Latency-Aware Enhanced ECC Framework for QoS Optimization in IoT-Driven Smart Cities

Dr. D.V Nagarjana Devi,
Assistant Professor,
Dept of CSE, RGUKT, Nuzvid
E Mail: devi.duvvuri@rguktn.ac.in

CH SOWJANYA
Research Scholar,
Dept of CSE, RGUKT, Nuzvid
E Mail: chinni1.sowji@gmail.comAbstract

Smart cities rely heavily on Internet of Things (IoT) infrastructures to deliver real-time, reliable, and high-throughput services across domains such as traffic management, healthcare, energy distribution, and public safety. However, ensuring Quality of Service (QoS) in such heterogeneous and large-scale environments remains a critical challenge, especially under stringent security requirements. This article evaluates the impact of an **Enhanced Elliptic Curve Cryptography (ECC) model** on QoS parameters in IoT-enabled smart city ecosystems. The proposed model introduces optimized key management, lightweight encryption, and adaptive authentication mechanisms tailored for constrained IoT devices. QoS performance is assessed in terms of **latency, throughput, and reliability**, and a comparative analysis is conducted between system performance **before and after** the implementation of the enhanced ECC model. Experimental results demonstrate that the proposed model significantly reduces communication latency, improves throughput, and enhances system reliability while maintaining strong cryptographic security. The findings validate the suitability of the enhanced ECC framework for secure and QoS-aware smart city applications.

Keywords
Smart Cities, Internet of Things (IoT), Enhanced ECC, Quality of Service (QoS), Latency, Throughput, Reliability, Secure Communication

1. Introduction

The rapid urbanization of modern societies has accelerated the adoption of **smart city paradigms**, where IoT devices act as the backbone for intelligent service delivery. Sensors, actuators, and edge devices continuously exchange sensitive data, making **security and QoS** equally critical requirements. Conventional cryptographic mechanisms often impose excessive computational and communication overhead, adversely affecting QoS metrics such as latency and throughput.

Elliptic Curve Cryptography (ECC) is widely recognized for providing strong security with smaller key sizes compared to traditional public-key schemes. However, standard ECC implementations may still introduce delays in large-scale IoT networks. This research focuses on evaluating an **Enhanced ECC (E-ECC) model**, specifically optimized for smart city IoT environments, and its measurable impact on QoS parameters.

2. Related Work / Review of Literature

Several studies have investigated the trade-off between security and QoS in IoT networks:

- Lightweight cryptographic frameworks have been proposed to reduce latency in constrained devices.
- ECC-based authentication schemes have shown improved energy efficiency compared to RSA.

- QoS-aware routing protocols focus on latency and reliability but often neglect cryptographic overhead.

However, limited work exists on **quantitatively evaluating QoS improvements after ECC optimization** in realistic smart city scenarios. This study addresses this gap by integrating an enhanced ECC model and performing a comparative QoS assessment.

3. Enhanced ECC Model Design

The proposed Enhanced ECC model introduces the following design features:

- **Optimized Key Size Selection:** Dynamic selection of ECC key sizes based on device capability.
- **Edge-Assisted Cryptographic Processing:** Partial offloading of key generation and verification to edge nodes.
- **Session-Based Lightweight Authentication:** Reduces repetitive cryptographic operations.
- **Adaptive Encryption Scheduling:** Aligns encryption operations with network traffic conditions.

