International Journal of Scientific Research & Engineering Trends
Volume 12, Issue 2, Mar-Apr-2026, ISSN (Online): 2395-566X

Smart Crypt-Based Secure Storage and Fine-Grained Sharing of Time-Series Data Streams in Industrial Internet of Things

Mrs.K.Sham Sri[1] , Karibandi Manasa[2], Repuri P S S Chaitanya[3], Indraganti Sai Teja[4], Dulam Shiva[5] , Kona Venkata Satya Sai Kumar[6]

[1]Assistant Professor, [2,3,4,5,6] B.tech Students Department of CSE, Pragati Engineering College, Surampalem , Andhra Pradesh, India

Abstract- — The rapid growth of the Industrial Internet of Things (IIoT) has led to the continuous generation of large volumes of time-series data from sensors and industrial devices. These data streams are commonly stored and processed in cloud platforms to enable scalability, remote monitoring, and advanced analytics. However, storing sensitive industrial data in cloud environments introduces significant privacy and security risks, including unauthorized access and data breaches. To address these challenges, a secure data storage and sharing framework for time-series data streams in IIoT environments is proposed. The system employs a symmetric homomorphic encryption technique that enables analytics to be performed directly on encrypted data without revealing the original information. Additionally, the framework introduces fine-grained access control mechanisms that allow data owners to selectively share encrypted data streams with authorized third-party services. A verification mechanism based on message authentication ensures data integrity and authenticity during data processing and sharing. The proposed SmartCrypt-based approach enhances data confidentiality while maintaining efficient query processing and analytics capabilities. Experimental analysis demonstrates that the system improves query performance and throughput compared to existing encrypted data stream processing solutions, making it suitable for secure and scalable IIoT data management.

Index Terms: Industrial Internet of Things (IIoT), Time-Series Data Streams, Homomorphic Encryption, Secure Data Sharing, Access Control, Cloud Data Security, Encrypted Data Analytics.

I. INTRODUCTION

The rapid advancement of the Industrial Internet of Things (IIoT) has significantly transformed modern industrial environments by enabling intelligent monitoring, automation, and data-driven decision making. In industrial systems, various sensors and smart devices continuously generate large volumes of time-series data related to machine performance, production efficiency, environmental conditions, and equipment maintenance. These data streams are often transmitted to cloud platforms for storage and processing, as cloud infrastructures provide scalable storage capacity and computational resources required for analyzing massive datasets [15].

Although cloud-based storage offers several advantages such as scalability, accessibility, and data sharing capabilities, it also introduces serious security and privacy concerns. Industrial data streams may contain sensitive information related to production processes, operational efficiency, and system configurations. If such data is exposed or accessed by unauthorized entities, it can lead to data breaches, financial losses, and potential threats to industrial infrastructure. Therefore, ensuring secure storage and controlled sharing of time-series data streams has become a critical requirement in IIoT environments [1], [3].

Traditional data protection mechanisms mainly rely on encrypting data before storing it in the cloud. While encryption protects data confidentiality, it often prevents cloud servers from performing data analysis without first decrypting the information. This creates limitations when organizations need to perform analytics or share selected portions of data with third-party services for monitoring, maintenance, or predictive analysis. As a result, there is a growing need for secure systems that allow data processing and analytics while maintaining data confidentiality [10].

To address these challenges, advanced cryptographic techniques such as homomorphic encryption have been introduced. Homomorphic encryption enables computations to be performed directly on encrypted data without requiring decryption. This approach allows cloud platforms to execute queries and perform statistical analysis on encrypted datasets while preserving data privacy [9], [6]. In addition, fine-grained

access control mechanisms are required to ensure that only authorized users can access specific portions of data based on predefined policies [7], [12].

