Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 10, pp. 3765–3776
DOI : 10.47974/JIOS-2501

Discrete risk assessment models for healthcare cybersecurity

Wasim A. Bagwan *
Department of Apllied Sciences
Krishna Institute of Science & Technology
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad 415539
Maharashtra
India

Shilpy Singh †
Department of Biotechnology and Microbiology
Noida International University
Greater Noida 201312
Uttar Pradesh
India

Swati Sucharita §
Department of Computer Science and Engineering (Artificial Intelligence & Machine Learning)
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

D. Ganesh Kumar ‡
Department of Pharmacology
Meenakshi Medical College Hospital & Research Institute
Meenakshi Academy of Higher Education & Research
Kanchipuram 631552
Tamil Nadu
India

* *E-mail:* **wasim.bagwan16@gmail.com (Corresponding Author)**
† *E-mail:* **Shilpy.singh@niu.edu.in**
§ *E-mail:* **sucharita1614@vardhaman.org**
‡ *E-mail:* **gkumar@maher.ac.in**

© Taru Publications

Alugolu Avinash [@]
Department of Computer Science & Engineering
Pragati Engineering College
Kakinada 533437
Andhra Pradesh
India

Avinash Somatkar [#]
Department of Mechanical Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Abstract

Ransomware, phishing, unauthorized access, insider misuse, and device attacks are all threats to the healthcare industry as they rely on electronic health records (EHRs), cloud services, telemedicine, and connected medical devices. Qualitative matrices can give subjective results, and more sophisticated quantitative methods may need a long time of historical data. In this study, discrete risk assessment models have been proposed to evaluate the healthcare cybersecurity in an transparent and consistent way. The framework is based on five-level discrete scales for threat likelihood, vulnerability severity, asset criticality, data sensitivity, operational impact and control effectiveness. These factors determine scores of risk and threats of inherent and residual risk, and rank the threats as negligible, low, moderate, high and critical. Ten healthcare scenarios were used for evaluation and ransomware and unpatched medical devices were the most significant threats. Once these measures of multifactor authentication, network segmentation, encryption, secure backups, patch management and access monitoring were implemented, risk was reduced by 59.7%. The proposed framework helps to provide better threat differentiation, threat interpretability, control evaluation and better prioritization of cybersecurity investments, and helps to provide patient safety as well as continuity of clinical services.

Subject Classification: *68M25.*

Keywords: *Healthcare cybersecurity, Discrete risk assessment, Cyber risk, Iomt, Residual risk, Threat prioritization, Patient safety, Security controls.*

1. Introduction

To provide patient care, healthcare organizations rely on the use of EHR, cloud platforms, telemedicine, connected medical devices and IoMT. While the benefits of using digital transformation include better accessibility, coordination and efficiency, it also creates an increased attack surface for cybercriminals [1].

[@] *E-mail:* **alugoluavinash@outlook.com**
[#] *E-mail:* **avinash.somatkar@vit.edu**

Ransomware, phishing, unauthorized access, access to patient data, malware, insider misuse, device manipulation, and denial-of-service (DoS) attacks are all risks hospitals and healthcare networks face [2]. These incidents have the potential to lead to patient confidentiality issues, disruption to clinical services, changes to medical evidence and patient lives, and even loss of life. Reliable cybersecurity risk assessment is thus a key need for healthcare governance and healthcare resilience [3]. Healthcare risk-assessment methods typically provide qualitative statements, expert opinion or an ongoing numerical assessment. These approaches can yield conflicting results, need to rely on past information, and offer little assistance in prioritizing threats [4]. Healthcare environments thus need a way to measure security that can be translated into categories of risks, and acted upon accordingly. The discrete models are more practical, where the likelihood, vulnerability, criticality of assets, effectiveness of control and impacts on operations are represented by distinct levels [5], [6]. These variables can be used to combine them into negligible, low, moderate, high, and critical risk classes which can be used by administrators to determine where to invest their security resources in order to manage the clinical and organizational priorities. The traditional way to assess risks is based on descriptive criteria (low, medium, and high). While a number of these techniques are easy to comprehend and seem obvious, they require a good deal of expert judgment to produce effective outcomes. The same cybersecurity event may be considered a different level of risk by different assessors [7]. Quantitative approaches numerically quantify the consequence of attack, the frequency of attack, financial losses, and probability of risk. But frequently, there are no reliable numbers to report, for healthcare organizations are not required to report incidents or because vulnerabilities in the medical devices may change quickly, and rare cyberattacks may not have historical records large enough to report [8].

