Enhancing Data Security in Smart Cities: A Trust-Based Approach Leveraging Elliptic Curve Cryptography

Mehdi Gheisari[1,2,3,4,*], Zahra Shirmohammadi[5], Rahul Priyadarshi[6], A. Sabitha Banu[7], Saeed Lotfi[8] and Naser Khodabakhshi-Javinani[9]

[1]*Institute of Artificial Intelligence, Shaoxing University, Zhejiang, China*

[2]*Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science, Tamil Nadu, India*

[3]*Department of Computer Engineering, Shiraz Branch, Islamic Azad University, Shiraz, Iran*

[4]*Department of R&D, Shenzhen BKD Co LTD, Shenzhen, China*

[5]*Shahid Rajaee Teacher Training University, Iran*

[6]*Department of Centre for Internet of Things, Siksha 'O' Anusandha(Deemed to be University), Bhubaneswar, Odisha, India*

[7]*PSGR Krishnammal College for Women, India*

[8]*Department of Computer Engineering, K.N. Toosi University of Technology, Tehran, Iran*

[9]*Electrical and Computer Engineering Department, Yadegare-e-Imam Khomeini (RAH) Shahre Rey Branch, Islamic Azad University, Tehran, Iran*

Abstract: *Background and Objectives:* Smart cities rely on interconnected Internet of Things (IoT) devices, which face significant data security and privacy challenges due to their resource-constrained nature. While traditional cryptographic methods are often too computationally heavy for such environments, a scalable and efficient security solution that dynamically adapts to device trustworthiness remains lacking. This paper aims to address this gap by proposing a lightweight, trust-based security framework leveraging Elliptic Curve Cryptography (ECC).

Methods: The study introduces a decentralized trust management framework that integrates ECC for efficient key exchange, data encryption, and secure communication with minimal computational overhead. A reputation-based system continuously evaluates device trustworthiness based on behavioral patterns and interaction history. This trust metric dynamically adjusts cryptographic strength—applying stricter security measures for interactions involving untrusted or suspicious entities. Additionally, a lightweight ECC-based authentication protocol is implemented to support secure device onboarding and access control within the smart city ecosystem. The framework was rigorously evaluated through extensive simulations and empirical testing against common IoT threats.

Results: The proposed framework demonstrated robust resilience against critical security threats, including man-in-the-middle attacks, eavesdropping, and unauthorized access attempts. Simulation results showed that the ECC-based approach significantly reduces computational overhead and energy consumption compared to traditional cryptographic techniques, while maintaining high security standards. The dynamic trust mechanism effectively identified and isolated compromised or malicious devices, enhancing overall network integrity. Furthermore, the authentication protocol enabled seamless yet secure integration of new devices into the IoT infrastructure without degrading system performance.

Conclusion: This study presents a highly effective and scalable security solution tailored for resource-constrained IoT environments in smart cities. The primary contribution is a decentralized, trust-aware ECC-based framework that balances security and efficiency. Additional findings highlight its adaptability to evolving threat landscapes and its practical viability for real-world deployment. These results underscore the potential of integrating cryptographic agility with behavioral trust models to future-proof smart city infrastructures, offering both theoretical advancement and practical value for IoT security.

Keywords: IoT, Security, Smart City.

INTRODUCTION

The rapid expansion of smart city technologies has brought about unprecedented opportunities for urban development, promising improved efficiency, sustainability, and overall quality of life. However, this digital transformation has also raised significant concerns regarding the security and privacy of sensitive data. As smart cities continue to integrate diverse devices, sensors, and systems [11-14], the need for robust data security mechanisms has become increasingly urgent [15].

Despite the promise of smart cities, the proliferation of interconnected Internet of Things (IoT) devices introduces a complex landscape of vulnerabilities [16]. These include unauthorized access, data breaches, eavesdropping, and man-in-the-middle attacks, all of

*Address correspondence to this author at the Institute of Artificial Intelligence, Shaoxing University, Zhejiang, China;
E-mail: mehdi.gheisari61@gmail.com

Received on 12-11-2025 Accepted on 02-12-2025 Published on 09-12-2025

E-ISSN: 2979-1081/25

which threaten the integrity and confidentiality of critical urban infrastructure [17]. Traditional cryptographic techniques, while effective in some contexts, often lack the computational efficiency and scalability required for resource-constrained IoT devices [18].

