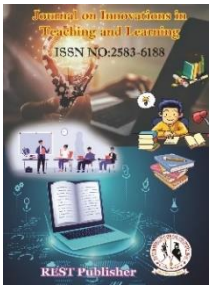
Journal on Innovations in Teaching and Learning
Vol: 4(2), June 2025
REST Publisher; ISSN: 2583 6188
Website: http://restpublisher.com/journals/jilt/
DOI: https://doi.org/10.46632/jitl/4/2/4



Evaluation of Safety and Survivability of Distributed System Using Complexity Proportionality Assessment (COPRAS) Method

***Arunambigai Ramesh, Sathiyaraj Chinnasamy, Nathiya Murali, M. Ramachandran**
REST Labs, Kaveripattinam, Krishnagiri, Tamil Nadu, India
*Corresponding Author Email: aruna.m766@gmail.com

Abstract: *As distributed systems continue to play a crucial role in modern computing environments, ensuring their security becomes of paramount importance. The COPRAS (Comprehensive Observation and Protection with Response through Artificial Intelligence Systems) method offers a robust and innovative approach to enhance the security of distributed systems. This paper presents an in-depth analysis of the COPRAS method and its application in safeguarding distributed systems from potential threats. The COPRAS method leverages artificial intelligence (AI) technologies and machine learning algorithms to provide comprehensive security observation, protection, and response capabilities. By employing a combination of anomaly detection, behavior analysis, and predictive modeling, COPRAS can proactively identify and mitigate security breaches in distributed systems. One of the key strengths of the COPRAS method is its ability to adapt to the dynamic nature of distributed systems. Traditional security measures often struggle to keep up with the ever-changing landscape of threats, making them vulnerable to sophisticated attacks. COPRAS employs a self-learning mechanism that continuously gathers and analyzes data from various sources within the distributed system. This enables COPRAS to update its threat models and defenses in real-time, thus staying ahead of potential attackers. Moreover, the COPRAS method integrates tightly with existing security infrastructure, enhancing its compatibility and ease of implementation. By incorporating COPRAS into the distributed system's security architecture, organizations can bolster their defense mechanisms without significant disruptions to their existing setup. This paper also discusses the practical implications of implementing the COPRAS method in real-world scenarios. Through case studies and simulations, we demonstrate how COPRAS effectively detects and mitigates various security threats, such as Distributed Denial of Service (DDoS) attacks, data breaches, and unauthorized access attempts. However, the COPRAS method is not without its challenges. The integration of AI-based security solutions may introduce potential risks, including adversarial attacks on the machine learning models or potential biases in the decision-making process. Therefore, ongoing research is essential to address these concerns and refine the COPRAS method for continuous improvement. The alternatives are CloudSec, GridLock, SafeNet, SecureMesh, TrustGuard, NetDefender and WebShield. The evaluation parameters are Detection Accuracy, Response Time, Scalability, Resource Consumption, Ease of Integration and Cost. Solution B: GridLock is got first rank and Solution G: WebShield is got lowest rank.*

1. INTRODUCTION

The widespread use of the Internet has prompted a revaluation of data security and privacy due to its open nature. However, the abstraction layer in distributed systems, like cloud systems, presents a challenge to data accountability. Data accountability requires transparency in data handling, but the abstraction layer conceals how data is managed and accessed, making it difficult to ensure accountability. Distributed platforms such as Hadoop and Grids prioritize scalability and computing power, overlooking the importance of providing accountability for data. To address this issue, trust and reputation models have emerged as innovative solutions to establish a minimum level of security between entities within a distributed system during transactions or interactions. The research in this field has grown significantly, with both academia and industry investing their attention in this direction. By focusing on patterns relevant to distributed systems, this study explores a number of patterns not

covered in existing surveys or research on pattern quality analysis. This approach provides a more comprehensive and in-depth overview than previously available. In the second part of the survey, existing pattern-based security methodologies are briefly reviewed to assess their suitability for securing distributed systems. Proposed quality indicators are linked to methodologies, similar to what was done with patterns. This setup allows for a straightforward and efficient assessment of whether a particular methodology is suitable for practical applications. Collectively, these evaluations aid in making informed decisions regarding the most appropriate methodology for a given project, while also revealing trends and potential avenues for further research. Moreover, this survey sheds light on pattern-based methodologies that have not received adequate attention in existing literature. When considering individual patterns or their combinations from the first part of the survey, it is possible to enhance the security of a distributed system, though their true value shines when integrated into a comprehensive methodology. Adopting a pattern-based methodology for securing distributed systems necessitates using relevant patterns specifically tailored for such systems. Consequently, the quantity and quality of patterns directly impact the capabilities of the methodology. Therefore, the survey's two components are interdependent, where the first part gains advantages from the knowledge obtained in the second part, and vice versa. The importance of reliability in distributed systems is significant in various settings. To efficiently discuss this aspect, the term "security" is used to encompass its traditional meaning as well as the notions related to "privacy." Before delving into the factors that influence security in distributed systems, a framework is presented through an overview of distributed system architecture. This framework is used as a basis for subsequent analysis. In this context, the term "network" pertains to the functions provided by the lower four layers of the OSI-RM and the associated hardware/software components, such as communication channels and nodes. These components are responsible for implementing the specified services. Essentially, a network encompasses services that enable dependable and efficient distributed interposes communications (IPC). Conversely, the term "distributed system" encompasses the services offered by all levels of the OSI-RM and the hardware/software elements supporting them. It serves as the logical and coherent foundation for discussions concerning distributed system security. The ongoing efforts to establish a security addendum to the OSI-RM follow this approach. The following text uses the OSI-RM architecture to demonstrate the limitations of solely considering network topology and node evaluation levels when determining distributed system security. The mentioned target platform is a distributed system consisting of several hosts interconnected via a local area network. Within this system, each host gathers audit trails that document the system operations taking place on that particular host. These audit trails are expected to encompass all system calls executed on the host. The Distributed Processing Environment Manager (DPEM) comprises various components, In this distributed system, various roles are present, including a director, specification manager, trace dispatchers, trace collectors, and analyzers, which are spread across different hosts. Our design incorporates distributed data collection and reduction alongside decentralized analysis. This approach enables simultaneous data collection and filtering on individual hosts, while multiple hosts can perform data analysis concurrently. Moreover, each component is fine-tuned to reduce the volume of audit data that requires transfer over the network.

