The Scientific Temper (2025) Vol. 16 (9): 4745-4761
E-ISSN: 2231-6396, ISSN: 0976-8653
Doi: 10.58414/SCIENTIFICTEMPER.2025.16.9.06
https://scientifictemper.com/

RESEARCH ARTICLE

Energy-aware Security Optimized Elliptic Curve Digital Signature Algorithm for Universal IoT Networks

R. Rita Jenifer*, V. Sinthu Janita

Abstract

Ensuring security, integrity, and energy efficiency in Internet of Things (IoT) networks is a critical challenge due to the resource constraints of IoT devices. Traditional digital signature algorithms such as RSA, ECDSA, and EdDSA provide security but often lack energy optimization, making them inefficient for large-scale IoT deployments. To address these challenges, this research proposes an Energy-aware Security Optimized Elliptic Curve Digital Signature Algorithm (EECDSA) for universal IoT networks. EECDSA enhances conventional ECDSA by integrating three novel functional modules: Lightweight Context Sensitivity Imposer (LCSI), Adaptive Computational Complexity Overseer (ACCO), and Energy-aware ECDSA Signer (EAES). These modules dynamically adjust security parameters based on contextual sensitivity, optimize computational complexity to balance security and resource consumption, and ensure energy-efficient digital signing in IoT environments. The proposed method is evaluated using OPNET simulations, measuring both security and network performance metrics, including Accuracy, Precision, Sensitivity, Specificity, F-Score, Throughput, Latency, Jitter, Energy Consumption, Packet Delivery Ratio, and Security Levels. Experimental results demonstrate that EECDSA outperforms existing security solutions, achieving higher security resilience (99.55%), reduced energy consumption (511.6mJ), and improved network performance. These findings validate EECDSA as an efficient and scalable security mechanism for IoT ecosystems.

Keywords: Digital Signature Algorithms, Energy-aware security, Network Security, Internet-of-Things.

Introduction

Digital signature algorithms use cryptographic techniques to generate a unique signature for a piece of data. This signature can be verified by the receiver to ensure that the data has not been tampered with and that it originates from a legitimate source (Lalem F, Laouid A, Kara M, Al-Khalidi M, Eleyan A.,2023). Many IoT devices have limited computational power, memory, and energy resources (S. R. Kawale, K. Prasad, D. Palanikkumar, P. A. Mary.,2023). Implementing digital signature algorithms that are both secure and resource-efficient is a significant challenge. IoT networks often consist of a large number of devices. The digital signature solutions need to be capable of scaling to manage a large number of devices and data exchanges (Hofheinz, D., Kiltz, E.,2022). Interoperability is essential, ensuring the DSA can function across diverse devices and platforms within the IoT ecosystem (Kim Y, Seo SC.,2022). Additionally, the algorithms must provide robust security features, including authentication, data integrity, and non-repudiation, to safeguard against unauthorized access and data tampering. Balancing these considerations is critical to developing effective and reliable digital signature solutions for IoT environments (Shabana Urooj, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz, S Kalathil.,2023).

Context sensitivity is one of the vital elements in IoT networks because it enables devices to make intelligent decisions based on their operating environment and the specific needs of the situation (Inshi S, Chowdhury R, Ould-Slimane H, Talhi C.,2023). IoT devices can optimize their performance, improve efficiency, and enhance user experiences by context acumen. For instance, A smart thermostat optimizes energy use and ensures comfort by adjusting the temperature according to room occupancy, the time of day, or the weather conditions. In industrial

Department of Computer Science, Cauvery College for Women (Autonomous) Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India.

***Corresponding Author:** R. Rita Jenifer, Department of Computer Science, Cauvery College for Women (Autonomous) Affiliated to Bharathidasan University, Tiruchirappalli, Tamil Nadu, India, E-Mail: rita.jenifer@gmail.com

How to cite this article: Jenifer, R.R., Janita, V.S. (2025). Energy-aware Security Optimized Elliptic Curve Digital Signature Algorithm for Universal IoT Networks. The Scientific Temper, **16**(9):4745-4761.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.9.06

Source of support: Nil

Conflict of interest: None.

Received: 06/09/2025 **Accepted:** 15/09/2025 **Published:** 23/09/2025

settings, context-aware sensors can detect anomalies in machinery and predict maintenance needs, preventing downtime and reducing costs (Picallo, I., Iturri, P.L., Celaya-Echarri, M. *et al*.,2023). In healthcare, wearable devices can monitor patient vitals and trigger alerts based on contextual data, such as activity levels or changes in health parameters (S. Das, S. Namasudra, S. Deb, P. M. Ger and R. G. Crespo.,2023).

Energy-awareness is crucial in IoT networks due to the widespread use of battery-powered devices and the need for long-term, sustainable operation. Many IoT devices operate in remote or inaccessible locations where frequent battery replacement is impractical and costly. Optimizing energy consumption extends device lifespan, reduces maintenance costs, and enhances the reliability of the network (Adnan Sabovic, Michiel Aernouts, Dragan Subotic, Jaron Fontaine, Eli De Poorter, Jeroen Famaey.,2023). Additionally, energy-efficient devices contribute to environmental sustainability by minimizing power usage and the associated carbon footprint (Almalki, F.A., Alsamhi, S.H., Sahal, R. *et al*.,2023). In scenarios with large-scale IoT deployments, energy awareness ensures that devices can perform their tasks effectively without draining power resources, thereby maintaining consistent performance and connectivity (R. Samadi, A. Nazari and J. Seitz.,2023). Balancing energy efficiency with security and functionality is crucial for optimizing IoT networks, ensuring their reliability and sustainability Energy efficiency ensures prolonged device operation while minimizing maintenance, but it can conflict with the need for robust security. At the same time, maintaining functionality is key to ensuring the network performs its tasks without delays or failures (Jabeen, A., & Shanavas, A. R. M. (2025). This work aims to address these challenges by finding solutions that balance these three elements, ensuring IoT networks are secure, efficient, and reliable.

The main Contribution of this research as follows,

- Proposes an EECDSA to enhance security and energy efficiency in IoT networks.
- Implements a context-aware mechanism LCSI to classify data sensitivity dynamically, optimizing security overhead based on real-time contextual factors.
- Introducing ACCO which adjusts cryptographic security parameters based on node processing capacity and memory availability, ensuring optimal performance.
- Integrating energy-aware signing strategies EAES to extend battery life and reduce computational overhead in IoT devices

Structure of Manuscript

The manuscript begins with an Introduction in section 1, highlighting the need for energy-efficient IoT security solutions. Section 2 reviews the existing method for recent digital signature and intrusion detection techniques, identifying their limitations. Section 3 explains the background of ECDSA's cryptographic foundations, leading to the Proposed Method. Section 4 explains the proposed methodology, Section 5 and 6 explains the experimental setup and results analysis. Finally Section 7 summarizes the conclusion.

Existing Methods

Various attempts have been previously made to achieve a balance between security and energy efficiency in heterogeneous IoT networks. This section examines some of the most relevant existing approaches to gain insights into their methodologies, implementation strategies, benefits, and limitations. The selected methods include IIDS-SIoEL: an intrusion detection framework for enhancing security in IoT-based smart environments using ensemble learning (Hazman, C., Guezzaz, A., Benkirane, S. *et al*.,2023), VBQ-Net: a novel vectorization-based boost quantized network model aimed at maximizing IoT system security to prevent intrusions (Perumal G, Subburayalu G, Abbas Q, Naqi SM, Qureshi I.,2023), a hybrid CNN+LSTM-based intrusion detection system designed for industrial IoT networks (Hakan Can Altunay, Zafer Albayrak.,2023), a highly secure intrusion detection system for IoT utilizing EXPSO-STFA feature selection with LAANN for attack detection (Jeyaselvi, M., Dhanaraj, R.K., Sathya, M. *et al*.,2023), and an attack-specific security-optimized RSA model for IoT (Jenifer RR, Prakash VS.,2024).

IIDS-SIoEL: Intrusion detection framework for IoT-based smart environments security using ensemble learning

IIDS-SIoEL work is proposed by Chaimae Hazman et.al (Hazman, C., Guezzaz, A., Benkirane, S. *et al*.,2023) to offer improved security for smart city IoT nodes those have mobility It is common that the nodes with higher mobility are more vulnerable to intruder attacks due to frequent position and cluster migrations. IIDS-SIoEL work is indented to overcome these intruder attacks. IIDS-SIoEL work is prepared based on the inspiration of applicable improvements in intruder detection system by incorporation of Machine learning and Deep learning concepts. In general, the IIDS-SIoEL framework functions based on an optimal anomaly detection model that utilizes AdaBoost, incorporating various feature selection techniques such as Boruta, mutual information, and correlation. The proposed model was tested on the IoT-23, BoT-IoT, and Edge-IIoT datasets using a GPU. Important intruder detection parameters such as Accuracy, Precision, Recall and F-Score are computed for the compared methods, in which IIDS-SIoEL secures better scores.

Improvement in accuracy and precision parameters is the main advantage of IIDS-SIoEL method whereas. The experiments carried out in a Kaggle cloud server-

based environment with a huge memory. This much of computational complexity negatively impacts the network performance metrics such as Throughput and Packet Delivery Ratio. Decayed performance is observed as the limitation of IIDS-SIoEL work.

VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions

In 2023, Perumal et.al. (Perumal G, Subburayalu G, Abbas Q, Naqi SM, Qureshi I.,2023) proposed VBQ-Net methodology to provide data security in a IoT network environment. In VBQ-Net dissertation, a Vector Space Bag of Words (VSBW) method is employed to lower the feature dimensionality and pinpoint key characteristics within the data. In addition, a novel classification technique named Boosted Variance Quantization Neural Networks (BVQNNs) is utilized to categorize various types of intrusions using a weighted feature matrix. During the classification process, a Multi-Hunting Reptile Search Optimization (MH-RSO) algorithm is applied to determine the probability values for making optimal choices in intrusion prediction. VBQNM method is evaluated using comprehensive experiments with real-world IoT datasets and simulated intrusion scenarios. Benchmark parameters such as Accuracy, Precision, Sensitivity, Specificity, F-Score, and Detection rate are measured during the evaluation process.

Improved accuracy and efficiency, and lower memory usage are the stated advantage of VBQ-Net method. Missing real-time optimizations may cause performance issues in heterogeneous IoT network environments – which is stated as the limitation of VBQ-Net method.

A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks (CLIDS)

Haka n Can Altunay et.al. (Hakan Can Altunay, Zafer Albayrak.,2023) proposed CLIDS work in 2022 for providing security in Industrial Internet-of-Things (IIoT) network environments. Three different models were proposed in CLIDS work for detecting intrusions in the IIoT network using deep learning architectures: Convolutional Neural Network (CNN), Long Short-Term Memory (LSTM), and a hybrid combination of CNN and LSTM. Performance evaluations are performed using UNSW-NB15 and X-IIoTID datasets to identify and compare normal and abnormal data. Both binary and multi-class classification are carried out in the evaluation process. There is no IoT network simulator or emulator used in the evaluation process. The dataset records are bluntly processed through mathematical model without any real-time intruder attacks.

High accuracy is the declared advantage of CLIDS method. Missing evaluation with a simulator or with other real-time tools is one of the limitations of CLIDS work, Stacking up CNN and LSTM to each other increase the computational overhead that impacts negatively in network performance parameters such as Throughput and Packet Delivery Rate is another identified limitation of CLIDS work.

A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks (LAANN)

LAANN work is introduced in 2022 by Jeyaselvi et.al (Jeyaselvi, M., Dhanaraj, R.K., Sathya, M. *et al*.,2023) as an attempt to achieve a new efficient intrusion detection system for IoT Network environments. As the first phase, the data underwent pre-processing to gain a clear understanding of potential attacks. This involved handling eliminates missing and NaN values. To gain insights into the data, an Improved Pearson Correlation Coefficient (IPCC) and Feature Extraction (FE) method was established, presenting the relationships within the data by considering causative factors. As the subsequent phase, feature extraction is performed to identify relevant features to ensure efficient computational time and accuracy using the Explorated Particle Swarm Optimization (PSO) centered Sea Turtle Foraging Algorithm (EXPSO-STFA). Finally, the selected features were trained and evaluated using the Look Ahead Artificial Neural Network (LAANN) classification to identify attacks. The LAANN method achieves a lower error rate, minimizes the chances of false alarm rates (FAR), and effectively and reliably detects attacks. All intrusion detection performance metrics such as accuracy, and precision are measured by the conducted experiments.

Attainment of higher accuracy and attack detection average are the advantages of LAANN work. Ensemble of multiple optimization algorithms causes higher computational overhead which leads to higher processing time. The high processing time naturally reduces the overall throughput of the IoT network – which is discovered as the limitation of LAANN work.

Rivest-Shamir-Adleman algorithm optimized to protect iot devices from specific attacks. Informatics and Automation

In 2024, Jennifer et.al. (Jenifer RR, Prakash VS.,2024) presented ASORI work to provide improved security for heterogeneous IoT network environments. ASORI work integrates three key contributions to enhance security in IoT network environments. The novel modules introduced are the Fast-Fuzzy Anomaly Detector, Legacy Naïve Bayes Attack Classifiers, and Variable RSA Security Schemer, collectively referred to as ASORI. The work also introduces innovative features such as the onboard IoT certification mechanism and dynamic security strategy selection. The ASORI model has been evaluated using the industry-standard network simulator OPNET to ensure improved security and enhanced performance of critical network parameters. Both intrusion

detection performance metrics such as Accuracy, Precision, Sensitivity, Specificity, and F-Score are measured along with network performance benchmark metrics such as Throughput, Latency, Jitter, Energy consumption, Packet Delivery Ratio, and overall security level are measured for compared methods at different timestamps.

Accomplishment of higher accuracy, precision, F-Score, throughput, packet delivery ratio with minimized communication delays such as jitter and latency are the witnessed advantage of ASORI method. Utilization of RSA as one of the functional elements is comparatively consumes higher computational resources with respect to a security threshold level. This high computational resource occupancy is the asserted limitation of ASORI.

A summary about used methodologies, their advantages and limitations of discussed methods are enumerated in Table 1.

Background

A succinct introduction about Elliptic Curve Digital Signature Algorithm (ECDSA) is required to explain the proposed EECDSA functional blocks at ease, provided in this section. ECDSA is one of the best cryptographic algorithms used for digital signatures, providing the same level of security as traditional algorithms like RSA but with shorter key lengths (G. Dimitoglou and C. Jim.,2023). It leverages the mathematical properties of elliptic curves over finite fields, resulting in more efficient computations and reduced storage requirements. ECDSA is widely adopted in various security protocols, including SSL/TLS for secure web browsing, and is a key component in blockchain technologies like Bitcoin, where it ensures the integrity and authenticity of transactions. These properties are the motivation behind incorporating the basic elements of ECDSA with the proposed EECDA operational units.

ECDSA operates by generating a pair of keys: a private key for signing data and a public key for verifying signatures. The private key, kept confidential by the signer, creates a unique signature for each message, while the public key, shared openly, allows anyone to verify the authenticity of the signature. The strength of ECDSA lies in the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) (Cheddour Z, Chillali A, Mouhib A.,2023), making it computationally infeasible to derive the private key from the public key. This robustness, combined with its efficiency, makes ECDSA an ideal choice for modern cryptographic applications where security and performance are paramount. While ECDSA is widely recognized for its security and efficiency, challenges remain in optimizing its performance, especially in resource-constrained environments like IoT networks. Current implementations of ECDSA can be computationally intensive and may not be suitable for devices with limited processing power and energy resources. Additionally, the key management and scalability aspects of ECDSA require further exploration to ensure its effectiveness in large-scale, dynamic IoT networks while maintaining a balance between security and energy efficiency.

Proposed Method

In the EECDSA work, three advanced functional modules are introduced, including the Lightweight Context Sensitivity Imposer (LCSI), the Adaptive Computational Complexity Overseer (ACCO), and the Energy-aware ECDSA Signer (EAES). These modules are designed to enhance both energy efficiency and security within a general IoT network environment. A conclusive disclosure about the

Table 1: Summarization of existing methods outline

Author	*Work*	*Methodology*	*Advantages*	*Limitations*
Hazmant et.al. (Hazman, C., Guezzaz, A., Benkirane, S. *et al*.,2023)	IIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning	Adaboost optimized anomaly detection	Higher Accuracy, Precision	Higher computational overhead
Perumal et.al. (Perumal G, Subburayalu G, Abbas Q, Naqi SM, Qureshi I.,2023)	VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions	Multi-Hunting Reptile Search Optimization	Improved Accuracy, Precision	Undermine heterogeneous network support
Altunay et.al. (Hakan Can Altunay, Zafer Albayrak.,2023)	A hybrid CNN+ LSTM-based intrusion detection system for industrial IoT networks (CLIDS)	Convolutional Neural Network and Long Short-Term Memory	Better attack detection accuracy	Lower Throughput and PDR
Jeyaselvi, M et.al (Jeyaselvi, M., Dhanaraj, R.K., Sathya, M. *et al*.,2023)	A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks	Improved Pearson Correlation Coefficient, PSO + Sea Turtle Foraging Algorithm	Higher attack detection accuracy	Higher processing time
Jennifer et.al (Jenifer RR, Prakash VS.,2024)	Attack specific Security Optimized RSA for IoT	RSA, Fast Fuzzy Anomaly detection, Legacy Naïve Bayes Classifier	Higher attack detection Accuracy, Precision, and Throughput	High computational resource occupancy

methodologies used in the modules and their purposes are articulated in this section.

Lightweight Context Sensitivity Imposer (LCSI)

The primary aimpoint of the LCSI is to adapt the operation of IoT devices based on the specific context or environment they are operating in. This includes factors like the device's current activity, network conditions, or environmental changes. By being context-sensitive, the LCSI aims to optimize both performance and security without adding significant overhead to the system. Contextual information helps to the subsequent modules to make more informed decisions about how to handle various tasks or security measures.

A domain specific Context Sensitivity Correlation Table (CSCT) is prepared using domain specific context lexicon and the sensitivity label assigned by the field experts. The structure of CSCT is very similar to a common lookup table, with two fields. The first one is the lexeme and the second one is its sensitivity label. CSCT is designed to handle 3 different sensitivity labels such as Low, Medium, and High. The low sensitive category are data that has less privacy concern. Medium sensitive category consists data with a little privacy data, but will not cause any significant harm if uncovered. High sensitive label is assigned to the data that are very delicate with highest privacy risks. Two sample CSCT those associated with electronic health record and industry 4.0 are given in Table 2.