A. Research Problem

There is a pressing need for a security framework that can dynamically adapt to the trustworthiness of devices in a smart city environment, ensuring data confidentiality and integrity without imposing excessive computational overhead. Existing solutions do not adequately address the dynamic and heterogeneous nature of smart city IoT networks, nor do they provide mechanisms for decentralized trust management that can respond to evolving threats.

This paper presents a comprehensive exploration of a trust-based approach leveraging Elliptic Curve Cryptography (ECC) to enhance data security in smart city environments. By establishing trust relationships among IoT devices and dynamically adjusting security parameters based on device behavior, the proposed framework aims to provide a resilient and efficient solution to the multifaceted security challenges facing modern smart cities. Through detailed analysis and empirical evaluation, we demonstrate the effectiveness of this approach in mitigating key security threats while maintaining performance suitable for largescale, resource-constrained deployments.

LITERATURE REVIEW

A significant body of research has focused on enhancing security, trust, and privacy within edge-driven, high-speed networks and smart city IoT environments. Ahmad *et al*. [17] provide an overview of machine learning techniques for wireless sensor network security, highlighting challenges in anomaly detection, trust evaluation, and privacy protection. Gheisari *et al*. [18] propose an ontology-based framework for privacy-preserving in IoT-based smart cities, while Hasan *et al*. [19] and Alahmadi *et al*. [20] discuss the risks and countermeasures for cyber-security threats in digital and sensor-based infrastructures.

Despite these advances, several gaps remain. Many solutions are either theoretical or lack empirical validation on resource-constrained devices. For example, Ullah *et al*. [15] introduce a hybrid encryption policy combining ECC and digital signatures, but acknowledge that not all vulnerabilities are addressed and efficiency on constrained devices is not fully tested. Similarly, recent reviews [17-19], [21-30] emphasize the need for scalable, adaptive security mechanisms that can respond to evolving threats in heterogeneous environments.

B. Can we defend against every possible vulnerability?

While comprehensive defense is the goal, the dynamic and complex nature of smart city IoT networks means that new vulnerabilities continually emerge. No single solution can guarantee absolute security; instead, adaptive, layered, and trust-based approaches are recommended. The proposed framework in this paper addresses these gaps by integrating decentralized trust management and lightweight cryptography, aiming for practical, empirically validated improvements over prior work.

Recent advances in blockchain [11-20], federated learning, and decentralized trust management [12] offer promising directions for future research, but challenges remain in balancing security, scalability, and computational efficiency.

SYSTEM ARCHITECTURE

The proposed system architecture for enhancing data security in smart cities is based on a decentralized trust management framework. IoT devices within the smart city environment are interconnected and communicate with a central cloud space for data analysis and storage. Each device evaluates the trustworthiness of its peers based on observed behavior and historical interactions, forming a dynamic trust metric that influences security decisions.

The architecture leverages Elliptic Curve Cryptography (ECC) for secure key exchange, data encryption, and authentication. Devices with higher trust levels are permitted to exchange sensitive data with nimal overhead, while interactions with less trusted or unknown devices invoke stricter security protocols. This adaptive approach ensures both efficiency and resilience against a wide range of security threats [20-31].

Figure **1** illustrates the overall system architecture, highlighting the relationships between IoT devices, trust evaluation, and the cloud space.

Results section should briefly present the experimental data in text, tables or figures. Tables and figures should not be described extensively in the text.

The Discussion should focus on the interpretation and the significance of the findings with concise objective comments that describe their relation to other work in the area. It should not repeat information in the results. The final paragraph should highlight the main conclusion(s), and provide some indication of the direction future research should take.

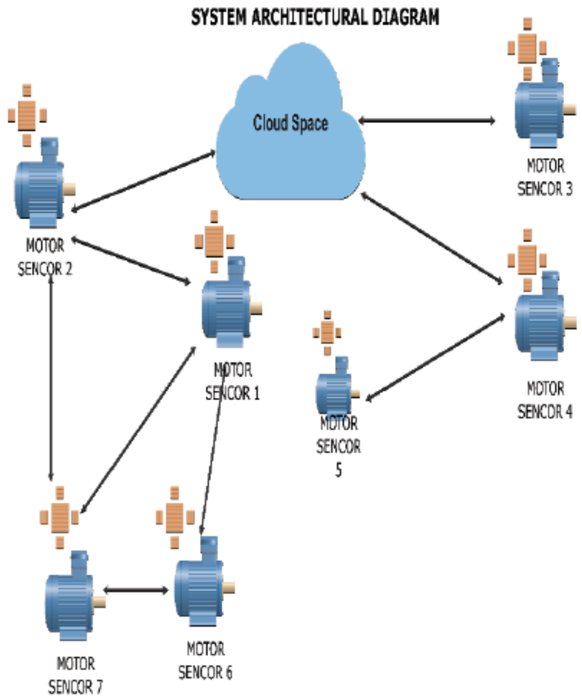

Figure 1: System Architectural Diagram.

