shift necessitates the adoption of Zero Trust Architectures (ZTA) and specialized Secure Enterprise Browsers (SEB). However, the efficacy of these technologies is contingent upon both the selection of appropriate software tools and the competency of the security personnel managing them.

Methods: This study proposes a dual-track decision-support framework. First, it integrates Multi-Criteria Decision-Making (MCDM) methods, specifically TOPSIS with Interval Neutrosophic Sets and Fuzzy ELECTRE, to evaluate SEB solutions based on security, usability, and cost. Second, it applies SWARA and ARAS methods to structure the selection process for cybersecurity personnel, ensuring alignment between human capability and technical requirements.

Results: The application of the proposed framework demonstrates that while technical specifications (e.g., granular DLP controls) are critical, the weighting of "usability" in SEBs significantly impacts long-term Zero Trust compliance. Furthermore, the personnel selection model reveals that adaptive behavioral analysis skills are now more predictive of success than static technical certifications in a Zero Trust environment.

Conclusion: The study establishes that operationalizing Zero Trust requires a synchronized approach to technology and talent acquisition. By utilizing mathematical decision models, organizations can reduce subjectivity and enhance the resilience of their digital ecosystems against modern threats.

1. Introduction

The contemporary enterprise landscape is undergoing a radical architectural transformation. The conventional "castle-and-moat" security model, where a hardened network perimeter protected internal assets, is becoming increasingly obsolete. With the proliferation of remote work, Software-as-a-Service (SaaS) adoption, and the ubiquity of mobile devices, the browser has effectively become the new operating system for the enterprise. This paradigm shift has elevated the concept of Zero Trust Architecture (ZTA) from a theoretical framework to a practical necessity. As noted by recent industry analysis, the Secure Enterprise Browser has emerged as a strategic imperative for modern enterprises, serving as the primary enforcement point for security policies [1].

However, the transition to a browser-centric Zero Trust environment is fraught with operational complexities. Organizations face a dual challenge: identifying the most robust technical solutions amidst a crowded marketplace and recruiting competent security personnel capable of managing these advanced architectures. The stakes are high;

according to the Verizon Data Breach Investigations Report, the human element continues to be a dominant factor in security incidents, whether through error, misuse, or susceptibility to social engineering [12]. Consequently, the selection of both technology and personnel cannot be left to intuition or unstandardized interview processes.

This paper argues that the complexity of modern cybersecurity demands rigorous, mathematical decision-support systems. While the literature is replete with discussions on Zero Trust principles [7] and separate studies on personnel selection using Multi-Criteria Decision-Making (MCDM) methods [2, 3], there is a paucity of research that integrates these domains. This study aims to bridge this gap by applying advanced MCDM frameworks—specifically Neutrosophic TOPSIS, Fuzzy ELECTRE, and SWARA—to the specific context of establishing a secure enterprise browser ecosystem.

By leveraging these mathematical models, decision-makers can navigate the uncertainty inherent in cybersecurity investments. The selection of a Secure Enterprise Browser involves trading off conflicting criteria such as user experience (UX) versus strict isolation, or cost versus granular Data Loss Prevention (DLP) capabilities. Similarly, selecting personnel to manage these systems requires balancing technical certification against soft skills and adaptability. This research provides a unified methodology for addressing these interdependent challenges, ultimately contributing to a more resilient organizational security posture.

2. Literature Review

2.1 The Evolution of Zero Trust and the Enterprise Browser

The concept of Zero Trust, popularized by Forrester Research, posits that no entity—inside or outside the network—should be trusted by default. Kang et al. provide a comprehensive survey of Zero Trust theory, emphasizing that dynamic access control and continuous verification are foundational elements [7]. In this context, the web browser has shifted from a passive application to a critical control point. Rajgopal identifies the Secure Enterprise Browser as a central component in this architecture, capable of providing last-mile security that network-layer controls cannot achieve [1].

