Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3925–3936
DOI : 10.47974/JDMSC-3020

Algebraic cryptographic primitives for secure IoT data aggregation

Yogesh Dinkar Jadhav [§]
Department of Mechanical Engineering
Sinhgad College of Engineering
Savitribai Phule Pune University
Pune 411041
Maharashtra
India

Jyotsna Suryavanshi [†]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Padmavati Shrivastava *
Department of Computer Science and Engineering (AI & ML)
Rungta International Skills University
Bhilai 490024
Chhattisgarh
India

Pawan Arunkumar Upadhye [‡]
Department of Electronics and Telecommunication Engineering
Symbiosis Institute of Technology (SIT)
Pune 412115
Maharashtra
India

[§] *E-mail:* sittpo3@gmail.com
[†] *E-mail:* jyotsna.suryavanshi@vit.edu
* *E-mail:* shrivastava.padmavati@gmail.com (Corresponding Author)
[‡] *E-mail:* pawan.arunkumar@gmail.com

© Taru Publications

Megha Jagga [@]
Centre for Research Impact and Outcome
Chitkara University
Rajpura 140417
Punjab
India

K. Parimala [#]
Department of Pharmacology
Meenakshi Medical College Hospital and Research Institute
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Kanchipuram 631552
Tamil Nadu
India

Abstract

The rapid growth of Internet of things (IoT) networks requires the effective and secure data aggregation systems that would maintain the confidentiality and provide real-time analytics. The present paper introduces an algebraic cryptographic approach to the problem of secure IoT data aggregation, basing it on structured mathematical primitives to guarantee computation on distributed sensor data upholding privacy. The framework combines algebraic encoding, homomorphic transformation and lightweight encryption schemes to facilitate aggregation in a secure manner without revealing raw data. A formalized mathematical model is built that models the aggregation operations in modular algebraic spaces which are computationally efficient and adversarial resilient. The recommended algorithms are measured in terms of the level of security, the accuracy of aggregation, and the rate of communication showing enhancements in efficiency and lower latency than traditional algorithms. Findings show improved scalability, resiliency and applicability in resource limited IoT settings, which make the framework viable in actual deployments.

Subject Classification: *11T71, 94A60, 94A62, 94B60.*

Keywords: *IoT security, Secure data aggregation, Algebraic cryptography, Homomorphic encryption, Lightweight encryption, Privacy preservation.*

I. Introduction

The rapid increase in Internet of Things (IoT) devices has revolutionized contemporary data-driven ecosystems to allow constant sensing, communication, and intelligent decision-making in many applications, including smart cities, healthcare, and industrial automation [1, 2]. Nevertheless, when using resource-constrained IoT nodes on a large scale, it poses a major challenge to guarantee secure and efficient data

[@] *E-mail:* **megha.jagga.orp@chitkara.edu.in**
[#] *E-mail:* **parim@maher.ac.in**

aggregation [3]. Conventional cryptographic algorithms are strong but they have high computational and communication load, and are not suitable in a lightweight context (aggregating data in real-time) [4, 5]. Furthermore, aggregation methods that are centralized put sensitive information at risk of breaches, hence compromising privacy and integrity of the systems [6]. Figure 1 indicates the secure aggregation of IoT with the help of algebraic cryptography framework.