Table 2: Sample CSCTs

Electronic Health Records		*Industry 4.0*	
Lexeme	*Sensitivity*	*Lexeme*	*Sensitivity*
Step count	Low	Machine uptime	Low
Calories burn	Low	Energy consumption	Low
Non-critical activity log	Low	Product count	Low
.	.	.	.
.	.	.	.
.	.	.	.
Heart rate	Medium	Machine performance metrics	Medium
Blood pressure	Medium	Process optimization data	Medium
Medication adherence	Medium	Batch traceability	Medium
.	.	.	.
.	.	.	.
.	.	.	.
Full ehrs	High	Proprietary manufacturing processes	High
Genetic data	High	Production bottlenecks	High
Real-time location	High	Trade secrets	High

Targeted to be lightweight, LCSI ensures minimal impact on the resource-constrained devices typical in IoT networks. This means that the module is optimized to use minimal computational power, memory, and energy, making it suitable for devices with limited capabilities. Thus, the memory occupation of LCSI is limited to 2-bits as in Table 3. This 2-bit sensitivity header will be added to the standard IoT data packet.

The scope of the sensitivity label header starts from the source sensor node to destination including all relay nodes. LCSI sensitivity header is just like a fragile postage stamp used to indicate that the mail or package is delicate and should be handled with care.

Adaptive Computational Complexity Overseer (ACCO)

ECDSA has three major operations namely, Key generation, Signing process, and verification process. The key generation phase has three important tasks such as Elliptic curve parameter definition, Private key generation, and public key calculation. The signing process includes the subtasks namely Message hashing, Random integer key selection, Elliptic curve point calculation for selected random key, the x-coordinate computation, the signature verification element computation, and Signature computation. The verification process has the following tasks listed as Verification of r and s, Message Hash, Calculation of , calculation of u_1, u_2, Point X calculation, and signature verification. The important variables involved in ECDSA are : the prime number, and : the curve coordinates, : the basepoint, Order , and Field size .

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic technique used to ensure data integrity and authentication in secure communications by generating and verifying digital signatures. It leverages elliptic curve cryptography to provide strong security with smaller key sizes, making it efficient for resource-constrained environments like IoT networks.

Selection of optimum security standard based on the data sensitivity label and current computation resource availability of the nodes is the core responsibility of ACCO Module. Secp192r1, secp256r1, secp384r1, and Secp512r1 are the acquired security standards in ACCO module to apply with ECDSA. Secp192r1, also known as P-192r1 or prime192v1, is an elliptic curve defined over a prime field. It is part of the

Table 3: Sensitivity label bits

Sensitivity Label	*Bit 1*	*Bit 0*
N/A	0	0
Low	0	1
Medium	1	0
High	1	1

set of elliptic curves recommended by the National Institute of Standards and Technology (NIST) for use in cryptographic applications, particularly for digital signatures, public key encryption, and key exchange protocols. Secp192r1 consumes relatively less energy than the higher standards and provide a decent security. Higher subsequent security standards can provide higher security and also consumes coextensive energy proportions.

Let be the sensitivity label with either Low/Medium/ High value assigned by LCSI module. Let and are the nodes involved in communication. Let p_n^{max} be the maximum provided processing power of node , and p_n^{max} be the maximum provided processing power of node . Similarly Let $m_{n_{max}}^{max}$ be the maximum provided memory for node , and m_n^{max} be the maximum provided memory for node onboard. In equivalent fashion, Let p_n^{con}, p_n^{con}, m_n^{con}, and m_n^{con} be the consumed processing power of , consumed processing power of node , consumed memory of node , and consumed memory of node in appropriate sequence.

Let ̂ be the available processing power, and ̂ be the available memory of node . Similarly let ̂ be the available processing power, and ̂ be the available memory of node . The available processing power and memory are computed using the following equations.

$$\hat{p}_{n_x} = p_{n_x}^{max} - p_{n_x}^{con} \quad (1)$$

$$\hat{p}_{n_y} = p_{n_y}^{max} - p_{n_y}^{con} \quad (2)$$

$$\hat{m}_{n_x} = m_{n_x}^{max} - m_{n_x}^{con} \quad (3)$$

$$\hat{m}_{n_y} = m_{n_y}^{max} - m_{n_y}^{con} \quad (4)$$

Since nodes and can me heterogeneous, there may be a difference between the availability of the computational resources. Therefore, in ACCO module, a percentage-based normalization among the computational resources is computed to balance the resources of different nodes. Let $\overline{p}_{n_x}$ be the normalized available processing power for node computed by the below equation.

$$\overline{p}_{n_x} = \frac{\left(\hat{p}_{n_x} + \hat{p}_{n_y}\right) - \frac{1}{2}\left(\left(\hat{p}_{n_x} + \hat{p}_{n_y}\right) - \left|\hat{p}_{n_x} - \hat{p}_{n_y}\right|\right)}{100} \times \hat{p}_{n_x} \quad (5)$$

Similarly, the normalized available processing power $\overline{p}_{n_y}$ of node is calculated by Equation 6.

$$\overline{p}_{n_y} = \frac{\left(\hat{p}_{n_x} + \hat{p}_{n_y}\right) - \frac{1}{2}\left(\left(\hat{p}_{n_x} + \hat{p}_{n_y}\right) - \left|\hat{p}_{n_x} - \hat{p}_{n_y}\right|\right)}{100} \times \hat{p}_{n_y} \quad (6)$$

Correspondingly the normalized available memory values for nodes and are computed using equations 7 and 8 respectively.

$$\overline{m}_{n_x} = \frac{\left(\hat{m}_{n_x} + \hat{m}_{n_y}\right) - \frac{1}{2}\left(\left(\hat{m}_{n_x} + \hat{m}_{n_y}\right) - \left|\hat{m}_{n_x} - \hat{m}_{n_y}\right|\right)}{100} \times \hat{m}_{n_x} \quad (7)$$

$$\overline{m}_{n_y} = \frac{\left(\hat{m}_{n_x} + \hat{m}_{n_y}\right) - \frac{1}{2}\left(\left(\hat{m}_{n_x} + \hat{m}_{n_y}\right) - \left|\hat{m}_{n_x} - \hat{m}_{n_y}\right|\right)}{100} \times \hat{m}_{n_y} \quad (8)$$

The maximum resource scalar $\hat{\Gamma}_{n_{xy}}$ for nodes and is computed as follows

$$\hat{\Gamma}_{n_{xy}} = \frac{1}{2} \times \left(\frac{\left(\hat{p}_{n_x} + \hat{p}_{n_y}\right)}{2} + \frac{\left(\hat{m}_{n_x} + \hat{m}_{n_y}\right)}{2} \right) \quad (9)$$

The available resource scalar $\Gamma_{n_{xy}}$ for the nodes and is computed as follows

$$\Gamma_{n_{xy}} = \frac{1}{2} \times \left(\frac{\left(\overline{p}_{n_x} + \overline{p}_{n_y}\right)}{2} + \frac{\left(\overline{m}_{n_x} + \overline{m}_{n_y}\right)}{2} \right) \quad (10)$$

ACCO module determines the optimum security standard based on the sensitivity label and computational resource availability by means of following algorithm.

Algorithm 1: ACCO Security Scheme Selection

Input: Sensitivity Label , Resource scalars $\hat{\Gamma}_{n_{xy}}$ and $\Gamma_{n_{xy}}$
Output: Security standard
Step 1: Fetch
Step 2: Obtain $\hat{\Gamma}_{n_{xy}}$ and $\Gamma_{n_{xy}}$
Step 3: If $\delta = Low$, then = Secp192r1
Step 4: else if $\delta = Medium$
Step 5:

$$\Omega = \begin{cases} Secp256r1 if\ \Gamma_{n_{xy}} \le \frac{1}{3}\hat{\Gamma}_{n_{xy}} \\ Secp384r1 if\ \frac{1}{3}\hat{\Gamma}_{n_{xy}} < \Gamma_{n_{xy}} \le \frac{2}{3}\hat{\Gamma}_{n_{xy}} \\ Secp512r1 otherwise \end{cases}$$

Step 6: else

Step 7: $\Omega = \begin{cases} Secp384r1 if = \Gamma_{n_{xy}} < \frac{1}{2}\hat{\Gamma}_{n_{xy}} \\ Secp512r1 otherwise \end{cases}$

Step 8: end if //
Step 9: return

Energy-aware ECDSA Signer (EAES)

Most of the IoT nodes are battery operated devices. Most of batteries used in IoT devices are powered between 1.8V to 5V operational voltage range, and 100 mAh to several thousand mAh based on the requirement. Any battery that is less than 20% is considered as Low battery. If the remaining battery is less than 10% is considered as the Critical Battery Level.