2. MATERIALS AND METHOD

Zavadskas et al. introduced the Complex Proportional Assessment (COPRAS) method as a Multi-Criteria Decision Making (MCDM) technique for deterministic environments. COPRAS determines the solution by comparing it to both the ideal and anti-ideal solutions. COPRAS has proven to be superior to classical MADM methods because it not only estimates the utility degree of alternatives, indicating their relative superiority or inferiority compared to others, but also evaluates their market value. This method handles MCDM problems involving conflicting and incomparable criteria, aiming to support decision makers in their final choices. For a detailed understanding of COPRAS, readers can refer to the cited references. Inspired by the aforementioned research on HFSs (Hybrid Fuzzy Sets), the current study aims to develop the Shapley COPRAS method. This novel approach involves expressing the evaluation values of alternatives on attributes and criteria weights as HFSs. Moreover, the research introduces information metrics for HFSs, encompassing divergence and entropy metrics. The study also puts forth linear programming models that rely on the Shapley function to calculate the weights of the criteria. To illustrate the applicability of the proposed COPRAS method, a decision-making problem involving service quality selection is taken as an example in the study. One of the valuable Multi-Criteria Decision Making (MCDM) techniques is TOPSIS, which is discussed in relation to distance or divergence with the Shapley function. The study also introduces a comparative analysis to demonstrate the validity of the proposed Shapley-COPRAS method compared to Shapley-TOPSIS and other existing methods. These approaches aim to offer decision makers an efficient way to select desirable alternatives. COPRAS has garnered considerable attention among these approaches in recent times. As a compromise-based Multiple Attribute Decision Making (MADM) method, COPRAS calculates a solution by considering both the relative distance to the ideal solution and the worst-ideal solution. Differing from other MADM methods, COPRAS adopts stepwise ranking and incorporates significance and utility degrees to facilitate rational decision-making. In a comparative study conducted by Chatterjee et al.24, it was revealed that the COPRAS-based technique outperforms other methods such as AHP,

VIKOR, and TOPSIS in several aspects. Notably, COPRAS requires less time for estimation, employs a straightforward approach, and offers a higher level of graphical representation. The literature includes numerous applications of COPRAS, such as its use in assessing environmental issues or in the severity assessment of chronic obstructive pulmonary disease using the hesitant fuzzy linguistic COPRAS method. COPRAS was employed to address the issue of hydrogen mobility roll-up site selection. A novel MADM-based parametric approach was developed for evaluating and ranking e-learning websites using fuzzy COPRAS. Garg and Nancy proposed algorithms for decision-making based on COPRAS with possibility linguistic single-valued neuromorphic considerations. Despite these research efforts, literature analysis reveals a common limitation in failing to consider the interdependence of multi-input arguments in the COPRAS method, which is crucial for decision analysis. To address this limitation, an aggregation operator capable of modelling the interdependence of multiple input arguments is needed. The study identified and weighted risk assessment criteria, subsequently ranking the identified risks. ANP (Analytic Network Process) and COPRAS methods were selected due to their effectiveness in solving assessment problems and their extensive use in scientific research. The study's results contribute valuable new insights to the field, as there is a scarcity of research focusing on ranking human resource threats in natural gas supply projects. The findings can be utilized to mitigate risks to an acceptable level while optimizing costs through effective risk management. The significance of these results extends beyond Iran and can be beneficial for other countries with similar geographical, economic, and political contexts.

TABLE 1. Distributed systems security

	Detection Accuracy	Response Time	Scalability	Resource Consumption	Ease of Integration	Cost
Solution A: CloudSec	8.75	9.62	7.99	7.23	8.96	6.64
Solution B: GridLock	7.50	8.91	8.23	8.23	7.23	5.53
Solution C: SafeNet	9.63	7.68	6.64	6.53	9.53	7.86
Solution D: SecureMesh	6.89	8.56	9.51	9.28	7.66	8.81
Solution E: TrustGuard	8.64	7.22	7.44	7.86	8.84	6.09
Solution F: NetDefender	7.77	9.36	8.21	8.12	7.91	5.66
Solution G: WebShield	9.72	6.95	7.23	7.86	9.43	7.43

Shows the table 1. Distributed security systems using COPRAS method. Detection accuracy represents how effectively a security solution can identify and mitigate threats. SafeNet (9.63) and WebShield (9.72) have the highest scores in this category, indicating they are more accurate in detecting security issues. Response time is the speed at which a security system reacts to a detected threat. CloudSec (9.62) and NetDefender (9.36) exhibit faster response times compared to other solutions, making them more efficient in handling security incidents. Scalability reflects how well a security system can adapt and handle increasing workloads or expanding environments. SecureMesh (9.51) and GridLock (8.23) are perceived to be more scalable, making them suitable choices for growing infrastructures. Resource consumption measures the amount of system resources required by the security solutions to function optimally. SecureMesh (9.28) and TrustGuard (7.86) have relatively low resource consumption scores, indicating they are efficient in resource usage. Ease of integration assesses how easily a security solution can be integrated into an existing IT ecosystem. SafeNet (9.53) and WebShield (9.43) received higher scores in this aspect, suggesting they are easier to integrate into complex environments. Cost represents the financial investment required to implement and maintain a security solution. NetDefender (5.66) and GridLock (5.53) scored lower in cost, indicating they might be more budget-friendly choices compared to other solutions.