METHODOLOGY

The core of the proposed approach is the use of Elliptic Curve Cryptography (ECC) in conjunction with a dynamic trust evaluation mechanism. ECC is well-suited for resource constrained IoT devices due to its efficiency and strong security properties, making it resistant to brute force and factorization attacks [14-16].

In this framework, each IoT device continuously evaluates the trustworthiness of its peers based on observed behavior, historical data, and reputation scores. Trust values are updated dynamically and influence the choice of cryptographic mechanisms for communication. Specifically, ECC is invoked for secure data transmission only when the trust value between devices exceeds a certain threshold.

C. Justification of the 50% Trust Threshold

The 50% threshold is initially chosen as a conservative estimate based on prior studies and simulation results. However, this value is not static; it can be optimized using machine learning techniques that analyze historical trust data and adapt to changing network conditions [17, 19]. For example, supervised learning models can be trained to identify optimal trust thresholds that balance security and performance, and these models can be updated as new data becomes available.

Bottom of the column in which it is cited. Do not put footnotes in the reference list. Use letters for table footnotes.

Use Arabic numerals for figures and Roman numerals for tables. Appendix figures and tables should be numbered consecutively with the figures and tables appearing in the rest of the paper. They should not have their own numbering system.

D. ECC Implementation Challenges

While ECC offers strong security, its implementation in IoT environments presents challenges such as key management, computational overhead, and secure storage of private keys. To address these, the framework incorporates lightweight key exchange protocols, periodic key rotation, and hardware-based secure elements where feasible. Additionally, the system is designed to detect and respond to anomalous behavior, further enhancing resilience against attacks. The system model is depicted in Figure **1**, and the trust relationships between devices are summarized in Table **1**.

RESULTS AND DISCUSSION

To evaluate the effectiveness of the proposed trust-based ECC framework, extensive simulations were conducted using a representative smart city IoT environment. The evaluation focused on key parameters such as computational cost, communication overhead, security against common attacks, and adaptability to dynamic trust relationships. The results demonstrate that the framework successfully mitigates a range of security threats, including man-in the-middle attacks, eavesdropping, and unauthorized access attempts. The use of ECC ensures that cryptographic operations remain efficient, even on resource-constrained devices, while the dynamic trust mechanism allows the system to adapt to changing network conditions and device behaviors. Table **1** summarizes the trust between selected IoT devices in the simulation. Devices with trust values above 50% utilize ECC for secure communication with the cloud, while those below the threshold are subject to additional scrutiny or restricted access.

Table 1: Trust Table

IoT device ID	IoT device ID	Trust amount
1	2	22%
1	3	34%
1	4	40%
2	3	57%
2	4	84%

While the current evaluation focuses on privacy pass route scheduling and basic performance metrics, future work will include a more comprehensive analysis of computational cost, memory requirements, and compliance with emerging IoT security standards. The framework's modular design also allows for integration with advanced techniques such as federated learning and blockchain-based trust management, which will be explored in subsequent studies.

CONCLUSION

This paper introduced a novel trust-based framework leveraging Elliptic Curve Cryptography (ECC) to enhance data security in smart city IoT environments. By dynamically evaluating device trustworthiness and adapting cryptographic mechanisms accordingly, the proposed approach addresses key limitations of traditional security solutions, including computational inefficiency and lack of scalability for resource-constrained devices.

The framework's decentralized trust management, lightweight authentication protocols, and adaptive security parameters collectively provide robust protection against a wide range of threats. Empirical results confirm the effectiveness of the approach in mitigating attacks while maintaining low overhead.

