

Combinatorial algebra and cryptographic graph structures for cluster-based hybrid intrusion detection in IoT networks

Ashok Kumar Saini [#]

Department of Computer Science and Engineering

Manipal University Jaipur

Jaipur 303007

Rajasthan

India

Manoj Wadhwa ⁺

Department of Computer Science and Engineering

University Institute of Engineering

Chandigarh University

Mohali 140413

Punjab

India

Ranjeeta Kaur Popli [§]

Department of Computer Science

Kamal Institute of Higher Education and Advance Technology

Guru Gobind Singh Indraprastha University

New Delhi 110059

India

Madan Lal Saini [‡]

Department of Computer Science and Engineering

Apex Institute of Technology

Chandigarh University

Mohali 140413

Punjab

India

[#] E-mail: ashok.saini@jaipur.manipal.edu

⁺ E-mail: manojkw11@yahoo.com

[§] E-mail: ranjeetapopli@gmail.com

[‡] E-mail: madan.e13485@cumail.in;
mlsaini@gmail.com

Sanjay Kumar [@]

*Department of Basic Sciences and Humanities
Pranveer Singh Institute of Technology
Kanpur 209305
Uttar Pradesh
India*

Prashant Vats *

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

Abstract

The rapid growth of Internet of Things (IoT) environments has led to significant security challenges due to their dispersed, resource-limited, and constantly evolving characteristics. This study introduces a hybrid intrusion detection model that combines combinatorial graph theory, algebraic frameworks, and lightweight cryptographic approaches to strengthen protection in clustered IoT systems. The network structure is represented through discrete graph models, while algebraic methods—such as elliptic curve operations over finite fields and group-oriented key generation—are applied to secure interactions between cluster heads and sensor nodes.

Subject Classification: 94A60, 68R10.

Keywords: IoT security, Hybrid intrusion detection system, Algebraic cryptography, Combinatorial clustering, Discrete structures, Graph-based intrusion detection, Lightweight encryption, Finite fields.

1. Introduction

The Internet of Things (IoT) is reshaping modern infrastructures by linking billions of smart devices across sectors like healthcare, transport, industry, and essential services. Yet, such extensive interconnectivity creates major risks to privacy and security, largely due to decentralized structures, resource-constrained hardware, and device diversity. Conventional security mechanisms often fail to handle these issues, driving the demand for lightweight, adaptive, and intelligent intrusion detection systems (IDS) tailored for IoT. Current studies highlight integrating mathematical precision with cryptographic resilience in designing secure network solutions. Within this scope, discrete mathematical tools—such as graphs, finite fields, algebraic groups, and

[@] E-mail: snjay1991@gmail.com

^{*} E-mail: prashant.vats@jaipur.manipal.edu (Corresponding Author)

combinatorial optimization—provide a strong framework for modeling protected communication and studying network dynamics.

