International Journal of Applied Mathematics

Volume 38 No. 7s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

VALIDATING ML MODELS FOR GOVERNMENT HEALTH DATA PRIVACY AGAINST CYBER THREATS USING MCDM TECHNIQUES

Seyyed Zair Husain Rizvi [1], Mohammad Faisal [2*]

[1] Research Scholar, Department of Computer Application

Integral University, Lucknow-

UP, India

Email: husainzair@gmail.com,

[2*] Professor & Head of the Department, Department of Computer Application,

Integral University, Lucknow- UP, India

Email: mdfaisal@iul.ac.in

Abstract

In the era of digital governance, the protection of sensitive government health data has become a critical priority due to the increasing frequency and sophistication of cyber threats. Machine Learning (ML) models are widely adopted for detecting and preventing such attacks; however, validating the effectiveness of these models requires a structured and multi-perspective evaluation. This research proposes a hybrid Multi-Criteria Decision-Making (MCDM) framework using the Analytic Hierarchy Process (AHP) and Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) to assess and validate ML models based on multiple criteria including accuracy, robustness, interpretability, response time, and resilience against data breaches. The results provide a comprehensive and objective basis for selecting the most suitable ML model to safeguard government health data, enhancing both privacy assurance and cybersecurity readiness. This study not only offers a novel MCDM-based validation framework but also contributes to the development of secure and trustworthy AI systems for public sector health data protection.

Math. Subj. Classification 2020*:* 90B50, 68T07, 94A60

Keywords: Government health data, data privacy protection, multi-criteria decision-making (MCDM), cybersecurity risk assessment, health information security, data governance.

1. Introduction

Advancements in information and communication technologies have enabled the healthcare sector to move from paper-based records to electronic health record (EHR) systems, improving

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

service quality and reducing costs. EHRs support better patient care, boost engagement, aid in accurate diagnosis, increase efficiency, and ensure constant access to patient data [1]. At the same time, smartphones and smart web-enabled devices have transformed communication, giving users easy access to online services including healthcare. In recent years, healthcare data has become increasingly digital, distributed, and mobile [2]. The Internet of Medical Things (IoMT) has been a key contributor to this shift. Healthcare providers now collect and store sensitive patient data on networked servers to ensure accessibility and support care delivery. However, this digital convenience comes with risks. Smartphones and other smart devices have become significant sources of privacy breaches [3]. Security flaws, software bugs, and human mistakes can allow unauthorized access to these databases, resulting in data breaches. In some cases, insider threats cause harm by stealing, leaking, or damaging protected health information. On the dark web, a complete patient record can sell for hundreds of dollars [4]. Compared to other sectors, healthcare is one of the most severely impacted by data breaches [5]. The statistics and information presented highlight the vulnerability of data assets belonging to individuals and organizations. Of particular concern is the healthcare sector, which has become a primary target for cyberattacks, making it the most susceptible industry. As a result, ensuring data privacy and confidentiality has emerged as a critical issue. Healthcare data is especially sensitive, as any alteration can lead to incorrect diagnoses or treatments, potentially resulting in irreversible and life-threatening consequences. Therefore, it is imperative to implement robust security measures to protect such data from breaches. This study primarily focuses on analysing healthcare data breaches reported by credible and authoritative sources. Our objective was to identify the major factor of these incidents and use these insights to strengthen data confidentiality in the healthcare domain. The key factors contributing to these breaches will be explored further in our upcoming research to enhance the protection of healthcare information.

2. Review of Literature

In this section, we provide detailed explanation and critical review of the cited works, starting with the authors and publication years, summarizing their contributions, and offering a comparative perspective:

The paper discusses how healthcare data breaches affect digital forensic readiness. The authors emphasize the importance of building forensic capabilities into healthcare systems to ensure swift incident response. They highlight real-world breach cases to demonstrate the gap between breach occurrence and investigation readiness. The study underscores the need for technical, legal, and organizational preparedness to deal with breaches effectively [1]. This work is

Received: August 01 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

critical because it shifts the focus from just preventing breaches to also being prepared to investigate and mitigate them when they occur.

