

International Journal of
Engineering Research and Science & Technology



ISSN : 2319-5991

www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

Secure Data Collection and Storage for IoT Devices Using Elliptic Curve Cryptography and Cloud Integration

¹**Surendar Rama Sitaraman**

Intel Corporation, California, USA

sramasitaraman@gmail.com

²**R. Pushpakumar**

Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology

Associate Professor

chennai,india

pushpakumarvelr@gmail.com

ABSTRACT

The proposed framework aims to enhance the security and efficiency of data collected from Internet of Things (IoT) devices by integrating advanced data pre-processing and encryption techniques. The workflow starts with the collection of diverse data from IoT devices, such as sensor readings, environmental parameters, and patient information. The collected data undergoes thorough pre-processing, including data cleaning, normalization, and transformation, to ensure high-quality inputs for the encryption phase. To secure sensitive data, Elliptic Curve Cryptography (ECC) is employed as the encryption technique. ECC is chosen for its efficiency, as it provides robust encryption with shorter key sizes, making it ideal for resource-constrained IoT devices. The encrypted data is subsequently stored in a secure cloud environment, ensuring that only authorized entities can decrypt and access the data using the private keys. This approach not only safeguards the integrity and privacy of the data but also enables scalable deployment across various IoT systems. The framework is designed to address challenges related to data security, storage, and processing in IoT-enabled environments, particularly in healthcare and environmental monitoring applications.

Keywords: IoT, Data Encryption, Elliptic Curve Cryptography (ECC), Data Preprocessing, Cloud Storage

1. INTRODUCTION

The rapid growth of Internet of Things (IoT) devices has led to an exponential increase in the amount of data generated, especially in sensitive areas like healthcare, environmental monitoring, and smart cities [1]. Ensuring the security and privacy of this data is crucial, as it often contains sensitive information that, if compromised, can lead to severe consequences [2]. Traditional methods of data encryption and storage are insufficient to handle the unique challenges posed by the resource constraints of IoT devices and the need for secure cloud-based storage [3]. This proposed framework addresses these concerns by integrating efficient encryption techniques and secure cloud storage for IoT data [4].

Existing methods for securing IoT data primarily include symmetric encryption and asymmetric encryption techniques [5]. While AES offers high-speed encryption, it requires secure key management for each device [6]. RSA, although secure, is computationally intensive, making it unsuitable for resource-constrained IoT environments. Furthermore, both methods face scalability issues when dealing with large IoT networks [7]. Elliptic Curve Cryptography (ECC) has been explored as an alternative due to its smaller key sizes and stronger security per bit, but challenges remain in terms of efficient integration and data storage [8].

The proposed framework overcomes these limitations by employing Elliptic Curve Cryptography (ECC), which provides robust security with smaller key sizes, making it ideal for IoT environments. The data is encrypted using ECC before being securely stored in the cloud, addressing both efficiency and security concerns. This approach

ensures scalable deployment and enhances data privacy, enabling seamless integration with IoT devices that have limited resources. The novelty of this study lies in its ability to combine ECC-based encryption with cloud storage in a manner that is both computationally efficient and highly secure, solving the challenges faced by existing methods in IoT-based systems.

2. LITERATURE REVIEW

[9] presents a survey and classification of IoT cloud providers, focusing on their features and capabilities designed to meet the specific needs of IoT applications. It highlights the growing importance of Platform-as-a-Service (PaaS) cloud solutions, which enable flexible resource provisioning and federation capabilities. The study emphasizes the increasing number of cloud providers catering to IoT, addressing key needs such as data generation, processing, and visualization. Additionally, the research underscores the necessity for an IoT device simulator to support the development of IoT cloud systems and facilitate future advancements in the field.

[10] surveys popular IoT cloud platforms, examining their role in key service domains such as application development, device management, and data management. It presents a comparative analysis of these platforms, evaluating their strengths and weaknesses in various IoT applications. The paper also identifies existing challenges in the field and provides valuable insights into the advantages and limitations of current IoT cloud service providers, highlighting areas for future research.

[11] provides a comprehensive list of functionalities and best practices for selecting an IoT cloud platform, addressing the rapid growth of internet-connected devices. It highlights the increasing number of "Things," surpassing the human population, and discusses various cloud frameworks, both open-source and commercial, developed to manage the vast scale of IoT devices, despite slow adoption. The research offers insights for comparing different platforms and summarizes the support levels provided by existing solutions, which can inform the development of new cloud frameworks tailored to IoT requirements.