The electrical power of the batteries can be converted to Joule energy units using the following formula.

$$Energy(J) = \frac{Capacity(mAh) \times Voltage(V) \times 3600(seconds\ in\ an\ Hour)}{1000}$$

Let ε_n^{max} be the energy at full capacity of the battery belongs to Node . Likewise, ε_n^{max} be the energy at full capacity of node . Let ε_n^{rem} and ε_n^{rem} be the remaining energy available in Node and in Node . The power scalar $\overline{\varepsilon}_{n_{xy}}$ is calculated by equation 11.

$$\overline{\varepsilon}_{n_{xy}} = \frac{\varepsilon_{n_x}^{rem} + \varepsilon_{n_y}^{rem}}{2} \tag{11}$$

The battery state $\beta_{n_{xy}}$ is determined as in equation 12

$$\beta_{n_{xy}} = \begin{cases} Critical\ if\ \overline{\varepsilon}_{n_{xy}} \le \frac{1}{10}\left(\frac{\varepsilon_{n_x}^{max} + \varepsilon_{n_y}^{max}}{2}\right) \\ Low\ if\ \frac{1}{10}\left(\frac{\varepsilon_{n_x}^{max} + \varepsilon_{n_y}^{max}}{2}\right) < \overline{\varepsilon}_{n_{xy}} \le \frac{1}{5}\left(\frac{\varepsilon_{n_x}^{max} + \varepsilon_{n_y}^{max}}{2}\right) \\ Normal\ otherwise \end{cases} \tag{12}$$

The following algorithm of EAES is used to sign the data packets with energy consciousness.

Algorithm 2: Energy-aware Signer

Input: Input data packet, Security schema , Battery state $\beta_{n_{xy}}$

Output: Signed data packet

Step 1: Read incoming data packet

Step 2: Extract security bits, and determine

Step 3: Read Security Schema from ACCO

Step 4: Let $\overline{\Delta}$ be the signing procedure

Step 5: If $\beta_{n_{xy}} = Critical$

Step 6: $\overline{\Delta} = \begin{cases} Secp256r1 if\ \Omega = Secp512r1 \\ Secp192r1 if\ \Omega = Secp384r1 \end{cases}$

Step 7: else If $\beta_{n_{xy}} = Low$

Step 8: $\overline{\Delta} = \begin{cases} Secp384r1 if\ \Omega = Secp512r1 \\ Secp256r1 if\ \Omega = Secp384r1 \\ Secp192r1 if\ \Omega = Secp256r1 \end{cases}$

Step 9: else assign $\overline{\Delta} = \Omega$

Step 10: end if // $\beta_{n_{xy}}$

Step 11: Sign input data packet using $\overline{\Delta}$

Step 12: return signed packet

These proposed functional modules optimize the energy efficiency of IoT network along with ameliorated security levels by selecting appropriate security scheme based on the dynamic network environment.

Experimental Setup

A computer equipped with an i7-8250U processor (with a 6MB Cache), 16GB of DDR4 RAM, and 1TB of SSD storage was used for developing and evaluating the discussed procedures. The implementation solution was created using Visual Studio IDE (https://visualstudio.microsoft.com/vs/), and the methodologies of EECDSA were coded in the C++ 20.0 programming language (https://www.geeksforgeeks.org/features-of-c-20/) OPNET (Sridevi, R., & Prakash, V. S. J. 2024), known as "Optimized Network Engineering Tool," is a popular software suite for network simulation, modeling, and performance analysis. This software allows engineers, researchers, and network professionals to simulate and analyze various aspects of computer networks, telecommunications systems, and other communication technologies. OPNET offers features such as network modeling, simulation, performance analysis, protocol evaluation, and resource monitoring/management. It enables testing of various network scenarios without the need for physical implementation, helping users identify potential issues before deployment. Users can analyze resource utilization, identify bottlenecks, and develop optimization strategies within the network. Additionally, OPNET is used in academia to teach networking concepts and provide hands-on experience with network simulation. OPNET simulations are primarily designed to assess and analyze the performance and behavior of networks and protocols within a controlled, predefined environment. As a result, the use of a dataset is not required for many simulation scenarios, as the focus is on evaluating network performance and protocol behavior under various configurations.

Results and Analysis

During the evaluation process, two distinct categories of results are obtained. The first category includes network intrusion detection parameters, such as Accuracy, Precision, Sensitivity, Specificity, and F-Score. The second category encompasses network performance metrics, including Throughput, Latency, Jitter, End-to-End Delay, Packet Delivery Ratio, Power Consumption, and Security. Measurements are taken over a period of 1 real-world hour, with readings logged every 6 minutes. Consequently, there are 10 different timestamps used to record the parameters throughout the evaluation.

6.1. Accuracy

Network anomaly detection accuracy is crucial for ensuring network stability. Given that anomalies can signify intruder attacks, the anomaly detection process plays a key role in network security. This accuracy is determined using True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) values. The formula for calculating accuracy is $\frac{TP+TN}{TP+TN+FP+FN}$.

The evaluation results show that the highest accuracy 99.31% is achieved by proposed EECDSA work. The accuracy average of EECDSA is 99.17% which is 0.19% higher than the nearest performing method ASORI. The performance rank sequence based on Accuracy average is EECDSA, ASORI, LAANN, CLIDS, VBQ-Net, and IIDS-SIoEL listed from the best in order. A comparison graph for Accuracy during is given in Figure 1.

Table 4: Accuracy

Accuracy (%)						
Time stamp	*IIDS-SIoEL*	*VBQ – Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	95.010002	94.940002	97.089996	98.540001	98.919998	99.290001
2	94.974998	94.904999	97.165001	98.544998	98.945	99.045006
3	95.010002	94.809998	97.239998	98.604996	99.160004	99.315002
4	95.035004	94.949997	97.339996	98.769997	98.889999	99.235001
5	94.830002	95.074997	97.330002	98.5	99.145004	99.169998
6	94.994995	95.07	97.105003	98.470001	98.93	99.190002
7	95.005005	95.199997	97.089996	98.720001	99.055	99.080002
8	94.904999	95.199997	97.295006	98.525002	99.004997	99.135002
9	94.915001	95.065002	97.284996	98.489998	98.889999	99.214996
10	94.970001	95.019997	97.18	98.5	98.945007	99.104996

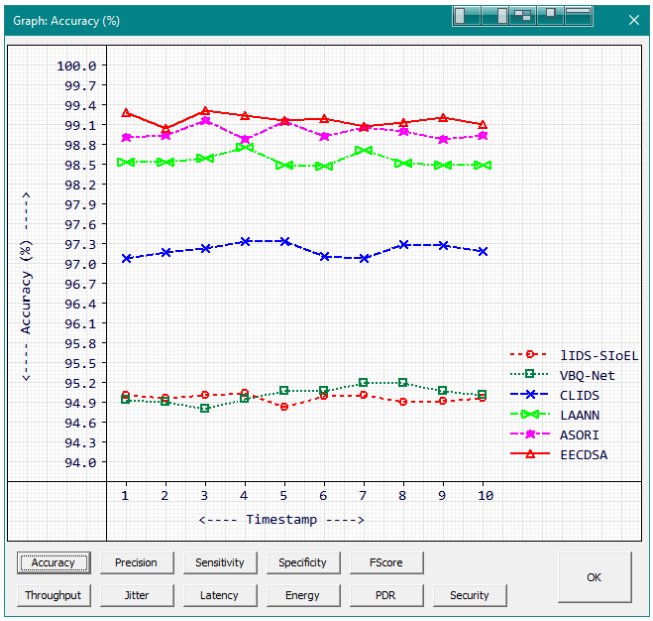

Figure 1: Accuracy (%)

Precision

Precision is a metric that assesses how accurately a model identifies positive instances. It is commonly applied in binary classification tasks, where the objective is to categorize instances into two groups namely Positive and Negative. $\frac{TP}{TP+FP}$ is the norm to calculate precision.

The highest precision achieved in the entire simulation process is 98.98% which is secured by proposed EECDSA method. The order of performance ranking in terms of precision average is EECDSA, ASORI, LAANN, CLIDS, IIDS-SIoEL, and VBQ-Net with the scores 98.73%, 98.35%, 98.13%, 97.25%, 95.35%, and 94.33% respectively listed from the best. The performance improvement of EECDSA is apparent in terms of precision. A precision graph is plotted with the observed readings which is given in Figure 2. The EECDSA method achieves superior precision and overall performance by integrating three key functional modules—LCSI, ACCO, and EAES, which work synergistically to optimize security and resource utilization. Unlike existing methods such as ASORI and VBQ-Net, which rely on static cryptographic operations, EECDSA dynamically adjusts its computational complexity through ACCO, ensuring that security enforcement is tailored to the available resources of IoT nodes. Additionally, LCSI enhances security adaptability by classifying data sensitivity in real time, reducing unnecessary computational overhead. The EAES module further improves efficiency by optimizing the signing process based on the device's battery level, minimizing power consumption while maintaining signature integrity. These adaptive mechanisms collectively enhance precision by reducing false positives and false negatives, leading to more accurate attack detection and response, outperforming than existing methods.

Sensitivity

Sensitivity is a metric used to assess the performance of a classification model, especially in binary classification tasks. It indicates how well the model correctly identifies positive cases out of all the actual positive cases. Sensitivity is crucial for identifying actual threats, minimizing missed detections, enhancing reaction speed, meeting regulatory requirements, and sustaining a strong security framework. Sensitivity, also known as recall, hit rate, or true positive rate, is calculated with the formula $\frac{TP}{TP+FN}$.

The computed sensitivity score of the compared methods during 10 different timestamps are recorded in Table 6.