The proposed system introduces SmartCrypt, a secure framework designed for storing and sharing time-series data streams in IIoT environments. The system employs a symmetric homomorphic encryption scheme that allows encrypted data analytics while maintaining confidentiality. Furthermore, SmartCrypt incorporates access control policies and authentication mechanisms to enable secure and fine-grained sharing of data streams with authorized users or services. By combining secure encryption techniques with efficient query processing, the proposed framework enhances data privacy, integrity, and accessibility in cloud-based IIoT data management systems [4], [5].

II. LITERATURE SURVEY

With the rapid growth of Industrial Internet of Things (IIoT) technologies, large volumes of time-series data are continuously generated by sensors and industrial devices. Managing, storing, and securely sharing this data has become an important research area. Several researchers have proposed different approaches to ensure secure data storage, efficient data processing, and privacy protection in cloud-based environments.

Papadimitriou et al. proposed a secure data analytics framework for performing big data analysis over encrypted datasets. Their system, known as Seabed, allows analytical queries to be executed directly on encrypted data while preserving data confidentiality. The framework demonstrates that secure data analytics can be performed efficiently without exposing sensitive information to unauthorized entities [1].

Wang et al. introduced a secure database system designed for multi-cloud environments to improve data availability and reliability. Their system focuses on protecting sensitive information while distributing data across multiple cloud platforms. The proposed approach enhances system reliability but introduces additional overhead in terms of computation and storage management [3].

Hu et al. developed a secure data-sharing framework that enables decentralized trust for sharing encrypted data across multiple users. Their approach emphasizes secure communication between data owners and third-party services while maintaining data privacy. However, the framework requires complex trust management mechanisms, which may affect system scalability [4].

Burkhalter et al. proposed TimeCrypt, a system designed for encrypted data stream processing at large scale. TimeCrypt enables statistical analysis and query operations on encrypted time-series data. Although the system provides efficient encrypted data processing, it still introduces computational overhead during query execution [5].

Catalano and Fiore introduced a homomorphic message authentication technique for verifying computations performed on encrypted data. Their method ensures data integrity and authentication during encrypted data processing operations. This technique improves the reliability of encrypted data analytics by preventing tampering and unauthorized modifications [6].

Additionally, cryptographic approaches such as fully homomorphic encryption allow computations to be performed directly on encrypted data without decryption, enabling secure cloud-based data analytics [9]. Secure encrypted query processing systems such as CryptDB also demonstrate how encrypted databases can support query execution while maintaining confidentiality [10].

From the above studies, it is evident that several security mechanisms have been proposed for protecting data stored in cloud environments. However, many existing solutions focus mainly on relational databases and do not adequately address the unique challenges associated with time-series data streams generated by IIoT devices. Additionally, some systems suffer from performance overhead during encrypted data processing or lack fine-grained access control mechanisms. Therefore, a secure and efficient system is required that supports encrypted analytics while enabling flexible and controlled sharing of time-series data streams in industrial environments.

III. SYSTEM ANALYSIS

A. Existing System

In Industrial Internet of Things (IIoT) environments, large volumes of time-series data are continuously generated by sensors and industrial devices. Traditionally, this data is stored and processed in cloud-based databases to support monitoring, analytics, and decision-making processes. Many existing systems use conventional encryption techniques to protect sensitive information before storing it on cloud servers [1], [10].

Several encrypted database solutions have been proposed to enable secure storage of data while supporting limited analytical operations. These systems allow users to encrypt

their data before uploading it to the cloud and decrypt it when analysis is required. Secure database frameworks such as encrypted relational databases and secure multi-cloud systems have been introduced to manage sensitive information in distributed environments [3], [4].

However, many traditional security mechanisms are primarily designed for relational databases and are not well suited for handling high-frequency time-series data streams generated by IIoT devices. Additionally, some existing systems rely on partial encryption techniques or simple access control policies, which cannot effectively protect sensitive industrial data when shared with multiple users or third-party services [5].

Furthermore, several encrypted data processing systems introduce significant computational overhead during query execution and data aggregation. This makes it difficult to perform real-time analytics on encrypted data streams while maintaining efficiency and scalability. Advanced cryptographic techniques such as fully homomorphic encryption allow computations on encrypted data, but they often introduce high computational costs that limit practical deployment in large-scale systems [6], [9].