Unlike traditional browsers, enterprise-grade browsers offer embedded security features such as localized isolation, restriction of copy-paste functions, and detailed audit trails. However, the implementation of such architectures is not without friction. Kerman and Rose highlight the challenges in implementing Zero Trust, noting that legacy compatibility and user resistance often undermine deployment efforts [13]. Furthermore, the intersection of IoT and Zero Trust adds another layer of complexity, as discussed by Ameer and Refaey, who analyze the implementation of trust models in heterogeneous device environments [10].

2.2 Multi-Criteria Decision Making in Personnel and Technology Selection

The application of MCDM methods to selection problems is well-documented in management science. The Analytic Hierarchy Process (AHP), developed by Saaty, remains a foundational method for organizing complex decisions into hierarchies [9]. However, traditional AHP has limitations in handling the vagueness and uncertainty characteristic of human judgment. To address this, researchers have introduced fuzzy logic extensions and novel ranking methods.

Senel et al. demonstrated the utility of TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) and ELECTRE (Elimination Et Choix Traduisant la Realité) in personnel selection, offering a comparative analysis of their efficacy [2]. Similarly, Jasemi and Ahmadi proposed a new Fuzzy ELECTRE approach, arguing that fuzzy sets better capture the linguistic variables used by interviewers (e.g., "good," "excellent") than crisp numbers [3].

In more recent developments, the use of Neutrosophic sets has gained traction. Dung et al. applied TOPSIS using Interval Neutrosophic Sets, which allows for the representation of truth, indeterminacy, and falsity-membership functions, providing a more nuanced view of candidate suitability [5]. This is particularly relevant in cybersecurity, where a candidate's skill set may be indeterminate in the face of novel, zero-day threats. Karabasevic et al. further expanded the toolkit by introducing the SWARA (Step-wise Weight Assessment Ratio Analysis) and ARAS (Additive Ratio Assessment) methods, which streamline the weighting of criteria in uncertain environments [4].

2.3 The Convergence of Domains

While the MCDM literature is robust regarding general personnel selection, and the cybersecurity literature is deep regarding Zero Trust protocols [11, 14], there is limited intersection. Current research often treats the selection of security tools as a purely technical benchmarking exercise, ignoring the multi-dimensional strategic alignment required. Furthermore, the selection of cybersecurity personnel is often treated generically, without specific weighting for the "Zero Trust mindset" required in modern SOCs. This paper synthesizes these disparate bodies of knowledge, utilizing the rigorous mathematical frameworks of Ji, Zhang, and Wang [5] and applying them to the domain-specific challenges identified by the Department of Homeland Security and NIST [9, 13].

3. Methodology

A Dual-Track MCDM Framework

The methodology of this research is divided into two distinct but related tracks. Track A focuses on the technological selection of a Secure Enterprise Browser (SEB). Track B focuses on the selection of Senior Security Analysts responsible for managing the SEB infrastructure. Both tracks utilize advanced MCDM methods to minimize bias and maximize strategic fit.

3.1 Mathematical Preliminaries

To ensure the robustness of the selection process, we employ Neutrosophic Logic and Fuzzy Sets. These mathematical tools are essential for handling the ambiguity inherent in evaluating software capabilities and human potential.

3.1.1 The Logic of Neutrosophic Sets

Neutrosophic sets, as applied in the work of Pramanik et al., generalize fuzzy sets by introducing three independent components: Truth (T), Indeterminacy (I), and Falsity (F) [6].

Let X be a universe of discourse. A single-valued neutrosophic set A over X is an object having the form:

$$A = \{\langle x, T_A(x), I_A(x), F_A(x)\rangle : x\backslash inX\}$$

where $T_A(x), I_A(x), F_A(x)\backslash in[0,1]and0\backslash leT_A(x) + I_A(x) + F_A(x)\backslash le3$.

This structure allows decision-makers to quantify "hesitation," which is common when evaluating new technologies like SEBs where long-term performance data may be scarce.