The sensitivity ranking progression of the compared methods is EECDSA, ASORI, LAANN, CLIDS, VBQ-Net, and IIDS-SIoEL with the sensitivity averages 99.63%, 99.62%,

Table 5: Precision (%)

	Precision (%)					
Time stamp	*IIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	95.379997	94.349998	97.169998	98.050003	98.360001	98.900002
2	95.419998	94.080002	97.129997	98.07	98.260002	98.480003
3	95.470001	94.089996	97.199997	98.220001	98.529999	98.980003
4	95.300003	94.150002	97.309998	98.489998	98.349998	98.949997
5	95	94.400002	97.580002	97.980003	98.529999	98.699997
6	95.43	94.330002	97.050003	97.970001	98.330002	98.809998
7	95.550003	94.529999	97.059998	98.360001	98.349998	98.589996
8	95.18	94.559998	97.540001	98.129997	98.519997	98.690002
9	95.260002	94.330002	97.209999	98.059998	98	98.720001
10	95.510002	94.519997	97.230003	97.940002	98.230003	98.459999

98.99%, 97.18%, 95.65%, and 94.6215736 respectively. The highest sensitivity score 99.75% which is achieved by proposed EECDSA method during the experiments at 10th timestamp. The Sensitivity graph is provided in Figure 3.

Specificity

Specificity is a key metric for assessing the performance of a binary classification model, especially when correctly identifying negative instances is essential. It gauges the model's ability to accurately recognize negative cases out of all actual negative cases. Specificity is calculated using the formula $\frac{TN}{TN+FP}$. The measured specificity values for both the proposed and existing methods are presented in Table 7. A comparison graph for discussed method with respect to specificity score is made available in Figure 4.

The order of performance rankings based on specificity score average is EECDSA, ASORI, LAANN, CLIDS, and IIDS-SIoEL with the values 98.74%, 98.37%, 98.14%, 97.25%, 95.31%, and 94.41%. The highest sensitivity score 98.98% is achieved by EECSDA method during the 3rd timestamp. The experimental results show that the EECDSA method is thriving better in the sensitivity category.

F-Score

The F-score, or F1-score, is a metric used in classification tasks to evaluate a model's performance, especially in cases of class imbalance. It combines precision and recall into one value, offering a balanced measure of the model's accuracy. In IoT security, high precision means that the detected threats are indeed real threats (minimizing false alarms), while high recall means that most threats are successfully identified (minimizing missed threats). The F-score merges these two metrics, providing a balanced assessment.

By focusing on the balance between precision and recall, the F-score encourages the development of models that are not only accurate but also robust in detecting threats, leading to more effective and reliable IoT network security solutions.

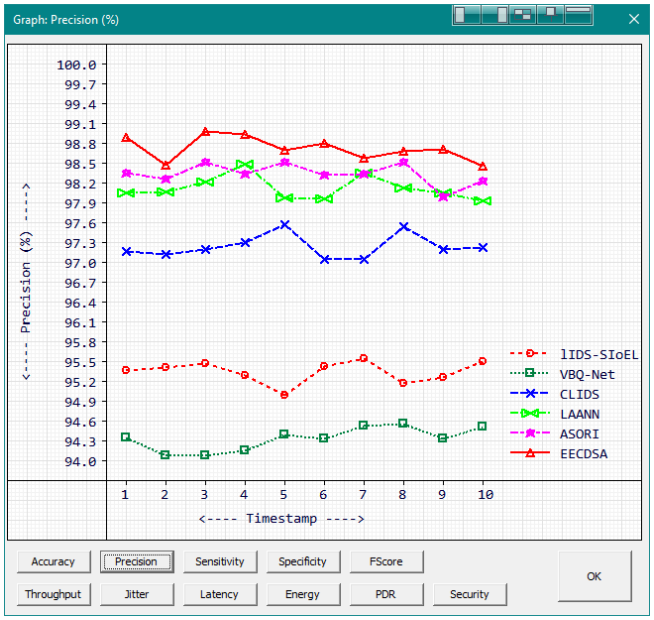

Figure 2: Precision (%)

The F-score is calculated using the formula $2\times\frac{Precision\times Sensitivity}{Precision+Sensitivity}$. The F-score values for the methods compared are presented in Table 8.

The EECDSA method achieves the highest F-Score of 0.9931 at the 3rd timestamp. The performance of the evaluated methods is ranked as follows: EECDSA (0.9917422), ASORI (0.9898193), LAANN (0.9856011), CLIDS (0.9721296), VBQ-Net (0.9498892), and IIDS-SIoEL (0.9498428). It is observed that the existing methods, IIDS-SIoEL and VBQ-Net, show close competition, with only a minor difference in their F-Scores. The EECDSA method, achieving the top F-Score of 0.9931, demonstrates its effectiveness in maintaining a balance between Sensitivity and Specificity. The EECDSA method introduces a novel approach to IoT

Table 6: Sensitivity (%)

Sensitivity (%)						
Time stamp	*lIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	94.679375	95.476624	97.014778	99.020401	99.474113	99.677483
2	94.578255	95.658371	97.198036	99.010597	99.624863	99.605545
3	94.599686	95.464691	97.277817	98.982162	99.787315	99.647644
4	94.797569	95.680893	97.368423	99.044647	99.423775	99.517242
5	94.678101	95.691841	97.094528	99.009697	99.757019	99.636581
6	94.606918	95.747055	97.156876	98.959595	99.524292	99.566704
7	94.519737	95.813904	97.118279	99.073334	99.756569	99.565742
8	94.65937	95.786057	97.064384	98.9114	99.485001	99.576225
9	94.607208	95.737343	97.356033	98.910629	99.776009	99.7071
10	94.489517	95.474747	97.132858	99.049347	99.655075	99.746735

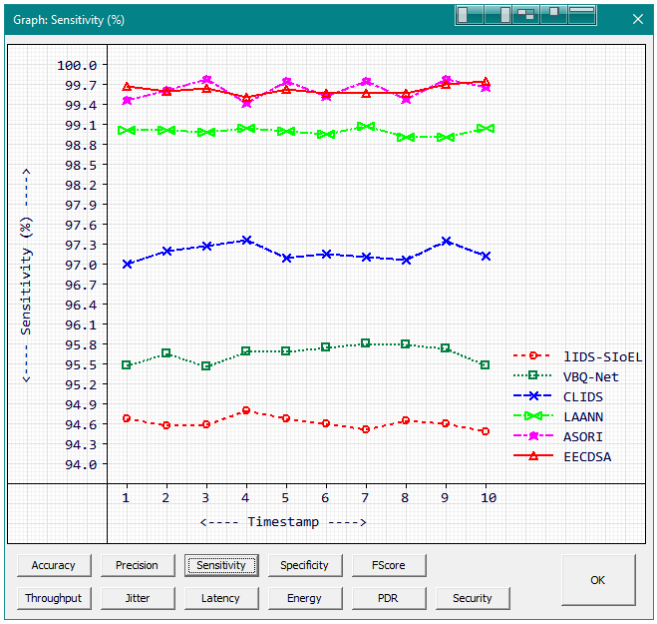

Figure 3: Sensitivity (%)

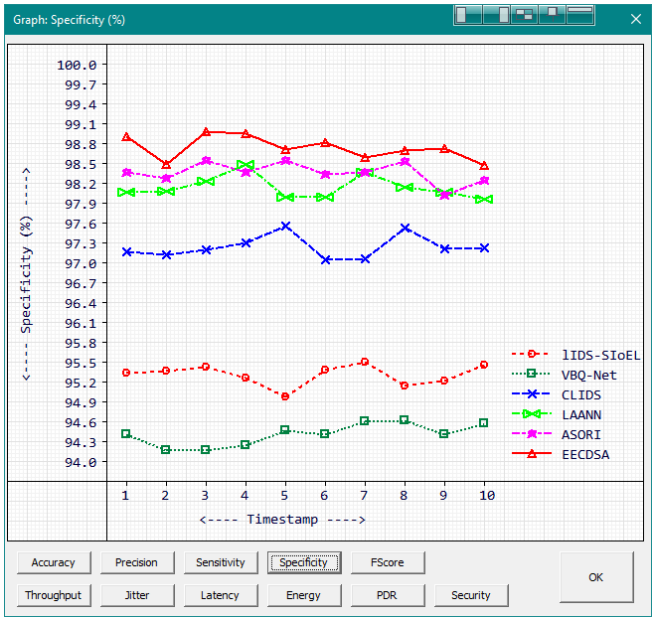

Figure 4: specificity

Table 7: Specificity

Specificity (%)						
Time stamp	*lIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	95.345558	94.415894	97.165466	98.068932	98.378166	98.908516
2	95.378868	94.176094	97.132004	98.088165	98.283516	98.496986
3	95.427933	94.173889	97.202232	98.233604	98.548294	98.986794
4	95.274963	94.242126	97.311607	98.498405	98.367622	98.955948
5	94.982941	94.474594	97.567841	98.000793	98.547859	98.712105
6	95.389893	94.412697	97.053238	97.990105	98.3498	98.818977
7	95.500961	94.602325	97.06176	98.371727	98.37294	98.603676
8	95.153343	94.628754	97.527885	98.144653	98.534218	98.701561
9	95.227066	94.41214	97.21418	98.076538	98.034981	98.732552
10	95.460983	94.574257	97.227226	97.962822	98.254951	98.479614

Table 8: F-Score

	F-Score					
Time stamp	*IIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	0.950284	0.9491	0.970923	0.985328	0.989139	0.992872
2	0.949973	0.948626	0.97164	0.98538	0.989377	0.990396
3	0.950329	0.947724	0.972389	0.985996	0.991547	0.993127
4	0.950481	0.949093	0.973392	0.987666	0.98884	0.992328
5	0.948388	0.950415	0.973367	0.984922	0.991397	0.991661
6	0.950167	0.950332	0.971034	0.984623	0.989235	0.991869
7	0.950321	0.951676	0.970891	0.987154	0.990483	0.990755
8	0.94919	0.951691	0.973016	0.985191	0.990001	0.991311
9	0.949325	0.950285	0.97283	0.984835	0.9888	0.992111
10	0.94997	0.94995	0.971814	0.984916	0.989374	0.990992

security by integrating context-aware security adaptation, computational resource optimization, and energy-efficient signing mechanisms, setting it apart from existing methods like ASORI and VBQ-Net. Unlike ASORI, which focuses primarily on anomaly detection using RSA, EECDSA dynamically adjusts cryptographic complexity based on real-time node resource availability through the Adaptive Computational Complexity Overseer (ACCO). Additionally, Lightweight Context Sensitivity Imposer (LCSI) enables real-time data classification based on sensitivity levels, ensuring optimal security enforcement while minimizing overhead—an aspect not addressed in VBQ-Net. Furthermore, Energy-aware ECDSA Signer (EAES) ensures energy-efficient signing, reducing power consumption while maintaining high security, making EECDSA uniquely scalable, adaptive, and resource-efficient for large-scale IoT networks.