[12] explores the complexities of integrating IoT and cloud services to create a unified software layer for continuous application deployment and execution. It analyzes the requirements for IoT cloud systems and proposes seven key engineering principles essential for their development and operation. The authors demonstrate the importance of these principles through recent work on concepts and tools designed to support the effective functioning of IoT cloud systems across various domains.

[13] explores the architecture, implementation, and performance of IoT cloud systems, highlighting the essential role of cloud computing in managing IoT applications by providing computational power and storage capacity. It discusses the integration of HTTP and MQTT servers to enhance service delivery and presents experimental results to demonstrate the IoT cloud's capabilities under various conditions. The research underscores the importance of these technologies in enabling efficient data collection, analysis, and management for IoT applications.

[14] explores the convergence of IoT and Cloud Computing to create an "Everything as a Service" model, enhancing service attributes such as ubiquity, reliability, and scalability. It proposes an innovative IoT-centric Cloud infrastructure designed to address the challenges faced by both IoT and Cloud Computing. The paper envisions a Cloud ecosystem with novel functionalities and cognitive-IoT capabilities, aiming to improve service provision and meet the evolving demands of IoT applications.

[15] addresses the optimization of IoT-Cloud services in next-generation smart environments, focusing on the challenges posed by centralized cloud architectures, including high network load and power consumption. It formulates the service distribution problem (SDP) in IoT-Cloud networks as a minimum cost mixed-cast flow problem, which can be solved using linear programming techniques. The study demonstrates that optimized, distributed cloud networking can effectively reduce energy consumption while delivering diverse IoT services, making it crucial for the development of energy-efficient and scalable smart environments.

2.1. PROBLEM STATEMENT

Based on the study, [16] several key challenges persist in the integration of IoT and cloud services. First, the rapid expansion of IoT devices leads to significant network load and power consumption, [17] particularly with centralized cloud architectures. [18] Second, security and privacy concerns remain critical, as sensitive data from IoT devices must be encrypted and securely stored in cloud environments. [19] Third, existing IoT cloud platforms often struggle with scalability and efficient management of the growing volume of data generated by connected devices. Fourth, many current cloud solutions lack adequate support for real-time processing and low-latency requirements essential for many IoT applications.[20] Finally, the slow adoption of standardized IoT device simulators hinders the efficient development and testing of IoT cloud systems, limiting the ability to create robust and adaptable cloud-based IoT solutions.

3. PROPOSED METHODOLOGY

The system for IoT data collection, pre-processing, encryption, and storage is illustrated in figure 1. The process begins with Data Collection, where IoT devices gather raw data. This data then undergoes Data Pre-processing, which includes two key steps: Data Cleaning to remove noise and ensure the data is usable, and Outlier Detection to identify and handle abnormal or erroneous data points. Once pre-processed, the data is encrypted using Elliptic Curve Cryptography (ECC) for security, ensuring that sensitive information is protected. The encrypted data is then stored securely in Cloud Storage, allowing for scalable and efficient access. Lastly, the system evaluates the performance of the process by generating Performance Metrics to measure the effectiveness of the data handling, encryption, and storage mechanisms. This workflow ensures the secure and efficient management of IoT data from collection to storage, addressing key concerns such as data security and system performance.