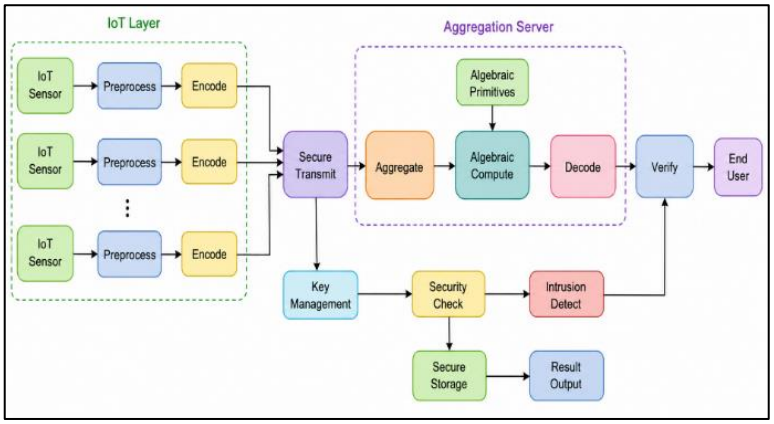


Figure 1

Algebraic Cryptographic Framework for Secure IoT Data Aggregation

To overcome these constraints, algebraic cryptographic primitives have appeared to be the way out to allow the secure aggregation of data and have minimum overhead [7, 8]. These primitives enable computations to be directly done on encrypted data with the use of algebraic structures like modular arithmetic, group operations, and homomorphic transformations without exposing any underlying information [9, 10]. In this paper, a new algebraic cryptography system to incorporate secure encoding, transformation, and aggregation protocols are suggested to work in the IoT context [11].

II. Proposed Algebraic Cryptographic Framework

The framework combines algebraic encryption, homomorphic aggregation, and lightweight protocols, which allow securely and efficiently fuse distributed IoT node data and maintain confidentiality and scalability [12].

A. *System architecture for secure IoT aggregation*

The architecture is layered with sensing, edge processing, encryption modules and aggregation servers where it provides communication

security, decentralized computation, and efficient encrypted data fusion across networks.

$$X_{i(t)} = \int^{1} \left[\sum_{\{i=1\}_{i(t)}^{\{n\}}} x \cdot \varphi_{i(t)} \right] dt \tag{1}$$

The sensor data acquisition is modeled by equation (1) which is a time-integrated weighted sensor observations by combining various inputs using basis functions to form a single algebraic representation.

$$X_{i_{norm}} = \int^{1} \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(\frac{(x_{i(t)} - \mu_i)}{\sigma_i} \right)^2 + \left(X_{i(t)} \right)^2} \, dt \tag{2}$$

In equation (2), preprocessing and normalization is shown, whereby the raw sensor values are normalized based on mean and variance, such that the scales have the same scale but don't alter the structural connections to be used later in the secure processing [13].

$$E_i = \int^{1} \left[\left(X_{i_{norm} mod} p \right) \cdot g^{\{r_i\}} + \sum_{\{k=1\}_{k}^{\{m\}\alpha}} X_{k_{norm}} \right] dt \tag{3}$$

The algebraic encoding at the edge nodes in equation (3) encodes normalized data into encrypted algebraic forms with the help of modular operations, randomization, as well as weighted aggregation to prepare encrypted data to be transmitted securely.

$$T_i = \int^{1} \sqrt{\sum_{\{i=1\}}^{\{n\}} (E_i + \beta_i)^2 + \prod_{\{j=1\}_{j}^{\{n\}}} E} \, dt \tag{4}$$

The secure transmission model, which includes the coded data and random noise and multiplicative interactions, is depicted in equation (4) and guarantees privacy and immunity to interception and adversarial reconstruction in the process of communication.

$$D = \int^{1} \sqrt{\left(A - \sum_{\{i=1\}_{i}^{\{n\}}} r \cdot g \right)^2 + \sum_{\{i=1\}}^{\{n\}} \left(X_{i_{norm}} \right)^2} \, dt \tag{5}$$

Decryption and final reconstruction, as described in equation (5) retrieves the aggregated information by eliminating randomness and verifying consistency, so that an actual retrieval of original normalized information is obtained using aggregated values that are encrypted.

B. *Design of algebraic primitives for encryption and aggregation*

Algebraic primitives use modular arithmetic, group operations and homomorphic properties to allow secure encryption and aggregation to allow computation over ciphertext, and maintain confidentiality. Figure 2 depicts algebraic primitives that make it possible to have safe encryption and aggregation workflow.