A F-Score comparison grid chart is given in Figure 5.

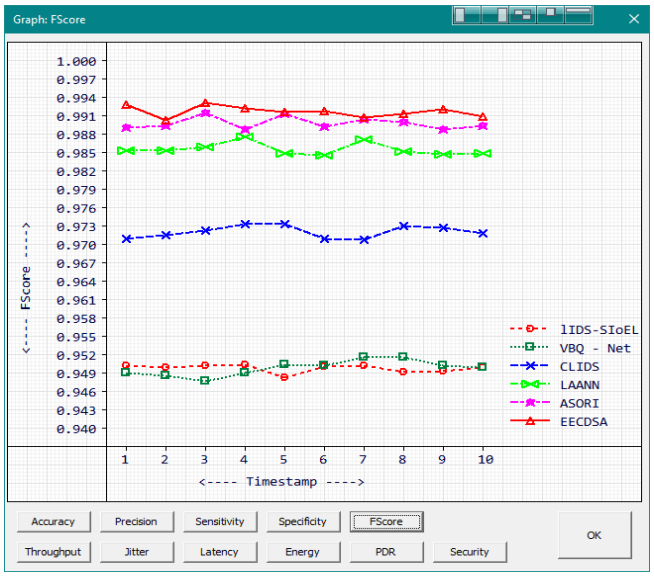

Figure 5: F-Score

Throughput

Throughput denotes the rate at which data is effectively transmitted or received over a network. It gauges the network's efficiency and capacity. The OPNET system records throughput values during simulations, and these values are detailed in Table 9.

The highest achieved throughput durintg the entire similation is 30103 kbps achieved by proposed EECDSA method. The achieved value by EECDSA is 333 kbps higher than the very next successful approach ASORI with the value 29770 kbps. The performance order with respect to throughput averages is EECDSA, ASORI, LAANN, VBQ-Net, IIDS-SIoEL, and CLIDS. A comparison grid graph is terdered in Figure 6.

Latency

Latency refers to the delay between the initiation of an action or request and the receipt of a response or the completion of that action. It is a critical performance metric for IoT systems, affecting how quickly devices can communicate and respond to commands or data. Minimizing latency in IoT is essential because it affects how quickly and effectively connected systems work. Low latency means data travels and is processed fast, which is crucial for applications that need real-time responses, like self-driving cars, factory automation, and smart home gadgets. Quick responses are important for keeping these systems reliable, safe, and user-friendly. The measurement unit of latency is milliseconds which is used to be referred as mS. Measured latency values of the examined methods are registered in table 10.

The ranking order with respect to Latency is EECDSA, ASORI, LAANN, VBQ-Net, IIDS-SIoEL, and CLIDS with the latency averages 159mS, 183mS, 237mS, 247mS, 289mS,

Table 9: Throughput

Throughput (kbps)						
Timestamp	*lIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	27632	28452	26843	28207	29120	29826
2	27743	28224	27390	28208	29306	29734
3	27344	28134	26937	28281	29770	30093
4	27309	28384	26944	28317	29122	30063
5	27684	28195	27387	28706	29576	30049
6	27480	28088	27381	28107	29533	29882
7	27223	27897	27336	28638	29566	29611
8	27704	28329	26932	28779	29638	29910
9	27206	28393	27195	28726	29474	30103
10	27392	28435	27181	28575	29519	29791

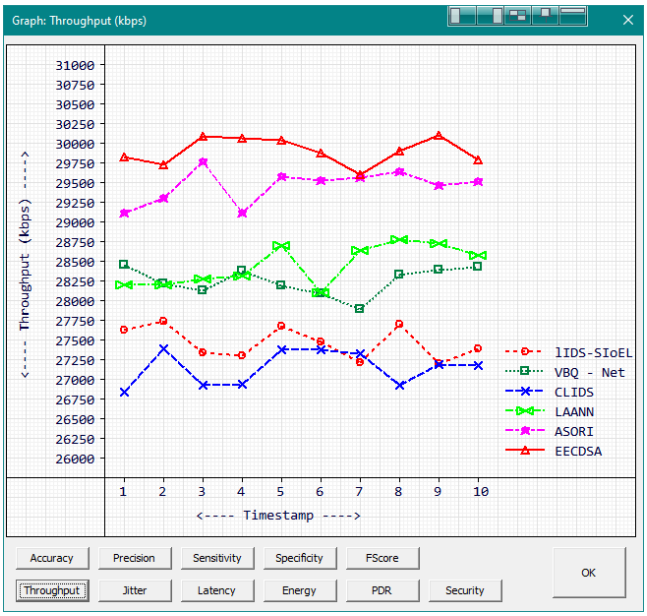

Figure 6: Throughput

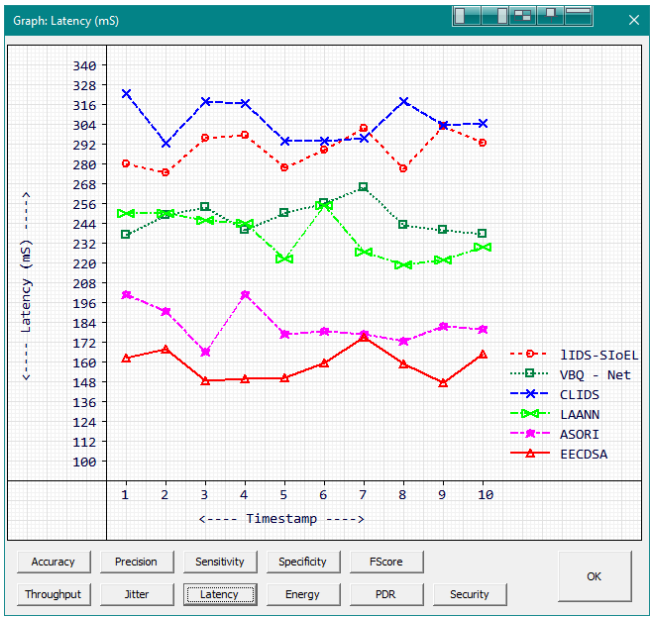

Figure 7: Latency

Table 10: Latency

Latency (mS)						
Timestamp	*lIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	280	237	323	250	201	163
2	275	249	293	250	191	168
3	296	254	318	246	166	149
4	298	240	317	244	201	150
5	278	250	294	223	177	151
6	289	256	294	255	179	160
7	302	266	296	227	177	175
8	277	243	318	219	173	159
9	303	240	304	222	182	148
10	293	238	305	230	180	165

Table 11: Jitter

Jitter (mS)						
Time stamp	*IIDS-SIoEL*	*VBQ – Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	96	83	109	87	73	61
2	95	87	100	87	70	63
3	101	89	108	86	62	57
4	102	84	107	86	73	57
5	96	87	101	79	66	58
6	99	89	101	89	66	60
7	103	92	101	81	66	65
8	95	85	108	78	64	60
9	103	84	104	79	67	57
10	100	84	104	81	66	62

and 306ms listed from the best. The lowest latency value 148mS is recorded for the proposed EECDSA method at the 9th timestamp during the experiment. Latency graph is provided in Figure 7.

Jitter

In networking, jitter refers to the variability in the delay of packet delivery across a network, resulting in irregular timing for data packets reaching their destination. High jitter values can lead to inconsistent network performance. The jitter values observed during the simulation are listed in Table 11 and the Latency comparison graph is given in Figure 8.

