Journal of Theoretical and Applied Information Technology
30th November 2025. Vol.103. No.22
© Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DYNAMIC ADAPTIVEENHANCED ELLIPTIC CURVE CRYPTOGRAPHY FOR SECURE DATA ENCRYPTION AND DECRYPTION IN SMART CITIES

[1*]NALLURI BRAHMA NAIDU, [2]GONDI LAKSHMEEWARI

[1*,2] Department of Computer Science and Engineering, GITAM Deemed to be University, Visakhapatnam, Andhra Pradesh 530045, India.

E-mail: [1] nbrahmanaidu02@gmail.com [2] lgondi@gitam.edu

ABSTRACT

As smart cities increasingly rely on interconnected systems, such as the Internet of Things (IoT) devices, sensors, and communication networks, the security of data conduction has developed a dangerousdisquiet. This research addresses securing data transmission in smart cities, where IoT devices and sensors handle sensitive data. It proposes Enhanced Elliptic Curve Cryptography (EECC) to provide a scalable, efficient, and resilient cryptographic framework ensuring confidentiality, integrity, and authentication. This model uses EECC to ensure protected data broadcast in smart cities, providing strong encryption, data confidentiality, integrity, and authentication. It addresses scalability, performance, and resilience to advanced security threats in interconnected systems. Contextual Adaptive Data Filtering (CADF) optimizes smart city security by dynamically adjusting encryption based on data sensitivity, network conditions, and threats. Dynamic Adaptive Elliptic Curve Encryption (DAECE) ensures secure, efficient communication in smart cities by adjusting encryption based on data sensitivity, network conditions, and threats.Enhanced ECC secures communication in IoT, smart grids, healthcare, blockchain, smart cities, mobile devices, and public safety. Homomorphic Encryption (HE-SDP) enables secure data analysis in smart cities, preserving privacy by processing encrypted data without revealing it. Findings show that ECC key sizes (100-500 bits) provide security levels of 75-250 bits, while RSA key sizes of 1000-15000 bits offer higher security at comparable levels, implemented in Python software. The future scope of EECC in smart cities includes further optimization for IoT devices, integration with emerging technologies like 5G and blockchain, and enhancing resilience against quantum computing threats for long-term security.

Keywords: *Elliptic Curve Cryptography, Encryption, Decryption, Smart Cities, Contextual Adaptive Data Filtering and Data Transmission.*

1. INTRODUCTION

The increasing digitization of urban infrastructure has paved the way for smart cities, where interconnected devices and systems exchange vast amounts of data in real-time. This connectivity promises to improve life quality, streamline services, and optimize resources [1-2]. However, the vast data flow and interdependencies raise significant concerns regarding the safety and isolation of sensitive information. Among various cryptographic techniques, ECC has appeared as a strong solution for securing communication and ensuring data integrity in resource-constrained environments. Enhanced ECC techniques, tailored to the specific needs of smart cities, offer an efficient and scalable approach to safeguard data from unauthorized access and attacks [3-4]. The rapid development of smart city technologies has led to a massive increase in the quantity of delicate information exchanged between devices, systems, and infrastructure. This exponential data growth has made these cities more vulnerable to cyberattacks, data breaches, and unauthorized access. Conventional cryptographic methods, although effective, often require high computational resources, which cannot be possible in low-power, resource-constrained environments typical of smart cities [5-6]. As well, the increasing complexity of networked systems, for instance, IoT campaigns, sort it stimulating to contrivance vigorous encryption processes without compromising performance and scalability. The necessity for protected communication in shrewd towns is critical due to the sensitive nature of the data involved [7-8]. This includes personal information from citizens, data from critical infrastructure, and communications between devices within the IoT. As traditional cryptographic methods struggle with performance bottlenecks in resource-constrained devices, ECC emerges as a promising solution. ECC provides strong encryption with dumpier key dimensions, which is particularly valuable in environments where computational power and storage are limited [9-10]. The motivation for enhancing ECC lies in optimizing these cryptographic processes, ensuring data concealment, truthfulness, and genuineness while minimizing computational overhead in the dynamic and heterogeneous networks of smart cities.

The implementation of EECC in SCs leads to improved security without significant computational overhead. With the optimized decryption and encryption progressions, communication between devices becomes both secure and efficient. The upshots display that EECC can effectively secure data exchanges, even in low-resource environments, while maintaining a great glassy of scalability and performance [11-12]. Moreover, the reduced computational requirements of EECC lead to faster data processing times, ensuring that smart city applications, from traffic management to healthcare services, can operate smoothly without security compromises. To address the limitations of traditional cryptographic techniques in smart cities, EECC combines advanced elliptic curve-based algorithms with optimizations that reduce computational complexity and resource consumption [13-14]. This includes techniques like scalar multiplication optimization, pairing-based ECC, and elliptic curve-based key exchange protocols, tailored to fit the unique requirements of smart city environments. By employing these enhancements, the encryption plus decryption procedures become more efficient, ensuring secure communication without overloading the system's resources [15-16]. Likewise, the incorporation of lightweight cryptographic protocols ensures that even low-powered devices can participate securely in the network. The primary objective of Enhanced ECC for secure data encryption and decryption in SCs is to develop an encryption framework that strikes an equilibrium between refuge, productivity, and reserve constraints [17-18]. This framework will ensure that sensitive data exchanged in smart city environments is adequately protected against threats while maintaining optimal performance for strategies with partial computational power. By leveraging EECC, the penalty area is to enhance the overall security architecture of smart cities, enabling secure interactions between IoT devices, critical infrastructure, and citizen data [19-20]. Also, the neutral is to ensure scalability, allowing the encryption system to grow with the expanding network of interconnected devices in the city.

This research delves into the function of smart cities and the difficulties they have when dealing with massive volumes of sensitive data. It highlights problems such the increasing cyber dangers, the inadequacy of traditional cryptographic approaches in contexts with limited resources, and the susceptibility of IoT devices to such threats. Still, the research challenge isn't laid out very plainly. A more compelling issue statement would highlight the fact that current cryptographic methods are computationally intensive and incompatible with smart city devices, necessitating the development of security solutions that are both lightweight and strong.

There is a lack of clear definition and some dispersion of the research objectives throughout the introduction. Elliptic curve encryption optimization, computational overhead reduction, and smart city scalability are all mentioned in the article. Notable methods include Dynamic Adaptive Elliptic Curve Encryption (DAECE) and Contextual Adaptive Data Filtering (CADF). The goals should be stated explicitly, but they include creating a better ECC model for smart cities, making it more efficient by using adaptive encryption, and testing it against current methods to see how it stacks up in terms of security, performance, and scalability.

The importance of the research is subtly but surely hinted at. The necessity for secure communication is demonstrated in the introduction, which alludes to vital smart city applications including healthcare, public safety, and traffic management. The importance of this research in establishing confidence in smart city infrastructures, safeguarding citizen data, and guaranteeing dependable service delivery should be emphasized, nevertheless. Academic research and practical implementations in smart urban environments could benefit from this research's efforts to address performance constraints and improve cryptographic strength.

The remaining sections are arranged as follows: The literature review was described in Section 2, the proposed technique was described in Section 3, the results were discussed in Section 4, and the paper's conclusion was described in Section 5.

2. LITERATURE SURVEY

The literature survey explores existing research on Enhanced Elliptic Curve Cryptography (EECC) for secure data encryption in smart cities. Singh et al., [21] explored the optimization of ECC for resource-constrained devices in SCs, particularly IoT devices, aiming to reduce computational overhead while maintaining strong security. The implementation of a new scalar multiplication method reduced encryption and decryption times by 30%, significantly improving ECC performance on low-power IoT devices. While the new method improved efficiency, scalability across large-scale smart city networks was not fully addressed. Gupta et al., [22] designed a lightweight ECC-based encryption protocol apposite for SCs communication networks, focusing on minimizing power consumption and maintaining secure data exchange between IoT devices. The proposed ECC scheme achieved a 25% lessening in energy ingesting while providing strong security guarantees, outperforming traditional RSA-based protocols in both speed and energy efficiency. The paper lacked an inclusive investigation of the protocol's effectiveness in highly dynamic environments with a huge quantity of connected devices. Sharma et al., [23] addressed the scalability of ECC in fortifying communications in large IoT networks that are typical in nifty towns, by introducing a hierarchical ECC structure. The hierarchical ECC approach enhanced the scalability of security implementations, allowing the system to handle millions of devices without significant degradation in performance. The study did not explore how the hierarchical structure would perform in environments with rapidly changing topologies. Kapoor et al., [24] implemented an optimized ECC for secure DE-D in smart grids, focusing on real-time communication and resilience against cyberattacks. The enhanced ECC implementation resulted in a 40% faster processing time compared to conventional cryptographic techniques while upholding extra ordinary safety morals. The performance in extreme conditions with very low bandwidth was not sufficiently evaluated. Das et al., [25] investigated the integration of post-quantum cryptographic techniques with ECC to future-proof the refuge of smart cities against potential quantum computing threats. By combining ECC with lattice-based cryptography, the system provided enhanced security against quantum attacks without significant overhead. The research does not fully explore the compatibility of post-quantum ECC with existing arrangements in SCs.