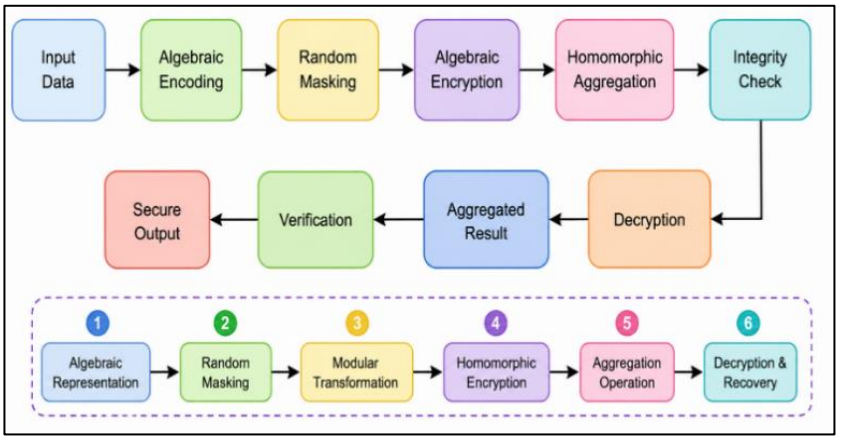


Figure 2

Algebraic Primitives-Based Encryption and Aggregation Workflow for Secure IoT Data Processing

Plaintext Algebraic Representation

$$M = \int^{1}\left[\sum_{\{i=1\}}^{\{n\}}(m_i \cdot x^i mod\ N)\right] dx \tag{6}$$

Plaintext algebraic encoding (Equation (6)) is an encoding that converts message components into a form of polynomies over modular arithmetic, making it possible to represent them in a structured way, allowing them to be subjected to a structured set of algebraic operations and encryption.

$$M1 = \int^{1}\sqrt{\sum_{\{i=1\}}^{\{n\}}\left((m_i + r_i) mod\ N\right)^2 + M^2}\, dx \tag{7}$$

In equation (7) randomized masking is presented, which entails mixing plaintext and random variables in an attempt to affect the original values, improving privacy and maintaining algebraic properties that will be required later to perform cryptographic operations in a secure way.

$$C = \int^{1}\left[\prod_{\{i=1\}}^{\{n\}}((m_i + r_i)^e mod\ N) + \sum_{\{i=1\}_i^{\{n\}\gamma}} r_i\right] dx \tag{8}$$

Modular exponentiation encryption (Equation 8) is the encryption of masked data where exponentiation and aggregation of random components are used to encrypt data, generating ciphertext that provides confidentiality and can be homomorphically processed.

$$V = \int^{1}\sqrt{\sum_{\{i=1\}}^{\{n\}}\left(C_i - \hat{C}_i\right)^2 + \sum_{\{i=1\}}^{\{n\}}(r_i)^2}\, dx \tag{9}$$

The consistency and integrity checking in Equation (9) are done by comparing the calculated and the predicted ciphertext values with

randomness checks to identify tampering to guarantee reliability and validity of the data transmission between sender and receiver.

$$R = \int^{1} \left[\sqrt{\left(C_{agg}\right)^{\frac{2}{e}} - \sum_{\{i=1\}}^{\{n\}} (r_i)^2} + \sum_{\{i=1\}_i^{\{n\}}} m \right] dx \tag{10}$$

The process of decryption and result recovery as outlined in equation (10) involves eliminating the effects of random masking and reversing algebraic transformations in order to recover the aggregated plaintext values in the correct format and still provide consistency and security assurance.

III. Mathematical Model and Algorithm Design

A formal model establishes algebraic aggregation operations and safe transformations, where algorithms guarantee correctness, efficiency and immunity to attacks by encoding and computation processes in a structured way.