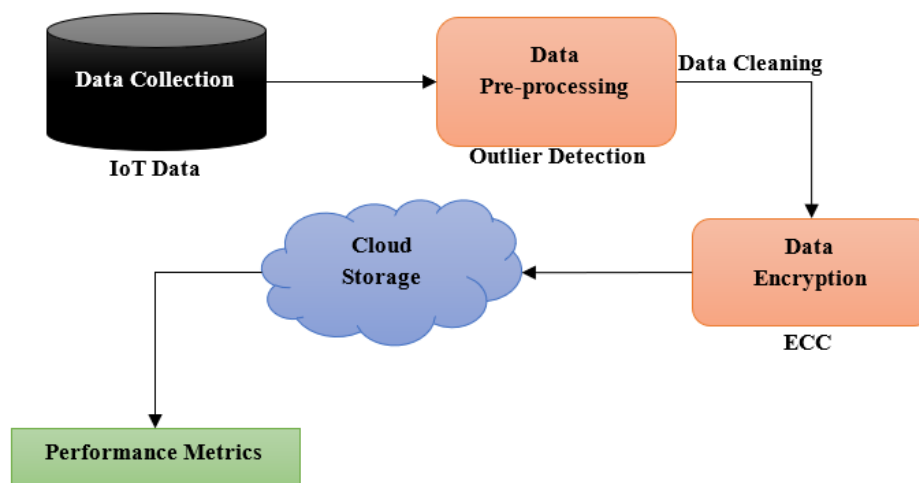


Figure 1: Cloud-Based IoT Data Security

3.1 Data Collection

Data collection in the proposed framework begins with IoT devices that gather real-time data from various sources such as sensors, smart appliances, or healthcare devices. This data may include environmental parameters, health metrics, or operational conditions, depending on the application domain. IoT devices continuously stream data, which is captured and stored in a centralized repository. The data collected is diverse in nature, such as numeric values, categorical data, or multimedia content. It is essential that the data collected is accurate, up-to-date, and sufficient in volume to ensure the success of subsequent stages in the workflow. The quality and completeness of this collected data are crucial to ensuring the effectiveness of data pre-processing, encryption, and eventual cloud storage. The next step involves preparing this raw data for further processing.

3.2 Data Pre-processing

The data preprocessing steps in the framework involve several key operations, including data cleaning, handling missing values, and outlier detection.

1. **Data Cleaning:** This step involves removing any noise or inconsistencies in the collected data. The cleaned data D_{cleaned} can be represented as:

$$D_{\text{cleaned}} = D_{\text{raw}} - \{ \text{noise} \}$$

where D_{raw} is the original dataset and noise refers to irrelevant or erroneous data points.

2. **Handling Missing Values:** Missing data can be handled using techniques like mean imputation, kNearest Neighbors (k-NN) imputation, or deep learning-based imputation. A common approach is mean imputation:

$$D_{\text{imputed}} = D_{\text{missing}} + \left(\frac{\sum D_{\text{observed}}}{n} \right)$$

where D_{missing} refers to missing data points, and $\sum D_{\text{observed}}$ is the sum of the observed data, with n being the total number of observed entries.

3. **Outlier Detection:** Outliers can be identified using statistical methods like Z-score or Interquartile Range (IQR). For Z-score detection, an outlier is defined as:

$$Z = \frac{X - \mu}{\sigma}$$

where X is the data point, μ is the mean, and σ is the standard deviation. Data points with $|Z| > 3$ are typically considered outliers.

3.3 Data Encryption using ECC

Elliptic Curve Cryptography (ECC) is employed for encrypting the preprocessed data to ensure its security. The working of ECC begins with generating a public and private key pair. The public key is used to encrypt the data, while the private key is used for decryption by authorized users. ECC operates over elliptic curves defined by equations of the form:

$$y^2 = x^3 + ax + b$$

where a and b are constants. The process of encryption involves mapping the plaintext data to a point on the elliptic curve. Once the data is mapped, ECC encryption uses scalar multiplication to perform the encryption. The encrypted data can only be decrypted by the owner of the corresponding private key, ensuring data confidentiality and security. This process is computationally efficient, even with large datasets, making ECC an ideal choice for IoT systems where devices have limited processing power.

3.4 Cloud Storage

The encrypted data is then securely stored in the cloud. Cloud storage allows for scalability and redundancy, ensuring that the data is available and protected from loss or unauthorized access. Cloud service providers ensure high availability and durability through data replication and advanced storage mechanisms. In this step, the encrypted data is uploaded to a cloud server, where it is stored in a secure database. The cloud platform also offers various functionalities like load balancing and automatic scaling to accommodate varying amounts of incoming IoT data. Data retrieval is facilitated through secure API calls, ensuring that only authorized users can access the data by using their decryption keys.