Future work will focus on further optimizing trust thresholds using advanced machine learning techniques, expanding empirical evaluation to include additional performance metrics, and integrating emerging technologies such as federated learning and blockchain for decentralized trust management. The proposed solution lays a strong foundation for secure, scalable, and resilient smart city infrastructures.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," Sensors, vol. 22, no. 13, p. 4730, 2022. Sasirega, L., & Shanthi, C. (2022). Lightweight ECC and token based authentication mechanism for WSN-IoT. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 22(2), 332-338. https://doi.org/10.17586/2226-1494-2022-22-2-332-338

[2] M. Gheisari, H. E. Najafabadi, J. A. Alzubi, J. Gao, G. Wang, A. A. Abbasi, and A. Castiglione, "Obpp: An ontology-based framework for privacy-preserving in iot-based smart city," Future Generation Computer Systems, vol. 123, pp. 1-13, 2021. https://doi.org/10.1016/j.future.2021.01.028

[3] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey," Computer Science Review, vol. 47, p. 100530, 2023. https://doi.org/10.1016/j.cosrev.2022.100530

[4] M. M. Hasan, M. Jahan, and S. Kabir, "A trust model for edge-driven vehicular ad hoc networks using fuzzy logic," IEEE Transactions on Intelligent Transportation Systems, 2023. https://doi.org/10.1109/TITS.2023.3305342

[5] M. Gheisari, Z. Safari, M. Almasi, R. G. Abel Sridharan, Y. Liu, and A. A. Abbasi, "A novel enhanced algorithm for efficient human tracking," Int J Inf Commun Technol, vol. 11, no. 1, pp. 1-7, 2022. https://doi.org/10.11591/ijict.v11i1.pp1-7

[6] Y. Liu, L. Lin, L. Jiang, W. Zhang, X. Wang, M. Gheisari, and H. E. Najafabadi, "A blockchain-based privacy-preserving advertising attribution architecture: Requirements, design, and a prototype implementation," Software: Practice and Experience, vol. 53, no. 8, pp. 1700-1721, 2023. https://doi.org/10.1002/spe.3209

[7] A. A. Abbasi, M. A. Al-qaness, M. A. Elaziz, H. A. Khalil, and S. Kim, "Bouncer: a resource-aware admission control scheme for cloud services," Electronics, vol. 8, no. 9, p. 928, 2019 https://doi.org/10.3390/electronics8090928

[8] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. AlFuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, data management, and ethical challenges," Computer Science Review, vol. 43, p. 100452, 2022. https://doi.org/10.1016/j.cosrev.2021.100452

[9] M. H. P. Rizi and S. A. H. Seno, "A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city," Internet of Things, vol. 20, p. 100584, 2022. https://doi.org/10.1016/j.iot.2022.100584

[10] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," Information Systems Frontiers, pp. 1-22, 2022.

[11] M. Gheisari, E. Shojaeian, A. Javadpour, A. Jalili, H. EsmaeiliNajafabadi, B. S. Bigham, and M. Rezaei, "An agile privacypreservation solution for iot-based smart city using different distributions," IEEE Open Journal of Vehicular Technology, vol. 4, pp. 356-362, 2023. https://doi.org/10.1109/OJVT.2023.3243226

[12] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," IEEE Access, vol. 9, pp. 18 706-18 721, 2021. https://doi.org/10.1109/ACCESS.2021.3053233

[13] A. Alzu'bi, A. A. Alomar, S. Alkhaza'leh, A. Abuarqoub, and M. Hammoudeh, "A review of privacy and security of edge computing in smart healthcare systems: issues, challenges, and research directions," Tsinghua Science and Technology, vol. 29, no. 4, pp. 1152-1180, 2024. https://doi.org/10.26599/TST.2023.9010080

[14] M. F. Khan, K. Saleem, M. Alotaibi, M. M. Hazzazi, E. Rehman, A. A. Abbasi, and M. A. Gondal, "Construction and optimization of trng based substitution boxes for block encryption algorithms," Computers, Materials Continua, vol. 73, no. 2, pp. 2679-2696, 2022. https://doi.org/10.32604/cmc.2022.027655

[15] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, "Secure healthcare data aggregation and transmission in iot—a survey," IEEE Access, vol. 9, pp. 16 849-16 865, 2021. https://doi.org/10.1109/ACCESS.2021.3052850

[16] A. Entezami, H. Sarmadi, and B. Behkamal, "Long-term health monitoring of concrete and steel bridges under large and missing data by unsupervised meta learning," Engineering Structures, vol. 279, p. 115616, 2023. https://doi.org/10.1016/j.engstruct.2023.115616