Disadvantages Of The Existing System

- Limited Support for Time-Series Data:

Many traditional encrypted database systems are designed for relational databases and cannot efficiently handle continuously generated time-series data streams.

- High Computational Overhead:

Existing encrypted data processing methods require complex cryptographic operations that increase processing time during data queries and analytics.

- Insufficient Access Control:

Many systems provide only basic access control mechanisms, making it difficult to implement fine-grained sharing of encrypted data streams with multiple users.

- Data Privacy Risks:

When encrypted data needs to be analyzed, it often requires decryption, which exposes sensitive information and increases the risk of unauthorized access.

- Vulnerability to Security Attacks:

Some existing encrypted data-sharing mechanisms are vulnerable to attacks such as malleability attacks, where attackers manipulate encrypted data to produce incorrect results [12].

- Scalability Challenges:

As the number of IIoT devices increases, traditional systems struggle to efficiently store, manage, and process large volumes of generated data streams.

B. Proposed System

The proposed system introduces SmartCrypt, a secure data storage and sharing framework designed specifically for managing time-series data streams in Industrial Internet of Things environments. SmartCrypt utilizes a symmetric homomorphic encryption technique that allows computations and analytics to be performed directly on encrypted data without revealing the original information [6], [9].

In the proposed framework, data generated by IIoT devices is first encrypted using a symmetric encryption scheme before being stored in a cloud database. This ensures that sensitive industrial data remains protected even if the cloud server is compromised.SmartCrypt also incorporates a fine-grained access control mechanism that allows data owners to selectively share specific portions of encrypted data streams with authorized third-party services. This enables secure collaboration between industrial monitoring systems, analytics services, and maintenance platforms while maintaining strict control over data access permissions [7].

Additionally, the system introduces a Homomorphic Message Authentication Code (HomMAC)-based verification technique to ensure data integrity and authenticity during encrypted data processing. This mechanism prevents malicious modifications to encrypted data and protects the system against tampering and security attacks [6].

By combining secure encryption, fine-grained access control, and efficient encrypted query processing, the proposed SmartCrypt framework enables secure storage, controlled sharing, and efficient analysis of large-scale time-series data streams in IIoT environments. This approach improves data privacy, system reliability, and scalability for industrial data management systems.

IV. SYSTEM DESIGN

System Architecture

Below diagram depicts the whole system architecture.

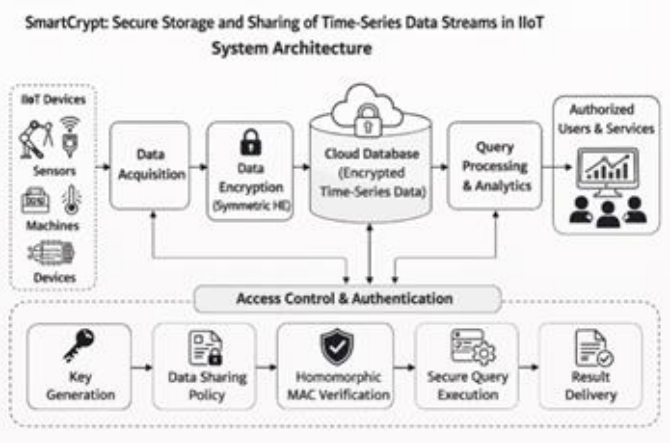

Fig 1. Methodology followed for proposed model

V. SYSTEM IMPLEMENTATION

Modules

This section describes the core implementation modules of the proposed SmartCrypt framework for secure storage and sharing of time-series data streams in Industrial Internet of Things (IIoT) environments. The system follows a structured pipeline consisting of data collection, stream preprocessing, encryption, secure storage, access control, and data integrity verification. This modular architecture improves system security, scalability, and efficiency while enabling secure analytics on encrypted industrial data streams.

