Volume: 1 **Issue:** 1 **Pages:** 86-94

International Journal of Research in Academic World

E-ISSN: 2583-1615
Impact Factor: 3.133

Received: 11/August/2021 **Int. J Res. Acad. World.** 2021; 1(1):86-94 **Accepted:** 18/September/2021

A Security Framework for IoT Sensor Data Management in Cloud Computing Environments

*1Kalyan Gattupalli and 2Purandhar N

*1Sunny Information Technology Services Inc, Ontario, Canada.

2Assistant Professor, Sri Venkateswara College of Engineering, Tirupati, Andhra Pradesh, India.

Abstract

The rise of the Internet of Things (IoT) has significantly increased the generation of sensitive and continuous sensor data, which poses significant security challenges when transmitted to the cloud. Cloud computing provides scalable storage and real-time processing solutions for such data but introduces concerns related to unauthorized access, data breaches, and system vulnerabilities. This paper proposes a comprehensive security framework that ensures the confidentiality, integrity, and availability of IoT sensor data throughout its lifecycle. The framework integrates data pre-processing, AES encryption, Intrusion Detection Systems (IDS), secure transmission, and access control mechanisms to build a robust defence against cyber threats, enhancing data protection and user trust in IoT-enabled services. The results demonstrate significant differences in key generation and encryption times between cryptographic algorithms. RSA-4096 has the longest key generation time, taking 3.0 seconds, indicating its computational complexity. The Proposed algorithm, on the other hand, performs faster with a key generation time of 0.3 seconds. The Proposed algorithm offers a good balance of speed and security, compared to RSA-4096, which offers strong security but comes at a cost. The cloud computing performance metrics demonstrate significant values in Network Bandwidth (Mbps), with a range reaching up to 700 Mbps, followed by Throughput (req/sec) at around 500 req/sec, indicating the system's capability to handle high traffic. The Latency (ms), Response Time (ms), and Disk I/O Speed (MB/s) show balanced performance, ensuring quick data transmission and efficient storage, confirming the robustness of the proposed methodology for secure and efficient cloud-based data management.

Keywords: Internet of Things (IoT), Cloud Computing, Security Framework, Sensor Data, Data Pre-processing, AES Encryption, Intrusion Detection System (IDS), Secure Data Transmission, Access Control, Data Integrity, Confidentiality, Real-time Threat Detection.

1. Introduction

The rapid proliferation of the Internet of Things (IoT) has fundamentally transformed the landscape of data generation, resulting in an unprecedented surge in sensor data collected from a diverse array of smart devices and interconnected environments [1]. These devices continuously monitor and capture vital information, spanning domains such as healthcare, smart cities, industrial automation, and environmental monitoring [2]. Due to the voluminous, continuous, and often sensitive nature of this data, cloud computing has emerged as the preferred infrastructure for its scalable storage capabilities and ability to facilitate near-instantaneous data processing and analytics [3]. Cloud platforms enable centralized management and computational resources that far exceed the capacity of individual IoT devices, thereby supporting sophisticated data-driven decision-making and services [4]. However, the transmission and management of IoT sensor data in cloud environments introduce significant security challenges that cannot be overlooked [5] [6]. The vast and often unprotected nature of IoT networks exposes them to threats such as unauthorized access, data breaches, man-in-the-middle attacks, and exploitation of software and hardware vulnerabilities inherent to both the IoT devices and cloud infrastructure [7]. The resource constraints typical of IoT devices—including limited processing power, memory, and energy—pose additional hurdles in implementing robust security protocols locally [8]. Moreover, the open and multi-tenant architecture of cloud platforms increases the attack surface, making the protection of data confidentiality, integrity, and availability throughout its lifecycle critically important [9] [10].

To address these concerns, it is imperative to develop a comprehensive and multilayered security framework that can safeguard IoT sensor data from the point of generation through transmission, storage, and access [11]. Such a framework must integrate several essential components: effective data pre-processing to enhance data quality, secure data transmission protocols fortified by strong encryption standards, real-time intrusion detection systems (IDS) to promptly identify malicious activities, and strict access control mechanisms that enforce user authentication and authorization policies [12]. By incorporating these mechanisms, organizations can significantly mitigate cyber threats, prevent data leakage, and ensure the trustworthiness of IoT-enabled services, which is fundamental for user confidence and broader adoption [13]. The proposed methodology in this paper outlines the design and implementation of a secure and efficient framework tailored for the end-to-end management of IoT sensor data within cloud ecosystems [14]. Initially, raw data is gathered from distributed IoT sensors and undergoes critical pre-processing steps such as noise filtering to remove irrelevant or corrupted signals, normalization to scale data uniformly, and timestamp alignment to synchronize asynchronous data streams [15]. These processes ensure that subsequent analysis and security mechanisms operate on high-quality, consistent data [16]. Subsequently, a real-time Intrusion Detection System (IDS) continuously monitors incoming data streams and system behavior to detect anomalies and potential cyber threats, enabling proactive response to security incidents [17].