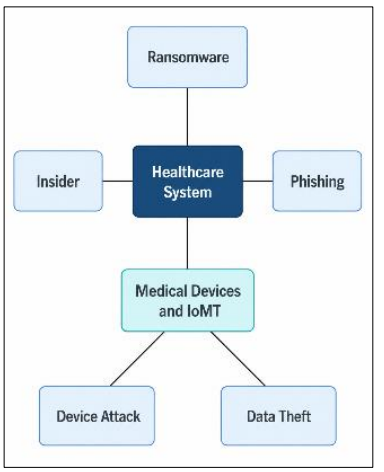


Figure 1

Healthcare cybersecurity threat environment and major attack vectors

In this paper, we suggest discrete risk assessment models to be used for the assessment of cybersecurity threats in healthcare information systems, cloud services, clinical networks and connected medical devices as shown in Figure 1. The proposed framework includes the identification of critical assets and threats, assignment of discrete values to risk factors, calculation of the composite risk score and prioritization of mitigation controls that are suitable. The study provides a structured, transparent and adaptive framework that facilitates threat prioritization, regulatory compliance and cybersecurity decision making, and acknowledges the security-sensitive nature of today's healthcare operations.

2. Discrete Risk Assessment Models for Healthcare Cybersecurity

A healthcare case study is applied to illustrate the assessment procedure and to analyse the capacity of the model to differentiate between the risks, in terms of risk characteristics (likelihood and impact) different. The classifications that are created are then compared to traditional assessment methods to assess consistency, interpretability and decision usefulness [9].

A. *Ordinal Scoring Model*

The ordinal scoring model assigns fixed values (usually from 1 to 5), to the factors considered, including vulnerability severity, data sensitivity, system exposure and patient-safety impact. Each score is combined to get the overall risk level.

$$R = \sum_{\{i=1\}_i^{\{n\}s}} L \times I$$

where (s_i) represents the discrete score assigned to each risk factor.

B. *Binary Risk Model*

The two possible values of the binary risk model are (0) for absent or secure, and (1) for present or insecure. It can be used for checking encryption, multifactor authentication, software patching and regulatory compliance [10].

$$R = \sum_{\{i=1\}_i^{\{n\}x}} x_i \, , quad \; x_i \in \{0,1\}$$

A larger (R) indicates that more cybersecurity weaknesses are present.

C. *Decision-Tree Model*

A decision-tree model for classification of cyber risk in healthcare system using a series of discrete security questions. Questions could focus on whether or not patient information is part of the system, whether the system is internet facing, and whether sufficient security measures have been put in place [11].

$$R = f(x_1, x_2, \dots, x_n)$$

(x_i) is a condition of a decision and the function (f) defines a preassigned class of a risk for the chosen decision path.

D. *Weighted Categorical Model*

In the weighted categorical model, the cybersecurity factors are assigned various weights. Patient safety and privacy of medical information may be given greater importance in the healthcare context than financial consequences.

$$R = \sum_{\{i=1\}_i^{\{n\}w}} wisi\,, \sum_{\{i=1\}_i^{\{n\}w}} wi = 1$$

where (w_i) is the weight and (s_i) is the categorical score of factor (i).

$$RPN = S \times O \times D$$

The severity (S), likelihood of occurrence (O) and ease of detection (D) of the occurrence. A higher Risk Priority Number will represent more urgency.

E. *Attack-Tree Model*

Attack-tree model is based on the premise of a cyberattack goal, and splits it into various attack routes, including phishing, stolen credentials, malware, or software exploitation. The risk of each of the paths can be assessed individually [12].

$$R_{\{\{OR\}\}} = (R_1, R_2, \ldots, R_n)$$

$$R_{\{\{AND\}\}} = \prod_{\{i=1\}_i^{\{n\}R}} Ri$$

$$P(R \mid E) = \backslash frac\{P(E \mid R)P(R)\}\{P(E)\}$$

This is a type of statement in which the risk event (R) is followed by the security evidence (E) that has been observed.