4. RESULT

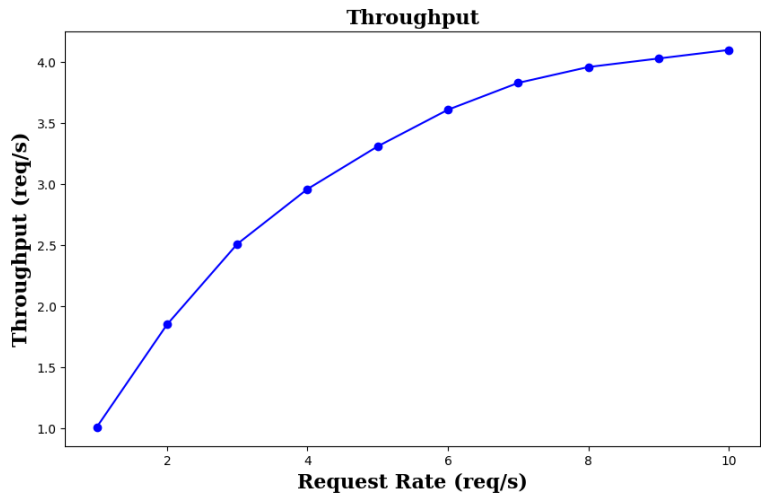


Figure 2: System Throughput vs Request Rate

Figure 2 illustrates the relationship between throughput (in requests per second) and request rate (in requests per second) for a system. As the request rate increases, the throughput also increases, indicating that the system can handle more requests per second as the load grows. The data points reveal the following throughput values at corresponding request rates: at 1 req/s, the throughput is 1.01 req/s; at 2 req/s, it rises to 1.85 req/s; at 3 req/s, it is 2.51 req/s; at 4 req/s, it increases to 2.96 req/s; at 5 req/s, it reaches 3.31 req/s; at 6 req/s, the throughput is 3.61 req/s; at 7 req/s, it is 3.83 req/s; at 8 req/s, the throughput is 3.96 req/s; at 9 req/s, it goes up to 4.03 req/s; and finally, at 10 req/s, the throughput is 4.10 req/s. This shows a steady improvement in throughput as the request rate increases, demonstrating the system's ability to scale efficiently under increasing load.

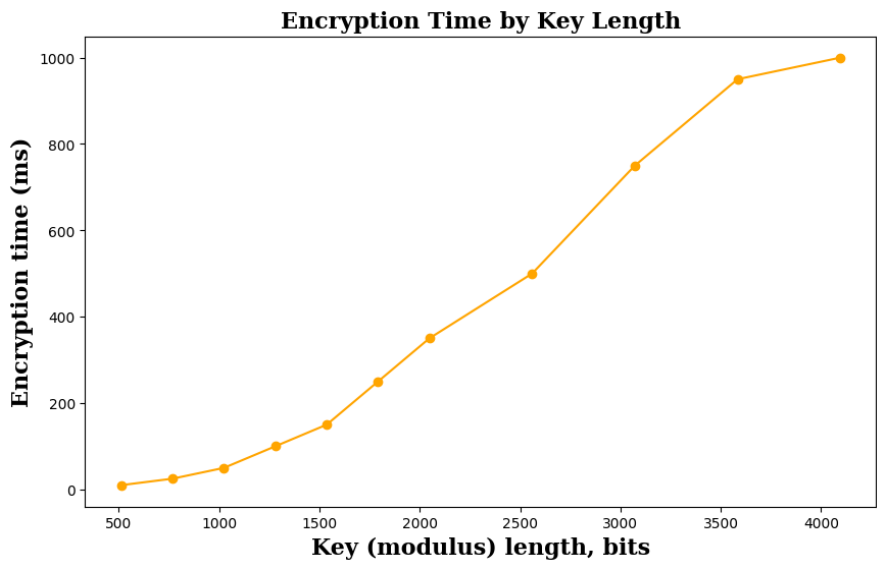


Figure 3: Impact of Key Length on Encryption Time

Figure 3 demonstrates the relationship between **encryption time** (in milliseconds) and **key length** (in bits) for RSA encryption. As the key length increases, the encryption time grows significantly, highlighting the computational complexity involved in encrypting data with longer keys. For example, with a key length of 512 bits, the encryption time is 5 ms, while at 768 bits, it increases to 15 ms. As the key length progresses, the encryption time rises to 1000 ms at 4096 bits, with notable intermediate values such as 30 ms at 1024 bits, 90 ms

at 1536 bits, 230 ms at 2048 bits, and 700 ms at 3584 bits. This shows that longer keys require exponentially more processing power, making the encryption process more time-consuming and resource-intensive.

5. CONCLUSION

In conclusion, the proposed framework effectively enhances the security and efficiency of data from Internet of Things (IoT) devices through advanced data pre-processing and Elliptic Curve Cryptography (ECC). By employing ECC for encryption, it ensures robust security while accommodating resource-constrained IoT devices. The pre-processing steps guarantee high-quality data for encryption, which is then stored securely in the cloud, ensuring authorized access and safeguarding data integrity and privacy. Future work could focus on optimizing ECC for better performance on limited devices, enabling real-time data processing, enhancing scalability for larger IoT networks, and incorporating AI and machine learning for improved data analysis and anomaly detection. Additionally, integrating edge computing could reduce latency, and ensuring interoperability across diverse IoT devices would further broaden the framework's applicability, particularly in critical areas such as healthcare and environmental monitoring.