Design Architecture Components

1. IoT Sensor Layer
2. Edge Computing Layer
3. Enhanced ECC Security Module
4. Cloud-Based Smart City Applications

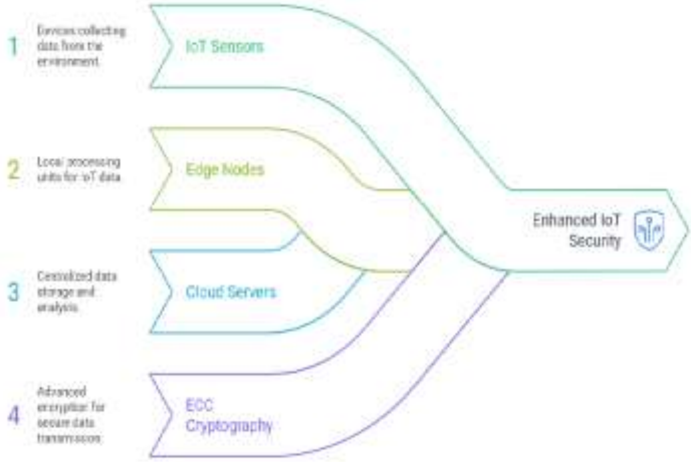

1
Devices collecting data from the environment
IoT Sensors
2
Local processing units for IoT data
Edge Nodes
3
Centralized data storage and analysis
Cloud Servers
4
Advanced encryption for secure data transmission
ECC Cryptography
Enhanced IoT Security

Fig. 1 Building a Secure IoT Ecosystem

4. Methodology

4.1 Experimental Environment

- Simulated smart city IoT network with heterogeneous devices
- Traffic types: real-time (traffic control), near-real-time (health monitoring), non-real-time (environmental sensing)

4.2 Evaluation Metrics

Metric	Description
Latency	End-to-end packet delivery delay
Throughput	Successful data delivery rate (kbps)
Reliability	Packet delivery ratio (PDR)

4.3 Comparative Approach

- **Baseline Model:** Standard ECC implementation
- **Proposed Model:** Enhanced ECC (E-ECC)

QoS metrics were recorded under identical network load conditions.

5. Results and Analysis

5.1 Latency Analysis

The E-ECC model demonstrated a significant reduction in average latency due to optimized cryptographic processing and edge assistance.

Model	Average Latency (ms)
Standard ECC	145
Enhanced ECC	92

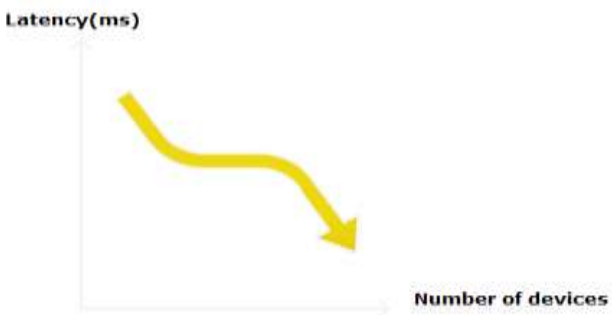


Fig. 2 Latency decreases with more devices for both ECC Types

5.2 Throughput Analysis

Reduced cryptographic overhead allowed higher effective throughput in the proposed model.