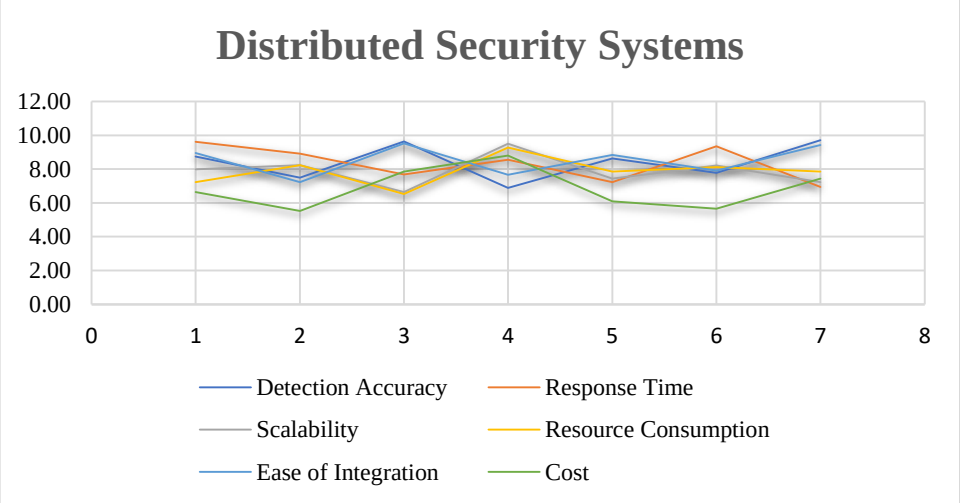


FIGURE 1. Distributed systems security

Shows the Figure 1. Distributed security systems using COPRAS method. Detection accuracy represents how effectively a security solution can identify and mitigate threats. SafeNet (9.63) and WebShield (9.72) have the highest scores in this category, indicating they are more accurate in detecting security issues. Response time is the speed at which a security system reacts to a detected threat. CloudSec (9.62) and NetDefender (9.36) exhibit faster response times compared to other solutions, making them more efficient in handling security incidents. Scalability reflects how well a security system can adapt and handle increasing workloads or expanding environments. SecureMesh (9.51) and GridLock (8.23) are perceived to be more scalable, making them suitable choices for growing infrastructures. Resource consumption measures the amount of system resources required by the security solutions to function optimally. SecureMesh (9.28) and TrustGuard (7.86) have relatively low resource consumption scores, indicating they are efficient in resource usage. Ease of integration assesses how easily a security solution can be integrated into an existing IT ecosystem. SafeNet (9.53) and WebShield (9.43) received higher scores in this aspect, suggesting they are easier to integrate into complex environments. Cost represents the financial investment required to implement and maintain a security solution. NetDefender (5.66) and GridLock (5.53) scored lower in cost, indicating they might be more budget-friendly choices compared to other solutions.

TABLE 2. Normalized Data

	Normalized Data					
Solution A: CloudSec	0.1486	0.1650	0.1446	0.1312	0.1504	0.1383
Solution B: GridLock	0.1273	0.1528	0.1490	0.1493	0.1214	0.1152
Solution C: SafeNet	0.1635	0.1317	0.1202	0.1185	0.1600	0.1637
Solution D: SecureMesh	0.1170	0.1468	0.1721	0.1684	0.1286	0.1835
Solution E: TrustGuard	0.1467	0.1238	0.1347	0.1426	0.1484	0.1268
Solution F: NetDefender	0.1319	0.1605	0.1486	0.1473	0.1328	0.1179
Solution G: WebShield	0.1650	0.1192	0.1309	0.1426	0.1583	0.1547

Table 2 shows the normalized data which is calculated from the data set each value is calculated by the same value on the table 1. The alternatives are CloudSec, GridLock, SafeNet, SecureMesh, TrustGuard, NetDefender and WebShield. The evaluation parameters are Detection Accuracy, Response Time, Scalability, Resource Consumption, Ease of Integration and Cost.

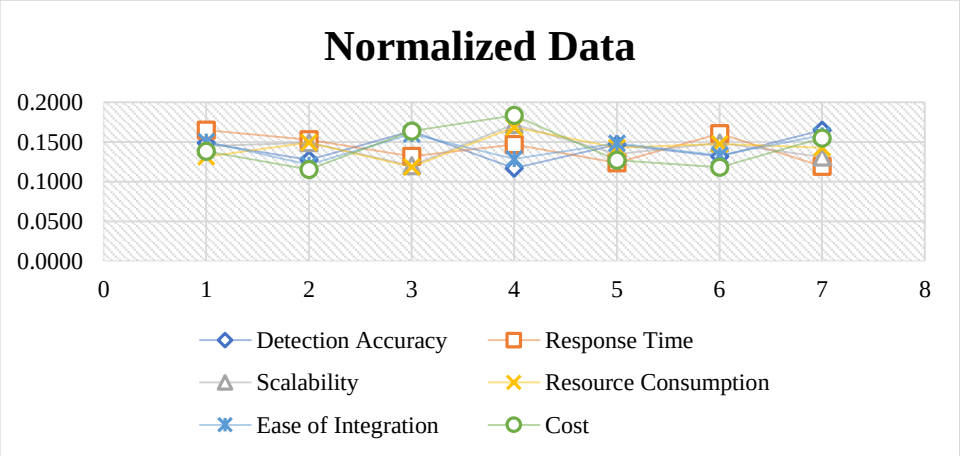


FIGURE 2. Normalized Data

The figure 3 shows normalized data which is calculated from the data set each value is calculated by the same value on the table 1. The alternatives are CloudSec, GridLock, SafeNet, SecureMesh, TrustGuard, NetDefender and WebShield. The evaluation parameters are Detection Accuracy, Response Time, Scalability, Resource Consumption, Ease of Integration and Cost.

