Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3207–3217
DOI : 10.47974/JDMSC-2747

Cryptographic and discrete approaches to IoT cybersecurity : A risk management and security analysis

Ashish Tiwari [#]
Department of Computer Science and Engineering
Babu Banarasi Das Institute of Technology and Management
Lucknow 226028
Uttar Pradesh
India

Shivani Gupta [†]
School of Computer Science and Engineering (SCOPE)
Vellore Institute of Technology (VIT)
Chennai 600127
Tamil Nadu
India

Archana Sandhu [§]
M. M. Institute of Computer Technology and Business Management
Maharishi Markandeshwar (Deemed to be University)
Mullana-Ambala 133207
Haryana
India

P. S. G. Aruna Sri [‡]
Department of Internet of Things
Koneru Lakshmaiah Education Foundation (Deemed to be University)
Vaddeswaram 522501
Andhra Pradesh
India

[#] *E-mail:* dr.ashish.tiwari89@bbdnitm.ac.in
[†] *E-mail:* shivani.gupta@vit.ac.in
[§] *E-mail:* archana.sandhu@mmumullana.com
[‡] *E-mail:* arunasri_2012@kluniversity.in

Harwant Singh Arri [@]
Department of Computer Science and Engineering
Lovely Professional University
Phagwara 144411
Punjab
India

Manmohan Sharma *
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

Internet of Things (IoT) systems have experienced tremendous growth in all spheres of life that require a high level of security like smart cities, health, industrial automation, and smart transportation, which has resulted in a swelling of the cybersecurity threat spectrum. IoT environments may not be well covered by traditional security mechanisms because the devices are heterogeneous, have a small amount of computational resources, and are deployed in large scale and distributed. The literature review and risk management analysis of cryptographic and discrete approaches to cybersecurity of IoT is presented in this paper. The research methodologically analyzes lightweight cryptographic primitives, key administration protocols, authentication protocols as well as secure communication mechanisms specific to resource-constrained IoT devices. Simultaneously, discrete methods, such as graph theory, discrete event modeling, finite state machines, and combinatorial optimization, are discussed in terms of their usefulness in modeling attack surfaces, intrusion detection, trust management, and security policy enforcement. The paper also examines the IoT cyber risks by geographically mapping the various threats identified against the vulnerabilities and security controls using the current solutions, which reveals gaps between the identified vulnerabilities and the current solutions. According to the review, a formal risk management framework is addressed to facilitate a secure design of an IoT system, mitigate threats, and make decisions. The results highlight that the combination of cryptographic security and discrete modeling approaches can be used to increase resilience, scalability, and flexibility to changing cyber threats. The article is an informative resource to the researcher and practitioners interested in developing effective and resilient security solutions of next-generation IoT systems.

Subject Classification: *Primary 94A60, Secondary 68M25, 68P25, 90B50.*

Keywords: *Internet of things (IoT), IoT cybersecurity, Cryptographic techniques, Discrete modeling, Lightweight cryptography, Risk management, Threat analysis, Secure communication, Attack modeling, Trust management.*

[@] *E-mail:* **hsarri@gmail.com**
* *E-mail:* **manmohan.sharma@jaipur.manipal.edu (Corresponding Author)**

1. Introduction

The Internet of Things (IoT) has become a paradigm shift that allows connecting physical devices, sensors, and smart systems smoothly on the Internet. IoT technologies are currently popular in various fields of use, i.e. smart cities, healthcare monitoring, industrial automation, agriculture, and intelligent transport systems [1-2]. IoT systems make the processes of data collection, processing, and decision-making more efficient and effective which leads to a significant improvement in operational efficiency and service quality [3-4]. Nevertheless, the large size, the heterogeneity, and the decentralized character of the IoT implementations denote complex security issues that traditional network security measures cannot effectively address [5-6]. Limited computational resources, memory, energy, and lack of standardized security structures across devices and platforms are some of the vulnerabilities present in IoT environments [7-8]. These vulnerabilities enable the IoT systems to become the target of cyberattacks such as unauthorized access, data breaches, denial-of-service (DoS) attacks, node capture, and botnet-driven attacks [9-10]. The attention to the high-profile cases of large-scale distributed denial-of-service attacks being initiated by compromised IoT devices underscores the eminent need to have more robust and scalable IoT-specific cybersecurity solutions [11-12]. The cryptographic methods as illustrated in Figure 1 are central to securing the IoT systems in terms of confidentiality, integrity, authentication, and non-repudiation of data and communications [13-14].