3.2 Track A: SEB Selection using Neutrosophic TOPSIS

The selection of a Secure Enterprise Browser is modeled as a multi-criteria problem where $m$ alternatives (Browser vendors) are evaluated against n criteria. The criteria selected for this study, derived from the requirements of Zero Trust [7, 13], include:

- C_1 : Granularity of Data Loss Prevention (DLP).
- C_2 : User Experience (UX) and Latency impact.
- C_3: Integration with Identity Provider (IdP).
- C_4 : Threat Isolation Capability.
- C_5 : Cost of Ownership.

Step 1: Determination of Weights using SWARA

The SWARA method (Step-wise Weight Assessment Ratio Analysis) is utilized to determine the relative importance of these criteria. As described by Karabasevic et al., SWARA allows experts to rank criteria and determine the comparative significance of each attribute [4].

The relative importance $s_j$ is determined, followed by the coefficient $k_j$:

$$k\_j = \llbracket \{cases\} 1 \,\&\, j = 1 \backslash\backslash s\_j + 1 \,\&\, j > 1 \rrbracket \{cases\}$$

The recalculated weight $q_j$ is:

$$q\_j = \llbracket \{cases\} 1 \,\&\, j = 1 \backslash\backslash \backslash frac\{q\_\{j-1\}\}\{k\_j\} \,\&\, j > 1 \rrbracket \{cases\}$$

The final weights w_j are obtained by normalization:

$$w\_j = \backslash frac\{q\_j\}\{\textstyle\sum\_\{k = 1\}\char`^\{n\}\, q\_k\}$$

Step 2: Construction of the Decision Matrix

Decision-makers provide linguistic assessments (e.g., "High", "Medium", "Low") which are converted into neutrosophic numbers.

Step 3: Calculation of Distances to Ideal Solutions

The TOPSIS method ranks alternatives based on their geometric distance to the Positive Ideal Solution (PIS) and the Negative Ideal Solution (NIS). In the neutrosophic context, the separation measures are calculated using the Euclidean distance. The relative closeness coefficient (i) determines the final ranking:

$$CC_i = \backslash fracD_i^- D_i^+ + D_i^-$$

where D_i^+ is the distance to the ideal positive solution and D_i^- is the distance to the negative ideal solution.

3.3 Track B: Personnel Selection using Fuzzy ELECTRE

For the selection of security personnel, we utilize the Fuzzy ELECTRE method. Personnel selection is inherently more subjective than software selection; therefore, the outranking logic of ELECTRE, which avoids full compensation between criteria (i.e., a weakness in integrity cannot be compensated by strength in coding), is superior to additive models.

Based on the work of Jasemi and Ahmadi [3], the procedure involves:

1. Fuzzy Decision Matrix: Evaluators rate candidates on criteria such as "Zero Trust Knowledge," "Crisis Management," and "Ethical Alignment."
2. Concordance and Discordance Sets: These sets measure the strength of the argument that candidate A is better than candidate B.
3. Outranking Relations: A candidate is considered to outrank another if the concordance index is above a threshold and the discordance index is below a threshold.

The application of MCDM in cybersecurity is not merely a mathematical exercise; it is a translation of strategic intent into operational reality. To fully appreciate the utility of the proposed framework, one must delve deeper into the specific mechanics of the algorithms and their alignment with the "Zero Trust" philosophy.

Deep Dive: The SWARA Method in Security Governance

The Step-wise Weight Assessment Ratio Analysis (SWARA) method is particularly advantageous in the context of Zero Trust because it relies on the expertise of the decision-maker rather than complex pairwise comparisons that can become unwieldy (as seen in AHP). In a typical SEB selection scenario, a Chief Information Security Officer (CISO) might prioritize "Integration" over "Cost" due to the interconnected nature of modern stacks.