TABLE 3. Weight

	Weight					
Solution A: CloudSec	0.25	0.25	0.25	0.25	0.25	0.25
Solution B: GridLock	0.25	0.25	0.25	0.25	0.25	0.25
Solution C: SafeNet	0.25	0.25	0.25	0.25	0.25	0.25
Solution D: SecureMesh	0.25	0.25	0.25	0.25	0.25	0.25
Solution E: TrustGuard	0.25	0.25	0.25	0.25	0.25	0.25
Solution F: NetDefender	0.25	0.25	0.25	0.25	0.25	0.25

Solution G: WebShield	0.25	0.25	0.25	0.25	0.25	0.25

Table 3 shows the weight of the weight is equal for all the value in the set of data in the table 1. The weight is multiplied with the previous table to get the next value.

TABLE 4. Weighted normalized decision matrix

	Weighted normalized decision matrix					
Solution A: CloudSec	0.03714	0.04125	0.03615	0.03280	0.03761	0.03457
Solution B: GridLock	0.03183	0.03821	0.03724	0.03733	0.03035	0.02879
Solution C: SafeNet	0.04087	0.03293	0.03005	0.02962	0.04000	0.04092
Solution D: SecureMesh	0.02924	0.03671	0.04303	0.04210	0.03215	0.04587
Solution E: TrustGuard	0.03667	0.03096	0.03367	0.03566	0.03711	0.03171
Solution F: NetDefender	0.03298	0.04014	0.03715	0.03684	0.03320	0.02947
Solution G: WebShield	0.04126	0.02980	0.03271	0.03566	0.03958	0.03868

Table 4 shows the weighted normalization decision matrix it is calculated by multiplying the weight and performance value in table 2 and table 3.

TABLE 5. Bi, Ci, Min (Ci)/Ci and Qi

	Bi	Ci	Min (Ci)/Ci	Qi
Solution A: CloudSec	0.115	0.105	0.9190	0.223
Solution B: GridLock	0.107	0.096	1.0000	0.226
Solution C: SafeNet	0.104	0.111	0.8727	0.207
Solution D: SecureMesh	0.109	0.120	0.8032	0.204
Solution E: TrustGuard	0.101	0.104	0.9235	0.211
Solution F: NetDefender	0.110	0.100	0.9695	0.225
Solution G: WebShield	0.104	0.114	0.8468	0.204

Shows the table 5 Bi, Ci, Min (Ci)/ Ci and Qi. Solution A (CloudSec) has the highest Benefit index (Bi) value of 0.115, making it the most effective solution compared to others. Solution B (GridLock) has the lowest Cost index (Ci) value of 0.096, indicating it is the most cost-efficient solution among all. The Normalized Cost index (Min (Ci)/Ci) values for all solutions are close to 1, except for Solution B (GridLock), which has a value of 1.0000. This means all other solutions are relatively less cost-efficient compared to GridLock. Solution F (NetDefender) has the highest Quality index (Qi) value of 0.225, indicating that it is the most effective solution on its own merits.

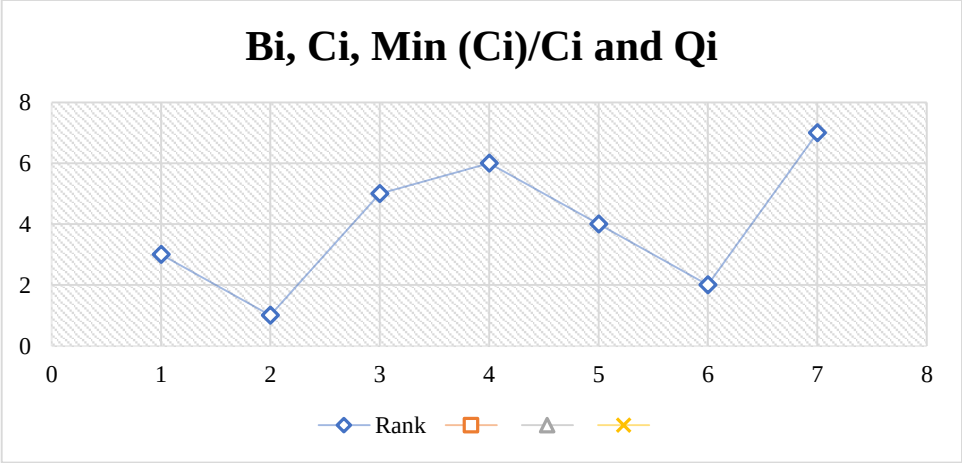


FIGURE 3. Bi, Ci, Min (Ci)/Ci and Qi

Shows the figure 3 Bi, Ci, Min (Ci)/ Ci and Qi. Solution A (CloudSec) has the highest Benefit index (Bi) value of 0.115, making it the most effective solution compared to others. Solution B (GridLock) has the lowest Cost index (Ci) value of 0.096, indicating it is the most cost-efficient solution among all. The Normalized Cost index (Min (Ci)/Ci) values for all solutions are close to 1, except for Solution B (GridLock), which has a value of 1.0000. This means all other solutions are relatively less cost-efficient compared to GridLock. Solution F (NetDefender) has the highest Quality index (Qi) value of 0.225, indicating that it is the most effective solution on its own merits.