Following threat analysis, the data undergoes encryption using the Advanced Encryption Standard (AES), a widely accepted symmetric-key algorithm known for its strong security and efficiency [18]. This step is crucial to maintain the confidentiality and integrity of data as it is transmitted over potentially insecure networks to the cloud [19]. Within the cloud environment, the encrypted data is securely stored using robust cloud storage solutions equipped with redundancy and fault tolerance [20]. To prevent unauthorized data access or manipulation, role-based access control (RBAC) mechanisms are enforced, ensuring that only authenticated and authorized users or systems can interact with sensitive sensor data [21]. This layered approach to security not only reduces system vulnerabilities but also enhances overall data governance and compliance with regulatory standards [22]. An essential phase of the framework involves rigorous evaluation and testing to measure the performance, security efficacy, and resilience of the implemented system [23]. Performance metrics such as encryption and decryption latency, detection accuracy of the IDS, and system throughput are analyzed to validate the feasibility of deploying the framework in practical IoT-cloud settings [24]. The evaluation also ensures that security enhancements do not introduce prohibitive overheads or degrade the quality of service [25].

Despite significant progress in integrating IoT with cloud platforms, many existing solutions fall short of providing holistic security coverage throughout the data lifecycle [26]. Commonly, current systems emphasize securing storage or transmission channels independently, neglecting comprehensive, end-to-end protection [27]. The underutilization of real-time Intrusion Detection Systems (IDS) in many frameworks leaves IoT ecosystems vulnerable to sophisticated and evolving cyberattacks that can bypass static security measures [28]. Moreover, the absence of systematic data pre-processing adversely affects data consistency, which in turn impairs the accuracy and responsiveness of threat detection mechanisms [29]. Traditional encryption methods, while robust, often fail to account for the computational and energy constraints of IoT devices, resulting in performance bottlenecks that limit practical adoption [30]. Additionally, inadequate access control policies and weak authentication protocols in cloud storage environments expose sensitive data to risks of unauthorized access, data leaks, and insider threats [31]. These critical shortcomings underscore the pressing need for a comprehensive and integrated security framework capable of addressing data integrity, confidentiality, availability, and real-time threat mitigation within IoT-cloud ecosystems [32].

In addition to ensuring robust security, the proposed framework emphasizes scalability and adaptability to accommodate the rapidly evolving landscape of IoT deployments and cloud technologies [33]. As the number of connected devices and volume of sensor data continue to grow exponentially, security solutions must scale efficiently without compromising performance or introducing significant latency [34]. This requires lightweight encryption and intrusion detection algorithms optimized for resource-constrained IoT devices, alongside elastic cloud infrastructure capable of dynamically allocating resources based on workload demands [35]. Furthermore, the framework is designed to be modular and extensible, enabling the integration of emerging technologies such as machine learning-based anomaly detection, blockchain for immutable audit trails, and post-quantum cryptography to future-proof data protection against next-generation threats [36]. By incorporating these forward-looking features, the framework aims not only to address current security challenges but also to provide a resilient foundation adaptable to the continuous innovation and diversification of IoT ecosystems [37].

This paper contributes to the state of the art by proposing a novel, layered security framework that addresses these gaps through the synergistic integration of data pre-processing, intrusion detection, encryption, secure transmission, and fine-grained access control tailored to the unique constraints and requirements of IoT sensor data and cloud computing platforms.

The contribution of the paper is below;

- The paper proposes a comprehensive security framework for managing IoT sensor data in cloud environments, integrating data pre-processing, AES encryption, and intrusion detection systems (IDS).
- It addresses challenges related to securing sensitive IoT data, ensuring confidentiality, integrity, and availability throughout its lifecycle.
- The methodology emphasizes real-time threat detection and secure data transmission and storage, enhancing overall system reliability and trust.