REFERENCE

- [1] Yang, Z., Zhou, Q., Lei, L., Zheng, K., & Xiang, W. (2016). An IoT-cloud based wearable ECG monitoring system for smart healthcare. *Journal of medical systems*, 40, 1-11.
- [2] Arulkumaran, G., & Gnanamurthy, R. K. (2014). Improving Reliability against Security Attacks by Identifying Reliance Node in MANET. *Journal of Advances in Computer Networks*, 2(2).
- [3] Celesti, A., Galletta, A., Carnevale, L., Fazio, M., Łay-Ekuakille, A., & Villari, M. (2017). An IoT cloud system for traffic monitoring and vehicular accidents prevention based on mobile sensor data processing. *IEEE Sensors Journal*, 18(12), 4795-4802.
- [4] Babu, S. M., Lakshmi, A. J., & Rao, B. T. (2015, April). A study on cloud based Internet of Things: CloudIoT. In *2015 global conference on communication technologies (GCCT)* (pp. 60-65). IEEE.
- [5] Jaiswal, K., Sobhanayak, S., Mohanta, B. K., & Jena, D. (2017, November). IoT-cloud based framework for patient's data collection in smart healthcare system using raspberry-pi. In *2017 International conference on electrical and computing technologies and applications (ICECTA)* (pp. 1-4). IEEE.
- [6] Celesti, A., Galletta, A., Carnevale, L., Fazio, M., Łay-Ekuakille, A., & Villari, M. (2017). An IoT cloud system for traffic monitoring and vehicular accidents prevention based on mobile sensor data processing. *IEEE Sensors Journal*, 18(12), 4795-4802.
- [7] Bellavista, P., & Zanni, A. (2016, September). Towards better scalability for IoT-cloud interactions via combined exploitation of MQTT and CoAP. In *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)* (pp. 1-6). IEEE.
- [8] Kum, S. W., Moon, J., Lim, T., & Park, J. I. (2015, January). A novel design of IoT cloud delegate framework to harmonize cloud-scale IoT services. In *2015 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 247-248). IEEE.
- [9] Pflanzner, T., & Kertész, A. (2016, May). A survey of IoT cloud providers. In *2016 39th International convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 730-735). IEEE.
- [10] Ganguly, P. (2016, January). Selecting the right IoT cloud platform. In *2016 International Conference on Internet of Things and Applications (IOTA)* (pp. 316-320). IEEE.

- [11] Ray, P. P. (2016). A survey of IoT cloud platforms. *Future Computing and Informatics Journal*, 1(1-2), 35-46.
- [12] Truong, H. L., & Dustdar, S. (2015). Principles for engineering IoT cloud systems. *IEEE Cloud Computing*, 2(2), 68-76.
- [13] Hou, L., Zhao, S., Xiong, X., Zheng, K., Chatzimisios, P., Hossain, M. S., & Xiang, W. (2016). Internet of things cloud: Architecture and implementation. *IEEE Communications Magazine*, 54(12), 32-39.
- [14] Biswas, A. R., & Giaffreda, R. (2014, March). IoT and cloud convergence: Opportunities and challenges. In *2014 IEEE World Forum on Internet of Things (WF-IoT)* (pp. 375-376). IEEE.
- [15] Barcelo, M., Correa, A., Llorca, J., Tulino, A. M., Vicario, J. L., & Morell, A. (2016). IoT-cloud service optimization in next generation smart environments. *IEEE Journal on Selected Areas in Communications*, 34(12), 4077-4090.
- [16] Aazam, M., Huh, E. N., St-Hilaire, M., Lung, C. H., & Lambadaris, I. (2016). Cloud of things: integration of IoT with cloud computing. *Robots and sensor clouds*, 77-94.
- [17] Nastic, S., Truong, H. L., & Dustdar, S. (2016, October). A middleware infrastructure for utility-based provisioning of IoT cloud systems. In *2016 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 28-40). IEEE.
- [18] Nastic, S., Copil, G., Truong, H. L., & Dustdar, S. (2015, November). Governing elastic IoT cloud systems under uncertainty. In *2015 IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom)* (pp. 131-138). IEEE.
- [19] Solapurkar, P. (2016, December). Building secure healthcare services using OAuth 2.0 and JSON web token in IOT cloud scenario. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 99-104). IEEE.
- [20] Le, D. H., Truong, H. L., & Dustdar, S. (2016, June). Managing on-demand sensing resources in IoT cloud systems. In *2016 IEEE International Conference on Mobile Services (MS)* (pp. 65-72). IEEE.