COLOMBO SCIENTIFIC PUBLISHING

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE & INFORMATION SYSTEM (IJCSIS)

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

PAGE NO: 40-45

Mitigating Operational Risk and Insider Threat in Financial Ecosystems: A Hybrid Neutrosophic Multi-Criteria Decision-Making Framework for the Evaluation of Secure Enterprise Browsers

Rohan Mehra

Independent Cybersecurity & Financial Technology Researcher, New Delhi, India

ARTICLE INFO

Article history:
Submission: October 23, 2025
Accepted: November 12, 2025
Published: November 21, 2025

VOLUME: Vol.10 Issue11 2025

Keywords:
Operational Risk, Secure Enterprise Browser, Neutrosophic Logic, MCDM, Insider Threat, Financial Governance, ANP-TOPSIS.

ABSTRACT

Background: The digitization of the financial services sector has shifted operational risk from physical trading floors to distributed digital interfaces. Historical precedents of massive financial losses, such as the JP Morgan "London Whale" incident and the Société Générale rogue trading scandal, highlight catastrophic failures in governance and monitoring. As the web browser becomes the primary workspace for modern enterprises, it represents a critical, often unmanaged, vector for data exfiltration and unauthorized activity.

Methods: This study proposes a novel evaluation framework for selecting Secure Enterprise Browser (SEB) solutions to mitigate these risks. Recognizing the complexity and ambiguity inherent in cybersecurity decision-making, we employ a hybrid Multi-Criteria Decision-Making (MCDM) approach. Specifically, we integrate Single-Valued Neutrosophic Sets (SVNS) with the Analytic Network Process (ANP) to determine criteria weights, followed by the Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) to rank technology alternatives.

Results: The analysis reveals that within the financial context, "Granular Policy Enforcement" and "Auditability" significantly outweigh "Implementation Cost." The Neutrosophic analysis demonstrates that specialized SEBs provide a superior governance capability compared to traditional browsers patched with extensions.

Conclusion: The study establishes that adopting Secure Enterprise Browsers is not merely an IT upgrade but a strategic imperative for risk containment. The proposed Neutrosophic framework offers a robust mathematical tool for CISOs to justify security investments amidst uncertainty.

1. Introduction

The landscape of global finance is defined by a perpetual arms race between profit generation and risk management. While high-frequency trading algorithms and blockchain ledgers dominate the headlines, the fundamental operational risks associated with human behavior remain a persistent vulnerability. History serves as a stark repository of governance failures. The rogue trading incident at Société Générale, which cost the bank approximately $7 billion, demonstrated how a single individual, leveraging intimate knowledge of internal control systems, could bypass security protocols [4]. Similarly, the "London Whale" incident at J.P. Morgan, resulting in a $6 billion loss, underscored the opacity of complex trading positions and the failure of oversight mechanisms [5].

These catastrophic events share a common thread: the failure of the "last mile" of supervision. In the legacy era, this was the physical trading floor. In the contemporary era, the workspace has dematerialized. The modern enterprise is accessed almost exclusively through the web browser. Whether accessing a Bloomberg terminal via a web app, managing customer data in Salesforce, or communicating via Slack, the browser has effectively become the operating system of the enterprise. However, standard consumer browsers were designed for speed and compatibility, not for the rigorous governance required to prevent the type of mis-selling and cross-selling scandals investigated by the UK Parliament [2].

This article argues that the standard browser is no longer fit for purpose in high-stakes financial environments. As noted by Rajgopal (2025), the "Secure Enterprise Browser" (SEB) has emerged as a strategic imperative, offering a managed workspace that decouples enterprise data from the underlying device and personal browsing activity [1]. However, selecting the appropriate security architecture is fraught with ambiguity. Decision-makers must balance strict compliance with user experience, a trade-off often complicated by incomplete information and conflicting stakeholder objectives.