A. *Algebraic formulation of data aggregation*

Algebraic structures are used to model the aggregation of data in which sensor values are coded into sets and allow summation, transformation, and fusion of data in regimes that are secure mathematically.

$$M(t) = \int^{1} \left[\sum_{\{i=1\}_{i(t)}^{\{n\}}} m \cdot \varphi_{i(t)} + \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(m_{i(t)}\right)^2} \right] dt \tag{11}$$

Equation (11) in-corporates sensor information in an algebraic space by incorporating weighted signals and magnitude signals and creates a structured representation that can undergo secure aggregation and transformation.

$$M_w = \int^{1} \left[\sum_{\{i=1\}_i^{\{n\}}} w \cdot m_{i(t)} + \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(w_i m_{i(t)}\right)^2 + M(t)^2} \right] dt \tag{12}$$

Equation (12) uses weighted algebraic mapping, which is a combination of sensor data and predetermined weights and normalization terms, to augment importance-based aggregation without compromising mathematical stability and computational stability.

$$A_h = \int^{1} \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(Enc(m_i)\right)^2 + \left(\prod_{\{i=1\}}^{\{n\}} Enc(m_i) \right)^{\frac{1}{2}} + M_{mod}^2} \, dt \tag{13}$$

Homomorphic aggregation is modeled by equation (13), and allows operations that act on encrypted data by squaring ciphertext terms and multiplying, and is privacy-preserving to aggregate data without revealing original inputs.

$$A_n = \int^1 \sqrt{\sum_{\{i=1\}}^{\{n\}} (Enc(m_i) + \eta_i)^2 + \sum_{\{i=1\}}^{\{n\}} \eta_i^2 + A_h^2}\, dt \tag{14}$$

The noise-resilient aggregation (14) proposes the introduction of noise-related elements, random noise to encrypted values, making the aggregation more resilient to adversarial interference with the accuracy of the aggregated outcomes retained in uncertainty.

$$A_{final} = \int^1 \left[\sqrt{A_n^2 + \sum_{\{i=1\}}^{\{n\}} \left(m_{i(t)}\right)^2} + \sum_{\{i=1\}_{i(t)}^{\{n\}}} m \right] dt \tag{15}$$

Final aggregated output is defined by equation (15), which takes into account noisy values and original magnitudes, reconstitutes meaningful aggregated information and does not compromise algebraic consistency, accuracy and security guarantees in the results.

B. *Secure encoding and transformation functions*

Encoding functions encode plaintext into homomorphic representations that are secure, and transformation functions perform homomorphic operations, to ensure that encrypted computations are consistent, verifiable, and resistant to adversarial inference.

$$P = \int^1 \left[\sum_{\{i=1\}}^{\{n\}} (m_i \cdot x^i mod\ N) + \sqrt{\sum_{\{i=1\}}^{\{n\}} (m_i)^2} \right] dx \tag{16}$$

In equation (16), plaintext is coded into a polynomial algebraic representation, modular terms mixed with magnitude normalization are used to allow structured representation to be obtained which could be transformed and encrypted in a secure way.

$$P_r = \int^1 \sqrt{\sum_{\{i=1\}}^{\{n\}} \left((m_i + r_i) mod\ N\right)^2 + P^2 + \sum_{\{i=1\}}^{\{n\}} r_i^2}\, dx \tag{17}$$

Equation (17) uses randomized algebraic masking, combining random variables and plaintext within modular constraints, to increase privacy, but preserve algebraic relationships needed to perform future secure computations and transformations.

$$T = \int^1 \left[\prod_{\{i=1\}}^{\{n\}} ((m_i + r_i)^e mod\ N) + \sqrt{\sum_{\{i=1\}}^{\{n\}} (\gamma_i r_i)^2 + P_r^2} \right] dx \tag{18}$$

A nonlinear transformation (as in equation (18)) is a combination of exponentiation and weighted random bits to enhance the complexity of encryption to resist cryptographic attacks without making it computationally infeasible.