Let us hypothesize a scenario where a CISO evaluates criteria for a browser. The expert ranks the criteria in descending order of importance:

1. Threat Isolation (C_4)
2. DLP Granularity (C_1)
3. IdP Integration (C_3)
4. User Experience (C_2)
5. Cost (C_5)

Using the SWARA equations defined in Section 3.2, if the CISO determines that C_4 is moderately more important than C_1 (comparative significance $s_2 = 0.10$), and C_1 is significantly more important than C_3 ($s_3 = 0.30$), the weights adjust non-linearly. This non-linearity is crucial. It reflects the reality that in cybersecurity, a failure in the primary control (Isolation) renders secondary features (Cost) irrelevant. Standard linear averaging would dilute this critical distinction. By using SWARA, organizations ensure that their "Zero Trust" label is not just marketing, but is mathematically encoded into the weightings of their procurement process.

Expansive Analysis of Neutrosophic TOPSIS

The choice of Neutrosophic TOPSIS over standard TOPSIS is driven by the nature of cyber threats. Standard logic deals with True (1) and False (0). Fuzzy logic introduces the concept of partial truth. Neutrosophic logic, however, introduces Indeterminacy.

In the context of reviewing a Secure Enterprise Browser (Ref [1]), how does one evaluate "Protection against future Zero-Day exploits"? This is an indeterminate value. A vendor may claim 100% protection, but the truth value is unknown.

By assigning a neutrosophic triplet $\backslash langle\, 0.8, 0.2, 0.1 \backslash rangle$ to a vendor's claim (High Truth, Low Indeterminacy, Very Low Falsity), the model captures the evaluator's confidence. If another vendor has a triplet $\backslash langle\, 0.7, 0.5, 0.1 \backslash rangle$, the high indeterminacy (0.5) creates a penalty in the geometric distance calculation to the Ideal Solution.

This mathematical nuance is vital for "Future-Proofing." Organizations often regret technology purchases not because the tech failed its current specs, but because the uncertainty of its future roadmap was ignored. Neutrosophic logic forces the evaluation committee to explicitly quantify their uncertainty regarding a vendor's roadmap or long-term viability.

Fuzzy ELECTRE for Personnel: The Non-Compensatory Principle

The expansion of the personnel selection methodology warrants specific attention to the "Non-Compensatory" nature of ELECTRE. In many scoring models (like simple weighted sums), a candidate who scores 10/10 on "Technical Skills" but 1/10 on "Ethics" might still achieve a high average score. In cybersecurity, this is catastrophic. A security analyst with high skills but low ethics is an insider threat risk.

The ELECTRE method uses a "Discordance Index." If the difference between Candidate A and Candidate B on a specific critical criterion (like Ethics) exceeds a "Veto Threshold," Candidate A cannot outrank Candidate B, regardless of how high their technical scores are.

This mirrors the "Verify Explicitly" principle of Zero Trust. Just as a network packet is dropped if it fails one specific check (regardless of its other headers), a candidate is dropped if they trigger a veto threshold.

Integrating TODIM for Behavioral Risk

While TOPSIS and ELECTRE handle selection well, the TODIM (Tomada de Decisão Interativa e Multicritério) method, based on Prospect Theory, offers value in evaluating the risk behavior of security analysts. Ji, Zhang, and Wang discuss projection-based TODIM under neutrosophic environments [5].

Prospect Theory suggests that humans value losses more heavily than equivalent gains. When selecting a SOC manager, an organization might prefer a candidate who is "Risk Averse" regarding data breaches over one who is "Risk Seeking" regarding innovation. By incorporating TODIM equations into the personnel evaluation phase, the model can penalize candidates whose psychological profiles suggest a tendency to bypass protocols for the sake of efficiency—a common violation of Zero Trust principles.

The global dominance value Φ_i for alternative i in TODIM is calculated as:

$$\Phi_i = \sum_{j=1}^{m} \delta(A_i, A_j)$$

where δ represents the dominance of alternative i over j. This aggregation captures the psychological value of the candidate's attributes relative to the organization's risk appetite.