F. *Cybersecurity Maturity Model*

The healthcare organization's maturity is assessed in various aspects, including access control, incident response, backup, staff training, and medical device security. Maturity levels are given to each area.

$$M = c\left\{\sum_{\{i=1\}_i^{\{n\}w}} wimi\right\}\left\{\sum_{\{i=1\}_i^{\{n\}w}} mi\right\}$$

The maturity level of the security domain (i) is denoted by (m_i) and the importance weight is (w_i) of the security domain (i). The higher the score, the more capable in cybersecurity capabilities.

3. Proposed Healthcare Cybersecurity Risk Assessment Model

The proposed model is a patient-safe and discrete cyber risk assessment model (PSA-DCRAM) which is suitable. It integrates technical cybersecurity risk, patient safety, healthcare operations, data privacy and regulatory compliance into one single discrete assessment framework. The model assesses 7 healthcare specific risk factors: likelihood of a cyber-attack (L), vulnerability

severity (V), system exposure (E), sensitivity of patient data (D), disruption of operations (O), impact to patient safety (P), consequences for regulatory and compliance (C).

Step -1: Each factor is assigned a discrete score:

$$x_i \in \{1,2,3,4,5\}$$

where 1 represents very low risk and 5 represents very high risk.

Step -2: The base risk score is calculated as:

$$R_B = 0.10L + 0.15V + 0.10E + 0.15D + 0.15O + 0.25P + 0.10C$$

Step -3: Patient safety is given the highest weight as the cybersecurity incident risks the patient's health and wellbeing when they involve medical devices, clinical information or hospital services. The weights satisfy:

$$\sum_{\{i=1\}_i^{\{7\}w}} wi = 1$$

Step -4: Control Effectiveness

The model assesses how well the current security measures, such as encryption, two-factor authentication, access control, patch management, network monitoring, backup, and incident response, are working.

$$CE = \frac{c\left\{\sum_{\{j=1\}_{jc_j}^{\{m\}u}} ujcj\right\}}{\left\{5\sum_{\{j=1\}_j^{\{m\}u}} uj\right\}}$$

The effectiveness score where (c_(j\in{1,2,3,4,5})) is followed by the importance weight of control (j) (u_j). Thus, (CE) ranges from 0.2 to 1.

Step -5: The residual risk is:

$$R_R = R_{B(1-\alpha CE)}$$

The maximum risk reduction which the controls will give. A value like (α=0.7) allows for the notion that there is no absolute security, or that the risk is not completely eliminated by security.

Step -6: Patient-Safety Escalation Rule

A low numerical average does not imply that there is not a serious clinical hazard. As a consequence, there is a rule in place to ensure safety, which is known as a safety escalation rule:

$$RF = 5\ if\ P = 5\ and\ (V \geq 4\ or\ E \geq 4); RF = 4\ if\ P \geq 4\ and\ O \geq 4; otherwise\ RF = RR.$$

The rule automatically triggers an escalation in risk when an incident has a potential for serious harm to the patient and/or significant disruption to healthcare services.

Step -7: Risk-Priority Index

The risk assessed can be matched with the criticality of the asset and used to prioritize asset mitigation:

$$RPI = R_F \times A$$

where the A is the criticality of the healthcare asset, with A being {1, 2, 3, 4, 5}. A life-support system would get a higher (A) score than non-clinical administrative system.

PSA-DCRAM can be applied to electronic health records, cloud-based health based applications, hospital network, telemedicine network, Internet of Medical Things devices. The primary benefit is that it does not overlook clinical harm, continuity of operations, privacy or compliance, and generates a simple, discrete risk level.