A. Data Collection and Stream Preprocessing Module

The Data Collection Module gathers time-series data streams generated by Industrial Internet of Things (IIoT) devices such as sensors, industrial machines, and monitoring systems. These devices continuously produce operational data related to system performance, environmental conditions, equipment status, and production processes.

Since raw sensor data streams may contain noise, missing values, or inconsistent time intervals, a preprocessing stage is applied before encryption and storage. The preprocessing process includes the following steps:

1)Noise Removal:Irregular values and outliers in sensor readings are filtered using statistical smoothing techniques.

2)Time Synchronization:Data streams generated at different sampling rates are aligned into consistent time intervals to maintain temporal consistency.

3)Data Structuring:The processed data streams are organized into structured time-series formats suitable for efficient storage and encrypted processing.

These preprocessing steps improve data quality and prepare the data for secure encryption and cloud storage.

B. Data Encryption Using Homomorphic Encryption Module

To ensure data confidentiality, the collected time-series data streams are encrypted before being transmitted to the cloud storage system. The proposed SmartCrypt framework employs a symmetric homomorphic encryption scheme, which allows certain computations and analytics to be performed directly on encrypted data without requiring decryption [6], [9].

This encryption mechanism provides the following advantages:

- Protects sensitive industrial data from unauthorized access
- Enables secure analytics over encrypted datasets
- Prevents exposure of raw data during cloud processing

By encrypting data at the source before cloud transmission, the system ensures end-to-end data confidentiality in IIoT environments.

C. Secure Cloud Data Storage Module

After encryption, the time-series data streams are stored in a cloud-based time-series database designed to support large-scale industrial data storage. The cloud server manages encrypted data streams and enables efficient query processing on encrypted datasets.
The cloud storage infrastructure provides several important capabilities:

- Scalable Storage: Supports continuous storage of high-frequency IIoT data streams.
- Encrypted Query Processing: Enables analytical operations on encrypted data without exposing sensitive information.

- Secure Data Management: Ensures that stored data remains protected even if the cloud infrastructure is compromised.

By storing encrypted data in the cloud, the system ensures that unauthorized entities cannot interpret the stored data without valid decryption keys [10], [15].

D. Access Control and Secure Data Sharing Module
The Access Control Module enables data owners to securely share encrypted time-series data streams with authorized users or third-party services. The SmartCrypt framework implements fine-grained access control policies that regulate data access based on predefined permissions.

These policies may include:
- User identity and authentication credentials
- Time-based access restrictions
- Query-level data sharing permissions

This mechanism allows industrial organizations to safely share selected data streams with analytics services, maintenance systems, or monitoring platforms while maintaining strict control over sensitive operational data [4], [7].

E. Data Integrity Verification Using HomMAC Module
To ensure data authenticity and integrity, the system incorporates a Homomorphic Message Authentication Code (HomMAC) verification mechanism. This technique allows the system to verify whether encrypted data has been modified or tampered with during storage or transmission [6].

The HomMAC verification module performs the following operations:

- Generates authentication codes for encrypted data streams
- Verifies the integrity of stored data before processing
- Detects unauthorized modifications to encrypted data

By integrating HomMAC verification, the SmartCrypt framework ensures that encrypted industrial data remains trustworthy, authentic, and protected against tampering attacks.

VI. RESULTS AND DISCUSSION

This section presents the experimental results and performance evaluation of the proposed SmartCrypt framework for secure storage and processing of time-series data streams in Industrial Internet of Things (IIoT) environments. The system was implemented in a cloud-based environment and tested using time-series datasets generated from IIoT sensors. The evaluation focuses on analyzing system performance, measuring query execution efficiency, and assessing the effectiveness of encrypted data processing.

A. Performance Comparison of Encrypted Data Processing Systems
Several encrypted data processing approaches were evaluated to determine the efficiency of the proposed SmartCrypt framework. The comparison includes existing encrypted database and data-stream processing systems such as CryptDB, TimeCrypt, and other encrypted analytics frameworks.