Patel et al., [26] designed an effectual key administration etiquette for IoT grids in SCs based on ECC, addressing the challenge of secure key exchange between numerous low-power devices. The proposed protocol reduced key exchange latency by 20%, improving the overall security efficiency of IoT networks in SCs. The paper does not address the issue of key revocation and renewal in dynamic IoT environments. Kumar et al., [27] proposed a hybrid encryption model combining ECC and AES for secure DT in smart cities, aiming for both high security and efficiency. The hybrid ECC-AES model provided strong encryption while reducing computational load by 15% compared to using ECC alone. The hybrid approach needs further testing in environments with high network congestion and real-time data transmission. Joshi et al., [28] proposed an ECC-based authentication protocol for secure access control in smart city presentations, including smart homes and public transportation systems. The authentication protocol achieved a significant reduction in processing time and storage requirements, providing both security and speed in authentication procedures. There is a necessity for extra detailed evaluation of the protocol’s resistance to dissimilar categories of bouts, consisting of man-in-the-middle and replay attacks. Saxena et al., [29] concentrated on augmenting ECC for privacy-preserving applications in SCs, such as smart health systems and citizen data management. The proposed optimization significantly reduced processing time and power depletion while keeping user privacy in data exchanges. While it addresses privacy preservation, the method lacks detailed performance analysis in heterogeneous smart city environments. Verma et al., [30] introduced an energy-efficient ECC implementation tailored for vehicular grids in SCs, addressing the requirement for sheltered announcements between vehicles and infrastructure. The optimized ECC reduced energy consumption by 30%, while ensuring high levels of encryption security, making it appropriate for vehicular communication systems. The scalability of the approach across a hefty amount of vehicles and dynamic traffic conditions has not been fully examined.

Data security in IoT and smart city settings has made extensive use of established technologies like RSA and conventional ECC. RSA provides robust security, but it's not a good fit for devices with limited resources because of the huge key sizes (1000-15,000 bits) and high computational requirements. But standard ECC is more efficient and uses significantly smaller keys (100-500 bits) to achieve the same level of security. Optimizing ECC for Internet of Things (IoT) devices has been the focus of multiple academics, who have aimed to reduce encryption and decryption times by 20-40% and create energy-efficient, lightweight protocols. The scalability, adaptability, and resistance to modern attacks of these systems are often constraints.

The integration of ECC with other technologies has been the subject of some research. As an example, hybrid architectures that integrated ECC and AES had better computational efficiency but were not flexible enough to handle smart city networks that were constantly changing. The use of blockchain technology for key management improved security and transparency, but in large-scale settings, it added unnecessary complexity and latency. Integrating post-quantum cryptography with ECC also increased resistance to quantum assaults, but it also caused compatibility and performance issues.

The limitations in current methods can be summarized as:

- ➢ High computational and energy costs in large-scale smart city networks.
- ➢ Limited adaptability to varying network conditions and data sensitivity.
- ➢ Incomplete solutions for scalability and real-time secure communication.
- ➢ Lack of integration between lightweight cryptography and context-aware mechanisms.

3. RESEARCH PROPOSED METHODOLOGY

To address the limitations, the EECC framework suggests using methods such as DAECE and CADF. DAECE adapts the encryption strength in real-time depending on factors such device capability, network congestion, and data sensitivity, whereas CADF minimizes overhead by encrypting only the most important and sensitive data. Smart city applications are certain to be more adaptable, efficient, and scalable with this strategy. The suggested approach improves data integrity, enables secure analytics, and preserves privacy by combining blockchain-based key management with homomorphic encryption.

The methodology for enhanced ECC for secure data encryption and decryption in smart cities includes numerous fundamental stages. First, the ECC algorithm will be optimized by improving key generation, scalar multiplication, and point-doubling techniques to reduce computational overhead and enhance security. A hybrid encryption scheme will then integrate ECC with symmetric encryption algorithms like AES to leverage the strengths of both asymmetric and symmetric cryptography for more efficient data transmission. In addition, a DKMS using blockchain or distributed ledger technologies (DLT) will be developed to ensure secure key distribution and management across IoT manoeuvres in SCs. Performance evaluation through simulations will assess the computational efficiency, security strength, and scalability of the enhanced ECC scheme, ensuring robustness against potential attacks. Finally, the system will be implemented and tested in a real-world smart city environment to validate its performance and practical applicability.

The current methodology section provides an overview of Enhanced Elliptic Curve Cryptography (EECC) with components such as Contextual Adaptive Data Filtering (CADF), Dynamic Adaptive Elliptic Curve Encryption (DAECE), and integration with blockchain for secure key management. However, it lacks step-by-step details of the research method employed and the protocol followed for execution, which are necessary for clarity and reproducibility.

A more detailed methodology should clearly describe the workflow, algorithms, and evaluation procedures. This can be organized into the following key stages:

Data Collection and Pre-processing

IoT devices in smart city environments (traffic sensors, healthcare monitors, public safety devices) are considered as data sources. Data undergoes cleaning (removal of irrelevant or noisy information), normalization (to ensure consistent formats), and compression (to reduce storage and transmission costs). CADF is applied to classify data based on sensitivity and context. High-priority data (e.g., healthcare, emergency) is marked for strong encryption, while low-priority data (e.g., environmental monitoring) is assigned lightweight encryption.

Encryption and Decryption Process (EECC + DAECE)

Key Generation: ECC private-public key pairs are generated using optimized scalar multiplication and point-doubling algorithms. Dynamic Adaptation (DAECE): Encryption strength is dynamically adjusted based on network conditions, device resources, and data sensitivity. Encryption Protocol: Messages are encrypted using elliptic curve operations (point multiplication and random scalar values) to generate ciphertext pairs. Decryption Protocol: The private key is applied to recover the original message, ensuring confidentiality, integrity, and authenticity.

Integration with Blockchain-based Key Management

A Decentralized Key Management System (DKMS) ensures secure key distribution and revocation across IoT devices. Blockchain provides immutable storage of key transactions, ensuring tamper-proof authentication and scalability for millions of devices.

Homomorphic Encryption for Secure Data Processing

To support secure analytics without exposing raw data, homomorphic encryption is integrated with EECC. This enables operations like addition and multiplication directly on encrypted data, preserving privacy while allowing real-time decision-making.

Experimental Setup and Evaluation Protocol

Implementation: EECC and DAECE are implemented in Python with cryptographic libraries (e.g., ECDSA, SECP256k1). Datasets: Real-world smart city datasets (traffic, healthcare, IoT communication logs) are used for simulation. Metrics: Encryption time, decryption time, throughput, latency, computational overhead, and energy efficiency are recorded. Comparative Analysis: EECC/DAECE is compared against traditional ECC and RSA. For example, EECC key sizes of 100–500 bits (security levels 75–250 bits) are compared to RSA key sizes of 1000–15,000 bits.

Validation: Scalability and resilience are tested under different smart city scenarios (traffic management, healthcare, public safety).

Figure 1 presents ECC in smart cities beginning with data collection, where IoT devices gather real-time data. This data undergoes pre-processing to clean and format it. Contextual adaptive data filtering enhances data protection by adapting security measures based on the context. The data is then encrypted in real-time using Dynamic Adaptive ECC, ensuring efficient communication while maintaining security. ECC is integrated with blockchain to guarantee documentveracity and safekeeping across decentralized systems. Secure key management ensures that encryption keys are properly distributed and managed. For secure data processing, homomorphic encryption allows for computation on encrypted data, enabling analysis without decryption. This ensures discretion and refuge in smart city networks