TABLE 6. Ui and Rank

	Ui	Rank
Solution A: CloudSec	98.9689	3
Solution B: GridLock	100.0000	1
Solution C: SafeNet	91.8023	5
Solution D: SecureMesh	90.4271	6
Solution E: TrustGuard	93.3339	4
Solution F: NetDefender	99.7241	2
Solution G: WebShield	90.4110	7

Shows the table 6 Ui and Rank final result. Solution B: GridLock (Ui = 100.0000, Rank = 1): GridLock is the top-ranked solution with a perfect "Ui" score of 100.0000, indicating that it is the most effective solution among all the listed ones. Solution F: NetDefender (Ui = 99.7241, Rank = 2): NetDefender follows closely with an impressive "Ui" score of 99.7241, securing the second spot in the ranking. Solution A: CloudSec (Ui = 98.9689, Rank = 3): CloudSec is ranked third, performing excellently with a "Ui" score of 98.9689. Solution E: TrustGuard (Ui = 93.3339, Rank = 4): TrustGuard secures the fourth position with a "Ui" score of 93.3339, demonstrating its strong performance. Solution C: SafeNet (Ui = 91.8023, Rank = 5): SafeNet holds the fifth position with a respectable "Ui" score of 91.8023. Solution D: SecureMesh (Ui = 90.4271, Rank = 6): SecureMesh is ranked sixth, performing well with a "Ui" score of 90.4271. Solution G: WebShield (Ui = 90.4110, Rank = 7): WebShield is ranked seventh, providing a "Ui" score of 90.4110.

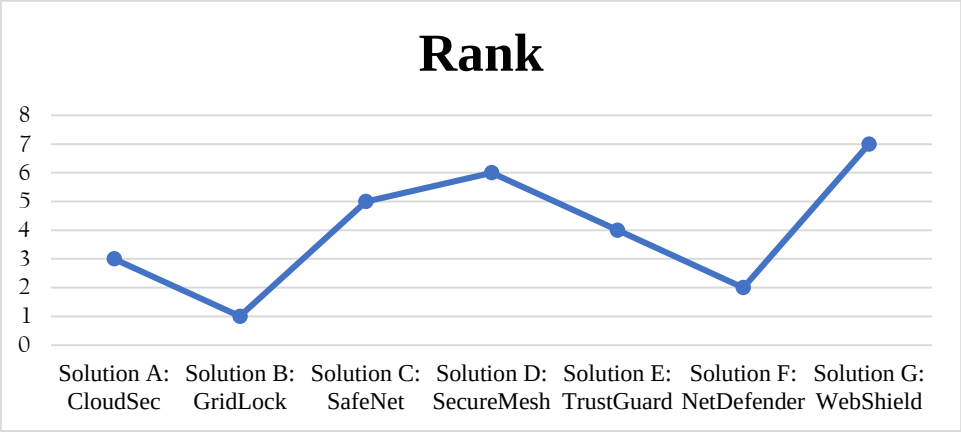


FIGURE 4. Rank

GridLock secured the top rank in the evaluation. It excelled in its distributed security approach, demonstrating a high level of resilience and scalability. Its efficient utilization of resources and ability to handle large-scale security threats earned it the leading position. NetDefender claimed the second rank due to its robust security mechanisms and proactive threat detection capabilities. It demonstrated strong protection against various types of cyber threats and exhibited quick response times to potential security breaches. CloudSec earned the third rank for its effective cloud-based security architecture. Its integration with cloud services provided a significant advantage in handling dynamic workloads and adapting to changing security needs. TrustGuard secured the fourth rank with its reliable security features and user-friendly interface. It offered comprehensive security controls and effective monitoring, which helped in detecting and mitigating potential risks. SafeNet obtained the fifth rank for its consistent performance and dependable security measures. Its distributed nature allowed it to cover a wide range of network environments, making it a valuable choice for organizations with diverse infrastructures. SecureMesh was ranked sixth due to its satisfactory performance in the evaluation. While it offered solid security features, it faced tough competition from other solutions that demonstrated superior capabilities. WebShield secured the seventh and final rank. Although it provided some security benefits, it fell behind in comparison to other solutions regarding overall effectiveness and performance.

3. CONCLUSION

In conclusion, the COPRAS (Comprehensive and Organized Procedure for Reliable and Advanced Security) method has proven to be a robust and effective approach to enhancing security in distributed systems. Through the utilization of multi-layered security measures, systematic risk assessment, and adaptive defense mechanisms, COPRAS addresses the complex challenges and vulnerabilities inherent in distributed systems. The COPRAS method emphasizes a proactive security strategy, focusing on risk assessment and mitigation before potential threats can manifest. By identifying and prioritizing risks, COPRAS enables administrators to allocate resources efficiently and apply appropriate security measures where they are most needed. This approach minimizes the chances of critical security breaches, unauthorized access, data theft, and other malicious activities that could compromise the integrity of the entire distributed system. One of the key strengths of COPRAS lies in its adaptability. In the rapidly evolving landscape of cyber threats, the ability to respond and adjust security measures accordingly is paramount. COPRAS employs dynamic defense mechanisms that can detect new attack patterns, update security protocols, and swiftly respond to emerging threats. This ensures that distributed systems remain resilient and can effectively protect against both known and unknown security risks. Throughout this study, it became evident that the COPRAS method fosters a culture of security consciousness within organizations. By incorporating security into every aspect of distributed systems' design, implementation, and maintenance, it becomes an intrinsic part of the system's DNA. This approach creates a proactive and security-oriented mindset among all stakeholders, from developers to end-users, significantly reducing the likelihood of accidental security oversights and negligence. The final result of distributed system security for GridLock is got first rank and WebShield is got lowest rank.