The lowest jitter is 57mS which is achieved by proposed EECDSA method during 3rd, 4th, and 9th timestamps. The performance rating sequence when concerning jitter is EECDSA, ASORI, LAANN, VBQ-Net, IIDS-SIoEL, and CLIDS with the jitter averages 60mS, 67.3mS,83.3mS, 86.4mS, 99mS, and 104.3mS respectively ordered from the best. Hence it is spotted that the EECDSA method seizes a lesser jitter values than the other methods in comparison during the entire

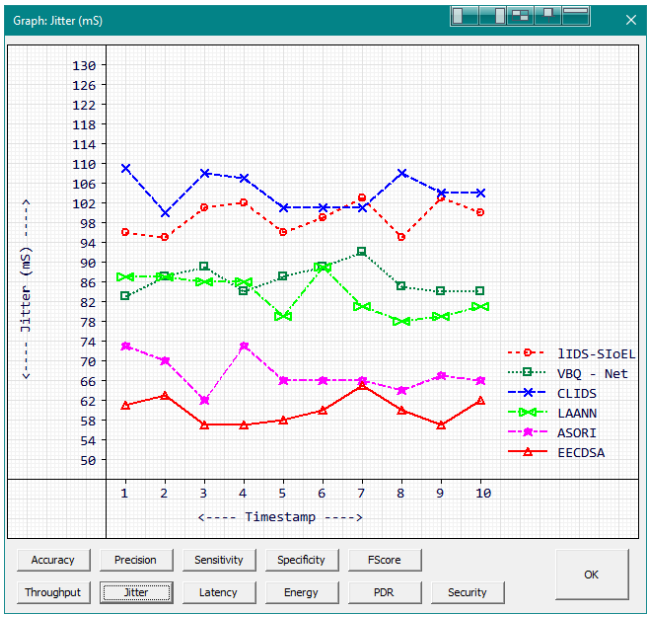

Figure 8: Jitter

Table 12: Energy

			Energy (mJ)			
Time stamp	*IIDS-SIoEL*	*VBQ – Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	590	638	712	730	568	551
2	550	641	703	716	544	526
3	622	635	697	786	501	533
4	564	643	701	733	563	485
5	555	602	746	713	546	508
6	628	667	689	779	523	516
7	583	656	717	747	581	492
8	626	631	717	762	504	489
9	550	667	689	717	576	527
10	628	626	724	768	541	489

simulation process.

Energy

Energy efficiency is vital in Internet of Things (IoT) networks for several reasons, including the limited power resources of the nodes, the scalability of the network, and the challenges in maintaining it. Energy consumption is measured in millijoules within the network. Energy consumption in IoT networks is typically measured in terms of the amount of energy used by the devices or nodes in the network. This measurement can be expressed in various units, such as millijoules (mJ), joules (J), or watt-hours (Wh), depending on the scale and precision required. In this experiment, the energy consumption of the nodes is measured in mJ.

Energy consumption and IoT network quality are inversely proportional: as energy consumption decreases, the battery life and operational efficiency of devices improve, enhancing overall network reliability and performance. Lower energy usage also supports scalability and reduces maintenance needs, contributing to higher network quality. Conversely, higher energy consumption can lead to more frequent device replacements and reduced network reliability. The energy readings from the simulation are provided in Table 12.

As per the readings observed during the experiments, the quality of the discussed methods is ranked as EECDSA, ASORI, IIDS-SIoEL, VBQ-Net, CLIDS, and LAANN with the energy averages 511.6mJ, 544.7mJ, 589.6mJ, 640.6mJ, 709.5mJ, and 745.1mJ respectively. EECDSA method consumed the very less energy share of 485mJ during the 4th timestamp during the throughput the entire experiment.

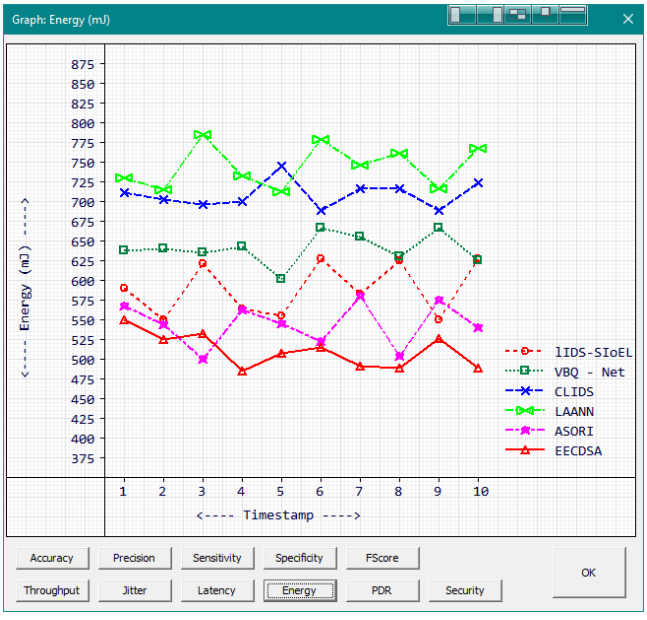

Figure 9: Energy

The comparison graph for energy consumption is given in Figure 9.

Packet Delivery Ratio

Packet Delivery Ratio (PDR) is a metric that quantifies the effectiveness of data transmission within a network. It is defined as the ratio of the number of packets successfully received by the intended destination to the number of packets sent by the source. PDR provides insight into how well the network facilitates communication between IoT devices, reflecting the efficiency of data routing and network reliability. It is crucial for evaluating the performance of network protocols and configurations in ensuring data integrity and successful delivery.

A high PDR indicates that most packets sent are successfully delivered, reflecting strong network performance and quality of service. It aids in evaluating and optimizing network protocols, managing resources effectively by reducing retransmissions and conserving energy, and supporting network scalability as it grows. Overall, PDR is a key metric for ensuring that IoT networks operate reliably and efficiently, enhancing both performance and user satisfaction. The PDR values have been measured and recorded for the discussed methods are comprehensively in Table 13

The highest packet delivery ratio 99.37% is achieved by the EECDSA method over the course of the entire dissection. The performance rank based on the PDR is EECDSA, ASORI, LAANN, VBQ-Net, IIDS-SIoEL, and CLIDS with the PDR averages 99.30%, 99.15%, 98.82%, 98.75%, 98.49%, and 98.38% have been meticulously arranged in descending order of excellence.

The PDR comparison grid graph is provided in Figure 10.

Security

Security is essential for IoT network for various important reasons, including the protection of privacy, ensuring data integrity, maintaining device control, addressing safety concerns, and supporting long device lifecycles. OPNET can assess the security level of a simulated network environment by initiating different types of intruder attacks. The security scores for the methods evaluated are detailed in Table 14, and a comparison graph is provided in Figure 11

The highest security score 99.75% is achieved by the proposed EECDSA method during the 10th timestamp of the simulation. The ranking arrangement of performance according to the security level is EECDSA, ASORI, LAANN, CLIDS, VBQ-Net, and IIES-SIoEL with the security scores averages 99.55%, 99.43%, 98.41%, 97.02%, 94.92%, and 94.23%. The most adverse security score of EECDSA is 99.4% which is also higher than the other compared methods, proves the exalted performance of the proposed method. The result scores include major attack types such as DoS, Probe, U2R, and R2L.

Table 13: Packet Delivery Ratio

Packet Delivery Ratio(%)						
Time stamp	*IIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	98.543999	98.817337	98.280998	98.735664	99.040001	99.27533
2	98.581001	98.741333	98.463333	98.736	99.101997	99.244667
3	98.447998	98.711334	98.312332	98.76033	99.256668	99.364334
4	98.436333	98.79467	98.314667	98.772331	99.040665	99.354332
5	98.561333	98.731667	98.462334	98.902	99.192001	99.34967
6	98.493332	98.695999	98.460335	98.702332	99.177666	99.293999
7	98.407669	98.632332	98.445335	98.879333	99.188667	99.203667
8	98.568001	98.776337	98.310669	98.926331	99.212669	99.303337
9	98.402	98.797668	98.398331	98.908669	99.157997	99.367668
10	98.463997	98.811668	98.393669	98.85833	99.172997	99.263664