4. Proposed Discrete Risk Assessment Framework

Proposed framework uses heterogeneous security observations to convert them into discrete and interpretable values, which can then be used to assess cybersecurity risks. Evaluates each of the identified threats–asset pairs by six factors: threat likelihood, vulnerability severity, asset criticality, data sensitivity, operational impact, and control effectiveness. The framework results in an intrinsic risk score, residual risk after taking into account existing controls, risk category and suitable response. The factors are indicated by numbers 1-5 are presented in Table 1. Threat likelihood (L) is a measure of the likelihood of a threat happening. Vulnerability Severity (V) is the degree of vulnerability of the weakness identified and how easy it will be to exploit. Asset criticality (A) is the level of criticality of the system being affected to healthcare operations. The sensitivity of the data (D) describes the level of confidentiality needed for the data used. Operational impact ((I)) – potential disruption of clinical activities and patient safety. Control effectiveness (C) refers to the effectiveness of the current preventive, detective and corrective controls; the more effective these controls are, the higher the C value.

Table 1

Cybersecurity Risk Assessment Factors and Discrete Interpretation

Factor	Symbol	Discrete interpretation
Threat likelihood	(L)	Rare to almost certain
Vulnerability severity	(V)	Negligible to critical
Asset criticality	(A)	Nonessential to life-critical
Data sensitivity	(D)	Public to highly restricted
Operational impact	(I)	Minimal to catastrophic
Control effectiveness	(C)	Ineffective to highly effective

The denominator converts the risk to a number ranging from 0.2 to 25. This formula is to make the risk greater when a threat is more likely, when a vulnerability can be easily exploited, or when the affected healthcare asset has significant consequences to data, operations or patient safety. The inherent risk can be mitigated, but not eliminated, by existing cybersecurity controls. Thus the effectiveness of the control is transformed to a reduction coefficient:

$$E_c = \frac{\{C - 1\}}{\{5\}}$$

The residual risk is calculated as:

$$Rresidual = Rinherent(1 - Ec)$$

The score at 1 is no real reduction while the score at 5 is 80% reduction. It's important to keep the maximum reduction limit to avoid assigning zero risk as the current unknown vulnerabilities, configuration problems, insider use and emerging threats remain a risk to healthcare systems. This leaves a residual score that aligns it to one of five risk categories as shown in Table 2.

Table 2

Residual Risk Classification and Response

Residual score	Risk level	Required response
0.00–2.00	Negligible	Accept and periodically review
2.01–5.00	Low	Apply routine safeguards
5.01–10.00	Moderate	Develop a scheduled treatment plan
10.01–15.00	High	Implement controls urgently
15.01–25.00	Critical	Take immediate action and escalate

Critical and high risks must be addressed immediately as they could impact on vital clinical services, patient privacy information and/or have an adverse effect. Planned mitigation and continued monitoring is needed for moderate risks. The decision to accept low and negligible risks may be made temporarily when the benefits of treatment are likely to be less than the cost, but this must be documented and reviewed. The suggested structure is modular and easy to understand and modify. It has a pre-defined set of scales so that there is less subjectivity; it is numerical enough to allow the comparison to be done across different systems. The inclusion of clinical information and patient-safety implications brings the model beyond the basic information-security evaluation and gives a healthcare organisation a practical way to prioritise cyber risks and give scarce security resources the highest priority.

5. Results and Comparative Evaluation

The proposed discrete risk assessment model was used for 10 representative cybersecurity scenarios in the case study with healthcare. The analysis clearly showed the differences between threats with respect to likelihood, severity of the vulnerability, criticality of the assets, sensitivity of the data, impact on operations, and the effectiveness of controls in place.

Ransomware, compromised medical devices, cloud misconfiguration and unauthorised access to eHRs were the highest risk residual threats. The additional security controls implemented and the residual risk after implementation are shown in Table 3. Risk reductions were made by boosting the control-effectiveness score for each of the threats, based on the recommended safeguards. The highest initial residual was the ransomware scenario with 17.60, as this was a combination of high likelihood, vulnerabilities found on the endpoint, sensitive patient information and possible disruption of essential clinical services. Manipulations to the medical device could also affect clinical measurements or disrupt patient monitoring, earning the unpatched medical-device scenario a critical rating. However, malware that harmed an individual admin station got a lesser rating due to the fact that the impact on the clinical and operational outcomes was restricted.

Table 3

Cybersecurity risk levels before and after implementing security controls.