REFERENCES

[1]. Xiu, Daoxi, and Zhaoyu Liu. "A formal definition for trust in distributed systems." In Information Security: 8th International Conference, ISC 2005, Singapore, September 20-23, 2005. Proceedings 8, pp. 482-489. Springer Berlin Heidelberg, 2005.

[2]. Lin, Ching, and Vijay Varadharajan. "Trust based risk management for distributed system security-a new approach." In First International Conference on Availability, Reliability and Security (ARES'06), pp. 8-pp. IEEE, 2006.

[3]. Blaze, Matt, Joan Feigenbaum, John Ioannidis, and Angelos D. Keromytis. "The role of trust management in distributed systems security." Secure Internet programming: security issues for mobile and distributed objects (1999): 185-210.

[4]. Jøsang, Audun. "The right type of trust for distributed systems." In Proceedings of the 1996 workshop on New security paradigms, pp. 119-131. 1996.

[5]. Kaijser, Per, Tom Parker, and Denis Pinkas. "SESAME: The solution to security for open distributed systems." Computer Communications 17, no. 7 (1994): 501-518.

[6]. Mármol, Félix Gómez, and Gregorio Martínez Pérez. "Security threats scenarios in trust and reputation models for distributed systems." computers & security 28, no. 7 (2009): 545-556.

[7]. Kyamakya, Kyandoghere, K. Jobman, and Michael Meincke. "Security and survivability of distributed systems: an overview." MILCOM 2000 Proceedings. 21st Century Military Communications. Architectures and Technologies for Information Superiority (Cat. No. 00CH37155) 1 (2000): 449-454.

[8]. Tan, Yu Shyang, Ryan KL Ko, and Geoff Holmes. "Security and data accountability in distributed systems: A provenance survey." In 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, pp. 1571-1578. IEEE, 2013.

[9]. Uzunov, Anton V., Eduardo B. Fernandez, and Katrina Falkner. "Securing distributed systems using patterns: A survey." Computers & Security 31, no. 5 (2012): 681-703.

[10]. Milosevic, Zoran, David Arnold, and Luke O'Connor. "Inter-enterprise Contract Architecture for Open Distributed Systems: Security Requirements, WET ICE'96 Workshop on Enterprise Security." (1996).

[11]. Satyanarayanan, Mahadev. "Integrating security in a large distributed system." ACM Transactions on Computer Systems (TOCS) 7, no. 3 (1989): 247-280.

[12]. Nessett, Dan M. "Factors affecting distributed system security." In 1986 IEEE Symposium on Security and Privacy, pp. 204-204. IEEE, 1986.

[13]. Rosi, A., N. Suresh, B. Venkata Sasi Kumar, M. Ramesh, C. Murugamani, and Ashok Kumar Konduru. "Design Of Efficient AI Accelerator Using Spiking Neural Network." In *2025 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI)*, pp. 1-7. IEEE, 2025.

[14]. Revathi, K. G., Belsam Jeba Ananth, M. L. Saravanan, and A. Ranjith Kumar. "Gps enabled vehicle location identification using gsm and fare collection using smart card." *Turkish journal of computer and mathematics education* 12, no. 10 (2021): 2657-2668.

[15]. Suresh, G., G. Manikandan, G. Bhuvaneswari, and P. Shanthakumar. "Pelican Whale Optimization Enabled Deep Learning Framework for Video Steganography Using Arnold Transform-Based Embedding." *International Journal of Pattern Recognition and Artificial Intelligence* 38, no. 02 (2024): 2359026.

[16]. Amutha, S., P. Kamarajapandian, J. Nirmaladevi, S. Saravanan, S. Vijayalakshmi, and S. Athimoolam. "Optimizing cloud resource allocation and load balancing through eco-efficient task scheduling." *International Journal of Intelligent Systems and Applications in Engineering* 12, no. 11s (2024): 137-143.

[17]. Balraj, Lavina, A. Prasanth, KK Devi Sowndarya, and T. Kuntavai. "A lightweight blockchain scheme for secure data communication in internet of things-enabled wireless sensor network." In *2024 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES)*, pp. 1-6. IEEE, 2024.

[18]. Sen, Souptik, Ramesh Krishnamaneni, and Ashwin Narasimha Murthy. "THE ROLE OF MACHINE LEARNING IN ENHANCING SLEEP STAGE DETECTION ACCURACY WITH SINGLE-CHANNEL EEG." (2021).

[19]. Ko, Calvin Cheuk Wang. "Execution Monitoring of security-critical programs in a distributed system: a specification-based approach." PhD diss., University of California, Davis, 1996.

[20]. Dorfeshan, Yahya, and S. Meysam Mousavi. "A group TOPSIS-COPRAS methodology with Pythagorean fuzzy sets considering weights of experts for project critical path problem." Journal of intelligent & fuzzy systems 36, no. 2 (2019): 1375-1387.

[21]. Rathi, K., and S. Balamohan. "A mathematical model for subjective evaluation of alternatives in fuzzy multi-criteria group decision making using COPRAS method." International Journal of Fuzzy Systems 19 (2017): 1290-1299.

[22]. Darko, Adjei Peter, and Decui Liang. "An extended COPRAS method for multiattribute group decision making based on dual hesitant fuzzy Maclaurin symmetric mean." International Journal of Intelligent Systems 35, no. 6 (2020): 1021-1068.

[23]. Shaikh, Abrar, Aman Singh, Dipanjan Ghose, and Shabbiruddin. "Analysis and selection of optimum material to improvise braking system in automobiles using integrated Fuzzy-COPRAS methodology." International Journal of Management Science and Engineering Management 15, no. 4 (2020): 265-273.