2. Literature View

The increasing diversity and intricacy of IoT ecosystems has amplified their exposure to numerous security flaws, creating the need for advanced mechanisms in vulnerability assessment, attack path modeling, and systematic risk evaluation. Arat and Akleyek introduced a refined graph-driven technique for analyzing IoT threats, where emphasis was placed on traversing attack graphs and prioritizing potential risks for early detection [1]. Building upon this contribution, their later research proposed a quantitative assessment approach that combined combinatorial analysis with graph-theoretic evaluation for IoT-specific risk management [3]. In a related line of work, Karakaya and Arat [9] compiled an extensive survey of Industrial IoT security mechanisms, drawing attention to critical attack vectors and cryptographic countermeasures within industrial settings. Airehrour, Gutierrez, and Ray [2] designed SecTrust-RPL, a lightweight trust-aware routing scheme integrating cryptographic primitives and trust evaluation metrics to secure RPL-based IoT topologies, significantly reducing malicious behaviors such as blackhole intrusions in constrained environments. Similarly, Stellios, Kotzanikolaou, and Grigoriadis [4] examined cyber-physical intrusion paths in IoT-enabled critical infrastructure using graph models to replicate realistic attack scenarios. This aligns with Konsta et al. [5], who surveyed methods for automatically generating attack trees and graphs, stressing scalable and formalized modeling in evolving systems. Zeng et al. [6] extended these studies by categorizing attack graph techniques according to their inference and data processing strategies, thereby making them more effective for semi-automated analysis. Earlier theoretical progress by Jha, Sheyner, and Wing [7] involved applying formal approaches like model checking and reachability analysis to attack graphs, which later informed practical IoT-based implementations, such as Yang, Yuan, and Zhang [8] host-oriented risk modeling framework. Further, Bilal, Hasany, and Pitafi [10] addressed sinkhole threats at the IoT sensing tier through edge-driven monitoring, enabling real-time anomaly detection and selective traffic filtering. Complementing this, Alshukri et al. [11] presented a border-security model that embedded IoT sensing devices with rule-based intrusion detection for ultra-low latency responses at the edge. Emerging contexts such as vehicular IoT and 5G mobility raised novel challenges; for example, Ikramov [12] investigated V2X vulnerabilities across operators, emphasizing trust-graph methods and collaborative verification to counter spoofing and hijacking. Analytical progress was furthered by Gaber, Wannes, and Zouari [13], who applied machine learning to industrial IoT vulnerability modeling using graph-structured, labeled datasets. Rani, Kumar, and Dohare [14] complemented this with a game-theoretic model where IoT nodes evaluated mutual trust through payoff strategies mapped in decision graphs. Finally, Goel, Gupta, and Kumari [15] proposed a dynamic risk identification framework that combined formalized

threat models with adaptive attack graph generation, enabling real-time IoT vulnerability scoring.

3. Proposed Work

This section presents a three-stage theoretical framework designed for secure, scalable, and intelligent intrusion detection in clustered IoT networks, as shown in Figure 1. The framework integrates algebraic cryptographic primitives, combinatorial clustering mechanisms, and a hybrid intrusion detection engine to address both computational constraints and dynamic threat landscapes inherent in IoT ecosystems [16, 17].

Stage I: Algebraic Cryptographic Initialization

The first stage focuses on establishing secure communication among IoT devices using lightweight, algebraic cryptographic schemes [18].

Elliptic Curve $\rightarrow E: y^2 \equiv x^3 + ax + b \pmod{p}; \forall a, b \in F_p$,
where p is a large prime number.
for Key generation $\rightarrow$ Each IoT device performs
{
Private Key (random scalar): $\rightarrow d \in Z_n$;
Public Key: $\rightarrow Q = d \cdot G$;
Encryption (Elliptic Curve ElGamal variant) for a message $M \rightarrow Pm \in E$
(F_p);
}

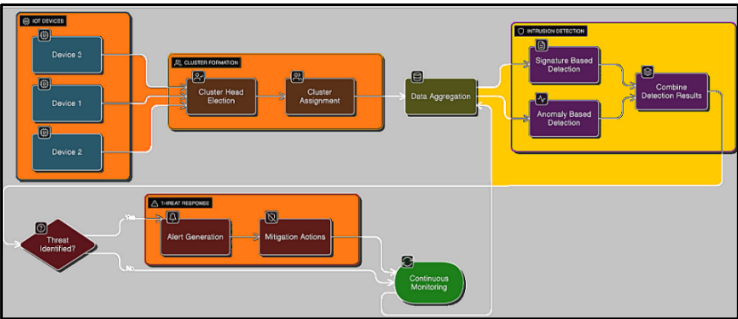
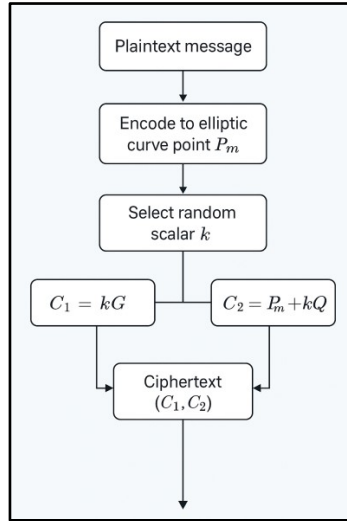


Figure 1
To show the hybrid intrusion detection engine for secure communication among IoT devices