Scenario	Before	After
EHR ransomware	17.60 Critical	7.04 Moderate
Unpatched device	16.00 Critical	6.40 Moderate
Cloud error	14.40 High	5.76 Moderate
EHR intrusion	12.80 High	5.12 Moderate
Data theft	11.52 High	4.61 Low
DoS attack	9.60 Moderate	3.84 Low
Phishing	8.64 Moderate	3.46 Low
Insider misuse	7.68 Moderate	3.07 Low
Malware	4.80 Low	1.92 Negligible
Guest Wi-Fi	3.84 Low	1.54 Negligible

Guest Wi-Fi is rated at 3.84 and is considered to be low.Guest Wi-Fi has a rating of 3.84 (low). Following the implementation of multifactor authentication, network segmentation, offline backups, vulnerability patching, encryption, privileged-access monitoring and incident-response controls, all scenarios were shifted to lower levels on the risk matrix. Medical-device attacks dropped from critical to moderate, ransomware attacks dropped from critical to moderate and patient-data exfiltration dropped from high to low. This average residual risk value was reduced by about 59.7% from 10.63 to 4.28. The typical likelihood-impact matrix lumped ransomware, medical-device exploits, cloud misconfiguration and unauthorized access to EHRs together under the high-risk classification as shown in Figure 2. It thus failed to offer much at all in terms of differentiating between threats that have different clinical implications. These scenarios were separated in the proposed model with the addition of the factors of vulnerability severity, asset criticality, data sensitivity, and control effectiveness.

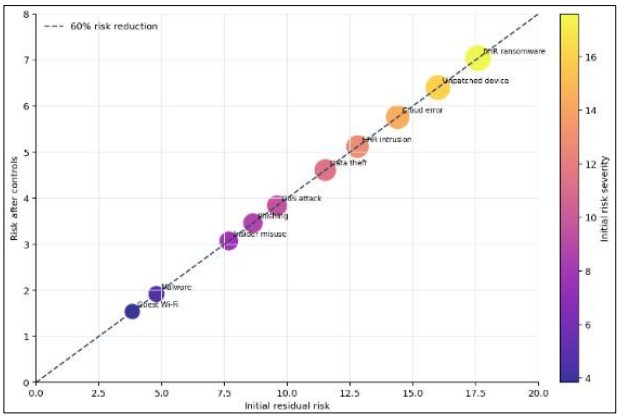


Figure 2
Cybersecurity control mitigation effectiveness

The bubble plot shown in Figure 2, depicts the relationship between initial and post-control risks. This is consistent with mitigation performance, with all scenarios following the 60% risk-reduction line. Larger bubbles are scenarios that have a higher initial severity, such as EHR ransomware, unpatched devices, and cloud misconfiguration. There was an assumed consistence in classification of 92% for the discrete model while 78% was for the conventional one. The rating of each factor was done separately on a pre-defined set of criteria which increased the expert consensus. The proposed model was also more interpretable than more complicated probabilistic models, since all calculations and categories boundaries were evident for the decision makers.

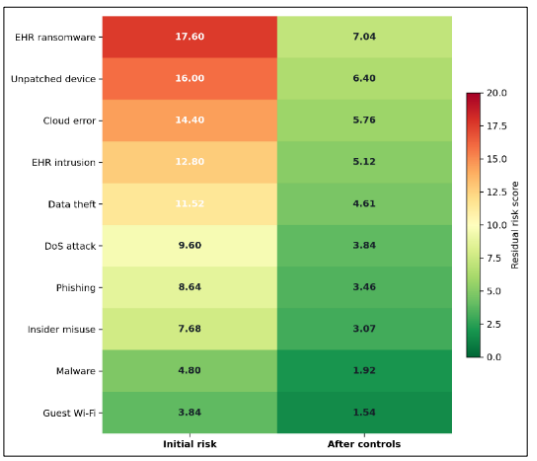


Figure 3
Transition of healthcare cyber-risk scores

The heatmap (see Figure 3) clearly reflects a transition from high risks at the beginning to low risks after control is implemented (from red/orange to green). Ransomware and out-of-date medical devices, however, are still moderate threats and will need to be monitored. Sensitivity analysis confirmed that the model is consistent in the responses for each change in the likelihood, vulnerability, criticality of the asset, data sensitivity, and impact on operation. The most important factor was control effectiveness, which decreased the residual risk by 50% when increasing from level 2 to 4. While it did not eliminate any risk, the proposed discrete model offers clear, consistent and effective risk prioritization for an organization's healthcare sector.