2. Literature Survey

The integration of Wireless Sensor Networks (WSNs) with cloud computing has garnered significant attention in recent years due to its potential to revolutionize data transmission, storage, and processing capabilities across various domains [38]. WSNs, composed of spatially distributed sensor nodes, are widely used for monitoring physical or environmental conditions [39]. However, these networks are inherently constrained by limited computational power, restricted energy resources, and bandwidth limitations, which pose challenges for continuous, reliable data collection and real-time processing [40]. Cloud computing, with its virtually unlimited scalable resources and advanced data processing capabilities, offers an attractive solution to these limitations by offloading computationally intensive tasks from sensor nodes to powerful cloud servers [41]. Various architectural models have been proposed to facilitate fast, secure, and reliable sensor data transmission from WSNs to cloud platforms [42]. These models aim to optimize the entire data lifecycle—ranging from collection, preprocessing, transmission, storage, to analytics—thereby enhancing communication speed, reducing latency, and strengthening system security through the adoption of robust protocols and encryption mechanisms [43].

The conceptual framework introduced in this study emphasizes the seamless management of sensor data, ensuring efficient flow from initial collection at the sensor level to sophisticated cloud-level processing and decision-making [44]. This approach is particularly critical in industrial applications where real-time monitoring of manufacturing equipment is essential [45]. In the context of Industry 4.0, characterized by smart factories and automation, there is an escalating demand for enhanced remote monitoring systems that enable predictive maintenance and operational efficiency improvements [46]. These systems rely heavily on the effective integration of IoT and cloud technologies to handle large-scale sensor data in near real-time [47]. However, this integration presents substantial challenges, commonly referred to as the "4Vs" of big data: volume, velocity, variety, and veracity [48]. These factors complicate data management due to the massive influx of heterogeneous data types, the need for rapid processing, and the necessity to ensure data quality and reliability [49]. Additionally, the incorporation of domain-specific knowledge into data analytics is critical but complex, further amplifying the challenges faced by conventional monitoring systems [50]. While traditional monitoring approaches are already struggling with these issues, the fusion of IoT and cloud computing introduces added complexity, particularly regarding infrastructure availability, system scalability, and consistent data quality assurance [51].

To mitigate these challenges, context information management has emerged as a pivotal strategy. By leveraging contextual data—such as temporal, spatial, and environmental factors—the system can make more informed decisions, improving the accuracy and relevance of monitoring and analytics processes [52]. The paper proposes a conceptual context-aware framework designed to integrate IoT and cloud computing technologies explicitly to enhance remote monitoring services [53]. This framework supports dynamic adaptation to changing environmental conditions and user requirements, facilitating improved system responsiveness and reliability [54]. With the rise of Big Data operations, cloud deployment architectures have become increasingly favored due to their inherent scalability, flexibility, and cost-effectiveness [55]. Cloud platforms enable organizations to dynamically allocate resources, manage large datasets efficiently, and deploy applications with reduced upfront infrastructure costs [56]. However, this transition to cloud-centric data management introduces significant security and privacy concerns [57]. As data and applications move beyond the physical control of organizations, traditional security paradigms become insufficient [58]. Data hosted in multi-tenant cloud environments is vulnerable to a wide array of cyber threats, including unauthorized access, insider attacks, data leakage, and compliance violations. Addressing these vulnerabilities requires a fundamental rethinking of security design principles [59].

In response, recent research has proposed a novel security-by-design framework termed "Big Cloud," which is grounded in a systematic security analysis methodology coupled with an automated security assessment mechanism [60]. This framework guides the integration of security requirements early in the design phase of cloud systems, aligning them with established best practices and industry standards [61]. By embedding security considerations throughout the development lifecycle, Big Cloud aims to reduce vulnerabilities, improve threat awareness, and facilitate more robust security implementations [62]. A practical case study deploying an Apache Hadoop stack demonstrated the framework's efficacy by enhancing security awareness among developers, shortening design cycles, and identifying both strengths and weaknesses of existing Big Cloud security practices [63]. The study further highlights persistent challenges such as the dynamic nature of threats, the complexity of cloud ecosystems, and the need for continuous innovation in cloud security solutions [64]. Cloud computing's rapid expansion is fueled by its scalable infrastructure, cost efficiency, and flexible service delivery models, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) [65]. Despite these advantages, the migration of sensitive organizational data and critical applications to cloud platforms raises pressing privacy and security issues [66]. New attack vectors continuously emerge, challenging the effectiveness of conventional security mechanisms such as firewalls, antivirus software, and access control policies [67]. Organizations lacking robust, adaptive security measures face severe risks, including data breaches that can lead to financial loss, regulatory penalties, and irreparable reputational damage [68].