[24]. Agrawal, Vikash K., Lalit N. Patil, Vikas S. Panwar, Lalit K. Toke, Srinivasa Rao Bogireddy, Kaustabh Vijay Chavan, U. D. Nimbalkar, Mahesh M. Sonekar, and Narendra R. Bhople. "Optimizing ventilated disk brake design for enhanced thermal performance: an analytical and experimental approach." *Multiscale and Multidisciplinary Modeling, Experiments and Design* 8, no. 4 (2025): 213.

[25]. Sridhar, P., S. Sri Nandhini Kowsalya, M. Venkatasudhahar, T. Sathish Kumar, Amit Gangopadhyay, Koppuravuri Gurnadha Gupta, and G. Manikandan. "Revolutionary building approach for maximal photovoltaic system results to improve maximum power point tracking in solar inverter." In *MATEC Web of Conferences*, vol. 392, p. 01146. EDP Sciences, 2024.

[26]. KUMAR, KRN KIRAN, and VAKA MURALI MOHAN. "AN EXHAUSTIVE REVIEW ON ACCOMPLISHMENTS IN THE EXPLORATION ZONE OF PICTURE RECOVERY IN CONTENT BASED PICTURES."1(10) 2016, 182 – 189.

[27]. Sridhar, P., S. Sri Nandhini Kowsalya, M. Venkatasudhahar, T. Sathish Kumar, Amit Gangopadhyay, Koppuravuri Gurnadha Gupta, and G. Manikandan. "Revolutionary building approach for maximal photovoltaic system results to improve maximum power point tracking in solar inverter." In *MATEC Web of Conferences*, vol. 392, p. 01146. EDP Sciences, 2024.

[28]. Murthy, Ashwin Narasimha, Souptik Sen, and Ramesh Krishnamaneni. "Enhanced image retrieval and classification frameworks for brain disease diagnosis using hybrid deep learning models." *International Journal of Computer Science and Information Technology Research* 3, no. 1 (2022): 37-47.

[29]. Vytautas, Bielinskas, Burinskienė Marija, and Palevičius Vytautas. "Assessment of neglected areas in Vilnius city using MCDM and COPRAS methods." Procedia Engineering 122 (2015): 29-38.

[30]. Stefano, Nara Medianeira, Nelson Casarotto Filho, Lizandra Garcia Lupi Vergara, and Rodrigo Ulisses Garbin da Rocha. "COPRAS (Complex Proportional Assessment): state of the art research and its applications." IEEE Latin America Transactions 13, no. 12 (2015): 3899-3906.

[31]. Kildienė, Simona, Arturas Kaklauskas, and Edmundas Kazimieras Zavadskas. "COPRAS based comparative analysis of the European country management capabilities within the construction sector in the time of crisis." Journal of Business Economics and Management 12, no. 2 (2011): 417-434.

[32]. Kustiyahningsih, Yeni, and Ismy Qorry Aini. "Integration of FAHP and COPRAS method for new student admission decision making." In 2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE), pp. 1-6. IEEE, 2020.

[33]. Roozbahani, Abbas, Hamed Ghased, and Mehdi Hashemy Shahedany. "Inter-basin water transfer planning with grey COPRAS and fuzzy COPRAS techniques: A case study in Iranian Central Plateau." Science of the Total Environment 726 (2020): 138499.

[34]. Keshavarz Ghorabaee, Mehdi, Maghsoud Amiri, Jamshid Salehi Sadaghiani, and Golnoosh Hassani Goodarzi. "Multiple criteria group decision-making for supplier selection based on COPRAS method with interval type-2 fuzzy sets." The international journal of advanced manufacturing technology 75 (2014): 1115-1130.

[35]. Mishra, Arunodaya Raj, Pratibha Rani, and Kamal Raj Pardasani. "Multiple-criteria decision-making for service quality selection based on Shapley COPRAS method under hesitant fuzzy sets." Granular Computing 4 (2019): 435-449.

[36]. Krishnamaneni, Ramesh, A. N. Murthy, and S. Sen. "A comparative study of big data mining algorithms for early detection of heart attack risk factors in electronic medical records." *International Journal of Computer Engineering and Technology (IJCET)* 10, no. 6 (2019): 139-154.

[37]. Ballamudi, S. "Performance Analysis of Machine Learning Algorithms in SAP Extended Warehouse Management Using ARAS Methodology." International Journal of Computer Science and Data Engineering 2, no. 2 (2025): 1-15.

[38]. Amutha, S., and Kannan Balasubramanian. "Energy-optimized expanding ring search algorithm for secure routing against blackhole attack in MANETs." *Journal of Computational and Theoretical Nanoscience* 14, no. 3 (2017): 1294-1297.

[39]. Kuntavai, T., and A. Jeevanandham. "RETRACTED ARTICLE: Adaptive wavelet ELM-fuzzy inference system-based soft computing model for power estimation in sustainable CMOS VLSI circuits." *Soft Computing* 24, no. 15 (2020): 11755-11768.

[40]. Karad, Sachin Chandravadan, Balpreet Singh, Gopal Krishna, C. Ambhika, Kanchan Yadav, and Shailendra Singh Sikarwar. "EAI Endorsed Transactions: AI Research." In *2025 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI)*, vol. 3, pp. 1-5. IEEE, 2025.

[41]. Sreelatha, Gavini, Veeresh Dachepalli, and Gudur Sahiti. "Data Analysis for Students Based on Geolocation Approach." *International Journal of Interpreting Enigma Engineers (IJIEE)* 1, no. 3 (2024): 33-41.

[42]. Manjula Selvam, Sathiyaraj Chinnasamy, M. Ramachandran, Chinnasami Sivaji, "Assessing the Growth and Challenges of Istanbul's Technology Sector: A Comparative Analysis of Key Industry Players", Journal on Innovations in Teaching and Learning3(4), December 2024, 21-29.