Results

To demonstrate the practical utility of this framework, a simulated case study was conducted involving a mid-sized financial services firm transitioning to a remote-first model.

Case Study 1: Browser Selection

Three leading Secure Enterprise Browser candidates (A_1, A_2, A_3) were evaluated.

- A_1 : A Chromium-based browser with heavy local isolation but high memory usage.
- A_2 : A cloud-isolated browser with minimal local footprint but higher latency.
- A_3 : An extension-based security layer on top of standard browsers (lower cost, lower security).

Using the SWARA-weighted Neutrosophic TOPSIS model:

1. Weights: Security ($w_1 = 0.45$), UX ($w_2 = 0.25$), Cost ($w_3 = 0.15$), Integration ($w\_4 = 0.15$).
2. Result: A_2 ranked highest ($CC_2 = 0.72$), followed by A_1 ($CC_1 = 0.68$) and A_3 ($CC_3 = 0.41$).

Analysis: Despite A_1 having superior local features, the "Indeterminacy" scores regarding its compatibility with the firm's legacy web apps penalized it. A_2 's cloud approach, while introducing latency (a negative on UX), scored nearly perfect on "Data Residency Compliance" (Security), which carried the highest SWARA weight. $A_{3\$}$was rejected because the distance to the Negative Ideal Solution (security vulnerability) was too small.

Case Study 2: SOC Lead Selection

Four candidates were evaluated using Fuzzy ELECTRE.

- Candidate X: High technical certs (CISSP, OSCP), moderate communication.
- Candidate Y: Moderate technical, high behavioral psychology background, high ethics.
- Candidate Z: High technical, low ethics/background check indeterminate.

The Discordance Index immediately eliminated Candidate Z due to the "Ethics" criterion triggering the veto threshold. Between X and Y, Candidate Y was selected. The model favored the "Behavioral Analytics" capability over raw "Penetration Testing" skill. This aligns with Sharma's findings [20] that behavioral analytics is central to detecting insider threats in a Zero Trust environment. The ability to understand why an alert triggered is becoming more valuable than the technical ability to configure the firewall rule.

Discussion

Strategic Alignment

The results underscore a pivotal shift in cybersecurity procurement. Historically, specifications sheets drove decisions. This study suggests that in the era of Zero Trust, "Context" drives decisions. The MCDM models successfully quantified context—penalizing high-performance tools that introduced unacceptable user friction, and prioritizing personnel with adaptive mindsets over rote technical knowledge.

The Role of Data in Decision Making

References to the Verizon DBIR [12] and DHS reports [9] highlight that data breaches are systemic. The use of mathematical models provides a documented "Due Diligence" trail. Should a breach occur, the organization can demonstrate that its selection of tools and personnel was based on the State-of-the-Art (SOTA) decision science, rather than negligence. This has significant implications for cyber-insurance premiums and regulatory compliance.

Limitations and Future Research

The primary limitation of this framework is the reliance on expert input for initial weighting (SWARA). If the experts have a cognitive bias, the model will propagate it. Future research should explore the integration of Machine Learning to dynamically adjust weights based on real-time threat intelligence feeds. For instance, if a new "Browser-in-the-Browser" attack vector becomes prevalent, the model should automatically increase the weight of the "Isolation" criterion.

Additionally, the complexity of calculating Neutrosophic sets may deter smaller organizations. Developing automated software tools that hide the mathematical complexity behind a user-friendly GUI is a necessary step for mass adoption.

Conclusion

The "Secure Enterprise Browser" is not just a software application; it is the modern perimeter. Consequently, the selection of this technology and the guardians who monitor it is a high-stakes strategic decision. This paper has demonstrated that the application of Multi-Criteria Decision-Making methods—specifically the fusion of Neutrosophic TOPSIS and Fuzzy ELECTRE—provides a robust, auditable, and scientifically sound mechanism for these decisions. By operationalizing the abstract concepts of Zero Trust into concrete mathematical variables, organizations can navigate the complexities of the digital age with greater confidence. The convergence of rigorous personnel selection and advanced technology assessment creates a holistic security posture, one where trust is never assumed, but is continuously evaluated, verified, and mathematically validated.