[17] M. Umair, M. A. Cheema, O. Cheema, H. Li, and H. Lu, "Impact of covid-19 on iot adoption in healthcare, smart homes, smart buildings, smart cities, transportation and industrial iot," Sensors, vol. 21, no. 11, p. 3838, 2021. https://doi.org/10.3390/s21113838

[18] M. Lotfi, G. J. Osorio, M. S. Javadi, A. Ashraf, M. Zahran, G. Samih, ´ and J. P. Catalao, "A dijkstra-inspired graph algorithm for fully ˜ autonomous tasking in industrial applications," IEEE Transactions on Industry Applications, vol. 57, no. 5, pp. 5448-5460, 2021. https://doi.org/10.1109/TIA.2021.3091418

[19] M. K. Hasan, M. M. Ahmed, S. S. Musa, S. Islam, S. N. H. S. Abdullah, E. Hossain, and N. Vo, "An improved dynamic thermal current rating model for pmu-based wide area measurement framework for reliability analysis utilizing sensor cloud system," IEEE Access, vol. 9, pp. 14 446-14 458, 2021. https://doi.org/10.1109/ACCESS.2021.3052368

[20] A. N. Alahmadi, S. U. Rehman, H. S. Alhazmi, D. G. Glynn, H. Shoaib, and P. Sole, "Cyber-security threats and side-channel ´ attacks for digital agriculture," Sensors, vol. 22, no. 9, p. 3520, 2022 https://doi.org/10.3390/s22093520

[21] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. IEEE Communications Surveys Tutorials 21, 3 (thirdquarter 2019), 2671-2701. https://doi.org/10.1109/COMST.2019.2896380

[22] Anirban Chakraborty, Manaar Alam, Vishal Dey, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. 2018. Adversarial Attacks and Defences: A Survey. x, x (2018). http://arxiv.org/abs/1810.00069

[23] Guillaume Chapron. 2017. The environment needs cryptogovernance. Nature 545, 7655 (2017), 403-405. https://doi.org/10.1038/545403a

[24] Baibhab Chatterjee, Debayan Das, and Shreyas Sen. 2018. RF-PUF: IoT security enhancement through authentication of wireless nodes using in-situ machine learning. Proceedings of the 2018 IEEE International Symposium on Hardware Oriented Security and Trust, HOST 2018 PP, c (2018), 205-208. https://doi.org/10.1109/HST.2018.8383916

[25] Konstantinos Christidis and Michael Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4 (2016), 2292-2303. http://ieeexplore.ieee.org/document/7467408/ https://doi.org/10.1109/ACCESS.2016.2566339

[26] Kelton A.P. da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz, and Victor Hugo C. de Albuquerque. 2019. Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks 151 (2019), 147-157. https://doi.org/10.1016/j.comnet.2019.01.023

[27] Tim Dalgleish, J. Mark G.. Williams, Ann-Marie J. Golden, Nicola Perkins, Lisa Feldman Barrett, Phillip J. Barnard, Cecilia Au Yeung, Victoria Murphy, Rachael Elward, Kate Tchanturia, and Edward Watkins. 2018. The Blockchain-enabled Intelligent IoT Economy. (2018). https://www.forbes.com/sites/cognitiveworld/2018/10/04/the-blockchain-enabled-intelligent-iot-economy/#14b65de82a59

[28] Guido Dartmann, Houbing Song, and Anke Schmeink. 2019. Big Data Analytics for Cyber-Physical Systems: Machine Learning for the Internet of Things. Elsevier. 1-360 pages.

[29] Tien Tuan Anh Dinh, Ji Wang, Gang Chen, Rui Liu, Beng Chin Ooi, and Kian-Lee Tan. 2017. BLOCKBENCH: A Framework for Analyzing Private Blockchains. (2017).

[30] Abebe Diro and Naveen Chilamkurti. 2018. Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications. IEEE Communications Magazine 56, 9 (2018), 124-130. https://doi.org/10.1109/MCOM.2018.1701270

[31] Ali Dorri, Salil S. Kanhere, and Raja Jurdak. 2016. Blockchain in internet of things: Challenges and Solutions. CoRR abs/1608.05187 (2016). http://arxiv.org/abs/1608.05187

[32] GhadakSaz, Ehsan, *et al*. "Design, Implement and Compare two proposed sensor data's storages Named SemHD and SSW." From Editor in Chief (2012): 78.

https://doi.org/10.31875/2979-1081.2025.01.04