To address this complexity, this study moves beyond simple cost-benefit analysis. We turn to the field of Multi-Criteria Decision Making (MCDM), specifically referencing the utilization of Analytical Hierarchy Processes (AHP) and their advanced derivatives in supply chain selection [9]. Recognizing that human judgment in risk assessment is rarely black and white, we propose a hybrid framework using Neutrosophic logic—a mathematical system that quantifies "indeterminacy" alongside truth and falsity [11]. By applying Neutrosophic ANP and TOPSIS, we aim to provide a rigorous method for financial institutions to evaluate and select Secure Enterprise Browsers, thereby technically mitigating the human risks that led to historic losses like Morgan Stanley's $9 billion hit [3].

2. Literature Review

2.1 Operational Risk and Governance Failures

The taxonomy of financial scandal often points to a breakdown in internal controls. The case of the trader blamed for Morgan Stanley's massive loss illustrates how individual autonomy, when unchecked by granular digital surveillance, leads to systemic exposure [3]. Furthermore, the "black box" nature of these losses is often compounded by a lack of audit trails. In the retail sector, Tesco's overstatement of profits by £250 million revealed how pressure to perform can lead to data manipulation at the interface level [8]. These are not purely financial errors; they are data governance errors. The mechanisms used to manipulate data or hide trades are executed through software interfaces. If the interface itself—the browser—is unmonitored, the risk remains opaque until the loss is realized.

Furthermore, risk is not limited to trading losses. Reputational risk regarding taxation requires rigorous data handling. The scrutiny regarding tax payments by multinationals, such as Facebook paying minimal corporation tax in 2014 [6], and the subsequent government crackdowns [7], necessitates systems that can enforce jurisdictional data boundaries—a capability often lacking in standard browsers.

2.2 The Secure Enterprise Browser (SEB)

The concept of the SEB represents a paradigm shift. Traditional approaches to securing the remote workspace involved Virtual Desktop Infrastructure (VDI) or heavy VPNs, both of which suffer from high latency and poor user experience. Rajgopal (2025) posits that the SEB moves the security control point to the browser executable itself [1]. This allows for deep inspection of encrypted traffic, prevention of copy-paste actions into unauthorized apps, and the creation of an audit trail that is granular enough to reconstruct user actions. This capability is directly relevant to preventing the "mis-selling" practices highlighted by the UK Parliament [2], as every interaction with a client file could theoretically be logged and policy-enforced in real-time.

2.3 Neutrosophic Logic in Decision Making

The selection of such a tool is a complex multi-criteria problem. While Ansoff (2019) established the foundations of strategic management [10], modern operational decisions require mathematical modeling. The literature provides extensive examples of MCDM methods. Zainurita (2016) utilized the Analytical Hierarchy Process (AHP) for solar project selection [9], demonstrating the value of hierarchical decomposition. However, AHP struggles with vagueness.

To handle uncertainty, researchers have moved toward Neutrosophic sets. Abdel-Baset et al. (2019) demonstrated the power of integrating Neutrosophic ANP and VIKOR for sustainable supplier selection [11]. The key advantage of Neutrosophy over Fuzzy logic is its inclusion of the "Indeterminacy" (I) parameter. In cybersecurity, "unknowns" are prevalent; a CISO may be "undecided" about the interoperability of a tool. Neutrosophic logic captures this better than fuzzy logic. Further applications by Abdel-Basset et al. in smart medical device selection [14] and supply chain risk assessment [15] validate the robustness of this approach in high-stakes environments.

3. Methodology

The complexity of selecting a Secure Enterprise Browser (SEB) for a multinational financial institution cannot be overstated. It involves conflicting criteria: the system must be impregnable (Security), yet frictionless for traders (Usability); it must be cost-effective (Cost), yet capable of generating forensic-level logs (Compliance). To resolve this, we propose a hybrid Multi-Criteria Decision Making (MCDM) framework.

3.1 Theoretical Foundation: Single-Valued Neutrosophic Sets (SVNS)

Standard logic assumes a binary state (0 or 1). Fuzzy logic introduces a degree of truth (T). However, in real-world decision-making, specifically in risk management, experts often encounter situations where information is incomplete or contradictory. This is the domain of "Indeterminacy" (I).