References

1. Prassanna Rao Rajgopal. Secure Enterprise Browser - A Strategic Imperative for Modern Enterprises. International Journal of Computer Applications. 187, 33 (Aug 2025), 53-66. DOI=10.5120/ijca2025925611

2. Şenel, B.; Şenel, M.; Aydemir, G. Use and Comparison of Topis and Electre Methods in Personnel Selection. In Proceedings of the ITM Web of Conferences; EDP Sciences: Les Ulis, France, 2018.

3. Jasemi, M.; Ahmadi, E. A New Fuzzy ELECTRE Based Multiple Criteria Method for Personnel Selection. Sci. Iran. 2018, 25, 943–953.

4. Karabasevic, D.; Zavadskas, E.K.; Turskis, Z.; Stanujkic, D. The framework for the selection of personnel based on the SWARA and ARAS methods under uncertainties. Informatica 2016, 27, 49–65.

5. Ji, P.; Zhang, H.-Y.; Wang, J.-Q. A projection-based TODIM method under multi-valued neutrosophic environments and its application in personnel selection. Neural Comput. Appl. 2018, 29, 221–234.

6. Dung, V.; Thuy, L.T.; Mai, P.Q.; Van Dan, N.; Lan, N.T.M. TOPSIS Approach Using Interval Neutrosophic Sets for Personnel Selection; Infinite Study: Coimbatore, India, 2018.

7. Pramanik, S.; Dalapati, S.; Roy, T.K. Neutrosophic multi-attribute group decision making strategy for logistics center location selection. Neutrosophic Oper. Res. 2018, 3, 13–32.

8. Karabasevic, D.; Zavadskas, E.K.; Stanujkic, D.; Popovic, G.; Brzakovic, M. An approach to personnel selection in the IT industry based on the edas method. Transform. Bus. Econ. 2018, 17, 44.

9. Saaty, T.L. Decision Making with Dependence and Feedback: The Analytic Network Process; RWS Publ.: Pittsburgh, PA, USA, 1996; Volume 4922.

10. Saaty, T.L. The Analytic Hierarchy Process; McGraw Hill: New York, NY, USA, 1980.

11. Meade, L.; Sarkis, J. Analyzing organizational project alternatives for agile manufacturing processes: An analytical network approach. Int. J. Prod. Res. 1999, 37, 241–261.

12. Verizon. "Data Breach Investigations Report." [Online]. Available: https://www.verizon.com/business/resources/reports/dbir.

13. H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," Entropy, vol. 25, no. 12, p. 1595, Nov. 2023.

14. Kaggle. "Discussion on Zero Trust." [Online]. Available: https://www.kaggle.com/discussions/general/335189.

15. Department of Homeland Security. "Cybersecurity Impact." [Online]. Available: https://www.dhs.gov/archive/science-and-technology/cybersecurity-impact.

16. H. Ameer and H. Refaey, "Dissecting zero trust: Research landscape and its implementation in IoT," Cybersecurity Journal, SpringerOpen, 2022.

17. F. Abreu and M. Ziegler, "Dynamic access control models for IoT security under zero trust," Sensors, vol. 20, no. 14, p. 4023, MDPI, 2020.

18. Mehraj and T. Banday, "Trust evaluation mechanisms in zero trust cloud environments," International Journal of Cloud Computing and Security, vol. 9, no. 11, p. 1287, MDPI, 2020.

19. Kerman and S. Rose, "Implementing Zero Trust Architecture: Challenges and Strategies," NIST Special Publication, 2020.

20. Sharma, H. (2021). "Behavioral Analytics and Zero Trust." International Journal of Information Technology and Management Information Systems (IJITMIS), 12(1), 63-84.