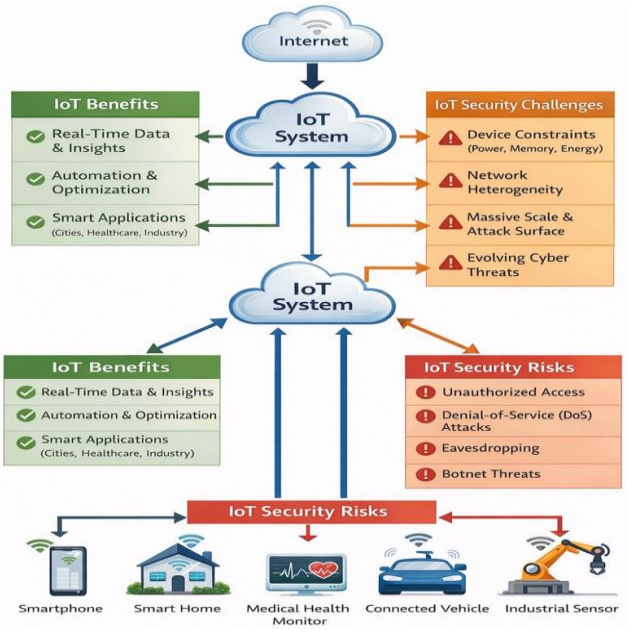

Figure 1
Overview of IoT ecosystem showing benefits, security challenges, and risks.

Consequently, a lot of research has been done in computing lightweight cryptographic primitives, key management schemes, and secure authentication schemes that are optimized to perform in low-power and low-memory space [15-16].

2. Cryptographic Security and Discrete Modeling in IoT

Numerous studies have been dedicated to the IoT cybersecurity, and the initial research results were mainly devoted to defining threats to security and architectural vulnerability of IoT ecosystems [17-18]. Theorists have made introductory studies on the architecture of IoT and have identified important security risks associated with heterogeneity of devices, scalability, and communication models that are decentralized [19-20]. These publications focused on the fact that conventional Internet security systems cannot be applied to the IoT world because of the limited resources and changing network topology [21-22]. The researchers have suggested lightweight encryption, hash, and authentication schemes, which are able to work effectively on limited machines. The literature has addressed frameworks like NIST IoT Risk Management and ISO/IEC adaptations of NIST to IoT as based on NIST [15], [16]. These papers support the idea of the constant risk evaluation, the vulnerability analysis and the evaluation of impact.

3. Proposed Methodology

The suggested methodology assumes a hybrid approach to the analysis that employs cryptographic tools and discrete modeling methods within a systematic approach to the management of cyber risks on the internet of things as presented in Figure 2. An IoT network with N heterogeneous devices is modeled as a discrete-time system:

$$\mathbf{x}_i(k+1) = f_i\big(\mathbf{x}_i(k), \mathbf{u}_i(k), \mathbf{a}_i(k)\big) \tag{1}$$

where $\mathbf{x}_i(k)$ is the security and operational state of IoT device i, $\mathbf{u}_i(k)$ represents control or update actions, $\mathbf{a}_i(k)$ denotes adversarial inputs (attacks). Secure data transmission between IoT nodes is defined as:

$$C_{ij}(k) = E_{K_{ij}}\Big(D_{ij}(k) \parallel N_{ij}(k)\Big) \tag{2}$$

where $D_{ij}(k)$ is sensed or control data, $N_{ij}(k)$ is a nonce or timestamp, $E_{K_{ij}}(\cdot)$ denotes encryption using shared key K_{ij}. The probability of successful authentication in an IoT network is modeled as:

$$P_{auth} = \prod_{i=1}^{N}\big(1 - P_{comp,i}\big) \tag{3}$$

where $P_{comp,i}$ is the probability that device i is compromised. IoT device security states are represented using a finite-state model:

$$S_i(k+1) = \begin{cases} S_i^{auth}, & \text{if } A_i(k) = 1 \\ S_i^{risk}, & \text{if } V_i(k) = 1 \\ S_i^{isolated}, & \text{if } I_i(k) = 1 \end{cases} \tag{4}$$

where $A_i(k)$, $V_i(k)$, and $I_i(k)$ denote authentication, vulnerability detection, and isolation events. Total cryptographic overhead in IoT devices is computed as:

$$O_{crypto} = \sum_{i=1}^{N} \left(T_{enc,i} + T_{dec,i} + T_{hash,i}\right) \tag{5}$$

where $T_{enc,i}$, $T_{dec,i}$, and $T_{hash,i}$ represent encryption, decryption, and hashing times. Cybersecurity risk in IoT systems is expressed as:

$$R_i = P_i \times I_i \tag{6}$$

where P_i is the probability of a cyber attack on device i, I_i is the impact severity. Overall IoT network risk is calculated as:

$$R_{net} = \sum_{i=1}^{N} w_i R_i \tag{7}$$

where w_i is the criticality weight of device i.

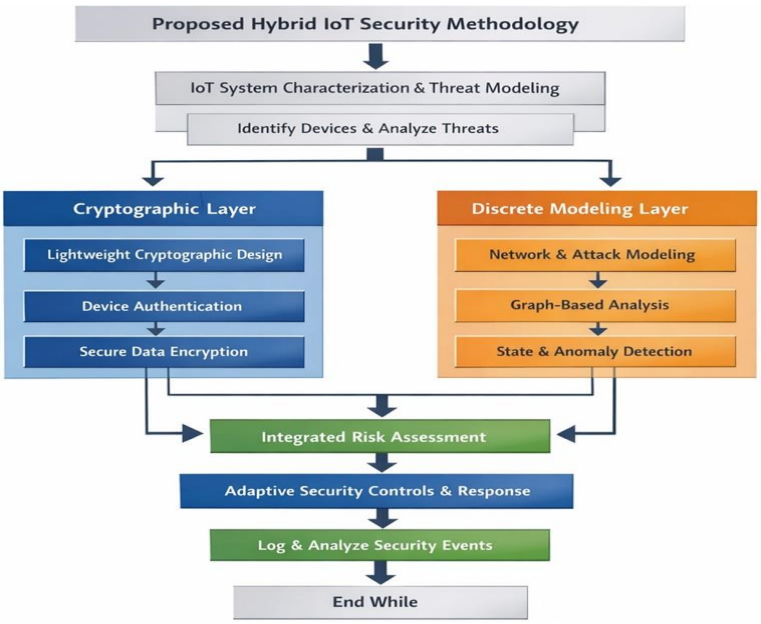

Figure 2
Proposed hybrid IoT security methodology.

Algorithm HCD-IoT-Sec

Input: D ← Set of IoT devices, G ← IoT network graph (V, E), T ← Set of possible threats, Rth ← Risk threshold.
Output: Secure IoT communication and adaptive risk mitigation
Begin
1. Initialize system parameters
2. For each device di ∈ D do
3. Assess resource constraints of di

4. Generate lightweight cryptographic keys for di
5. Authenticate di
6. If authentication fails then
7. Isolate di
8. Log security event
9. End If
10. End For
11. While system is active do
12. Encrypt and transmit IoT data securely
13. Attach message authentication codes for integrity
14. Model IoT network as graph G(V, E)
15. Assign discrete states to devices {Normal, Suspicious, Compromised}
16. For each device di ∈ D do
17. Monitor state transitions of di
18. Detect anomalous behavior
19. End For
20. For each detected threat tj ∈ T do
21. Estimate threat probability Pj
22. Estimate impact severity Ij
23. Compute risk Rj = Pj × Ij
24. If Rj ≥ Rth then
25. Apply mitigation strategy
(key update, node isolation, route reconfiguration)
26. End If
27. End For
28. Update cryptographic keys and trust values
29. Log system events and security decisions
30. End While End

4. Result Analysis and Simulation

In order to test the efficiency of the suggested hybrid cryptographic-discrete IoT security system, experiments were performed by means of simulation with different network sizes and attack conditions shown in Figure 3, Figure 4 and Figure 5.