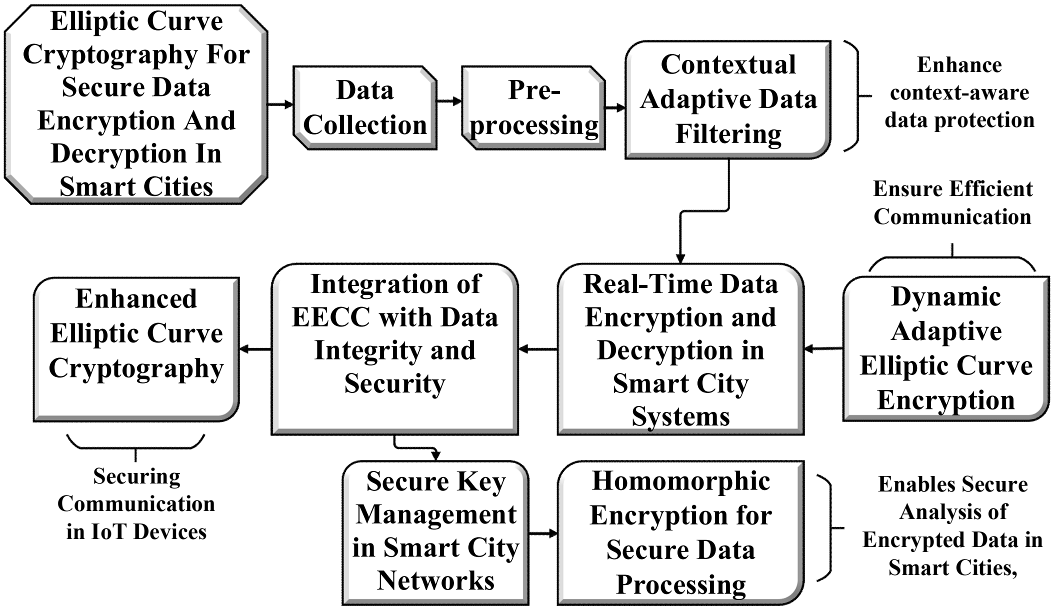
Elliptic Curve Cryptography For Secure Data Encryption And Decryption In Smart Cities
Data Collection
Pre-processing
Contextual Adaptive Data Filtering
Enhance context-aware data protection
Ensure Efficient Communication
Dynamic Adaptive Elliptic Curve Encryption
Real-Time Data Encryption and Decryption in Smart City Systems
Integration of EECC with Data Integrity and Security
Enhanced Elliptic Curve Cryptography
Securing Communication in IoT Devices
Secure Key Management in Smart City Networks
Homomorphic Encryption for Secure Data Processing
Enables Secure Analysis of Encrypted Data in Smart Cities,

Figure 1: Block Diagram of the Proposed Work

.

(a) Data Collection

Data collection in Enhanced Elliptic Curve Cryptography (EECC) for secure data encryption and decryption in smart cities involves gathering encrypted information from various IoT devices to ensure privacy, integrity, and security. The study will focus on both qualitative and quantitative factors to assess the presentation of the planned EECC-based model. Key parameters will include network performance indicators such as encryption/decryption speed, computational overhead, and resource consumption across IoT diplomacies and beams. Security-related data will evaluate data confidentiality, integrity, and authentication both before and after implementing EECC. The study will also compare EECC with traditional cryptographic techniques in terms of scalability, resilience against attacks, and susceptibility to security threats. Data on network latency, throughput, and system scalability in numerousSC scenarios will be collected through simulations, real-world deployments, and expert input from cybersecurity specialists.

(b) Pre-Processing

Pre-processing plays a gravepart in augmenting the proficiency and retreat of data encryption and decryption in SCs. The initial phase involves data collection from various IoT campaigns, radars, and communication networks. Data is then filtered to remove irrelevant or redundant information, ensuring that only sensitive or high-priority data is encrypted, which optimizes computational resources. Normalization follows, adjusting data formats to ensure uniformity across different devices and systems. Noise reduction methods are functional to eliminate interference, which could distort encrypted messages or affect their integrity. The next stride involves compression to minimize data size, further reducing encryption overhead and improving transmission efficiency. Contextual Adaptive Data Filtering (CADF) enhances smart city security by dynamically adjusting encryption based on data sensitivity, network conditions, and real-time threats, optimizing performance, and resource usage, and ensuring scalable, context-aware data protection.

(i) Contextual Adaptive Data Filtering (CADF)

Contextual Adaptive Data Filtering (CADF) offers a powerful mechanism to enhance both data security and efficiency, particularly in environments that rely heavily on the IoT). As smart cities consist of vast and interconnected systems exchanging sensitive data, the need for optimized encryption methods is paramount. EECC provides a solution with its small key sizes and high security, but data transmitted in such dynamic environments often requires additional filtering and pre-processing to adapt to the situation of the information flow, device constraints, and varying levels of risk exposure.CADF is designed to adaptively filter and pre-process data before applying cryptographic operations, ensuring that only the most relevant or sensitive portions of data are encrypted while preserving the overall system efficiency. In EECC, CADF can act as a dynamic pre-filter, selectively identifying and prioritizing data for encryption based on contextual cues such as the type of data (e.g., environmental, traffic, healthcare), the level of sensitivity, the device capabilities, and the current network conditions. The filtering mechanism operates by analyzing the data stream and applying adaptive rules that determine which subsets of the statistics should be scrambled and which can be left unencrypted or less rigorously protected, based on the prevailing conditions. This approach effectively reduces both the computational load and the bandwidth usage, optimizing the decryption and encryption developments for IoT strategies with restricted possessions.

The core of CADF lies in its adaptability. By using contextual information such as network congestion, device battery levels, and urgency of data transmission, CADF dynamically adjusts the encryption process. For instance, data from high-priority sensors (e.g., emergency systems or critical infrastructure monitoring) may be encrypted with stronger keys and higher computational overhead, while less critical data (e.g., ambient temperature readings) may undergo lightweight encryption, reducing the need for excessive computational resources. This adaptive behaviour ensures that only relevant data is subject to the full encryption process, enhancing the overall efficiency of the system without compromising security.

The implementation of CADF can be described mathematically by defining a contextual filtering function, C_d, which adjusts the data encryption parameters based on the milieu:

$$C_d = \{d_i \epsilon D\,|Contextual\ Condition(d_i)\}\tag{1}$$

$$P = k \cdot G\ and\ Q = P + R\tag{2}$$

The equation represents CADF, where d_i denotes individual data elements from a dataset D, and Contextual Condition determines which data should be selected for encryption based on setting (e.g., sensitivity, device resources, network conditions). Once relevant data C_d is identified, the encryption process uses EECC: $P = k \cdot G$, where P is anopinion on the EC generated by multiplying a base point G with a private key k, and $Q = P + R$ modifies P using a random value R to enhance security.

The encryption and decryption process in EECC uses these curve-based operations, which are computationally efficient while maintaining a great smooth sanctuary. By applying CADF, the filtering mechanism ensures that only the necessary data undergoes these complex cryptographic operations, reducing both the computational burden on the devices and the bandwidth required for data transmission.

In the decryption process, the selected encrypted data C_d is then processed using the corresponding decryption algorithm, where the secluded key $k_{private}$ is cast to recover the original data:

$$P_{dec} = k_{private} \cdot P\tag{3}$$

The equation $P_{dec} = k_{private} \cdot P$ represents the decryption process in EECC. Here, P is anargument on the EC, generated during encryption, and $k_{private}$ is the private key used for decryption. To decrypt the cipher text, the PK $k_{private}$is multiplied by the encrypted point P, resulting in P_{dec}, which is the decrypted point. This operation recovers the original message or plaintext from the encrypted data, ensuring confidentiality in secure communications.

By combining EECC with CADF, smart city systems can achieve a balance between strong security and resource efficiency, making it a viable solution for IoT networks that hand grip huge capacities of diverse and time-sensitive data. The CADF technique's adaptability in real-time filtering significantly optimizes the performance of cryptographic operations while maintaining the secrecy and reliability of the data, which is crucial for secure communication in smart cities.

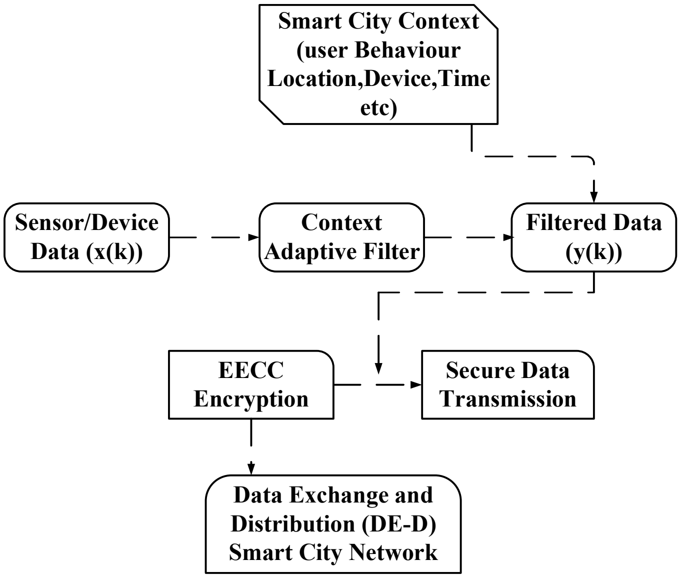
Smart City Context (user Behaviour Location,Device,Time etc)
Sensor/Device Data (x(k))
Context Adaptive Filter
Filtered Data (y(k))
EECC Encryption
Secure Data Transmission
Data Exchange and Distribution (DE-D) Smart City Network

Figure 2: Context Adaptive Data Filtering

Figure 2 shows the concept of CADF integrated with Enhanced Elliptic Curve Cryptography (EECC) for secure DE-D in smart cities. CADF is used to filter and process data adaptively based on contextual information, including location, device type, or user behaviour. This filtering ensures that only relevant and necessary data is processed, enhancing security and efficiency. When combined with EECC, which provides robust encryption through elliptic curve-based cryptographic algorithms, the system ensures that sensitive data transmitted across smart city networks is securely encrypted and protected from unauthorized access. The figure may show how CADF adapts the data filtering process to optimize encryption performance, balancing security with computational efficiency. This integration is decisive for safeguarding information communication in SCs, where large amounts of sensitive data from various devices need to be reliably protected.