Emerging technologies and evolving threats continue to shape the landscape of IoT and cloud integration, driving the development of more sophisticated security solutions [69]. Recent trends emphasize the adoption of artificial intelligence (AI) and machine learning (ML) techniques to enhance anomaly detection, threat prediction, and automated response within IoT-cloud ecosystems [70]. These intelligent systems can analyze vast streams of sensor data in real time, identify subtle patterns indicative of cyberattacks, and adapt dynamically to new and unknown threats [71]. Furthermore, blockchain technology is gaining traction as a decentralized, tamper-resistant ledger for securing IoT data provenance, access logs, and device authentication, addressing trust and transparency challenges inherent in distributed environments [72]. Edge and fog computing paradigms are also becoming integral by enabling data processing closer to the source, reducing latency, and alleviating bandwidth constraints while providing additional layers of security through localized analytics and policy enforcement [73]. Despite these advancements, challenges remain in standardizing security protocols, ensuring interoperability among heterogeneous devices, and balancing the trade-offs between security, privacy, and resource consumption [74]. Future research is poised to focus on developing unified frameworks that holistically integrate these technologies, fostering resilient, scalable, and secure IoT-cloud infrastructures that can meet the demands of increasingly complex and mission-critical applications [75].

To confront these risks, comprehensive security and management frameworks tailored for cloud environments have been developed. One such framework identifies the key threats and vulnerabilities specific to cloud-hosted data and applications and proposes a layered security architecture to mitigate these risks effectively. Implemented in virtualized cloud environments using platforms such as VMware ESXi-6 and vCloud-6, this framework emphasizes the enforcement of data integrity, confidentiality, and availability through combined technical, administrative, and procedural controls. By employing virtualization security best practices, secure hypervisor configurations, network segmentation, encryption, and continuous monitoring, the framework enhances the overall resilience of cloud-based systems against internal and external threats. Such solutions are critical for organizations aiming to securely harness cloud computing benefits while maintaining compliance with regulatory standards and safeguarding stakeholder trust.

3. Problem Statement

The rapid growth of IoT devices has led to an enormous amount of sensor-generated data, which is highly vulnerable to cyber threats such as unauthorized access, data breaches, and malicious attacks. Traditional security measures often fall short due to the diverse nature of IoT devices and their limited computing power [76]. As IoT data is continuously transmitted to cloud storage, it becomes susceptible to man-in-the-middle attacks, data interception, and tampering [77]. Additionally, poor data pre-processing can lead to inconsistencies, reducing the accuracy of security mechanisms [78]. One of the major challenges in IoT security is the lack of an efficient Intrusion Detection System (IDS), which can result in delayed or missed detection of threats [79]. Moreover, unencrypted data transmission makes IoT networks an easy target for cybercriminals [80]. Without strong encryption and secure access control mechanisms, sensitive IoT data remains at risk [81]. To address these challenges, a secure IoT data management framework is needed to ensure data confidentiality, integrity, and secure storage in cloud environments [82]. The proposed framework includes data pre-processing techniques like noise filtering, normalization, and timestamp alignment to improve data quality. It also integrates an Intrusion Detection System (IDS) to identify and prevent potential threats. AES encryption is applied to protect data before transmission to the cloud, ensuring secure communication. Additionally, strict access control mechanisms are enforced to prevent unauthorized access. By implementing end-to-end security measures from data collection to cloud storage, this framework minimizes security risks and enhances IoT data protection. The use of advanced security techniques, encryption, and continuous evaluation ensures a robust and reliable system for managing IoT sensor data securely in cloud computing environments.

4. Proposed Methodology

The proposed methodology begins with the collection of data from IoT sensors, forming the IoT Sensor Dataset. This raw data undergoes several pre-processing steps to ensure its quality and consistency. The first step is Noise Filtering, which removes any unwanted noise from the data. Next, Normalization is applied to standardize the data, ensuring it is on a consistent scale. The final pre-processing step is Timestamp Alignment, which ensures that all sensor data is synchronized properly. Once pre-processed, the data is analysed by an Intrusion Detection System (IDS). The IDS scans the data for any potential threats or malicious activities that could compromise the system's security. After analysis, the data undergoes AES Encryption, which encrypts the data to protect its confidentiality and integrity. The encrypted data is then securely transmitted to the Cloud, ensuring that no unauthorized access occurs during transmission. Upon reaching the cloud, the data is stored in Cloud Storage. To ensure that only authorized users can access the data, appropriate Access Control measures are implemented. Finally, the entire system undergoes Evaluation. This step assesses the effectiveness of the security measures, including the IDS and encryption processes. The evaluation helps ensure that the system functions as intended, with all data securely stored and transmitted, and potential threats successfully detected. The whole workflow is illustrated in Figure 1.