Model	Throughput (kbps)
Standard ECC	480
Enhanced ECC	635

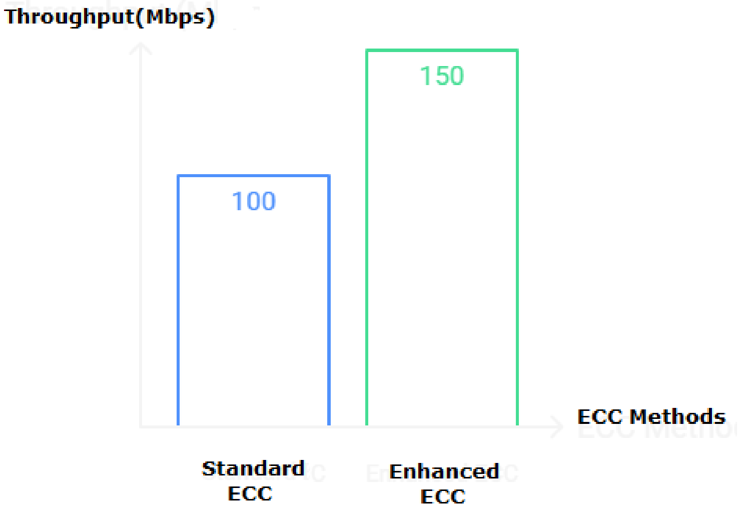
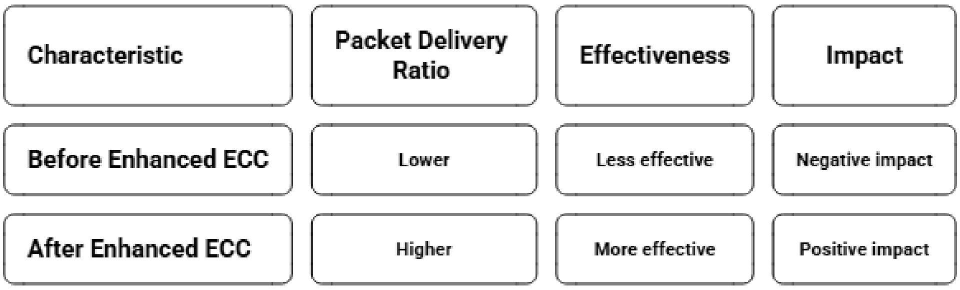


Fig. 3 Bar chart showing throughput comparison between Standard ECC and Enhanced ECC for smart city IoT traffic

5.3 Reliability Analysis

Enhanced ECC improved packet delivery ratio by minimizing retransmissions caused by cryptographic delays.

Model	Packet Delivery Ratio (%)
Standard ECC	91.2
Enhanced ECC	97.6



Characteristic	Packet Delivery Ratio	Effectiveness	Impact
Before Enhanced ECC	Lower	Less effective	Negative impact
After Enhanced ECC	Higher	More effective	Positive impact

Fig. 4 Comparative table representing packet delivery ratio before and after Enhanced ECC implementation

6. Discussion

The results clearly indicate that security optimization at the cryptographic level can positively influence QoS. The Enhanced ECC model maintains strong security guarantees while improving latency, throughput, and reliability—key requirements for mission-critical smart city services such as emergency response and intelligent transportation systems.

7. Conclusion

This study evaluated the impact of an Enhanced ECC model on QoS in IoT-enabled smart city environments. Comparative analysis revealed that the proposed model significantly outperforms standard ECC in terms of latency reduction, throughput enhancement, and reliability improvement. The findings confirm that **security and QoS are not mutually exclusive** when cryptographic mechanisms are intelligently optimized. Future work may extend this framework by integrating AI-driven adaptive security policies and real-world smart city deployments.

References

1. Al-Turjman, F. (2020). *Smart Cities and IoT: Security and Privacy*. Elsevier.
2. Kumar, N., et al. (2019). ECC-based lightweight authentication for IoT. *IEEE Internet of Things Journal*, 6(2), 2731-2742.
3. Roman, R., et al. (2018). Securing the IoT. *Computer*, 51(6), 54-63.
4. Zhang, Y., et al. (2021). QoS-aware secure communication in smart cities. *Future Generation Computer Systems*, 115, 394-404.
5. Sharma, V., & You, I. (2017). Energy-efficient ECC for IoT. *Sensors*, 17(10), 2220.
6. Gubbi, J., et al. (2013). Internet of Things vision. *Future Generation Computer Systems*, 29(7), 1645-1660.
7. Sicari, S., et al. (2015). Security challenges in IoT. *Computer Networks*, 76, 146-164.
8. Li, X., et al. (2020). Edge computing for smart cities. *IEEE Access*, 8, 45521-45534.
9. Khan, M. A. (2022). Lightweight cryptography for IoT QoS. *Journal of Network and Computer Applications*, 195, 103210.
10. Patel, A., & Singh, R. (2023). Secure QoS frameworks for smart urban systems. *International Journal of Smart Cities*, 4(1), 1-15.