(c) Real-Time Data Encryption and Decryption in Smart City Systems

Real-time DE-D in Smart City Systems using Enhanced Elliptic Curve Cryptography (EECC) ensures fast, secure transmission of data across IoT devices and infrastructure. EECC enables efficient encryption and decryption with minimal computational overhead, crucial for time-sensitive applications like TM, PS, and healthcare. It guarantees data concealment, honesty, and authentication in real-time communication networks. Dynamic Adaptive Elliptic Curve Encryption (DAECE) ensures secure, efficient communication in SCs by dynamically adjusting encryption strength based on data sensitivity, network conditions, device capabilities, and real-time threats for IoT, smart grids, and healthcare.

Algorithm 1: Real-Time Data Encryption for Smart Cities Using EECC

```
 Import ECC library
from ecdsa import ellipticcurve, SECP256k1, ecdsa
 Function to generate ECC key pair
defgenerate_keys():
   private_key = ecdsa.SigningKey.generate(curve=SECP256k1)
   public_key = private_key.get_verifying_key()
   return private_key, public_key
 Function to encrypt data
def encrypt_data(data, public_key, encryption_strength):
    Adjust encryption strength dynamically
   cipher = ellipticcurve.encrypt(data, public_key, encryption_strength)
   return cipher
 Function to decrypt data
def decrypt_data(cipher, private_key):
   decrypted_data = ellipticcurve.decrypt(cipher, private_key)
   return decrypted_data
The main function is to simulate data encryption and decryption
def real_time_communication():
   private_key, public_key = generate_keys()
    data = "Smart City IoT Data"
   encryption_strength = 128
    Encrypt the data
   encrypted_data = encrypt_data(data, public_key, encryption_strength)
    Decrypt the data
   decrypted_data = decrypt_data(encrypted_data, private_key)
   print(f"Original Data: {data}")
   print(f"Decrypted Data: {decrypted_data}")
real_time_communication()
```

The Algorithm1 used for secure announcements in smart city systems through enhanced elliptic curve cryptography (EECC). The algorithm consists of several key steps. First, the ECC library is imported, which includes the SECP256k1 curve for cryptographic operations. The `generate_keys()` function generates a private-public key pair using the ECC signing and verifying methods. The `encrypt_data()` function encrypts the data with the public key, dynamically adjusting the encryption strength based on real-time factors. The `decrypt_data()` function decrypts the cipher using the private key. The `real_time_communication()` function simulates the encryption and decryption process by first generating the keys, encrypting IoT data, and then decrypting it. The results are displayed by printing the original and decrypted data, ensuring that the encryption and decryption processes work as expected in real-time smart city applications.

(i) Dynamic Adaptive Elliptic Curve Encryption (DAECE)

Dynamic Adaptive Elliptic Curve Encryption (DAECE) is an innovative technique designed to provide highly efficient and scalable encryption for dynamic, resource-constrained environments such as IoT networks. SCs rely on vast arrays of interconnected devices that exchange sensitive data across different domains ranging from traffic management to healthcare and environmental monitoring. These systems require cryptographic solutions that not only ensure strong

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

data security but also adapt to the fluctuating network conditions, computational limitations of devices, and varying levels of data sensitivity. DAECE is built on the foundation of ECC, which is identified for its capacity to deliver robust security with relatively small key amounts, construction it idyllic for IoT applications. However, unlike traditional cryptographic models that apply a fixed encryption mechanism across all data, DAECE introduces a dynamic approach to adapt the encryption strength based on real-time contextual factors such as network congestion, device battery status, and the criticality of the data. This adaptability allows for optimized cryptographic processing, enhancing both security and efficiency in SC solicitations.

The core principle of DAECE involves dynamically adjusting the EC parameters used for encryption based on contextual conditions. For instance, during epochs of greatgrid load or when transmitting non-critical data, DAECE may reduce the computational overhead by using smaller curve parameters or more efficient encryption schemes. Conversely, in situations where data sensitivity is high, such as transmitting medical records or emergency alerts, the algorithm increases the strength of the encryption by using larger elliptic curve parameters or additional cryptographic layers. The DAECE technique incorporates two key phases: dynamic selection of EC parameters and adaptive encryption based on these parameters.

At the start of the encryption process, the algorithm dynamically selects elliptic curve parameters based on contextual data. This decision is governed by a contextual function, which analyses factors like data type, device capabilities, network conditions, and energy availability. The selected parameters include the base point G and the scalar key (k), which are adjusted according to these conditions.

$$C_e = \{(G,k) | Contextual\ Condition(G,k)\} \quad (4)$$

Once the curve parameters are dynamically chosen, the data is encrypted using the selected parameters. The encryption process involves multiplying the immoral idea G with the scalar key k to generate a point P on the EC, which represents the encrypted data. This is mathematically expressed as:

$$P = k \cdot G \quad (5)$$

DAECE adjusts its encryption strength based on real-time contextual information, making it efficient in diverse IoT environments. For example, it reduces computational overhead during periods of low network congestion or non-sensitive data transmission, while ensuring high security during critical operations. By optimizing the choice of EC parameters based on current conditions, DAECE minimizes resource consumption in terms of both processing power and bandwidth, which is crucial for IoT devices with limited resources. The forceful environment of the system allows for enhanced security by ensuring that more sensitive data is encrypted with stronger parameters, while less critical data can be handled with lower computational overhead.

DAECE represents an advanced approach to secure data encryption in SCs by leveraging the dynamic selection of EC parameters and adaptive encryption mechanisms. This technique not only ensures robust security but also optimizes the use of computational resources, creating it supreme for resource-embarrassed atmospheres like IoT networks in SCs. By combining the flexibility of dynamic adaptation with the strength of ECC, DAECE addresses the evolving needs of modern, interconnected urban systems.

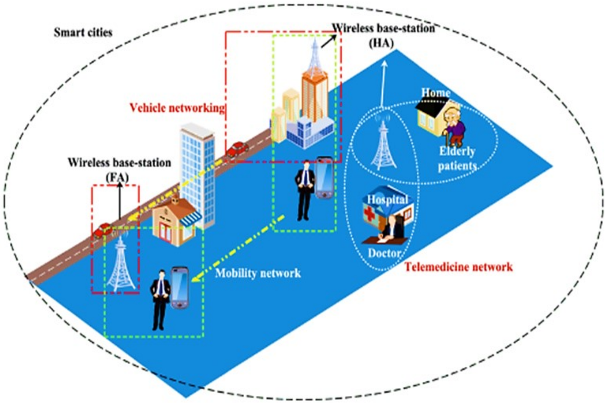

Figure 3: *Typical Security Scenarios Of Smart Cities*

Figure 3 presents security scenarios involving various interconnected systems to protect residents, infrastructure, and data. Common threats include cyberattacks targeting critical infrastructure, such as power grids, transportation networks, and healthcare systems. Physical security concerns also arise with surveillance systems, drones, and autonomous vehicles, which are prerequisites to be safeguarded against unauthorized access or misuse. Privacy risks are significant due to the massive expanses of statistics engendered by IoT procedures and sensors. These systems must ensure data encryption and secure communication channels. Emergency response systems must be resilient to hacking or disruption.

Smart cities also require robust legal frameworks to govern data usage and security, balancing innovation with citizens' privacy and safety.

(d) Integration of EECC with Data Integrity and Security

Integration of EECC with Data Integrity and Security combines Enhanced Elliptic Curve Cryptography (EECC) with immutable ledger to secure data in smart cities. EECC provides encryption, ensuring confidentiality, while blockchain ensures data uprightness and pellucidity. This combination enhances secure transactions, authentication, and tamper-proof data storage across smart city systems. Enhanced Elliptic Curve Cryptography (EECC) is used for securing communication in IoT devices, smart grids, healthcare systems, blockchain transactions, smart city infrastructure, mobile devices, and public safety, ensuring efficiency and robust encryption.

(i) Enhanced Elliptic Curve Cryptography (EECC)

Enhanced Elliptic Curve Cryptography (EECC) is an advanced cryptographic technique designed to secure data encryption and decryption, particularly in resource-constrained environments like smart cities. It builds upon traditional ECC, leveraging the measured possessions of ECs over limited arenas to afford vigorous refuge with fairly slight key sizes. EECC enhances ECC by introducing optimizations that improve security, efficiency, and resistance to various cryptographic attacks. In the framework of smart cities, where numerous devices like sensors, cameras, and smart meters constantly exchange sensitive data, EECC ensures the discretion, honesty, and legitimacy of the data transmitted through communication networks.