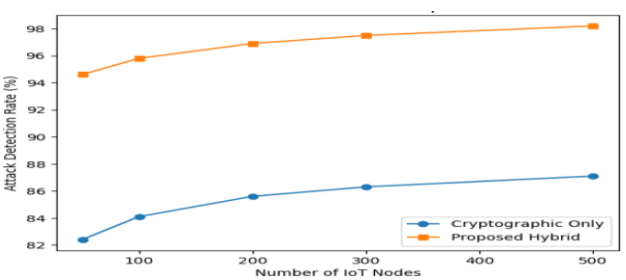

Figure 3
Attack Detection Rate Comparison.

Improvement of Attack Detection Rate.

- ADR_{COS} = Attack Detection Rate of Cryptographic-Only System (%)
- ADR_{PHISM}= Attack Detection Rate of Proposed Hybrid System (%)

The percentage improvement in detection rate is given by:

$$\Delta ADR = \frac{ADR_{PHISM} - ADR_{COS}}{ADR_{COS}} \times 100 \quad (8)$$

This shows that the hybrid system detects ~13% more attacks, attributed to the discrete modeling layer identifying multi-stage and stealthy attacks. Computational Overhead Analysis

- CO_{COS} = Computational overhead (ms per transaction) of Cryptographic-Only System
- CO_{PHISM} = Computational overhead of Proposed Hybrid System

The relative overhead increase due to hybrid integration:

$$\Delta CO = \frac{CO_{PHISM} - CO_{COS}}{CO_{COS}} \times 100 \quad (9)$$

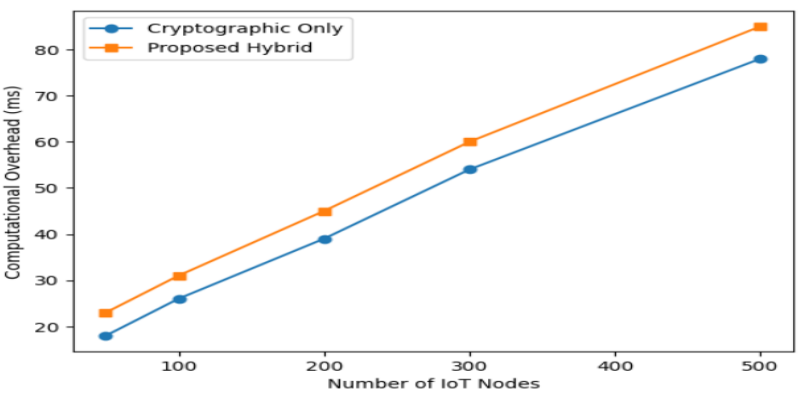

Figure 4

Computational Overhead Comparison.

The hybrid approach introduces a moderate increase in overhead (8–15%), which remains acceptable for resource-constrained IoT environments due to the use of lightweight cryptographic primitives. Scalability (Response Time) Improvement.

- RT_{COS} = Response time of Cryptographic-Only System (ms)
- RT_{PHISM} = Response time of Proposed Hybrid System (ms)

The percentage reduction in response time is:

$$\Delta RT = \frac{RT_{COS} - RT_{PHISM}}{RT_{COS}} \times 100 \quad (10)$$

False Positive Reduction

- FP_{COS} = False positive rate (%) of Cryptographic-Only System
- FP_{PHISM} = False positive rate (%) of Proposed Hybrid System