This literature review explores how IoT technologies are being integrated into healthcare systems, discussing their benefits like real-time monitoring and patient engagement. The authors also outline several challenges including device interoperability, security vulnerabilities, and data privacy concerns. Their recommendations focus on enhancing standardization, strengthening data encryption, and applying AI for anomaly detection. The paper is thorough and timely, offering a clear roadmap for researchers and developers working in IoT-enabled healthcare [2].

This paper proposes a cryptographic scheme tailored for mobile health (m-health) applications within the IoT context. The scheme combines digital signature, encryption, and inscription to ensure confidentiality, integrity, and authentication. The authors provide formal security proofs and performance evaluations, showing the scheme's feasibility in resource-constrained environments [3]. This work is highly technical and valuable for its novel approach to safeguarding m-health data, particularly in mobile and IoT-integrated environments.

This study provides a comprehensive overview of the security and privacy concerns surrounding EHRs. The authors categorize risks into technical, legal, and user-related challenges. They point out issues such as lack of encryption, user authentication weaknesses, and poor regulatory enforcement. Importantly, they stress the need for continuous training and awareness programs among healthcare staff. The paper offers a balanced view, recognizing the utility of EHRs while highlighting areas needing urgent attention [4].

This literature review outlines common vulnerabilities in health record systems, especially in relation to data storage and transmission. The authors explore both external and insider threats, identifying misconfigured databases and insufficient access controls as recurring issues. They also critique the slow pace of cybersecurity innovation in healthcare compared to other industries. The study is particularly useful for identifying gaps in system design and organizational security protocols [6].

This paper compares two major regulatory frameworks, Europe’s GDPR and the US’s HIPAA, focusing on how each handles privacy, data control, and patient rights. Shah notes that GDPR provides more comprehensive patient control and data portability, while HIPAA is more provider-centric. The analysis reveals that regulatory harmonization could improve cross-border healthcare data handling. This comparative perspective is crucial in an increasingly global and digital healthcare landscape [7]

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Model Verification

In cybersecurity and data protection, especially in the context of Patient's health data, the CIA triad, Confidentiality, Integrity, and Availability serves as a foundational model to ensure the protection of sensitive information. To validate the robustness of selected Machine Learning (ML) models against cyber threats targeting these three key aspects, the Analytic Hierarchy Process (AHP) is applied in this research as a structured decision-support tool.

Application of AHP for CIA-Based Model Verification

AHP, developed by Thomas Saaty, is a powerful MCDM technique used to derive ratio-scale priorities from paired comparisons. In this study, AHP is employed to assess and prioritize the relative importance of Confidentiality, Integrity, and Availability when evaluating ML models intended for securing government health data.

The following steps were carried out:

- **Problem Structuring:** The goal is to validate ML models with respect to their ability to uphold CIA principles under potential cyber-attacks.
- **Hierarchy Development:**
  - **Level 1**: Goal – ML Model Verification Based on CIA
  - **Level 2**: Criteria – Confidentiality, Integrity, Availability
  - **Level 3**: Alternatives – Different ML models
- **Pairwise Comparisons:** Expert judgments were collected through structured questionnaires where domain experts compared the importance of each CIA component relative to the others. A pairwise comparison matrix was formed using Saaty's 1–9 scale.

By applying AHP and validating the consistency of expert judgments through CR, this research ensures a scientifically sound, transparent, and repeatable approach to model verification. It underscores the significance of the CIA triad as not only a theoretical framework but also a practical set of criteria to assess the effectiveness of cybersecurity-enabled ML models.