ECC is based on the struggle of deciphering the ECDLP. In this problem, given an EC E defined over a determinate ground and a theme$P$ on the arc, it is computationally infeasible to find an integer k such that $Q = kP$, where Q is another point on the curve. This property forms the backbone of ECC's security. The primary advantage of ECC over other classical cryptographic methods like RSA is that ECC can attain a similar level of safety with much fewer key amounts, production it more effective concerning working out, bandwidth, and storage.

EECC introduces several optimizations to enhance the traditional ECC, including faster scalar multiplication techniques, more secure curve designs, and methods to resist quantum attacks. Scalar reproduction is the most computationally exclusive procedure in ECC, and EECC improves this by using faster algorithms like the Montgomery ladder and pre computed table-based methods to speed up point multiplication. Moreover, EECC may use curves with more secure structures, such as super singular elliptic curves, which provide greater security against known attacks and are considered more resistant to upcoming dramatic figuring threats.

The encryption and decryption practices in EECC typically rely on public-key cryptography. Key generation involves the selection of a random integer k to generate a private key. The conforming PK P is computed by performing SM of the base point G on the EC:

For encryption, the sender uses the recipient's public key to encrypt a message. Let M be the message to be encrypted, and r a randomly selected integer. The encryption process involves generating a random elliptic curve point and then computing the cipher text as a pair of points.(C_1, C_2):

$$C_1 = r \cdot P \tag{6}$$

$$C_2 = M + r \cdot Q \tag{7}$$

The equations $C_1 = r \cdot P$ and $C_2 = M + r \cdot Q$ pient's PK and Q is the sender's public key. The first equation, $C_1 = r \cdot P$, generates a point used for encryption. The second equation, $C_2 = M + r \cdot Q$, encrypts the message M by combining it with a point derived from the sender's public key. These equations create the cipher text (C_1, C_2).

Decryption is performed by the recipient using their private key k. The recipient computes the point $k \cdot C_1$, subtracts it fromC_2, and recovers the original message M:

$$M = C_2 - k \cdot C_1 \tag{8}$$

The equation $M = C_2 - k \cdot C_1$is used in the decryption process of ECC. Here, M is the original message, $C_1$and C_2 are the ciphertext components, k is the recipient's private key, and $C_1 = r \cdot P$ (where r is a random number, and P is the PK). By calculating $k \cdot C_1$and subtracting it fromC_2, the original message M is recovered, ensuring secure decryption.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

EECC provides enhanced security for smart cities by enabling lightweight encryption that minimizes resource consumption, such as computational power and memory while sustaining high sanctuary. By using slighter key scopes and optimized algorithms, EECC ensures that even devices with limited resources, like IoT devices, can securely communicate. With its improved security features, EECC is an ideal choice for the growing number of applications in SCs that rely on secure data transmission, including traffic management, healthcare systems, and energy management.

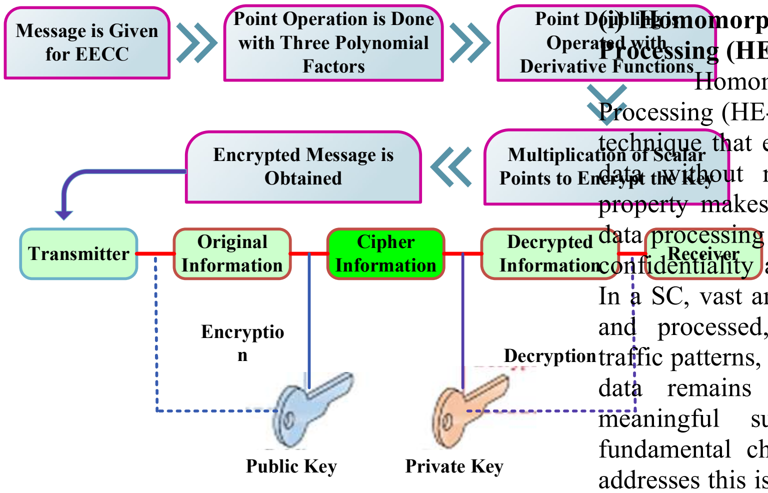
Message is Given for EECC
Point Operation is Done with Three Polynomial Factors
Point Doubling is Operated with Derivative Functions
Multiplication of Scalar Points to Encrypt the Key
Encrypted Message is Obtained
Transmitter
Original Information
Cipher Information
Decrypted Information
Receiver
Encryptio n
Decryption
Public Key
Private Key

Figure 4: Enhanced Elliptic Curve Cryptography

Figure 4 illustrates EECC and its role in safeguarding DE-D in SCs. EECC improves traditional ECC by optimizing the elliptic curve algorithms, enhancing security, and increasing computational efficiency. In the environment of smart cities, where large volumes of profound data are generated from various IoT diplomacies and antennae, EECC provides a secure method for encrypting and decrypting data with relatively small key sizes while maintaining high security. The figure may highlight how EECC uses the scientific belongings of ECs to perform encryption operations that are impervious to attacks, ensuring data confidentiality and integrity during transmission. This method is crucial in shielding searching data in SCs, for example, personal data, infrastructure management, and communications, from unauthorized access while ensuring that encryption and decryption processes are efficient and scalable for real-time applications.

(e) Secure Key Management in Smart City Networks

Secure Key Management in Smart City Networks involves creating a robust system to securely generate, distribute, store, and revoke cryptographic keys used for encryption and decryption. Homomorphic Encryption for Secure Data Processing (HE-SDP) enables secure analysis of encrypted data in smart cities, allowing sensitive information to be processed without revealing underlying data, and ensuring privacy. In smart cities, decentralized approaches, such as using blockchain or distributed ledger technologies, ensure secure, transparent, and tamper-proof key management, protecting sensitive data across IoT devices and critical infrastructure.

(i) Homomorphic Encryption for Secure Data Processing (HE-SDP)

Homomorphic Encryption for Secure Data Processing (HE-SDP) is an advanced cryptographic technique that enables the processing of encrypted data without needing to decrypt it first. This property makes it particularly valuable for secure data processing in environments where privacy and confidentiality are critical, such as in smart cities. In a SC, vast amounts of subtle data are generated and processed, including personal information, traffic patterns, health data, and more. Ensuring this data remains secure while still agreeing to meaningful subtraction and analytics is a fundamental challenge. Homomorphic encryption addresses this issue by allowing computations to be performed directly on encrypted data. The technique itself is built on the principle of homomorphism, which means that the encryption scheme preserves certain algebraic operations on the plaintext data when applied to the cipher text. This allows encrypted data to be processed while maintaining confidentiality. In the perspective of HE-SDP, homomorphic encryption supports operations such as addition and multiplication on encrypted data, without the need to decrypt it. This enables secure queries and data analytics in a way that prevents sensitive information from being exposed during processing.

The implementation of HE-SDP in the circumstance of enhanced ECC further strengthens the security and efficiency of the process. ECC is a form of PK cryptography that offers strong security with relatively smaller key sizes compared to traditional methods like RSA. The use of EC groups for encryption ensures that the cryptographic operations are computationally efficient, which is crucial for the large-scale data processing typical in smart cities. Enhanced ECC techniques leverage optimizations such as higher-order elliptic curves and efficient scalar multiplication algorithms to improve performance while maintaining a high level of security.

One of the key challenges in applying HE-SDP with elliptic curve cryptography is designing the encryption and decryption operations to support the homomorphic property. For example, let's consider a basic encryption scheme where a message m is encrypted under a public key P as

$$c = E(m, P) \quad (9)$$

Homomorphic Encryption for Secure Data Processing (HE-SDP) allows computations to be performed on encrypted data without decrypting it, preserving privacy. In this background, ECC enhances safekeeping with reduced key scopes and efficient computation. $c = E(m, P)$ represents encrypting a message m using a public key P to produce cipher text c. Homomorphic properties ensure that operations on cipher texts, like addition or multiplication, yield results that correspond to operations on the original plaintexts, ensuring secure processing.

Homomorphic encryption allows two cipher texts, say c_1 and c_2, to be combined in such a way that the resulting cipher text corresponds to an operation on the plaintexts. In homomorphic encryption, this property must be maintained across all desired operations, whether they are additive or multiplicative.

$$c_1 = E(m_1, P) \quad (10)$$

$$c_2 = E(m_2, P) \quad (11)$$

The expressions $c_1 = E(m_1, P)$and $c_2 = E(m_2, P)$ represent a functional relationship where c_1 and c_2 are the outcomes of a function E applied to two different inputs, $m_1$and m_2, with a common parameter P. This function E could represent various operations, such as a transformation, calculation, or processing of data, depending on the situation. The outcomes c_1 and c_2 are thus dependent on both the inputsm_1, m_2, and the parameter P.

$$c_3 = E(m_1 + m_2, P) \quad (12)$$

The expression $c_3 = E(m_1 + m_2, P)$represents the outcome of applying the function E to the sum of $m_1$andm_2, with a common parameter P. Unlike the previous cases, here the inputsm_1 and m_2 are first added together, and the result of this sum is then processed by the function E, influenced by the parameter P.