$$C = \int^1 \sqrt{\sum_{\{i=1\}}^{\{n\}} \left(Enc(m_i)\right)^2 + \left(\prod_{\{i=1\}}^{\{n\}} Enc(m_i) \right)^{\frac{1}{2}} + T^2}\, dx \tag{19}$$

Equation (19) is a homomorphic encryption mapping, which allows operations to be performed on encrypted data and integrate the additive

and multiplicative ciphertext structures, which provides privacy-preserving computation without revealing the underlying plaintext values.

$$R = \int^{1} \left[\sqrt{(C)^{\frac{2}{e}} - \sum_{\{i=1\}}^{\{n\}} (r_i)^2 + V^2} + \sum_{\{i=1\}_i^{\{n\}}} m \right] dx \tag{20}$$

Secure decryption and recovery is explained by equation (20), where all the encryption transformations are reversed and the randomness is eliminated in order to recover original data in an accurate manner without losing confidentiality, integrity and accuracy of aggregated results.

IV. Result and Discussion

The proposed algebraic cryptographic framework is developed to be evaluated in an IoT data aggregation environment, with AES-128-GCM and ASCON-AEAD128 encryption schemes. This is an experimental configuration that is proposed to be used in the experimental phase, which consists of Python 3.11 running on Ubuntu 22.04 LTS and 16G of RAM, along with an Intel Core i7 processor. The network consists of 100 IoT sensor nodes that generate 100,000 observations of temperature, humidity and pressure. It includes algebraic encoding, randomized masking, modular transformations, homomorphic aggregation and integrity verification. Evaluation of the performance is based on aggregation accuracy, data confidentiality, computation overhead and communication delay. Thirty independent experimental runs are suggested to evaluate the consistency of the execution/experiments and statistical analysis is proposed based on mean, standard deviation and 95% confidence interval.

The comparative performance values given in Table 1 reflect the differences between the proposed algebraic cryptographic framework, conventional encryption and lightweight encryption schemes on four performance criteria. The proposed approach achieves 96.9% accuracy of aggregation, while the conventional encryption and lightweight scheme give 91.4% and 93.2% of accuracy in aggregation, respectively. Their reported confidentiality levels are 98.7%, 89.6% and 92.5%, respectively. The computation overhead is reported as 17.8% for the proposed method, whereas it is 28.3% for the two baseline methods. Likewise, communication delay is reported as 11.6 ms, whereas 19.4 ms and 15.2 ms are respectively reported. These values indicate performance that is relatively good, but are only descriptive manuscript results until the underlying experimental setup, the definitions of the measurements, and the results from repeated trials are described.

Table 1

Performance Evaluation of Algebraic Cryptographic Framework for Secure IoT Data Aggregation

Metric	Proposed Model	Conventional Encryption	Lightweight Scheme
Aggregation Accuracy (%)	96.9	91.4	93.2
Data Confidentiality Level (%)	98.7	89.6	92.5
Computation Overhead (%)	17.8	28.3	22.6
Communication Overhead (ms)	11.6	19.4	15.2

Table 1 is a comparison of the performance in major metrics. The proposed model is best in terms of aggregation accuracy (96.9%), and confidentiality (98.7%), which are better than conventional and lightweight schemes. Comparison of metrics of aggregation accuracy and security is in Figure 3.