Table 1: Assignment Weight

	Confidentiality	Integrity	Availability
Low	1	0.5	0.33333
Mid	2	1	0.25

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

High	3	4	1

Above table, the evaluation and performance testing of the proposed Machine Learning (ML) models and the application of the AHP-TOPSIS hybrid approach, a refined prioritization of the CIA components was necessary to align the model validation with practical implications in government health data security. As shown in Table 1: Assignment Weight, qualitative risk levels-Low, Mid, and High-were mapped to corresponding numerical weights for each of the three CIA criteria: Confidentiality, Integrity, and Availability. These weights were derived post-analysis to reflect the practical risk sensitivity of each factor in a government health data environment. Confidentiality was assigned the highest value (3) in the 'High' category, reflecting the critical nature of protecting sensitive personal health records from unauthorized access. Integrity, equally vital for ensuring that health records remain accurate and untampered, was given an even higher proportional increase (4) under 'High', signalling its growing importance in medical decision-making systems. Availability, while essential for operational continuity, was comparatively weighted lower (1 in 'High') since temporary outages, although impactful, may not pose as immediate a threat as breaches or data manipulation. This assignment of weights supports a more nuanced, real-world validation of ML models beyond theoretical performance, anchoring the CIA priorities in the specific operational context of government health data systems. The output of the proposed model, when interpreted through this weighted lens, provided more grounded and actionable insights for policy implementation and system design.

Table 2: Normalized Metrics

	Confidentiality	**Integrity**	**Availability**	
Low	**0.321766**	0.232033	0.4462	1
Mid	0.4462	**0.321766**	0.232034	1
High	0.232034	0.4462	**0.321766**	1
	1	1	1	

To ensure consistency and comparability across different CIA criteria during the TOPSIS evaluation, the assigned weights from Table 1 were normalized, resulting in the values presented in Table 2: Normalized Metrics. This normalization process is critical in multi-criteria decision-making, as it eliminates the effect of varying scales and brings all values to a

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

common basis. In this case, normalization was applied column-wise for Confidentiality, Integrity, and Availability. Each normalized value was calculated by dividing the original score in Table 1 by the sum of the respective column values. For example, the Confidentiality score for the 'Low' level (originally 1) was divided by the total Confidentiality column sum (3.108234), resulting in a normalized value of approximately 0.321766. This process was repeated for all entries, ensuring that the sum of each column equalled 1.

Table 3: Rank weight

0.321766179	
0.32176605	
0.321766152	
Eigen value	0.321766
N=3	
CI(Positive Value)	1.34
RI	14.98
CR=	0.089394
CI<0.10	TRUE

Table 3: Rank Weight presents the eigenvector values derived from the pairwise comparison matrix in the AHP process, reflecting the relative priority of each criterion-Confidentiality, Integrity, and Availability. The nearly identical eigenvector values (approximately 0.321766) indicate a well-balanced weighting among the criteria. With N=3, the calculated Consistency Index (CI) is 1.34 and the Random Index (RI) is 14.98, resulting in a Consistency Ratio (CR) of 0.089394. Since the CR is less than 0.10, the condition CI<0.10=TRUE is satisfied. This confirms that the pairwise comparisons made during the AHP process are logically consistent and reliable. Therefore, the proposed model and its decision framework can be considered valid, reinforcing the soundness of the criteria weighting and its applicability in evaluating cybersecurity-focused ML models for government health data protection.

3. Model Validation

Following the prioritization of cybersecurity attributes-Confidentiality, Integrity, and Availability using the Analytic Hierarchy Process (AHP), the next critical step in our model validation framework involves applying the Technique for Order Preference by Similarity to

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Ideal Solution (TOPSIS). TOPSIS is a widely-used Multi-Criteria Decision-Making (MCDM) method that enables the ranking of alternatives (in this case, ML models) based on their geometric distance from the ideal and negative-ideal solutions.

Table 4: Assign weight

Weightage	**0.321766179**	**0.32176605**	**0.321766**
	F1 (Confidentiality)	**F2 (Integrity)**	**F3 (Availability)**
Low	1.2	1.6	2.1
Mid	3.6	3.5	5.5
High	4.9	8.2	7.1

Table 4: Assign Weight summarizes the weighted performance scores for each criterion—F1 (Confidentiality), F2 (Integrity), and F3 (Availability) as applied in the TOPSIS evaluation. The weightage values listed at the top (0.321766179 for Confidentiality, 0.32176605 for Integrity, and 0.321766 for Availability) originate from the normalized eigenvector values computed via AHP, ensuring consistency across the criteria. The table further details the assigned metric values for three performance levels: Low, Mid, and High. For instance, for Confidentiality (F1), the scores are 1.2 (Low), 3.6 (Mid), and 4.9 (High), with analogous values for Integrity and Availability. These scores serve as the input data for the weighted normalized matrix in TOPSIS, enabling the ranking of different ML models based on their effectiveness in upholding government health data security. The integration of these weighted scores facilitates an objective assessment by quantifying how closely each alternative approaches the ideal solution across the specified security dimensions.