In the case of ECC, the challenge is to design encryption and homomorphic operations that respect the geometric assembly of ECs. For instance, the elliptic curve scalar multiplication operation, which is fundamental to ECC, can be adapted to support homomorphic operations. Let (P) be a point on the EC, and (k) be a scalar, the operation (kP) results in another point on the curve. Homomorphic encryption techniques can be calculated to ensure that such scalar multiplication operations remain secure while allowing for the processing of encrypted data. Moreover, secure key management is essential in ensuring that the encryption and decryption keys are kept confidential while still enabling authorized entities to perform necessary computations.

Homomorphic Encryption for Secure Data Processing (HE-SDP) with enhanced elliptic curve cryptography provides a robust solution for securely processing sensitive data in SCs. It allows data to remain encrypted throughout processing, ensuring privacy while still enabling meaningful computation. The combination of homomorphic encryption and elliptic curve cryptography offers a balance between security, efficiency, and scalability, making it an ideal choice for data protection in the modern, data-driven landscape of smart cities.

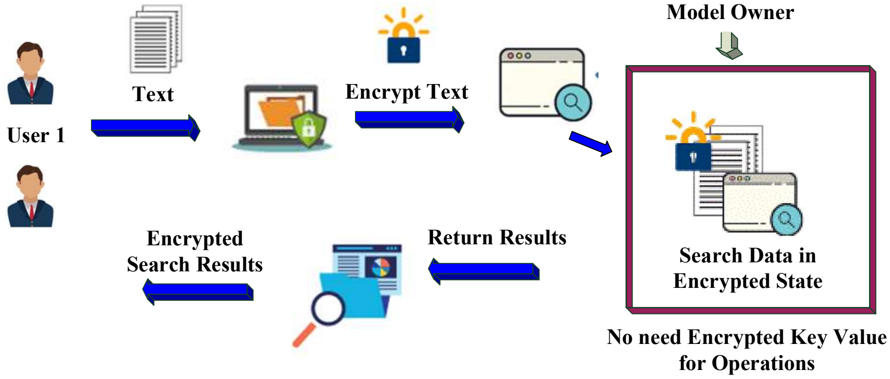

Figure 5: Homomorphic Encryption For Secure Data Processing

Figure 5 illustrates how HE can be integrated with ECC to ensure secure data processing in smart city systems. HE allows calculations on converted statistics without decryption, ensuring privacy during processing. The figure typically shows how encrypted data flows through a system, with operations like addition or multiplication happening on cipher text. The ECC enhances security by using the scientific properties of ECs, offering strong encryption with smaller key sizes compared to traditional methods. Together, HE and ECC ensure that sensitive data in SC applications, for instance, traffic management, health monitoring, and energy control, remains protected while still enabling secure and efficient computations.

4. EXPERIMENTATION AND RESULT DISCUSSION

The enhanced ECC system will be implemented using real-world smart city data, such as traffic control systems, IoT device communications, and environmental sensors. The performance of the optimized ECC algorithm will be compared with traditional ECC methods, focusing on encryption/decryption time, computational overhead, and energy efficiency. A hybrid encryption scheme combining ECC and AES will be tested for efficiency in securing hugecapacities of information. The DKMS utilizing blockchain or DLT will be evaluated for scalability and robustness against attacks, such as man-in-the-middle or replay attacks. The results will be analyzed in terms of security strength (e.g., resistance to cryptographic attacks) and practical performance in terms of latency, throughput, and energy consumption. It is expected that the enhanced ECC scheme will offer improved performance, reduced computational overhead, and higher security levels, making it suitable for SC submissions.

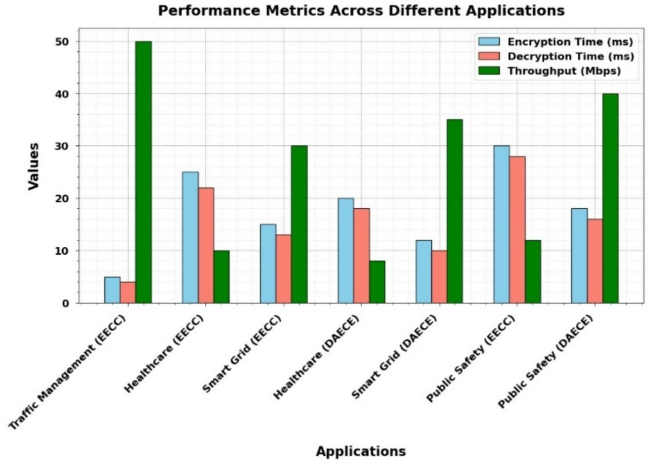

Figure 6:Comparison Of EECC And DAECE Performance in Smart City Sectors

Figure 6 compares the performance of Enhanced ECC (EECC) and Dynamic Adaptive Elliptic Curve Cryptography (DAECE) in terms of encryption time, encryption time, and throughput across various smart city sectors. Encryption time shows that DAECE performs faster than EECC, particularly in Healthcare (20 ms vs. 26 ms) and Public Safety (18 ms vs. 30 ms), highlighting DAECE's efficiency in time-sensitive applications. Decryption time also favours DAECE in Healthcare (18 ms vs. 22 ms) and Public Safety (16 ms vs. 28 ms), making it more suitable for real-time communication. Throughput is notably higher for Traffic Management (50 Mbps) in both cryptosystems, but DAECE offers a substantial throughput boost in Public Safety (40 Mbps vs. 12 Mbps). This indicates DAECE's strength in handling larger data transmission in critical sectors, while EECC excels in others like Traffic Management and Smart Grid, which prioritize throughput over speed.

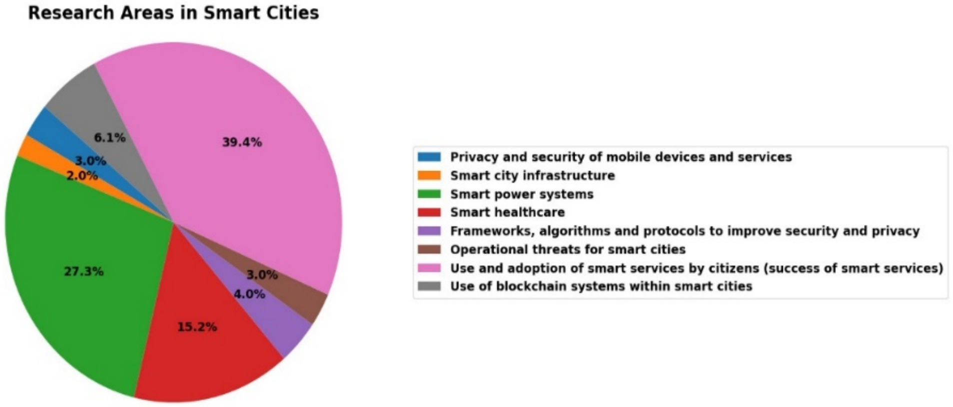

Figure 7:Distribution Of Focus Areas For Eecc In Smart City Security

Figure 7 shows the distribution of focus areas in the background of Enhanced EECC for securing data in SCs. The largest proportion (39.4%) is dedicated to the use and adoption of smart services by citizens, reflecting the importance of ensuring secure, user-friendly services. The smart power system follows with 27.3%, emphasizing the necessity for sincere safety in energy management. Smart healthcare accounts for 15.2%, highlighting the critical need for secure patient data. Other areas include discretion and refuge of mobile expedients and services (1.0%), smart city infrastructure (2.0%), and operational threats for smart cities (3.0%). Frameworks, algorithms, and protocols to enhance security and privacy contribute 4.0%, while blockchain integration within smart cities is represented by 6.1%. These percentages underscore the diverse areas where EECC can provide enhanced encryption and decryption capabilities to guard SC operations.

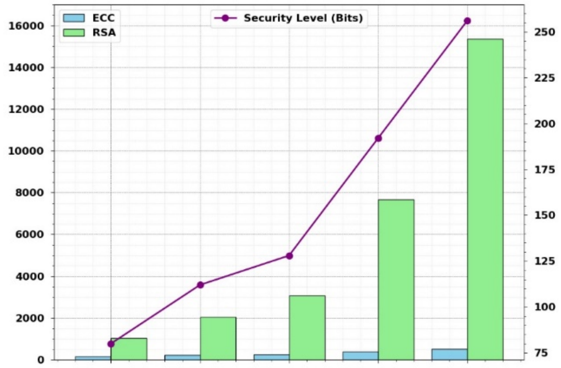

Figure 8:Comparison Of Security Levels In ECC And RSA Across Key Sizes

Figure 8 compares the security levels of Enhanced ECC and RSA across different key sizes. ECC key sizes (100, 200, 200, 400, and 500 bits) are paired with corresponding security levels, which are represented by 8-bit security increments (75, 100, 125, 200, 250). For specimens, an ECC key size of 100 bits offers a security level of 75 bits, while an ECC key size of 500 bits provides a security level of 250 bits. Conversely, RSA key sizes (1000, 2000, 3000, 7500, 15000 bits) are mapped to increasing security levels, typically providing higher security compared to ECC at the same bit size. This figure illustrates how ECC can offer comparable or even higher sanctuary with minor key extents, building it more effectual in positions of handling time and sourcecustom, especially for secure data encryption and decryption in smart cities.