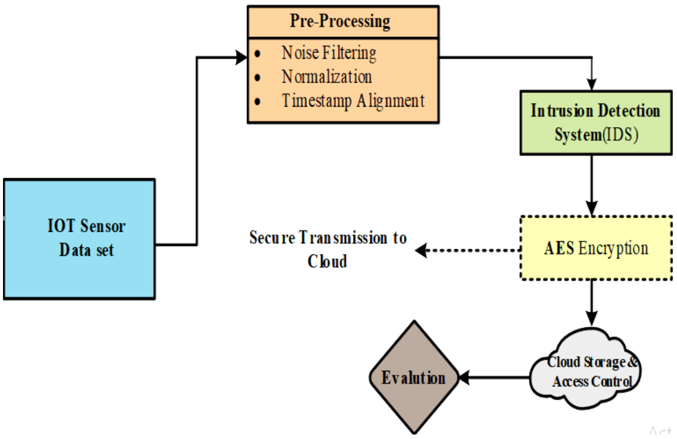

Fig 1: Overall architecture of the proposed method

4.1. Dataset Collection

The dataset collection begins with the acquisition of IoT Sensor Data, which contains real-time readings from various IoT devices. These sensors monitor different environmental and system parameters, such as temperature, humidity, pressure, etc. The raw data collected from these IoT sensors typically requires further pre-processing to ensure its quality and suitability for subsequent analysis.

4.2. Pre-processing

The pre-processing phase involves preparing the raw IoT sensor data for analysis. This begins with Noise Filtering, where irrelevant or erroneous data caused by sensor malfunctions or environmental disturbances is removed to ensure the data's validity. Afterward, Normalization is applied to standardize the data, bringing all values to a consistent scale, preventing any feature from disproportionately influencing the analysis. Lastly, Timestamp Alignment is performed to synchronize the data collected from different sensors, ensuring all data points are aligned on a unified time scale for accurate comparison and analysis. These steps are crucial for ensuring data quality and consistency before it is passed to the Intrusion Detection System (IDS) and other stages of processing.

4.3. Noise Filtering

Noise filtering removes irrelevant or erroneous data that may distort the analysis. This can include sensor malfunctions or environmental disturbances. The goal is to retain only clean, valid data for further processing. A common method for noise filtering is the Moving Average Filter, expressed as:

$$y(t) = \frac{1}{N}\sum_{i=t-N+1}^{t} x(i) \quad (1)$$

Where y(t)y(t)y(t) is the filtered value at time t, $x^{(i)}$The raw data, and N is the number of data points used for averaging.

4.4. Normalization

Normalization scales the data to a common range, ensuring all features contribute equally. This is especially useful when combining data from sensors with different units. A common formula is min-max normalization:

$$x_{norm} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (2)$$

Where xxx is the original value, x_{norm} Is the normalized value, and min(x) and max(x) are the minimum and maximum values in the dataset.

4.5. Timestamp Alignment

Timestamp alignment synchronizes data from multiple sensors to the same time scale, ensuring accurate comparison and analysis. A basic formula for linear interpolation is:

$$x(t) = x(t_0) + \frac{(t - t_0)}{(t - t_0)}.(x(t1) - x(t0)) \quad (3)$$

Where x(t) is the interpolated value at time t, x(t0) and x(t1) are values at times t0 and t1, respectively.

4.6. Intrusion Detection System

An Intrusion Detection System (IDS) is a security mechanism that monitors network traffic and system activities to detect unauthorized access and cyber threats in IoT-cloud environments. It identifies suspicious patterns, anomalies, and attacks like malware injection, DDoS, and unauthorized API requests. IDS is classified into Network-based IDS (NIDS), which analyzes network traffic, and Host-based IDS (HIDS), which monitors activities on individual devices or servers. Modern IDS solutions integrate machine learning (ML) and artificial intelligence (AI) to detect zero-day attacks and evolving threats. Once an intrusion is detected, IDS triggers alerts and can collaborate with encryption techniques like AES (Advanced Encryption Standard) to enhance data security. Cloud service providers like AWS, Google Cloud, and Microsoft Azure offer built-in IDS solutions such as AWS Guard Duty, Google Security Command Centre, and Azure Security Center. IDS ensures data integrity, confidentiality, and compliance with regulations like GDPR and HIPAA. It enhances the security of IoT-cloud systems by preventing unauthorized data access and mitigating security breaches. IDS works alongside firewalls, encryption, and authentication mechanisms to provide a robust security framework. Its deployment in cloud-based environments is essential for securing sensitive IoT sensor data. The architecture of intrusion detection system is illustrated in Figure 2.