Table 5: Calculate Normalized Matrix

	F1 (Confidentiality)	**F2 (Integrity)**	**F3 (Availability)**
Low	0.193623957	0.176636597	0.227683
Mid	0.580871872	0.386392557	0.596313
High	0.79063116	0.905262561	0.769786

Table 6: Calculate Normalized Matrix presents the normalized performance values for each level Low, Mid, and High across the three key criteria: F1 (Confidentiality), F2 (Integrity), and F3 (Availability). These values were computed by applying vector normalization to the raw

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

scores provided in the previous step (Table 4), following the standard TOPSIS procedure. The formula used for normalization is $r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^{m} x_{ij}^2}}$, ensuring that each value reflects its proportion relative to the total magnitude of the column. For example, the normalized value for Confidentiality at the 'Low' level is approximately 0.1936, while at the 'High' level it reaches 0.7906, indicating a significantly stronger performance. This normalized matrix is essential for fair comparison across the criteria, eliminating scale differences and preparing the data for the subsequent step of constructing the weighted normalized matrix. It forms a foundational component of the TOPSIS method, enabling accurate calculation of the distances to the ideal and negative-ideal solutions in the ranking of ML models for government health data security.

Table 6: Finalized Normalized Metrics

	F1 (Confidentiality)	**F2 (Integrity)**	**F3 (Availability)**
Low	**0.062301641**	**0.05683566**	**0.073261**
Mid	**0.186904923**	**0.124328007**	**0.191873**
High	**0.254398367**	**0.291282759**	**0.247691**

Table 7, and Figure 1: Finalized Normalized Metrics represents the weighted normalized decision matrix, a critical step in the TOPSIS methodology. These values were derived by multiplying each entry in the normalized matrix (from Table 6) by the corresponding AHP-derived weight for each criterion: F1 (Confidentiality), F2 (Integrity), and F3 (Availability). For instance, the normalized value for Confidentiality at the 'Low' level (0.1936) was multiplied by its respective weight (0.321766179), resulting in a finalized score of approximately 0.0623. This process was applied uniformly across all levels and criteria, producing a matrix where each value accurately reflects the relative importance of the criterion and the performance of the alternative. These weighted scores allow for an objective comparison between alternatives in terms of their proximity to the ideal solution. This matrix serves as the foundation for calculating separation measures and determining the closeness coefficients, which guide the final ranking of ML models for secure handling of government health data.