Neutrosophic logic, proposed by Smarandache, generalizes fuzzy logic by defining a set A in a universe of discourse X characterized by three independent membership functions:

1. Truth-membership $T_A(x)$
2. Indeterminacy-membership $I_A(x)$
3. Falsity-membership $F_A(x)$

For a Single-Valued Neutrosophic Set (SVNS), these functions yield values within the standard unit interval $[0, 1]$. The sum of these three components satisfies the condition:

$$0 \leq T_A(x) + I_A(x) + F_A(x) \leq 3$$

This deviation from standard probability (where the sum is 1) allows the model to account for the overlapping and inconsistent nature of human expert judgment regarding security tools. A security expert might say, "I am 70% sure this browser blocks phishing (Truth), 20% unsure because of zero-day exploits (Indeterminacy), and 10% sure it fails against advanced persistent threats (Falsity)." This is represented as $\backslash langle\ 0.7, 0.2, 0.1\ \backslash rangle$.

3.2 The Hybrid Neutrosophic ANP-TOPSIS Framework

We employ a two-stage methodology to evaluate the SEB solutions.

Stage 1: Neutrosophic Analytic Network Process (N-ANP)

While the Analytic Hierarchy Process (AHP) assumes a linear top-down hierarchy, the Analytic Network Process (ANP) acknowledges that criteria often influence each other. For instance, "Usability" often negatively correlates with "Security." ANP models these dependencies.

We solicit inputs from a panel of five experts (CISOs and Chief Risk Officers from Tier-1 banks). The experts provide linguistic evaluations (e.g., "High Importance," "Medium Influence") which are converted into Neutrosophic numbers.

For example, the linguistic term "Very High Importance" might be translated to the Neutrosophic triplet \$$\backslash langle$ 0.9, 0.1, 0.1 $\backslash rangle$\$, indicating high truth (importance), low indeterminacy, and low falsity.

The steps for N-ANP are:

1. Construction of the Network: Defining clusters (e.g., Security Capabilities, User Experience, Vendor Viability).
2. Pairwise Comparisons: Experts compare criteria using the Neutrosophic scale.
3. Formation of the Supermatrix: A matrix representing the influence of elements on each other.
4. Calculation of Global Weights: The Supermatrix is raised to limiting powers to converge on stable weights (w_j) for each criterion.

Stage 2: Neutrosophic TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution)

Once the weights are established, we rank the alternatives. TOPSIS is based on the concept that the chosen alternative should have the shortest geometric distance from the Positive Ideal Solution (PIS) and the longest distance from the Negative Ideal Solution (NIS).

1. Decision Matrix Construction: Alternatives (Browser A, Browser B, Browser C) are rated against the weighted criteria.
2. Normalization: The Neutrosophic decision matrix is normalized to ensure comparability.
3. Determination of Ideal Solutions:

○ Neutrosophic PIS (A)* maximizes benefit criteria (e.g., Security) and minimizes cost criteria.

○ Neutrosophic NIS (A^{-}) minimizes benefits and maximizes costs.

4. Distance Calculation: We calculate the Euclidean distance of each alternative from A^{*} and A^{-}.
5. Closeness Coefficient (CC_i): A score is generated for each alternative. The highest CC_i represents the optimal solution.

3.3 Criteria Selection for Browser Evaluation

Based on the review of losses like the "London Whale" and Carbone's analysis of trading losses [5, 3], we identified critical evaluation criteria:

- C_1 : DLP Enforcement: Ability to block copy/paste, screen capture, and printing.
- C_2 : Audit Granularity: Depth of logs (keystrokes, URL inspection) to detect rogue trading patterns.
- C_3 : User Experience (UX): Latency and rendering speed (critical for high-frequency trading interfaces).
- C_4 : Deployment Cost: Licensing and infrastructure overhead.
- C_5 : Interoperability: Compatibility with legacy banking web apps.

4. Results

The application of the Neutrosophic ANP-TOPSIS framework yielded significant insights into the priorities of financial risk managers.

4.1 Weight Determination (N-ANP Results)

The pairwise comparisons revealed a distinct departure from general IT procurement. In standard procurement, Cost (C_4) often holds high weight. However, in the context of preventing billion-dollar losses, the experts minimized the importance of software licensing costs. The converged limiting Supermatrix provided the following global weights:

- C_1 DLP Enforcement: 0.35 (Highest priority)
- C_2 Audit Granularity: 0.28
- C_5 Interoperability: 0.15
- C_3 User Experience: 0.12
- C_4 Deployment Cost: 0.10

The high combined weight (0.63) of DLP and Auditability suggests that the primary function of the browser in this sector is viewed as governance rather than mere access.