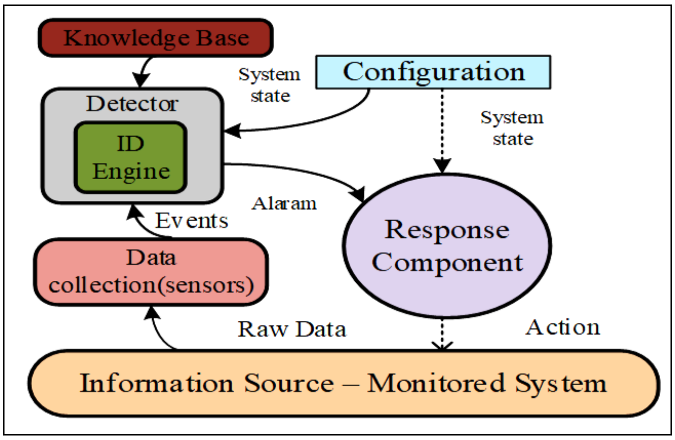

Fig 2: Intrusion Detection System (IDS) Model architecture

4.7. AES – Encryption

AES Encryption (Advanced Encryption Standard) is a widely used symmetric encryption algorithm designed for secure data transmission and storage. It operates on fixed block sizes of 128 bits and supports key lengths of 128, 192, or 256 bits, ensuring robust security. AES follows a substitution-permutation network (SPN) structure, consisting of multiple rounds of transformations, including Sub Bytes, Shift Rows, Mix Columns, and Arounder operations. It is resistant to brute-force attacks due to its complex key expansion process. In IoT-cloud environments, AES encryption safeguards sensor data during transmission and storage, preventing unauthorized access and data breaches. It is commonly used in TLS (Transport Layer Security) protocols to establish secure cloud connections. Cloud providers such as AWS, Azure, and Google Cloud integrate AES-based encryption in their storage and security services. AES enhances data confidentiality, ensuring that only authorized entities can decrypt sensitive IoT data. It is an essential security mechanism in Intrusion Detection Systems (IDS) to maintain data integrity and protect against cyber threats.

4.8. Google Cloud Platform (GCP)

Google Cloud Platform (GCP) is a comprehensive suite of cloud computing services provided by Google, offering secure and scalable infrastructure for data storage, computation, and machine learning applications. It provides compute power (Google Compute Engine, Kubernetes Engine), storage solutions (Cloud Storage, Big Query), networking (Cloud VPN, Load Balancing), and AI/ML services (Vertex AI, TensorFlow Cloud) to support various workloads. GCP ensures high security through AES-256 encryption, IAM (Identity and Access Management), and VPC Service Controls to protect sensitive IoT sensor data. Its Cloud IoT Core service enables seamless integration of IoT devices for real-time data processing and analytics. GCP also offers Intrusion Detection and Prevention Systems (IDPS) through the Security Command Centre, providing advanced monitoring against cyber threats. With global data centres and auto-scaling capabilities, GCP is ideal for managing large-scale IoT data securely. It also complies with HIPAA, GDPR, and ISO/IEC security standards, making it a preferred choice for cloud-based IoT applications in healthcare, finance, and industrial automation.

5. Dataset Description

An IoT dataset for Intrusion Detection Systems (IDS) typically consists of network traffic and device activity logs collected from various IoT environments, such as smart homes, healthcare devices, and industrial IoT networks. The dataset includes features such as timestamp, source and destination IP addresses, protocol types (TCP, UDP, ICMP), packet sizes, and payload data, helping in identifying malicious activities. It often contains both normal and attack traffic, categorized into different intrusion types like DoS (Denial of Service), Man-in-the-Middle (MITM), data injection, botnet attacks, and scanning attacks. Some datasets also incorporate device behaviour metrics, such as CPU usage, memory consumption, and command execution logs, to detect anomalies at the device level. Publicly available datasets, such as NSL-KDD, UNSW-NB15, Bot-IoT, and N-BaIoT, serve as benchmarks for IDS research, offering labelled data with attack and normal instances. These datasets enable the training and evaluation of machine learning models, deep learning-based IDS, and AI-driven threat detection mechanisms. By analysing such datasets, researchers and security experts can improve real-time intrusion detection, anomaly detection accuracy, and cyber defence strategies for IoT ecosystems.