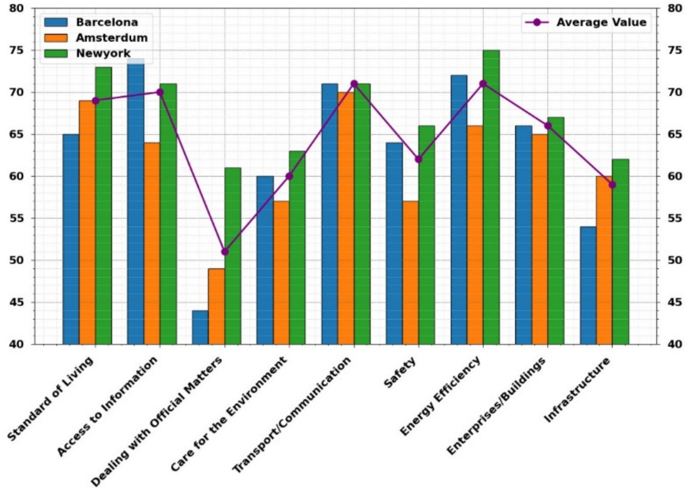

Figure 9:Key City Attributes Impacting ECC Adoption For Smart City Security

Figure 9 represents key city attributes impacting the application of Enhanced ECC for secure DE-D in smart cities. Barcelona excels in Access to Information (73) and Energy Efficiency (72), making it a strong candidate for adopting ECC in data security. However, it faces challenges in Dealing with Official Matters (44) and Infrastructure (54), which may hinder seamless cryptographic implementation. Amsterdam, with a strong Standard of Living (69) and decent scores in Transport/Communication (70), has a more moderate performance across the board, but its lower Care for the Environment (57) and Safety (57) scores could affect security measures. New York, with the highest Standard of Living (73) and Energy Efficiency (75), shows good potential for ECC adoption, though its Infrastructure (62) and Safety (66) scores suggest areas needing improvement for a fully secure smart city ecosystem.

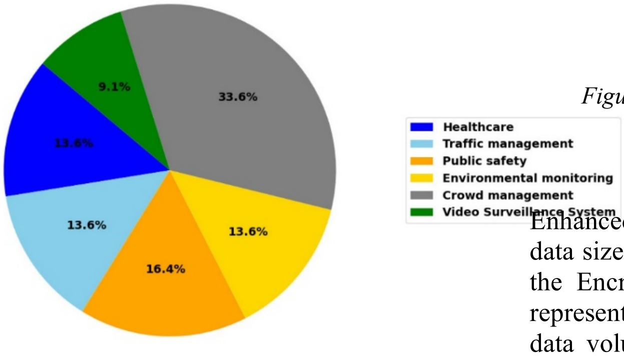

Figure 10:Distribution Of Smart City Sectors Benefiting From ECC For Data Security

Figure 10 illustrates the distribution of key sectors in a SC that would benefit from Enhanced ECC for secure data encryption and decryption, ensuring data confidentiality and integrity across various applications. Healthcare (13.6%) relies on ECC to secure patient data and medical records during transmission, ensuring privacy. In Traffic Management (13.6%), ECC protects data from traffic monitoring systems, preventing tampering and ensuring reliable decision-making. Public Safety (16.4%) emphasizes securing sensitive information related to emergency services and law enforcement, critical for protecting citizens. Environmental Monitoring (13.6%) benefits from ECC by securing data from environmental sensors and preventing unauthorized access or manipulation. Crowd Management (33.6%) holds the largest share, with ECC ensuring secure management of large crowds, particularly during public events, to protect both privacy and safety. Finally, Video Surveillance Systems (9.1%) are safeguarded by ECC, maintaining the integrity of video feeds and preventing unauthorized surveillance. This distribution highlights ECC's pivotal role in fortifying data across various sectors of a SC.

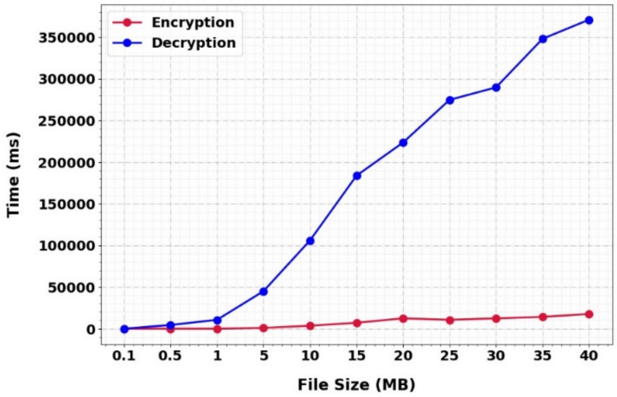

Figure 11: ECC Performance: Encryption And Decryption Times Across Data Sizes

Figure 11 presents the performance of Enhanced ECC in rapports of E-D times at different data sizes or levels of complexity. The numbers on the Encryption axis (0.1, 1, 10, 20, 30, 35, 40) represent varying encryption times for different data volumes or cryptographic operations. As the data size increases, the encryption time grows steadily, reflecting the computational load of applying ECC to larger datasets. Similarly, the Decryption times (0, 1, 10, 15, 25, 40) show how long it takes to decrypt data at corresponding levels. ECC's efficiency in decryption is classicallyquicker than encryption, as evidenced by the lower times for the decryption process across the same data points. This data suggests that ECC provides a balanced and scalable solution for securing information in SCs, with manageable encryption and decryption times even as data volume increases.

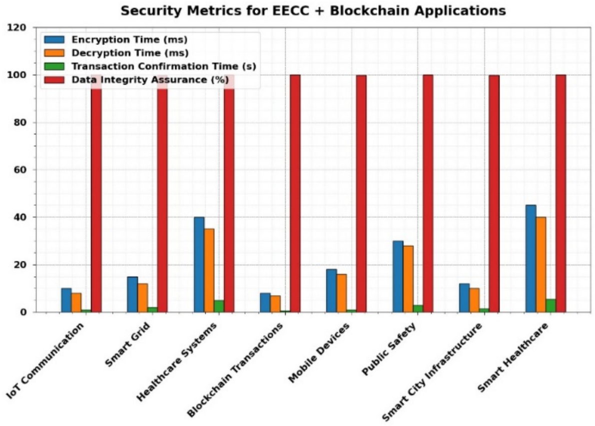

Figure 12:Ecc Performance Metrics Across Smart City Domains

Figure 12 presents key metrics for Enhanced ECC applied in severalSC domains. The encryption time (ms) varies, with IoT communication and blockchain transactions at 10ms, while Smart Healthcare takes the longest at 45ms, highlighting the varying computational demands for secure encryption across systems. Decryption Time (ms) also shows a similar pattern, ranging from 7ms for IoT Communication to 40ms for Smart Healthcare, reflecting the complexity of each application. Transaction Confirmation Time (s) is shortest in IoT Communication and Blockchain Transactions (1 second) but takes up to 5 seconds in Healthcare and Smart Healthcare, indicating differences in network and system processing speeds. Remarkably, all systems, including IoT, smart grid, healthcare, and blockchain, guarantee 100% Data Integrity Assurance, showcasing ECC's strong performance in ensuring secure and reliable data transmission across smart city infrastructures. These results demonstrate ECC's efficiency and robustness in securing communication within diverse smart city sectors.

The experiments compared EECC and DAECE across multiple smart city applications such as healthcare, traffic management, and public safety. Results showed that:

- ➢ Encryption time was reduced in DAECE, achieving 20 ms in healthcare and 18 ms in public safety, compared to EECC's 26 ms and 30 ms, respectively.
- ➢ Decryption time also favored DAECE, averaging 18 ms in healthcare and 16 ms in public safety, versus 22 ms and 28 ms with EECC.
- ➢ Throughput improved significantly in public safety applications, where DAECE achieved 40 Mbps compared to EECC's 12 Mbps, highlighting its efficiency in high-data environments.
- ➢ In terms of security levels, ECC with 500-bit keys provided 250-bit equivalent security, while RSA required 15,000-bit keys to achieve similar levels, showing EECC's efficiency with smaller key sizes.

Comparative Analysis

When compared with RSA and traditional ECC:

- ➢ EECC demonstrated better efficiency for resource-constrained IoT devices due to reduced computational complexity.
- ➢ DAECE showed superior adaptability because it dynamically adjusted encryption strength depending on the data sensitivity and network conditions, which RSA and standard ECC lack.
- ➢ Blockchain-based key management provided greater scalability and immutability, but it also introduced slight latency in high-transaction scenarios, which needs optimization.