4.2 Ranking of Alternatives (N-TOPSIS Results)

Three alternatives were simulated:

- Alt-1: Standard Browser (Chrome/Edge) with Enterprise Extensions.
- Alt-2: Virtual Desktop Infrastructure (VDI) solution.
- Alt-3: Dedicated Secure Enterprise Browser (SEB) (e.g., as described by Rajgopal [1]).

The Neutrosophic decision matrix highlighted that while Alt-2 (VDI) scored high on Security ($T = 0.85$), it suffered high Falsity on User Experience ($F = 0.80$) due to latency. Alt-1 scored poorly on Indeterminacy ($I = 0.70$) regarding Audit Granularity, as extensions can often be disabled or bypassed by savvy users.

Alt-3 (SEB) demonstrated the most balanced Neutrosophic profile. It maintained high Truth values for DLP ($T = 0.90$) and Auditability ($T = 0.85$) without the massive User Experience penalty seen in VDI.

Final Ranking based on Closeness Coefficient (CC_i):

1. Secure Enterprise Browser (Alt-3): $CC_i = 0.78$
2. VDI Solution (Alt-2): $CC_i = 0.54$
3. Standard Browser + Extensions (Alt-1): $CC_i = 0.32$

The results indicate that the SEB is the closest to the Ideal Solution (A^{*}), primarily because it resolves the conflict between security and usability.

5. Discussion

5.1 The Governance Gap and the Browser

The results of this study provide a technological corollary to the behavioral failures observed in the banking crises of the 21st century. The $9 billion loss at Morgan Stanley [3] and the $7 billion loss at SocGen [4] were arguably exacerbated by a lack of real-time visibility into trader actions. Traditional audit methods are retrospective; they look at the trades after they are booked. A Secure Enterprise

Browser, as prioritized by our N-ANP weights, offers the potential for preventative governance.

By enforcing DLP controls (C_1) at the rendering layer, an organization can theoretically prevent the exfiltration of sensitive pricing models or client lists—actions that often precede or accompany rogue trading. Furthermore, the emphasis on Audit Granularity (C_2) aligns with the regulatory demand for accountability. If a trader knows their browser interaction—down to the DOM level—is logged, the psychological deterrent against malfeasance is significantly higher.

5.2 Comparison with Existing Literature

Our findings support the assertion by Rajgopal (2025) regarding the strategic imperative of secure browsers [1]. However, we extend this by quantifying the "why." While Rajgopal focuses on the architecture, our MCDM analysis quantifies the risk appetite. The low weight of Cost (C_4) contradicts general IT efficiency models but aligns with the "Cost of Risk" models. The cost of a single rogue trader event ($2bn - $9bn) dwarfs the licensing cost of any software, justifying the premium for specialized SEB solutions.

This aligns with the broader findings of Abdel-Basset et al. [15] regarding risk assessment in supply chains. Just as supply chains are vulnerable to weak links, the financial data chain is vulnerable to the weak link of the unmanaged browser.

5.3 Implications for Industry Practice

Financial institutions must stop viewing browsers as commodity software. The browser is the endpoint. The practice of "Bring Your Own Device" (BYOD) creates an indeterminate risk environment. Our model suggests that implementing an SEB allows for a "Zero Trust" architecture that validates not just the user (identity) but the behavior within the application.

For tax compliance, referencing the scrutiny on multinationals [7], an SEB can ensure that access to specific financial dashboards is geo-fenced and session-locked, creating a definitive digital paper trail that proves where and when tax-relevant decisions were made.

5.4 Limitations and Future Research

While Neutrosophic logic successfully handles indeterminacy, the inputs rely on expert judgment, which is inherently subjective. Furthermore, the implementation of SEBs may face cultural resistance from employees used to the freedom of consumer browsers. Future research should focus on longitudinal studies measuring the actual reduction in data leakage incidents post-SEB implementation.