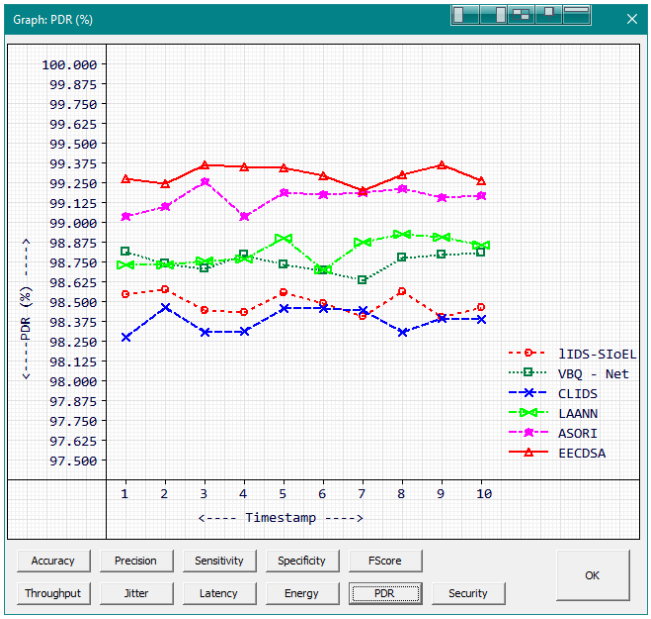

Figure 10: Packet Delivery Ratio

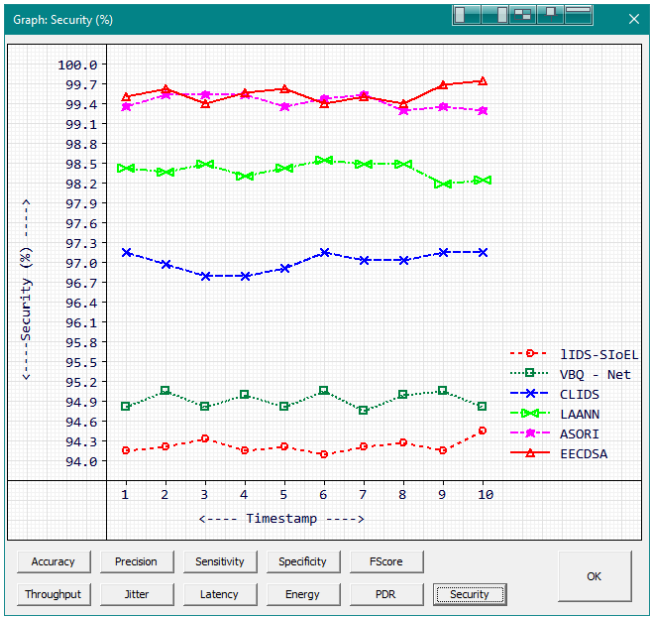

Figure 11: Security

Table 14: Security

Security (%)						
Time stamp	*IIDS-SIoEL*	*VBQ - Net*	*CLIDS*	*LAANN*	*ASORI*	*EECDSA*
1	94.158821	94.81765	97.152939	98.435295	99.358826	99.517647
2	94.217644	95.05294	96.976471	98.376472	99.535294	99.635292
3	94.335297	94.81765	96.800003	98.494118	99.535294	99.400002
4	94.158821	94.994118	96.800003	98.31765	99.535294	99.576469
5	94.217644	94.81765	96.917648	98.435295	99.358826	99.635292
6	94.099998	95.05294	97.152939	98.55294	99.476471	99.400002
7	94.217644	94.758827	97.035294	98.494118	99.535294	99.517647
8	94.276474	94.994118	97.035294	98.494118	99.300003	99.400002
9	94.158821	95.05294	97.152939	98.199997	99.358826	99.694115
10	94.452942	94.81765	97.152939	98.258827	99.300003	99.752945

The EECDSA framework offers significant performance improvements by balancing energy efficiency and security in IoT networks, making it ideal for resource-constrained devices. Through the integration of advanced modules like LCSI, ACCO, and EAES, it enhances key metrics such as Accuracy, Precision, and Sensitivity, while optimizing network performance in terms of Throughput, Jitter, and Latency. This approach not only improves security through advanced cryptographic techniques but also minimizes energy consumption, ensuring the long-term sustainability of large-scale IoT deployments. Overall, EECDSA proves to be an efficient, scalable, and secure solution that meets the growing demands of IoT networks while maintaining optimal performance and resource utilization.

Conclusion

Based on the evaluations conducted with most recent establishments related to IoT network security and achievements, the new EECDSA offers advanced features, including the Lightweight Context Sensitivity Imposer (LCSI), Adaptive Computational Complexity Overseer (ACCO), and Energy-aware ECDSA Signer (EAES), which enhance both energy efficiency and security. The effectiveness of these innovations is evaluated using metrics such as Accuracy, Precision, Sensitivity, Specificity, and F-Score for monitoring network attacks, as well as Throughput, Jitter, Latency, and Energy consumption, showing notable improvements in both security and network performance. While EECDSA achieves enhanced energy efficiency and greater security, there may be potential for further security improvements by integrating multiple digital signature concepts, which could be a notable feature. Future research could explore the integration of post-quantum cryptographic techniques with EECDSA to further enhance security resilience against emerging quantum computing threats while maintaining energy efficiency in IoT networks.

Acknowledgements

We sincerely acknowledge our colleagues for their support.

Availability of Dataset

The work is indented to ensure dynamic IoT network security, thus dynamic network transactional simulation is used for evaluation.

Code Availability

The complete implementation source code is available in GitHub, link will be provided on request

References

Adnan Sabovic, Michiel Aernouts, Dragan Subotic, Jaron Fontaine, Eli De Poorter, Jeroen Famaey, "Towards energy-aware tinyML on battery-less IoT devices," in *Internet of Things*, Volume 22, 2023, 100736, SSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100736

Almalki, F.A., Alsamhi, S.H., Sahal, R. *et al*. Green IoT for Eco-Friendly and Sustainable Smart Cities: Future Directions and Opportunities. *Mobile Netw Appl* 28, 178–202 (2023). https://doi.org/10.1007/s11036-021-01790-w

Cheddour Z, Chillali A, Mouhib A. Generalized Fibonacci Sequences for Elliptic Curve Cryptography. *Mathematics*. 2023; 11(22):4656. https://doi.org/10.3390/math11224656

G. Dimitoglou and C. Jim, "Benchmarking the Elliptic Curve Digital Signature Algorithm and RSA in Key Signing and Verification Operations with Parallelism," 2023 Congress in Computer Science, *Computer Engineering, & Applied Computing (CSCE)*, Las Vegas, NV, USA, 2023, pp. 2521-2527, https://doi.org/10.1109/CSCE60160.2023.00405

Hakan Can Altunay, Zafer Albayrak,,"A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," in *Engineering Science and Technology*, an International Journal, Volume 38, 2023, 101322, ISSN 2215-0986, https://doi.org/10.1016/j.jestch.2022.101322.

Hazman, C., Guezzaz, A., Benkirane, S. *et al*. IIDS-SIoEL: intrusion detection framework for IoT-based smart environments security using ensemble learning. *Cluster Compute* 26, 4069–4083 (2023). https://doi.org/10.1007/s10586-022-03810-0

Hofheinz, D., Kiltz, E. (2022). Scalable Cryptography. In: Bast, H., Korzen, C., Meyer, U., Penschuck, M. (eds) Algorithms for Big Data. Lecture Notes in Computer Science, vol 13201. *Springer*, Cham. https://doi.org/10.1007/978-3-031-21534-6_9

https://visualstudio.microsoft.com/vs/

https://www.geeksforgeeks.org/features-of-c-20/

Inshi S, Chowdhury R, Ould-Slimane H, Talhi C. Secure Adaptive Context-Aware ABE for Smart Environments. *IoT*. 2023; 4(2):112-130. https://doi.org/10.3390/iot4020007

Jabeen, A., & Shanavas, A. R. M. (2025). Bradley Terry Brownboost and Lemke flower pollinated resource efficient task scheduling in cloud computing. *The Scientific Temper*, 16(05), 4220-4231.

Doi: 10.58414/SCIENTIFICTEMPER.2025.16.5.07

Jenifer RR, Prakash VS. Rivest-Shamir-Adleman algorithm optimized to protect iot devices from specific attacks. *Informatics and Automation*. 2024;23(5):1423-53. https://doi.org/10.15622/ia.23.5.6

Jeyaselvi, M., Dhanaraj, R.K., Sathya, M. *et al*. A highly secured intrusion detection system for IoT using EXPSO-STFA feature selection for LAANN to detect attacks. *Cluster Compute* 26, 559–574 (2023). https://doi.org/10.1007/s10586-022-03607-1

Kim Y, Seo SC. Signature Split Method for a PQC-DSA Compliant with V2V Communication Standards. *Applied Sciences*. 2023; 13(10):5874. https://doi.org/10.3390/app13105874

Lalem F, Laouid A, Kara M, Al-Khalidi M, Eleyan A. A Novel Digital Signature Scheme for Advanced Asymmetric Encryption Techniques. *Applied Sciences*. *2023*; 13(8):5172. https://doi.org/10.3390/app13085172

Perumal G, Subburayalu G, Abbas Q, Naqi SM, Qureshi I. VBQ-Net: A Novel Vectorization-Based Boost Quantized Network Model for Maximizing the Security Level of IoT System to Prevent Intrusions. *Systems*. 2023; 11(8):436. https://doi.org/10.3390/systems11080436

Picallo, I., Iturri, P.L., Celaya-Echarri, M. *et al*. Deterministic Wireless Channel Characterization towards the Integration of Communication Capabilities to Enable Context Aware Industrial Internet of Thing Environments. *Mobile Netw Appl* 28, 4–18 (2023). https://doi.org/10.1007/s11036-022-01993-9

R. Samadi, A. Nazari and J. Seitz, "Intelligent Energy-Aware Routing Protocol in Mobile IoT Networks Based on SDN," in *IEEE Transactions on Green Communications and Networking*, vol. 7, no. 4, pp. 2093-2103, Dec. 2023, https://doi.org/10.1109/TGCN.2023.3296272

S. Das, S. Namasudra, S. Deb, P. M. Ger and R. G. Crespo, "Securing IoT-Based Smart Healthcare Systems by Using Advanced Lightweight Privacy-Preserving Authentication Scheme," in *IEEE Internet of Things Journal*, vol. 10, no. 21, pp. 18486-18494, 1 Nov.1, 2023, https://doi.org/10.1109/JIOT.2023.3283347

S. R. Kawale, K. Prasad, D. Palanikkumar, P. A. Mary, A. Y. Begum and D. G. V, "A Novel IoT Framework and Device Architecture for Efficient Smart city Implementation," 2023 7th *International Conference on Trends in Electronics and Informatics (ICOEI),* Tirunelveli, India, 2023, pp. 420-426, http://doi.org/10.1109/ICOEI56765.2023.10125677

Shabana Urooj, Sonam Lata, Shahnawaz Ahmad, Shabana Mehfuz, S Kalathil, "Cryptographic Data Security for Reliable Wireless Sensor Network," in *Alexandria Engineering Journal*, Volume 72, 2023, Pages 37-50, ISSN 1110-0168, https://doi.org/10.1016/j.aej.2023.03.061

Sridevi, R., & Prakash, V. S. J. (2024). Load aware active low energy adaptive clustering hierarchy for IoT-WSN. *The Scientific Temper*, 15(02), 2123-2131.