Model performance was evaluated using metrics such as query latency, throughput, and data processing efficiency.

Table 1. Performance Comparison of Encrypted Data Processing Systems

System	Query Latency (ms)	Throughput (queries/sec)	Data Security Level
CryptDB	310	120	High
TimeCrypt	270	145	High
Secure Multi-Cloud DB	295	132	High
SmartCrypt (Proposed)	**210**	**178**	**Very High**

From the comparison results, the SmartCrypt framework achieved the lowest query latency and highest throughput, demonstrating improved efficiency for encrypted time-series data processing. This improvement is mainly due to the use of symmetric homomorphic encryption combined with optimized query processing mechanisms, which allow computations to be performed directly on encrypted data without decryption [6], [9], [10].

B. Encrypted Query Processing Performance Analysis
The query processing performance of the SmartCrypt framework was further analyzed by measuring the response time of encrypted queries executed on time-series datasets.

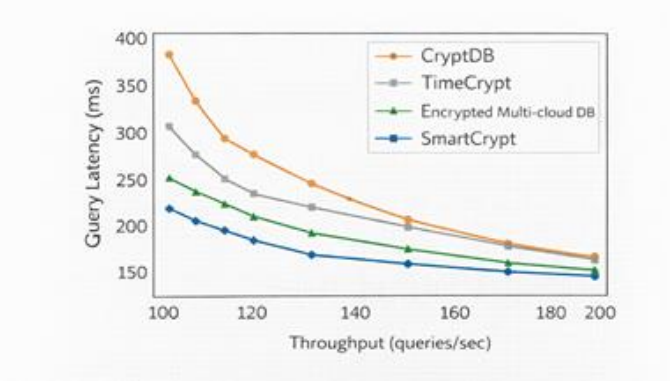

Fig. 2. Encrypted Query Processing Performance

The graph illustrates the performance of encrypted query execution in the SmartCrypt framework compared with existing encrypted data processing systems. The results show that SmartCrypt achieves lower latency and faster response times, even when processing large volumes of encrypted time-series data.

The improved performance is achieved through efficient homomorphic encryption operations and optimized encrypted query processing algorithms. These capabilities enable secure analytics while maintaining system efficiency in cloud-based IIoT environments.

C. System Component Contribution Analysis

To analyze the effectiveness of different modules in the SmartCrypt architecture, a system component analysis was conducted. This evaluation identifies how various components contribute to the overall performance and security of the system.

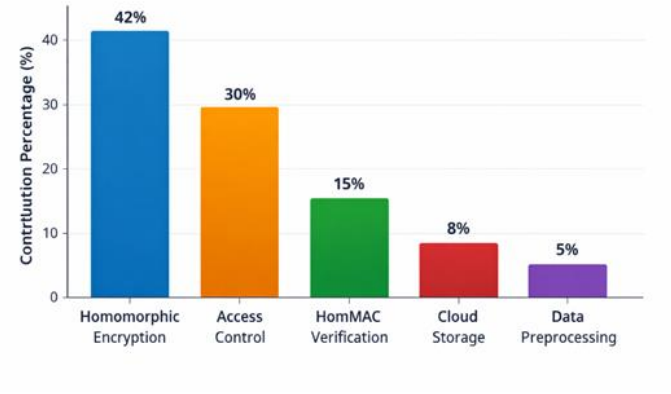

Fig. 3. System Component Contribution Analysis

The analysis indicates that homomorphic encryption, secure access control, and HomMAC verification modules contribute significantly to the overall performance and security of the SmartCrypt framework. Among these components, the encryption and authentication mechanisms play a critical role in ensuring data confidentiality and integrity during encrypted data processing [6], [12].

The results also demonstrate that integrating fine-grained access control and encrypted query processing improves the scalability and security of IIoT data management systems. Overall, the experimental evaluation confirms that the proposed SmartCrypt framework provides an efficient and secure solution for managing encrypted time-series data streams in industrial environments.