Dataset Link: https://www.kaggle.com/datasets/azalhowaide/iot-dataset-for-intrusion-detection-systems-ids

6. Result and Discussion

The proposed methodology outlines a comprehensive approach to secure IoT sensor data management, starting with data collection and pre-processing steps such as noise filtering, normalization, and timestamp alignment to ensure data consistency and quality. The application of an Intrusion Detection System (IDS) helps identify and mitigate potential threats in real time, enhancing the security of the data. AES encryption is then applied to protect the data's confidentiality and integrity before secure transmission to the cloud. Once stored in cloud storage, access control measures prevent unauthorized access, safeguarding the data further. The system's effectiveness is evaluated through a thorough assessment of the security measures, including the performance of the IDS and encryption mechanisms. This ensures the system operates as intended, with secure data storage, transmission, and threat detection.

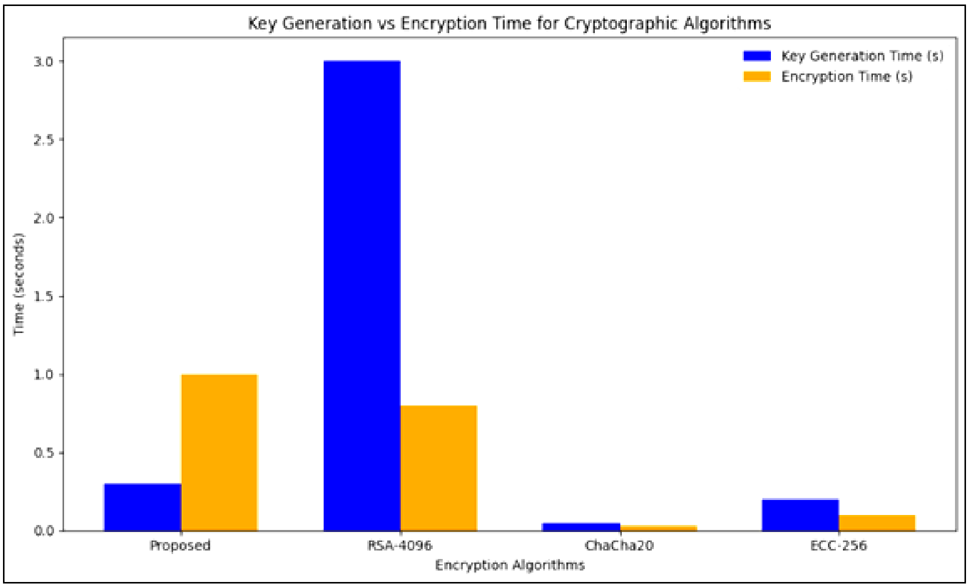

Fig 3: Encryption algorithms

Figure 3 shows the comparison of the key generation and encryption times for four cryptographic algorithms: Proposed, RSA-4096, ChaCha20, and ECC-256. The Proposed algorithm demonstrates the fastest performance in both key generation and encryption, making it highly efficient for real-time applications. RSA-4096 shows significantly longer key generation times, reflecting its computational complexity, while its encryption time remains moderate. ChaCha20 is exceptionally fast, with very low-key generation and encryption times, making it ideal for IoT and mobile environments. ECC-256 provides a good balance of performance and security, with low key generation and encryption times, suitable for secure applications requiring efficiency.