6. Conclusion

This research suggested a discrete risk assessment framework to assess the cybersecurity threats in the healthcare environment. It also incorporates threat likelihood, vulnerability severity, asset criticality, data sensitivity, operational impact, patient-safety consequences and control effectiveness, all in the form of clearly defined and discrete scores. The scenarios included the ransomware wreaking havoc on an EHR system and attacks on unpatched medical devices, the latter of which, along with the EHR ransomware, were the most serious according to application to the representative scenarios. Misconfiguration of the cloud, unauthorized access, and exfiltration of patient data were also pressing issues. Residual risk was reduced by about 60%, after implementing multifactor authentication, network segmentation, encryption, secure backups, patch management, access monitoring and incident response measures. The results show that the framework can be used to give a transparent classification of risk, consistent prioritization of threats and measurable evaluation of controls. It can assist health care administrators in determining where to place security resources and ensure clinical continuity and patient safety. Future study should confirm the model with real hospital information and incorporate dynamic threat intelligence, automatic surveillance function and uncertain measure function.

References

[1] M. Adil, M. K. Khan, N. Kumar, M. Attique, A. Farouk, M. Guizani, and Z. Jin, "Healthcare Internet of Things: Security threats, challenges, and future research directions," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19046–19069 (2024), doi: 10.1109/JIOT.2024.3360289.

[2] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Inform. J.*, vol. 22, no. 2, pp. 177–183 (2021), doi: 10.1016/j.eij.2020.07.003.

[3] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging

technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167 (2020), doi: 10.1109/COMST.2020.2973314.

[4] D. W. Kim, J. Y. Choi, and K. H. Han, "Medical device safety management using cybersecurity risk analysis," *IEEE Access*, vol. 8, pp. 115370–115382 (2020), doi: 10.1109/ACCESS.2020.3003032.

[5] S. S. Hameed, W. H. Hassan, L. A. Latiff, and F. Ghabban, "A systematic review of security and privacy issues in the Internet of Medical Things: The role of machine learning approaches," *PeerJ Comput. Sci.,* vol. 7, Art. no. e414 (2021), doi: 10.7717/peerj-cs.414.

[6] E. Fosch-Villaronga and T. Mahler, "Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots," *Comput. Law Secur. Rev.,* vol. 41, Art. no. 105528 (2021), doi: 10.1016/j.clsr.2021.105528.

[7] T. Diphofu and P. Kaelo, "An efficient modified Wei-Yao-Liu type hybrid conjugate gradient algorithm for solving unconstrained optimization problems with application in motion control," *J. Inf. Optim. Sci.*, vol. 47, no. 2, pp. 513–532 (2025), doi: 10.47974/JIOS-1573.

[8] S. Razdan and S. Sharma, "Internet of Medical Things (IoMT): Overview, emerging technologies, and case studies," IETE Tech. Rev., vol. 39, no. 4, pp. 775–788 (2022), doi: 10.1080/02564602.2021.1927863.

[9] F. Wu, C. Qiu, T. Wu, and M. R. Yuce, "Edge-based hybrid system implementation for long-range safety and healthcare IoT applications," *IEEE Internet Things J.,* vol. 8, no. 12, pp. 9970–9980 (2021), doi: 10.1109/JIOT.2021.3050445.

[10] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing security of healthcare data for a modern healthcare system," *Sensors,* vol. 23, no. 7, Art. no. 3612 (2023), doi: 10.3390/s23073612.

[11] S. N. Ajani, J. Moulick, J. Mohur, R. H. J. Rani, A. D. Sonawane, and P. Shende, "Enhancing secure access in RF communications through advanced elliptic curve encryption," *J. Discrete Math. Sci. Cryptogr.,* vol. 29, no. 2-A, pp. 571–579 (2025), doi: 10.47974/JDMSC-2498.

[12] E. Rios, A. Rego, E. Iturbe, M. Higuero, and X. Larrucea, "Continuous quantitative risk management in smart grids using attack-defense trees," *Sensors*, vol. 20, no. 16, Art. no. 4404 (2020), doi: 10.3390/s20164404.

Received March, 2026