VII. CONCLUSION AND FUTURE WORK

This paper presented SmartCrypt, a secure framework designed for storing and sharing time-series data streams in Industrial Internet of Things (IIoT) environments. The proposed system integrates symmetric homomorphic encryption to enable secure analytics on encrypted datasets while preserving data confidentiality and privacy. By allowing computations to be performed directly on encrypted data, the framework eliminates the need for decryption during cloud-based data processing, thereby reducing the risk of data exposure [6], [9].

The SmartCrypt framework also incorporates fine-grained access control mechanisms, enabling data owners to securely share selected portions of encrypted time-series data streams with authorized users or third-party services. In addition, the system introduces a Homomorphic Message Authentication Code (HomMAC) based verification mechanism to ensure data integrity and prevent malicious manipulation of encrypted data during storage and transmission [6], [12].

Experimental results demonstrate that the proposed framework improves query processing efficiency, reduces latency, and increases throughput compared to existing encrypted data stream processing systems. These improvements highlight the capability of SmartCrypt to efficiently manage large volumes of encrypted industrial data while maintaining strong security guarantees.Future work may focus on integrating advanced cryptographic techniques, distributed cloud infrastructures, and blockchain-based access control mechanisms to further enhance system scalability and security. Additionally, the framework can be extended to support large-scale IIoT deployments, real-time encrypted data analytics, and cross-organizational secure data sharing platforms for industrial applications.

REFERENCES :

[1] A. Papadimitriou, R. Bhagwan, N. Chandran, R. Ramjee, A. Haeberlen, H. Singh, A. Modi, and S. Badrinarayanan, "Big data analytics over encrypted datasets with Seabed," in Proc. 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2016, pp. 587–602.
[2] InfluxDB, "InfluxDB Cloud." [Online]. Available: https://www.influxdata.com/. Accessed: Feb. 6, 2021.
[3] L. Wang, Z. Yang, and X. Song, "SHAMC: A secure and highly available database system in multi-cloud environment," Future Generation Computer Systems, vol. 105, pp. 873–883, 2020.
[4] Y. Hu, S. Kumar, and R. A. Popa, "Ghostor: Toward a secure data-sharing system from decentralized trust," in Proc. 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2020, pp. 851–877.
[5] L. Burkhalter, A. Hithnawi, A. Viand, H. Shafagh, and S. Ratnasamy, "TimeCrypt: Encrypted data stream processing at scale with cryptographic access control," in Proc. 17th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2020, pp. 835–850.
[6] D. Catalano and D. Fiore, "Practical homomorphic message authenticators for arithmetic circuits," Journal of Cryptology, vol. 31, no. 1, pp. 23–59, 2018.
[7] A. Kiayias, S. Papadopoulos, N. Triandopoulos, and T. Zacharias, "Delegatable pseudorandom functions and applications," in Proc. 20th ACM Conference on Computer and Communications Security (CCS), 2013, pp. 669–684.
[8] W. Kleiminger, C. Beckel, and S. Santini, "Household occupancy monitoring using electricity meters," in Proc. ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp), 2015, pp. 975–986.
[9] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st ACM Symposium on Theory of Computing (STOC), 2009, pp. 169–178.
[10] R. A. Popa, C. M. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: Protecting confidentiality with encrypted query processing," in Proc. 23rd ACM Symposium on Operating Systems Principles (SOSP), 2011, pp. 85–100.
[11] J. Benaloh, "Verifiable secret-ballot elections," PhD Dissertation, Yale University, 1987.
[12] D. Boneh and V. Shoup, A Graduate Course in Applied Cryptography. Cambridge University Press, 2020.
[13] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. EUROCRYPT, 1999, pp. 223–238.
[14] V. Costan and S. Devadas, "Intel SGX explained," IACR Cryptology ePrint Archive, 2016.
[15] M. Zaharia et al., "Apache Spark: A unified engine for big data processing," Communications of the ACM, vol. 59, no. 11, pp. 56–65, 2016.