When defined over a finite prime field, elliptic curve computations are restricted to arithmetic modulo a large prime. The resilience of ECC depends on the computational challenge posed by the Elliptic Curve Discrete Logarithm Problem (ECDLP) [19]. To encrypt a message, as shown in Figure 2, the sender first maps the plaintext to a point P_m on a predefined elliptic curve. A random scalar k is then selected from the curve's underlying finite field. The sender computes two elliptical curve points: $C_1=kG$, representing the randomness, and

Stage II: Combinatorial Clustering and Graph-Based Modeling

In the second stage, the IoT network is modeled as a combinatorial graph, enabling efficient clustering, communication, and reduction of the attack surface. Each node is represented as a vertex, and communication links are modeled as undirected or weighted edges. This abstraction allows the use of well-established graph-theoretic algorithms to optimize network structure and minimize vulnerability.

**Figure 2**

To show the Elliptic Curve Cryptographic Initialization Process

Model the IoT network as a graph: $\rightarrow G = (V, E)$

where,

- V : Set of vertices (IoT devices);
- E : Set of edges (communication links)

For $\forall e_{ij} \in E: w_{ij} \in R$; such that w_{ij} is the weight of e_{ij} .

Clustering Objective Function (K Means) $\rightarrow$ Find $\{C_1, C_2, \dots, C_k\}$;

Given a dataset X for $J = \{x_1, x_2, \dots, x_n\} \subset R_d \rightarrow$
partition $\{C_1, C_2, \dots, C_k\}$;

$$\min_{\{c_1, c_2, \dots, c_n\}} J = \sum_{i=1}^k \sum_{x \in C_i}^j \|x - \mu_i\|^2$$

Partition Constraint:
$$\bigcup_{i=1}^k C_i = x$$

$$C_i \cap C_j = \emptyset, \forall i \neq j$$

Centroid Definition:
$$\mu_i = \frac{1}{|C_i|} \sum_{x \in C_i} x, \forall i \in \{1, 2, \dots, k\}$$

The clustering process partitions the graph into multiple subgraphs or clusters based on topological and behavioral characteristics. Algorithms such as

K-means, spectral clustering, or modularity-based partitioning are employed to minimize intra-cluster communication cost while maximizing inter-cluster independence.

Minimum Spanning Tree (MST) for Cluster-Head Connectivity $\rightarrow$

MST objective (optimization form) $\rightarrow \min \sum \min_{T \subseteq E_H} \sum_{e \in T} w(e)$

There exists a subgraph $T^* \subseteq E_H(H, T^*)$, which is a binary tree and

$$\sum_{e \in T^*} w(e) = \min_{T \text{ spans } HT \text{ is a tree}} \sum_{e \in T} w(e)$$

$$\text{for } a \text{ w: } H \times H \rightarrow R \geq 0, w(hi, hj) = \begin{cases} E(hi, hj), & (\text{energy cost}) \\ \text{hop}(hi, hj), & (\text{hop cost}) \end{cases}$$

$$T^* = \arg \min_{T \subseteq E_H(H, T) \text{ tree}} \sum_{e \in T} w(e), \text{ i. e., } (H, T^*) \text{ is a connected, acyclic graph,}$$

$$|T^*| = |H| - |1| ;$$

$$\text{Energy - Aware Cost Function} \rightarrow C = \alpha \cdot i = \sum_1^k E.C_i + \beta \cdot i = \sum_1^k L.(C_i);$$

Each cluster elects a cluster head (CH), which aggregates data and monitors the internal behavior of its nodes.

Stage III: Hybrid Intrusion Detection Engine (H-IDE)

The final stage integrates both signature-based and anomaly-based detection methods to form a hybrid intrusion detection engine (H-IDE). This engine is deployed at the cluster-head level, which has relatively higher computational capabilities than edge nodes.

For Normal Behavior Baseline $\forall f_{i \in F} \rightarrow \mu_i, \sigma_i \in R;$

$$z_{i,j} = \sigma_{i,j} \cdot x_{i,j} - \mu_i, \text{ and } |z_{i,j}| > \tau;$$

If $|z_{i,j}| > \tau$, then n_j is anomalous for every f_i ;

$$\text{Entropy } H \text{ of a feature distribution } X \rightarrow H(X) - i = \sum_1^n p.(x_i) \cdot \log_2 p.(x_i);$$

The anomaly detection module applies statistical methods such as Z-score normalization and entropy analysis to detect deviations in traffic patterns, transmission frequency, and behavioral metrics.