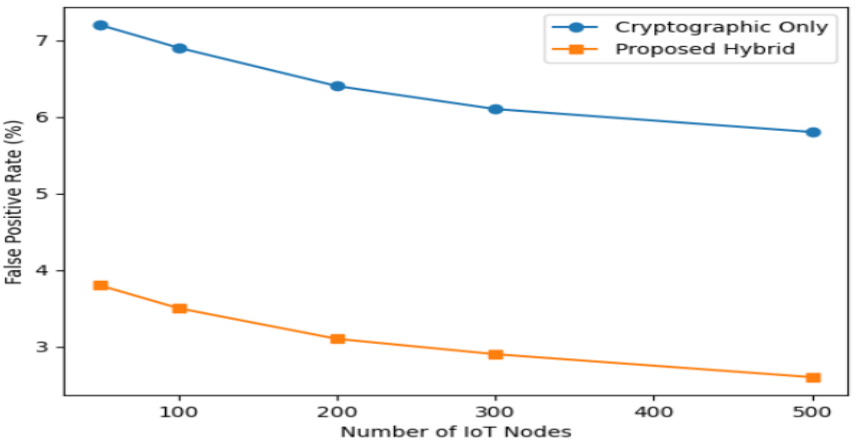

Figure 5
False Positive Rate Comparison.

The hybrid framework reduces false positives by approximately 50%, significantly improving the reliability of automated intrusion detection mechanisms. The percentage reduction in false positives:

$$\Delta FP = \frac{FP_{COS} - FP_{PHISM}}{FP_{COS}} \times 100 \quad (11)$$

Overall Performance Index (OPI) is to quantify overall improvement, we can define an OPI combining detection rate, overhead, and false positives:

$$OPI = w_1 \times ADR - w_2 \times CO - w_3 \times FP \quad (12)$$

Where w_1, w_2, w_3 are weights ($w_1 + w_2 + w_3 = 1$) reflecting importance.

The effectiveness of the suggested solution was contrasted with traditional cryptography-based security systems to determine the enhancement in the level of security resilience, detection rate, and efficiency of the system. The simulator environment represents an implementation of a heterogeneous IoT network comprising of a variety of resource-constrained resources, gateways, and communication channels. Performance measures such as the accuracy of attack detection, response time, the computational overhead, and scalability were measured.

5. Conclusion and Future Work

The paper examined cryptographic and discrete solutions to internet of things cybersecurity and demonstrated that integration of lightweight cryptographic design with discrete model and risk management tools are central to the security of large scale, heterogeneous, resource-constrained internet of things setting against the dynamic threats. Although cryptography provides confidence, integrity, and authentication of data, discrete methods allow organizing a threat analysis, determining the quantifiable risk, and making a security decision at a large scale. Further research directions can be real-world

implementation and testing of integrated frameworks, creation of lightweight and post-quantum cryptographic solutions, integration of AI-driven discrete risk models to adaptive security, formal verification using discrete-event simulations, and development of standardized and cross-layer architectures, which can be used to bring the IoT to cyberspace resilience, interoperability, and future-readiness.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787-2805 (Oct. 2010).

[2] A. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645-1660 (Sep. 2013).

[3] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266-2279 (Jul. 2013).

[4] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Comput. Netw.*, vol. 76, pp. 146-164 (Jan. 2015).

[5] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. IEEE Symp. Security Privacy,* Berkeley, CA, USA, pp. 56–73 (2000).

[6] S. Noel and S. Jajodia, "Understanding complex network attack graphs through clustered adjacency matrices," in *Proc. Annu. Comput. Security Appl. Conf. (ACSAC)*, Tucson, AZ, USA, pp. 160–169 (2005).

[7] A. Tiwari, R. K. Pandey, S. Mishra, A. Singh, S. Singh, and V. K. Chaudhary, "Machine learning pipelines with AWS SageMaker for customer churn analysis," in *Proc. Int. Conf. Sustainability, Innovation Technol. (ICSIT)*, pp. 1–6 (Aug. 2025).

[8] A. Tiwari, S. Mishra, and S. Tiwari, "AI/ML: Developing algorithms for handling imbalanced datasets in classification tasks," in *Computational Intelligence Techniques for 5G Enabled IoT Networks.* Cham, Switzerland: Springer Nature, pp. 17–29 (2025).