[43]. Varma, P. Bharat Siva, Prathap Adimoolam, Yamini Lahari Marna, Anantharamaiah Vengala, VS Divya Sundar, and MVT Ram Pavan Kumar. "Enhancing robust object detection in weather-impacted environments using deep learning techniques." In 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), pp. 599-604. IEEE, 2024

[44]. Kumar, KRN Kiran, and K. Bhavani. "Folded spined cube: new topology in interconnection networks." In *2022 6th International Conference on Computing Methodologies and Communication (ICCMC)*, pp. 314-319. IEEE, 2022.

[45]. Ravuri, Ananda, R. Josphineleela, G. V. S. Kumar, and T. SathishKumar. "Machine learning-based distributed big data analytics framework for IoT applications." *J. Electr. Syst.* 20, no. 3 (2024): 1788-1802.

[46]. Sreeram, Indraneel, and Venkata Praveen Kumar Vuppala. "HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm." Applied computing and informatics 15, no. 1 (2019): 59-66.

[47]. Balali, Amirhossein, Alireza Valipour, Rodger Edwards, and Robert Moehler. "Ranking effective risks on human resources threats in natural gas supply projects using ANP-COPRAS method: Case study of Shiraz." Reliability Engineering & System Safety 208 (2021): 107442.

[48]. Chowdaiah, Naveen Kumar, and Annapurna Dammur. "Resource-efficient workload task scheduling for cloud-assisted internet of things environment." International Journal of Electrical and Computer Engineering 13, no. 5 (2023): 5898-5907.

[49]. Chakraborty, R., S. Sen, M. Kurni, A. N. Murthy, and R. Krishnamaneni. "A Novel Framework for Enhancing Speech Pattern Recognition for Early Detection of Alzheimer's Disease Using machine learning Approach." *International Journal of Intelligent Systems and Applications in Engineering* 12 (2024): 421-428.

[50]. Karad, S. C., A. K. Chaitanya, and O. J. Sujayasree. "Advancement of sensors vision-based robotics (SVR) in precision farming: An imperative tool for crop productivity assurance." *Indian J. Plant Prot.* 48 (2020): 51-56.

[51]. Annapurna, D. "ENERGY EFFICIENT DATA TRANSMISSION MODEL FOR INTERENT OF THINGS APPLICATION." International Journal on Information Technologies & Security 14, no. 2 (2022).

[52]. C Murugamani, "Machine Learning for Robot Precision: Predicting End-of Operation Errors Using Regression Techniques", Computer Science, Engineering and Technology, 3(2), 2025, 211-224.

[53]. Sasidevi, J., R. Dinesh Kumar, A. Ranjith Kumar, and R. Gopi. "VAWGAN-NPOA: Energy-Aware Routing for Innocuous Data Transmission in WSN." *IETE Journal of Research* 70, no. 7 (2024): 6444-6452.

[54]. Vamsikrishna, M., Srinivasa Rao Bogireddy, Amit Gangopadhyay, Nilamadhab Mishra, Ajith Sundaram, and Priya Sharma. "Investigating Writer-Independent Deep Learning Techniques for Offline Handwritten Signature Verification." In *2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N)*, pp. 1658-1663. IEEE, 2024.

[55]. Manikandan, G., G. Bhuvaneswari, and M. Robinson Joel. "Artificial Intelligence to the Assessment, Monitoring, and Forecasting of Drought in Developing Countries." In *2023 International Conference on Circuit Power and Computing Technologies (ICCPCT)*, pp. 886-892. IEEE, 2023.

[56]. Ragavan, V. K., N. S. Nithya, Anantharamaiah Vengala, Balambigai Subramanian, and C. Ambhika. "Refractive Index Biosensor–Based Detection of Mycobacterium Tuberculosis Using Sea Lion Political Optimizer and Deep Learning." Plasmonics (2025): 1-19.

[57]. Mohan, VakaMurali, MalliKarjuna Reddy, and KRN Kiron Kumar. "A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment." In *IJCA Special Issues on "2nd National Conference-Computing, Communication and Sensor Network" CCSN*. 2011.

[58]. VUPPALA, VENKATA PRAVEEN KUMAR, PAZHANIRAJAN SAMBANDAM, and INDRANEEL SREERAM. "An efficient point-of-interest recommendation for LOcation-based social networks system with spatio-temporal model." (2022).

[59]. Maheswari, G. Uma, S. Amutha, C. Rajeshkumar, M. Vargheese, G. Nallasivan, and J. Hilda Selvarani. "Multimedia wireless sensor network platform Data encryption algorithm based on blockchain technology." In *2024 2nd International Conference on Networking and Communications (ICNWC)*, pp. 1-7. IEEE, 2024.

[60]. Seetha, J., D. Nagaraju, T. Kuntavai, and K. Gurnadha Gupta. "The Smart Detection and Analysis on Skin Tumor Disease Using Bio Imaging Deep Learning Algorithm." *ICTACT Journal on Image & Video Processing* 13, no. 4 (2023).
[61]. Prabhakara, T., V. Vidyasagar, and I. Naga. "Deep Long and Short Term Memory with Tunicate Swarm Algorithm for Skin Disease Detection and Classification." *J. Electrical Systems* 20, no. 7s (2024): 613-624.
[62]. Karad, S., and S. S. Mundhe. "Smart NPK Soil Sensor: Step towards Precision Agriculture." (2023).
[63]. Ballamudi, S. "Evaluating IoT Platforms: An Approach Using the COPRAS Method." Journal of Data Science and Information Technology 2, no. 1 (2025): 55-65.
[64]. Dachepalli, Veeresh, and Sreelatha Gavini. "A Virtually assisted digital twin enabled object detection in smart industrial manufacturing." *Expert Systems with Applications* (2025): 128574.