4. Results On Benchmark Datasets

This section presents the empirical validation of the proposed Hybrid Intrusion Detection Engine (H-IDE), developed to enhance intrusion detection in IoT environments by integrating algebraic cryptography, combinatorial clustering, and hybrid detection mechanisms.

4.1 Overall Model Performance

To assess the effectiveness of the proposed Hybrid Intrusion Detection Engine (H-IDE), we carried out a series of comparative experiments on widely used benchmark datasets. The evaluation employed standard performance indicators, including Precision, Accuracy, F1-Score, Recall, and False Alarm Rate (FAR), to provide a comprehensive measure of both detection efficiency

and system reliability. Table 1 and Figure 3 collectively illustrate that the proposed H-IDE outperforms traditional machine learning algorithms, including Random Forest, SVM, XG-Boost, and KNN, across all major performance metrics.

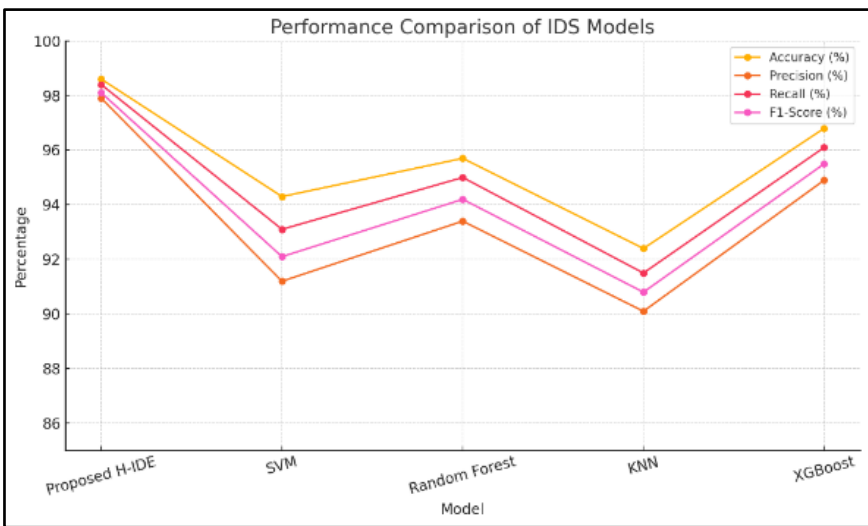


Figure 3
Performance Comparison of IDS Models

Table 1
Benchmark Evaluation of Intrusion Detection Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)
Proposed HIDE	98.6	97.9	98.4	98.1	1.1
SVM	94.3	91.2	93.1	92.1	3.4
Random Forest	95.7	93.4	95	94.2	2.8
KNN	92.4	90.1	91.5	90.8	4.3
XGBoost	96.8	94.9	96.1	95.5	2.5

4.2 Dataset-Specific Analysis

To examine its generalization ability, H-IDE was tested on individual datasets. Table 2 shows that on CIC-IDS2017, the model achieved 97.8% accuracy, outperforming XGBoost (95.3%) and Random Forest (94.2%). In Table 3, results on NSL-KDD demonstrate that H-IDE maintained a strong 98.1% accuracy, again outperforming all competing models.

Table 2
CIC-IDS2017 Benchmark Results

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)
Proposed H-IDE	97.8	96.5	97.2	96.8	1.4
SVM	93.5	90.4	91.8	91.1	3.9
Random Forest	94.2	92.1	93.3	92.7	3.1
KNN	91	88.9	90	89.4	4.7
XGBoost	95.3	93	94.5	93.7	2.8

Table 3
NSL-KDD Benchmark Results

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	False Alarm Rate (%)
Proposed H-IDE	98.1	97.4	97.9	97.6	1.2
SVM	94	90.7	92.5	91.6	3.6
Random Forest	95.1	93	94.1	93.5	2.9
KNN	92.3	89.6	90.8	90.2	4.1
XGBoost	96	94.2	95.5	94.8	2.6

5. Conclusion

In this study, a novel Hybrid Intrusion Detection Engine (H-IDE) was proposed for enhancing security in resource-constrained Internet of Things (IoT) environments. The framework integrates three key stages: algebraic cryptographic initialization, combinatorial clustering with graph modeling, and a hybrid detection engine that fuses both anomaly-based and signature-based techniques.