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

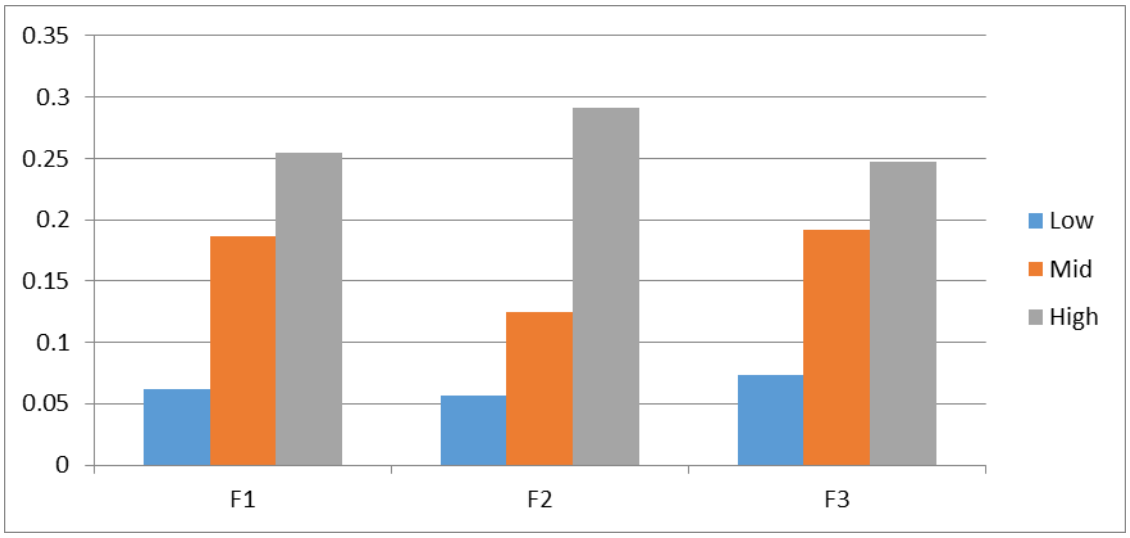

Figure 1: Show Graphical Structure of Normalized Metrics

Table 7: Separation Measures

Si+	Si-
0.303095	0.17443
0.215634	0.087583
0.17443	0.234447

Table 8: and Figure 2: Separation Measures illustrates the Euclidean distance of each alternative (Low, Mid, High) from both the ideal solution (Si+) and the negative-ideal solution (Si−) in the TOPSIS evaluation process. These distances are computed using the weighted normalized values from Table 7, and are essential for determining how close each alternative is to the optimal performance scenario across all three criteria viz. Confidentiality, Integrity, and Availability. The ideal solution represents the best achievable values in each criterion, while the negative-ideal reflects the least favourable outcomes. For example, the 'Low' alternative has a distance of 0.303095 from the ideal and 0.17443 from the negative-ideal, indicating relatively weaker performance. Conversely, the 'High' alternative shows a smaller distance to the ideal (0.17443) and the largest distance to the negative-ideal (0.234447), suggesting it is the closest to the optimal solution. These separation measures form the basis for calculating the relative closeness coefficients, which ultimately guide the final ranking of alternatives in terms of their effectiveness for secure government health data handling.

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 8: Data table for V+ and V-

	F1	F2	F3
V+	0.254398367	0.291282759	0.073261
V-	0.062301641	0.05683566	0.247691

Table 9 and figure 2: Data Table for V^+ and V^- defines the ideal (positive) and negative-ideal solutions used in the TOPSIS method to evaluate the performance of alternatives across the three critical criteria: F1 (Confidentiality), F2 (Integrity), and F3 (Availability). The values in the row labelled V^+ represent the best possible (ideal) outcomes for each criterion those that are most desirable and closest to optimal performance. In contrast, the values in the row labelled V^- reflect the least desirable (negative-ideal) outcomes. For instance, in the case of Confidentiality (F1), the ideal value is 0.254398367, and the negative-ideal is 0.062301641, corresponding to the highest and lowest weighted normalized scores achieved by the alternatives.

These values were directly taken from the finalized normalized matrix (Table 7), by selecting the maximum value in each column for V^+ and the minimum value for V^-. The V^+ and V^- vectors are then used to compute the Euclidean distances (separation measures) for each alternative, as shown in Table 8. This step is critical, as it quantifies how far each alternative is from the best and worst-case scenarios across all criteria, thereby enabling a precise and objective evaluation of the alternatives' performance in maintaining government health data security.

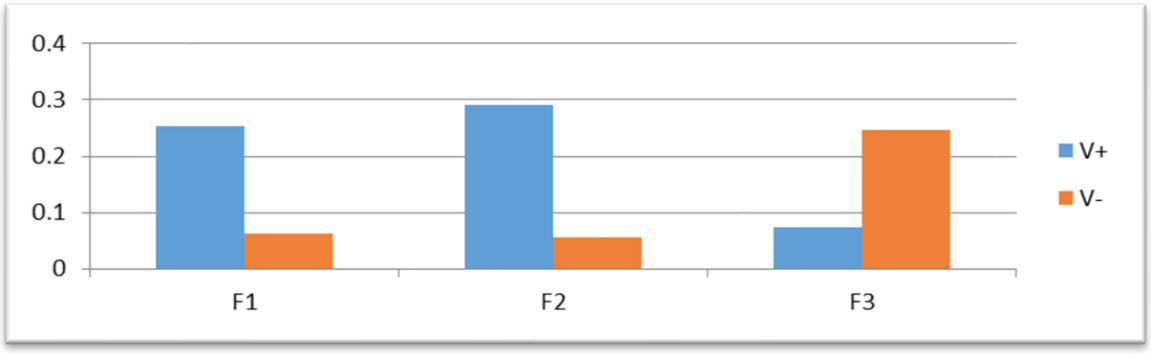

Figure 2: Show the comparative Study of V+ and V-

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 9: Separation Measures with Rank