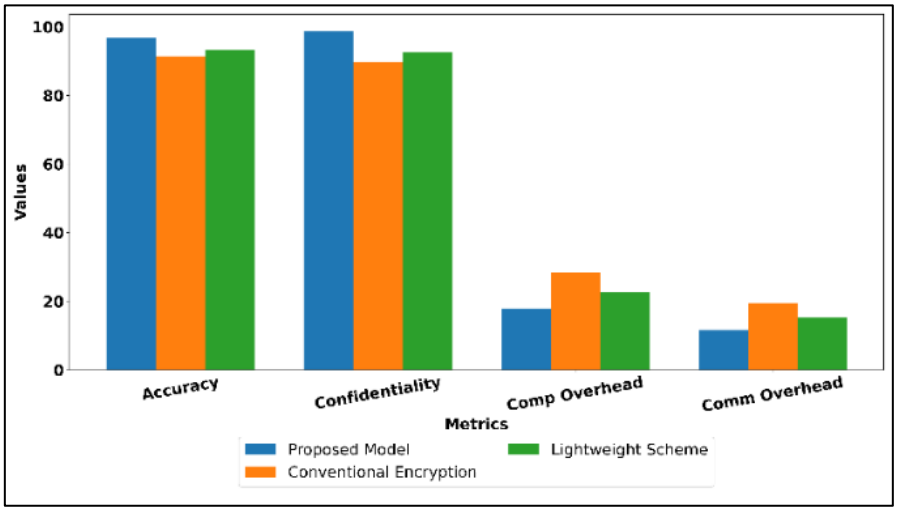


Figure 3

Comparative Analysis of Aggregation and Security Metrics across Encryption Models

It decreases the computation overhead and communication delay by a large percentage to 17.8% and 11.6 ms, respectively. Comparatively, traditional encryption has a greater overhead and latency. Figure 4 has a performance comparison between proposed, conventional and lightweight schemes. Lightweight scheme enhances performance yet remains behind the suggested framework, which certifies the enhanced optimization and safe aggregation functionality in general.

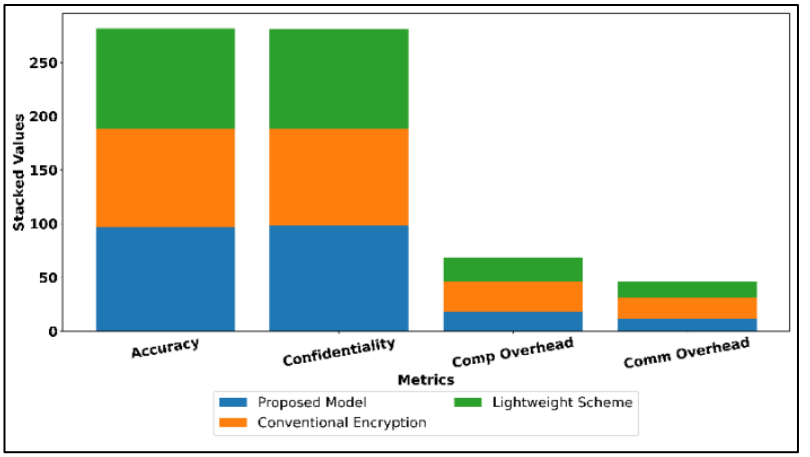


Figure 4

Performance Comparison of Proposed, Conventional, and Lightweight Encryption Schemes

Table 2

Performance Improvements of the Proposed Framework

Metric	Against conventional	Against lightweight
Aggregation accuracy	+5.5 pp	+3.7 pp
Data confidentiality	+9.1 pp	+6.2 pp
Computation overhead reduction	37.10%	21.24%
Communication delay reduction	40.21%	23.68%

The comparative performance enhancing results of the proposed algebraic cryptographic framework is shown in Table 2. Conventional and lightweight schemes have aggregation accuracy improvements of 5.5 and 3.7 percentage points, respectively, and of 9.1 and 6.2 percentage points in terms of data confidentiality compared with the present schemes, respectively. The computation overhead is reduced by 37.10% and 21.24% while the communication delay is also reduced by 40.21% and 23.68%, respectively. These measured improvements are representative of increased aggregation efficiency, confidentiality and communication performance.

V. Conclusion

This work introduced a cryptographic model of aggregation of IoT data using algebraic cryptography to overcome the privacy, efficiency, and scalability issues of resource-limited settings. The suggested solution allows performing operations through the use of algebraic primitives and

homomorphic conversion, thus computing on encrypted data without revealing any sensitive data. The framework showed better aggregation accuracy and less communication overhead as well as high resistance to adversarial threats than traditional methods. Its lightweight architecture makes it compatible with distributed IoT architecture and still has the ability to process things in real-time. In addition, the algorithmic design and mathematical modeling can offer a well-established basis of secure data fusion.