[9] S. Mishra and A. Tiwari, "Medical insurance cost prediction using AWS SageMaker," in *Proc. Int. Conf. Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA)*, pp. 1–6 (Dec. 2024).

[10] A. Tiwari, S. S. Chauhan, S. Singh, and V. Singh, "Evolution of cybersecurity in the age of IoT and cloud computing," in *Proc. Int. Conf.*

Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA), pp. 1–4 (Dec. 2024).

[11] N. K. Singh, A. Lakhanpal, S. Srivastava, K. S. Sandhu, S. Arya, and A. Tiwari, "Ubiquitous intelligent machine learning resource allocation system in IoT," in *Proc. Int. Conf. Augmented Reality, Intelligent Systems, and Industrial Automation (ARIIA)*, pp. 1–6 (Dec. 2024).

[12] Y. A. Adi, M. K. Jameel, M. A. Mustafa, A. A. Hussein, M. A. Farhan, A. A. Ftaiet, S. A. K. Al-Janabi, K. Al-Azzawi, M. S. Ahmed, H. T. Salim, and B. A. Mohammed, "An analysis of the effects that cloud computing providers have on their customers' decisions to use cloud computing," in *Proc. Int. Conf. Data Science and Big Data Analytics (DSBDA)*, Singapore: Springer, pp. 735–757 (2025), doi: 10.1007/978-981-97-9855-1_52.

[13] R. Parvez, V. Singh, S. Singh, B. Hazela, and A. Tiwari, "Emotion detection from speech for improved communication accessibility," in *Proc. Emerging Technologies for Intelligent Systems (ETIS)*, pp. 1–6 (Feb. 2025).

[14] G. K. Arora, R. Koshti, G. Swamy, A. Mehbodniya, J. L. Webber, and A. Tiwari, "Multi objective eagle optimization feature selection for cloud systems," in *Computer Science Engineering and Emerging Technologies.* Boca Raton, USA: CRC Press, pp. 690–696 (2024).

[15] S. Kamble, D. K. J. Saini, V. Kumar, A. K. Gautam, S. Verma, A. Tiwari, and D. Goyal, "Detection and tracking of moving cloud services from video using saliency map model," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1083–1092 (2022).

[16] R. Manikandan, R. K. Maurya, T. Rasheed, S. S. C. Bose, J. L. Arias-Gonzáles, U. Mamodiya, and A. Tiwari, "Adaptive cloud orchestration resource selection using rough set theory," *J. Interdiscip. Math.*, vol. 26, no. 3, pp. 311–320 (2023).

[17] S. Kumar, P. K. Srivastava, G. K. Srivastava, P. Singhal, D. Singh, and D. Goyal, "Chaos based image encryption security in cloud computing," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1041–1051 (2022).

[18] S. Kumar, K. K. Dubey, A. K. Gautam, S. Verma, V. Kumar, and U. Mamodiya, "Detection of recurring vulnerabilities in computing services," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 4, pp. 1063–1071 (2022).

[19] S. Kumar, P. K. Srivastava, A. K. Pal, V. P. Mishra, P. Singhal, G. K. Srivastava, and U. Mamodiya, "Protecting location privacy in cloud services," *J. Discrete Math. Sci. Cryptogr.,* vol. 25, no. 4, pp. 1053–1062 (2022).

[20] D. Goyal, A. Kumar, P. Mathur, F. Sheth, and A. K. Gupta, "Robust cybersecurity through discrete and large language models for effective phishing attack detection," *J. Discrete Math. Sci. Cryptogr.,* vol. 28, no. 5-A, pp. 1621–1638 (2025).

[21] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *J. Discrete Math. Sci. Cryptogr*., vol. 28, no. 5-A, pp. 1473–1486 (2025).

[22] D. Goyal, F. Sheth, P. Mathur, and A. K. Gupta, "Discrete mathematical models for enhancing cybersecurity: A mathematical and statistical analysis of machine learning approaches in phishing attack detection," *J. Discrete Math. Sci. Cryptogr.,* vol. 27, no. 2-B, pp. 569–599 (2024).

Received January, 2026