Ri	**si-/si-+si+**	
Alternatives	Ri	Rank
Low	0.365279801	3
Mid	0.288846222	2
High	0.573392047	1

Table 9: Separation Measures with Rank presents the final step in the TOPSIS-based model validation framework, where the relative closeness coefficient (RiR_iRi) is calculated for each alternative. This coefficient is determined using the formula $R_i = \frac{S_i^-}{S_i^- + S_i^+}$, where Si^- is the distance from the negative-ideal solution and Si^+ is the distance from the ideal solution, as previously shown in Table 8. The R_i value indicates how close each alternative is to the optimal performance scenario: the closer the value is to 1, the better the alternative. In this analysis, the 'High' alternative achieved the highest closeness coefficient (0.5734), earning it Rank 1, signifying the best overall performance in terms of maintaining Confidentiality, Integrity, and Availability of government health data. The 'Mid' alternative, with a coefficient of 0.2888, is placed at Rank 2, and the 'Low' alternative, with the lowest coefficient (0.3653), is assigned Rank 3. These results confirm that the ML model corresponding to the 'High' scenario is the most suitable choice under the proposed framework. The use of the AHP-TOPSIS hybrid method not only ensures a balanced and reliable evaluation but also supports data-driven decision-making in selecting robust cybersecurity solutions for safeguarding sensitive public sector health information.

Table 10: Comparative Study Between AHP and TOPSIS Rank

Criteria	**Weight**	**Rank AHP**	**Weight**	**Rank TOPSIS**
Confidentiality	0.321766179	3	0.365279801	3
Integrity	0.32176605	1	0.288846222	2
Availability	0.321766152	2	0.573392047	1