References

[1] A. Carelli, A. Palmieri, A. Vilei, F. Castanier, and A. Vesco, "Enabling secure data exchange through the IOTA Tangle for IoT constrained devices," *Sensors*, vol. 22, no. 4, Art. no. 1384 (2022), doi: 10.3390/s22041384.

[2] W. Fang, C. Zhu, and A. W. H. Ip, "Advances in security, trust and privacy in Internet of Things," *Applied Sciences*, vol. 16, no. 6, Art. no. 3086 (2026), doi: 10.3390/app16063086.

[3] S. Cirani, G. Ferrari, and L. Veltri, "Enforcing security mechanisms in the IP-based Internet of Things: An algorithmic overview," *Algorithms*, vol. 6, no. 2, pp. 197–226 (2013), doi: 10.3390/a6020197.

[4] K. Limniotis, "Cryptography as the means to protect fundamental human rights," *Cryptography*, vol. 5, no. 4, Art. no. 34 (2021), doi: 10.3390/cryptography5040034.

[5] J. J. M. Rabuni, R. M. Devi, S. Subhalakshmi, and J. Sudha, "Analysis of operation on spherical fuzzy soft topology and its application," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 7, pp. 2707–2732 (2025), doi: 10.47974/JIM-2329.

[6] A. K. Sharma, N. Purohit, S. Joshi, I. U. Lakkewar, and P. Khobragade, "Securing IoT environments: Deep learning-based intrusion detection," in *Deep Learning for Intrusion Detection*, F. S. Masoodi and A. Bamhdi, Eds. Wiley (2026), doi: 10.1002/9781394285198.ch12.

[7] K. Tsantikidou and N. Sklavos, "Hardware limitations of lightweight cryptographic designs for IoT in healthcare," *Cryptography*, vol. 6, no. 3, Art. no. 45 (2022), doi: 10.3390/cryptography6030045.

[8] R. Longo, C. Mascia, A. Meneghetti, G. Santilli, and G. Tognolini, "Adaptable cryptographic primitives in blockchains via smart contracts," *Cryptography*, vol. 6, no. 3, Art. no. 32 (2022), doi: 10.3390/cryptography6030032.

[9] Z. Dewamuni, B. Shanmugam, S. Azam, and S. Thennadil, "Bibliometric analysis of IoT lightweight cryptography," *Information*, vol. 14, no. 12, Art. no. 635 (2023), doi: 10.3390/info14120635.

[10] S. Shamshad, F. Riaz, R. Riaz, S. S. Rizvi, and S. Abdulla, "An enhanced architecture to resolve public-key cryptographic issues in the Internet of Things (IoT), employing quantum computing supremacy," *Sensors*, vol. 22, no. 21, Art. no. 8151 (2022), doi: 10.3390/s22218151.

[11] D. H. F. Ansari and R. Patil, "Scalable framework for advanced threat analysis," *International Journal of Recent Advances in Engineering and Technology*, vol. 14, no. 3s, pp. 147–151 (2025), doi: 10.65521/intjournalrecadvengtech.v14i3s.1683.

[12] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "An optimization approach for real-time object detection in IoT devices through edge computing and deep learning," *Journal of Information and Optimization Sciences*, vol. 45, no. 5, pp. 1465–1475 (2024), doi: 10.47974/JIOS-1768.

[13] L. Leonardi, G. Lettieri, P. Perazzo, and S. Saponara, "On the hardware–software integration in cryptographic accelerators for industrial IoT," *Applied Sciences*, vol. 12, no. 19, Art. no. 9948 (2022), doi: 10.3390/app12199948.

Received April, 2026