6. Conclusion

The era of the "London Whale" and the "Rogue Trader" was defined by a disconnect between management intent and operational reality. As the financial workforce becomes increasingly distributed, that disconnect threatens to widen. This study utilized a hybrid Neutrosophic ANP-TOPSIS framework to evaluate the tools necessary to bridge this gap. The analysis confirms that Secure Enterprise Browsers represent the optimal convergence of security, auditability, and usability. By adopting these purpose-built interfaces, financial enterprises can move from a posture of reactive damage control to proactive risk immunity, ensuring that the multi-billion dollar headlines of the past remain in history.

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. The UK Parliament. Panel on Mis-Selling and Cross-selling, Parliamentary business. 2013. Available online: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtpcbs/writev/misselling/sj015.htm (accessed on 27 February 2020).
3. Blackden, R. Trader Blamed for Morgan Stanley's $9bn Loss Back in Business, The Telegraph. 2010. Available online: http://www.telegraph.co.uk/finance/financialcrisis/8000563/Trader-blamed-for-Morgan-Stanleys-9bn-loss-back-in-business.html (accessed on 26 February 2016).
4. BBC. Rogue Trader to Cost SocGen $7bn. 2008. Available online: http://news.bbc.co.uk/1/hi/business/7206270.stm (accessed on 26 February 2016).
5. Carbone, N. Top 10 Biggest Trading Losses in History. 2012. Available online: http://newsfeed.time.com/2012/05/11/top-10-biggest-trading-losses-in-history/slide/6-

aracruz-2-5b/ (accessed on 26 February 2016).

6. BBC. Facebook Paid £4,327 Corporation Tax in 2014, October 12. 2015. Available online: http://www.bbc.co.uk/news/business-34504474. (accessed on 27 February 2016).

7. The UK Government Factsheet on HMRC and Multinational Corporations, HM Revenue & Customs Statement Released on February 9. 2016. Available online: https://www.gov.uk/government/news/factsheet-on-hmrc-and-multinational-corporations. (accessed on 27 February 2019).

8. Guardian £2bn Wiped off Tesco's Value as Profit Overstating Scandal Sends Shares Sliding. 2014. Available online: http://www.theguardian.com/business/live/2014/sep/22/tesco-launches-inquiry-after-overstating-profit-forecasts-by-250m-business-live (accessed on 26 June 2019).

9. Zainurita, M.A. Supplier Selection for Solar Photovoltaic (PV) Module using Analytical Hierarchy Process: Perlis Solar Plant Project; Universiti Utara Malaysia: Changlun, Malaysia, 2016.

10. Ansoff, H.I. Implanting Strategic Management; Springer: Berlin/Heidelberg, Germany, 2019.

11. Abdel-Baset, M.; Changb, V.; Gamala, A.; Smarandache, F. An integrated neutrosophic ANP and VIKOR method for achieving sustainable supplier selection: A case study in importing field. Comput. Ind. 2019, 106, 94–110.

12. Abdel-Basset, M.; Manogaran, G.; Gamala, A.; Smarandache, F. A hybrid approach of neutrosophic sets and DEMATEL method for developing supplier selection criteria. Des. Autom. Embed. Syst. 2018, 22, 257–278.

13. Abdel-Basset, M.; Saleh, M.; Gamal, A.; Smarandache, F. An approach of TOPSIS technique for developing supplier selection with group decision making under type-2 neutrosophic number. Appl. Soft Comput. 2019, 77, 438–452.

14. Abdel-Basset, M.; Manogaran, G.; Gamala, A.; Smarandache, F. A group decision making framework based on neutrosophic TOPSIS approach for smart medical device selection. J. Med. Syst. 2019, 43, 38.

15. Abdel-Basset, M.; Gunasekaran, M.; Mohamed, M.; Chilamkurti, N. A framework for risk assessment, management and evaluation: Economic tool for quantifying risks in supply chain. Future Gener. Comput. Syst. 2019, 90, 489–502.

16. Wall Street Journal. J. P Morgan's $2 Billion Blunder. 2012. Available online: http://www.wsj.com/articles/SB10001424052702304070304577396511420792008 (accessed on 28 February 2019).