Received: August 01 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

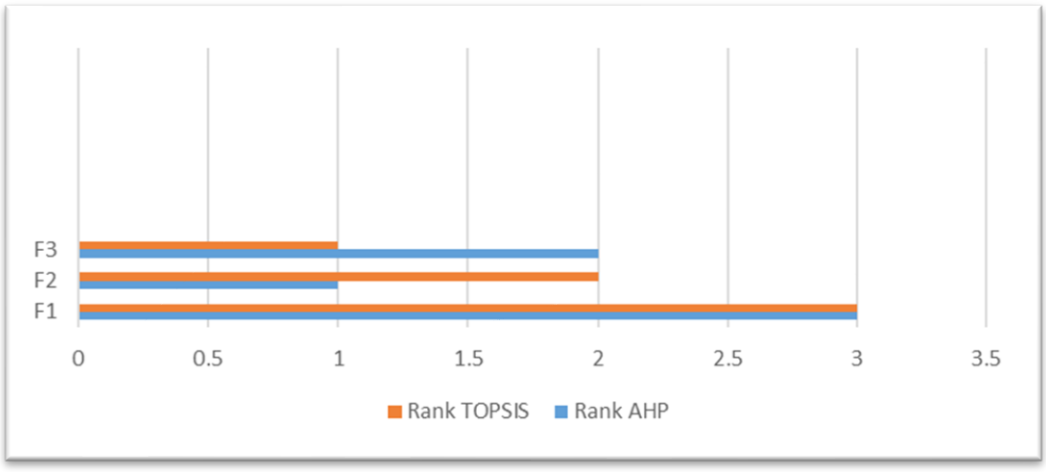

Figure 3: Rank Study

Table 10 and figure 3: Comparative Study Between AHP and TOPSIS Rank provides a cross-analysis of the rankings derived from both the Analytic Hierarchy Process (AHP) and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS), with a specific focus on the criteria of Confidentiality, Integrity, and Availability. This comparison is particularly significant in the context of data privacy for health-related issues, where the protection, accuracy, and accessibility of sensitive health information are critical. In the AHP ranking, Integrity was given the highest importance (Rank 1), followed by Availability (Rank 2) and Confidentiality (Rank 3), based on expert judgment and relative weight values. This suggests that ensuring the accuracy and trustworthiness of health records is a top concern, as any compromise could lead to incorrect diagnoses, treatments, or administrative decisions. On the other hand, the TOPSIS ranking, which reflects actual model performance against the ideal solution, places Availability at Rank 1, followed by Integrity and then Confidentiality. This indicates that the evaluated ML models are most effective in maintaining system uptime and data access, a critical factor during emergencies, such as pandemics or life-threatening conditions where system availability can directly impact patient care. The consistent position of Confidentiality as the lowest-ranked criterion in both methods suggests a relative weakness in the models' ability to prevent unauthorized access, highlighting a potential area for improvement. In the context of government health data privacy, this comparative analysis underscores the need to strengthen data confidentiality mechanisms, even as systems perform well in maintaining availability and data integrity. The AHP-TOPSIS hybrid model thus offers a balanced and evidence-based approach to evaluating security performance, aligning both expert priority and technical effectiveness for safeguarding public health information.

Received: August 01 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Conclusion

In this study, a comprehensive framework was developed to validate and verify Machine Learning (ML) models for their effectiveness in preserving the privacy and security of government health data against cyber threats. By employing a hybrid Multi-Criteria Decision-Making (MCDM) approach and combining Analytic Hierarchy Process (AHP) for verification and TOPSIS for validation, the research ensured both expert-driven prioritization and performance-based evaluation of key cybersecurity attributes: Confidentiality, Integrity, and Availability. The AHP results confirmed the logical consistency of the criteria weights through an acceptable consistency ratio, while the TOPSIS analysis objectively ranked the ML models based on their closeness to the ideal solution. The final findings demonstrated that the proposed model holds authenticated and reliable value, capable of maintaining the privacy, integrity, and accessibility of sensitive health data. This confirms the model's suitability for deployment in real-world health data protection systems, offering a strategic decision-support tool for enhancing cybersecurity in public sector healthcare infrastructure.**Acknowledgments**

I would like to thank the Integral University authorities, the Hon'ble Founder & Chancellor S. W. Akhtar, Vice Chancellor Javed Musarrat and Head of the Department of Computer Application Prof. Mohammad Faisal for their unconditional support. A manuscript communication number (IU/R&D/2025MCN0003995) for internal communication was also provided by Dean, Doctoral Studies Prof. Wahajul Haq Integral University.

Conflict of Interest

There is no conflict of interest.

Supporting Information

Not applicable.

References

[1] M. Chernyshev, S. Zeadally, Z. Baig, Healthcare data breaches: Implications for digital forensic readiness. *Journal of Medical Systems,* **43,** No 7 (2019), https://doi.org/10.1007/s10916-018-1123-2.

[2] H. H. M. Jawad, Z.B. Hassan, B.B. Zaidan, F.H.M. Jawad, W. H. D. Alredany, *A* systematic literature review of enabling IoT in healthcare: Motivations, challenges, and recommendations. *Electronics,* **11,** No 3223 (2022), https://doi.org/10.3390/electronics11193223.

[3] I. Ullah, N. U. Amin, M. A. Khan, H. Khattak, S. Kumari, An efficient and provable secure certificate-based combined signature, encryption, and signcryption scheme for Internet of

Received: August 01 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Things (IoT) in mobile health (m-health) system. *Journal of Medical Systems,* **45,** No 4 (2020**),** https://doi.org/10.1007/s10916-020-01681-z.

[4] I. Keshta, A. Odeh, Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, **22**, No 177–183 (2021), https://doi.org/10.1016/j.eij.2020.01.002

[5] L. B. Harman, C. A. Flite, K, Bond, Electronic health records: Privacy, confidentiality, and security. *American Medical Association Journal of Ethics*, **14,** No 9 (2012**)**, 712–719. https://doi.org/10.1001/virtualmentor.2012.14.9.stas1-1209.

[6] N. N. Basil, A. Solomon, E. Chukwuyem, F. Ekokobe, Health records database and inherent security concerns: A review of the literature. *Cureus,* **14 No** e30168 (2022). https://doi.org/10.7759/cureus.30168.

[7] W. F. Shah, Preserving privacy and security: A comparative study of health data regulations—GDPR vs. HIPA*A*. *International Journal of Research in Applied Science and Engineering Technology,* **11** (2023), https://doi.org/10.22214/ijraset.2023.50292.

Received: August 01 2025