References

- [1] F. Arat and S. Akleyek, "Modified graph-based algorithm to analyze security threats in IoT," *PeerJ Computer Science*, vol. 9, p. e1743 (Dec. 2023).
- [2] D. Airehrour, J. A. Gutierrez, and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Generation Computer Systems*, vol. 93, pp. 860–876 (Apr. 2019).

- [3] F. Arat and S. Akleylek, "A new method for vulnerability and risk assessment of IoT," *Computer Networks*, vol. 237, Art. no. 110046 (Dec. 2023).
- [4] I. Stelliös, P. Kotzanikolaou, and C. Grigoriadis, "Assessing IoT-enabled cyber-physical attack paths against critical systems," *Computers & Security*, vol. 107, Art. no. 102316 (Aug. 2021).
- [5] A.-M. Konsta, A. Lluch Lafuente, B. Spiga, and N. Dragoni, "Survey: Automatic generation of attack trees and attack graphs," *Computers & Security*, vol. 137, Art. no. 103602 (Feb. 2024).
- [6] J. Zeng, S. Wu, Y. Chen, R. Zeng, and C. Wu, "Survey of attack graph analysis methods from the perspective of data and knowledge processing," *Security and Communication Networks*, vol. 2019, pp. 1–16 (Dec. 2019), doi: 10.1155/2019/2031063.
- [7] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW-15)*, pp. 49–63 (Jun. 2002).
- [8] H. Yang, H. Yuan, and L. Zhang, "Risk assessment method of IoT host based on attack graph," *Mobile Networks and Applications*, pp. 1–10 (Aug. 2023).
- [9] A. Karakaya and F. Arat, "A survey on security requirements, threats and protocols in industrial Internet of Things," *International Journal of Information Security Science*, vol. 10, no. 4, pp. 138–152 (2021).
- [10] A. Bilal, S. M. N. Hasany, and A. H. Pitafi, "Effective modelling of sinkhole detection algorithm for edge-based Internet of Things (IoT) sensing devices," *IET Communications*, vol. 16, no. 8, pp. 845–855 (May 2022).
- [11] D. Alshukri, V. R. Lavanya, E. P. Sumesh, and P. Krishnan, "Intelligent border security intrusion detection using IoT and embedded systems," in *Proceedings of the 4th MEC International Conference on Big Data and Smart City (ICBDSC)*, pp. 1–3 (Jan. 2019).
- [12] A. Ikramov, "On retrieval of secret key parameters from symmetric block cipher O'zDST 1105:2009 using modified SQUARE cryptanalysis," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 6, pp. 2309–2322 (2025), doi: 10.47974/JDMSC-2230.
- [13] A. Gaber, W. Wannes, and H. Zouari, "On the friable mean-values of some arithmetic functions," *Journal of Discrete Mathematical Sciences*

- and Cryptography*, vol. 28, no. 6, pp. 2337–2350 (2025), doi: 10.47974/JDMSC-2283.
- [14] R. Rani, S. Kumar, and U. Dohare, “Trust evaluation for light-weight security in sensor-enabled Internet of Things: Game theory-oriented approach,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8421–8432 (Oct. 2019).
 - [15] S. Goel, M. K. Gupta, and S. Kumari, “An improved attribute-based signature using elliptic curve cryptography,” *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 6, pp. 2371–2382 (2025), doi: 10.47974/JDMSC-2302.
 - [16] B. L. V. S. Aditya and S. N. Mohanty, “Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques,” *Journal of Information and Optimization Sciences*, vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.
 - [17] S. D. Bahinipati and B. K. Pattanayak, “A novel blockchain-enabled smart contract for smart city e-governance ecosystem,” *Journal of Information and Optimization Sciences*, vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.
 - [18] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, “Trends in IoT applications in smart campuses: A topic modeling approach,” *COLLNET Journal of Scientometrics and Information Management*, vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.
 - [19] W. Sripanya, W. Rungrottheera, and P. Hyunsin, “Fourier series analysis and computation based on function characteristics,” *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

Received July, 2025