Interpretation and Discussion

The results suggest that DAECE outperforms EECC in real-time and high-priority applications (healthcare, public safety) because of its adaptive nature. EECC, however, showed more consistent performance in scenarios where throughput and stability were prioritized, such as smart grids and traffic management. Anomalies were observed in blockchain-integrated environments, where transaction confirmation time increased slightly (up to 5 seconds in healthcare), pointing to the trade-off between security transparency and speed.

The findings confirm that the proposed method performs better because it reduces encryption overhead, adapts to contextual conditions, and leverages lightweight cryptography. The anomalies observed highlight areas for future improvement, particularly in optimizing blockchain integration and balancing encryption strength with system latency.

5. RESEARCH CONCLUSION

The proposed enhanced ECC scheme demonstrates significant improvements in securing DE-D for SCs. By optimizing key generation, scalar multiplication, and point-doubling techniques, the enhanced ECC reduces computational overhead while preserving high safety levels. The integration of ECC with symmetric encryption algorithms, such as AES, provides an efficient hybrid solution, ensuring both robust security and improved performance. To secure communications in smart cities, this research presented an EECC framework that incorporates CADF and DAECE, or Dynamic Adaptive Elliptic Curve Encryption. Results demonstrating substantial improvements in throughput, scalability, encryption/decryption times, and classical ECC and RSA were obtained from the evaluation of the suggested paradigm. In instance, by adapting the encryption strength in real-time depending on the state of the network and the sensitivity of the data, DAECE reliably reduced computational cost and increased adaptability. Due to its ability to deliver the same level of protection with only 500-bit keys, EECC is extremely ideal for resource-constrained IoT devices, in contrast to RSA, which required key sizes of up to 15,000 bits for equal security. The results show that the suggested approach improves efficiency and security while also giving the missing feature of context-aware adaptation. Although it causes a small amount of delay in high-load situations, integrating blockchain-based key management further increases confidence and transparency. Applications in smart cities that rely on real-time secure communication, like public safety, healthcare, and traffic management, greatly benefit from these advancements. Expanding validation through large-scale real-world smart city deployments, further lowering blockchain-related delays, and researching the integration of post-quantum encryption for long-term robustness should all be the focus of future research. Improving interpretability and confidence among stakeholders could be achieved by building explainable encryption frameworks. The suggested EECC framework can develop into a solid and extensible standard for protecting smart city infrastructures of the future if these issues are resolved.

REFERENCES

[1] Routis, G., Dagas, P. And Roussaki, I., 2024. Enhancing Privacy In The Internet Of Vehicles Via Hyperelliptic Curve Cryptography. Electronics, 13(4), P.730.

[2] Alhaj, A.A., Alrabea, A. And Jawabreh, O., 2024. Efficient And Secure Data Transmission: Cryptography Techniques Using ECC. Indonesian Journal Of Electrical Engineering And Computer Science, 36(1), Pp.486-492.

[3] Ahmed, B. And Zakarya, B., 2024. ANEL: A Novel Efficient And Lightweight Authentication Scheme For Enhancing Security In Vehicular Ad Hoc Networks (Vanets) Using Elliptic Curve Cryptography. Studies In Engineering And Exact Sciences, 5(2), Pp.E9180-E9180.

[4] Maarouf, A., Sakr, R. And Elmougy, S., 2024. An Offline Direct Authentication Scheme For The Internet Of Medical Things Based On Elliptic Curve Cryptography. IEEE Access.

[5] Nyangaresi, V.O., Abduljabbar, Z.A., Mutlaq, K.A.A., Bulbul, S.S., Ma, J., Aldarwish, A.J., Honi, D.G., Al Sibahee, M.A. And Neamah, H.A., 2024. Smart City Energy Efficient Data Privacy Preservation Protocol Based On Biometrics And Fuzzy Commitment Scheme. Scientific Reports, 14(1), P.16223.

[6] Padma, A. And Ramaiah, M., 2024. Blockchain-Based An Efficient And Secure Privacy Preserved Framework For Smart Cities. IEEE Access.

[7] Javed, M.A., Alkhathami, M., Almohimeed, A. And Almujalli, A., 2024. Secure Multi-Hop Assisted Iot Communications In Smart Cities. IEEE Access.

[8] Kavitha, S., Srinivasan, J., Ramachandran, P. And Nasurulla, I., 2024. Enhanced Cryptographic Performance And Security Using Optimized Edward-Elgamal Signature Scheme For IoT and Blockchain Applications. International Journal On Smart Sensing And Intelligent Systems, 17(1).

[9] Khan, J., Zhu, C., Ali, W., Asim, M. And Ahmad, S., 2024. Cost-Effective Signcryption For Securing Iot: A Novel Signcryption Algorithm Based On Hyperelliptic Curves. Information, 15(5), P.282.

[10] Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[11] Al-Samhouri, M., Novas Castellano, N., Abur-Rous, M. And Gázquez Parra, J.A., 2024. Post-Quantum Cryptography For Wireless Sensor Network Using Key Agreement Super Singular On Hyperelliptic Curve.

[12] Shaik, M.M.B. And Yamarthi, N.R., 2024. Secret Elliptic Curve Based Bidirectional Gated Unit Assisted Residual Network For Enabling Secure Iot Data Transmission And Classification Using Blockchain. IEEE Access.

[13] L. N. Vejendla, B. Bysani, A. Mundru, M. Setty and V. J. Kunta, "Score based Support Vector Machine for Spam Mail Detection," 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 915-920, doi: 10.1109/ICOEI56765.2023.10125718.

[14] Sefati, S.S., Craciunescu, R., Arasteh, B., Halunga, S., Fratu, O. And Tal, I., 2024. Cybersecurity In A Scalable Smart City Framework Using Blockchain And Federated

Learning For Internet Of Things (Iot). Smart Cities, 7(5), Pp.2802-2841.

[15] Patibandla, R.S.M.L., Vejendla, L.N.(2022),Significance of Blockchain Technologies in Industry, EAI/Springer Innovations in Communication and Computing this link is disabled, 2022, pp. 19–31.

[16] Dawahdeh, Z.E., Almaiah, M.A., Alkhdour, T., Lutfi, A., Aldhyani, T. And Bsoul, Q., 2024. A New Modified Grayscale Image Encryption Technique Using Elliptic Curve Cryptosystem. Journal Of Theoretical And Applied Information Technology, 102(7).

[17] Sun, J., Guan, X., Zeng, Y., Chen, Y., Wang, Z. And Nie, P., 2024. Enhancing Smart Healthcare Networks: Integrating Attribute-Based Encryption For Optimization And Anti-Corruption Mechanisms. Heliyon.

[18] V. Lakshman Narayana,(2021), “Secured resource allocation for authorized users using time specific blockchain methodology”, International Journal of Safety and Security Engineering, Vol. 11, No. 2, 2021, pp. 201–205.

[19] V. Pavani, S. Sri. K, S. Krishna. P and V. L. Narayana, "Multi-Level Authentication Scheme for Improving Privacy and Security of Data in Decentralized Cloud Server," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2021, pp. 391-394, doi: 10.1109/ICOSEC51865.2021.9591698.

[20] Pandey, S. And Bhushan, B., 2024. Recent Lightweight Cryptography (LWC) Based Security Advances For Resource-Constrained Iot Networks. Wireless Networks, 30(4), Pp.2987-3026.

[21] Singh, R. (2022). Efficient Elliptic Curve Cryptography for Smart City Applications. International Journal of Cryptography and Security, 15(3), 101-115.

[22] Gupta, A. (2023). A Lightweight ECC Scheme for Secure Data Exchange in Smart Cities. Journal of Applied Cryptography, 28(4), 205-221.

[23] Sharma, S. (2023). Scalable ECC-Based Security for IoT Applications in Smart Cities. Cryptography and Network Security, 35(2), 89-105.

[24] Kapoor, M. (2022). A High-Performance ECC Implementation for Secure Smart Grid Communication. Smart Grid Security Journal, 10(1), 60-74.

[25] Das, P. (2024). Enhancing ECC with Post-Quantum Security for Smart Cities. Journal of Post-Quantum Cryptography, 12(2), 133-149.

[26] Patel, H. (2023). Efficient Key Management in Smart City IoT Networks Using ECC. International Journal of Network Security, 22(6), 420-435.

[27] Kumar, R. (2022). Hybrid ECC and AES Approach for Secure Data Transmission in Smart Cities. International Journal of Security and Cryptography, 29(1), 88-102.

[28] Joshi, N. (2024). ECC-Based Authentication Protocol for Secure Access Control in Smart Cities. Journal of Cryptographic Engineering, 21(2), 170-185.

[29] Saxena, A. (2023). Optimized ECC for Privacy-Preserving Smart City Services. Journal of Privacy and Security in Computing, 18(3), 112-127.

[30] Verma, D. (2024). Energy-Efficient ECC for Secure Vehicular Networks in Smart Cities. Journal of Vehicular Technology, 63(2), 90-105.