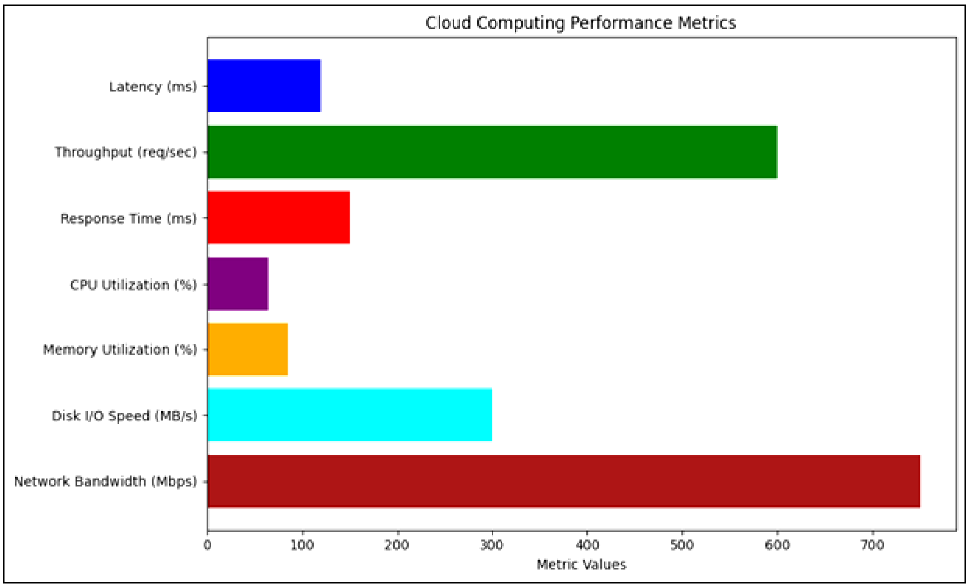

Fig 4: Performance metrics for cloud computing

Figure 4 represents various cloud computing performance metrics, with Network Bandwidth (Mbps) having the highest value, indicating its importance in determining the overall data transfer speed in cloud environments. Throughput (req/sec) follows closely, showcasing the system's capability to handle a high number of requests per second. Response Time (ms) and CPU Utilization (%) are also significant, reflecting the system's efficiency in processing tasks and the demand on computational resources. Disk I/O Speed (MB/s) and Memory Utilization (%) provide insights into storage performance and how efficiently the system utilizes available memory. Lastly, Latency (ms), though relatively lower in value, is crucial for ensuring quick response times in real-time applications.

7. Conclusion

The proposed security framework offers a holistic approach to managing IoT sensor data securely in cloud environments. By integrating multiple security measures such as noise filtering, normalization, timestamp alignment, AES encryption, and IDS, the framework ensures data confidentiality and integrity while addressing potential threats in real-time. It provides an effective solution to the challenges of secure data transmission, storage, and access control in IoT-cloud systems. The evaluation of the framework confirms its reliability and effectiveness in maintaining the security of sensitive data. This work highlights the importance of comprehensive security mechanisms and provides a foundation for further research and improvement in the field of IoT data security.

References

1. Tawalbeh LA, Muheidat F, Tawalbeh M & Quwaider M. IoT Privacy and security: Challenges and solutions. Applied Sciences. 2020; 10(12):4102.
2. Pulakhandam W & Samudrala VK. Automated Threat Intelligence Integration To Strengthen SHACS For Robust Security in Cloud-Based Healthcare Applications. *International Journal of Engineering & Science Research*, 2020, 10(4).
3. Zhu C, Leung VC, Rodrigues JJ, Shu L, Wang L & Zhou H. Social sensor cloud: framework, greenness, issues, and outlook. IEEE Network. 2018; 32(5):100-105.
4. Dondapati K. Clinical implications of big data in predicting cardiovascular disease using SMOTE for handling imbalanced data. *Journal of Cardiovascular Disease Research*. 2020; 11(9):191-202.
5. Ammar M, Russello G & Crispo B. Internet of Things: A survey on the security of IoT frameworks. *Journal of information security and Applications*. 2018; 38, 8-27.
6. Grandhi SH. Blockchain-enabled software development traceability: Ensuring secure and transparent software lifecycle management. *International Journal of Information Technology & Computer Engineering*, 2020, 8(3).
7. Ojha T, Misra S & Raghuwanshi NS. Sensing-cloud: Leveraging the benefits for agricultural applications. Computers and electronics in agriculture. 2017; 135:96-107.
8. Natarajan DR. AI-Generated Test Automation for Autonomous Software Verification: Enhancing Quality Assurance through AI-Driven Testing. *Journal of Science and Technology*, 2020, 5(5).
9. Manogaran G, Varatharajan R, Lopez D, Kumar PM, Sundarasekar R & Thota C. A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system. Future Generation Computer Systems. 2018; 82:375-387.
10. Srinivasan K. Neural network-driven Bayesian trust prediction model for dynamic resource management in cloud computing and big data. *International Journal of Applied Science Engineering and Management*, 2020, 14(1).
11. Srinivas J, Das AK & Kumar N. Government regulations in cyber security: Framework, standards and recommendations. Future generation computer systems. 2019; 92:178-188.
12. Chauhan GS. Utilizing data mining and neural networks to optimize clinical decision-making and patient outcome predictions. *International Journal of Marketing Management*. 2020; 8(4):32-51.
13. Gonzalez C, Charfadine SM, Flauzac O & Nolot F. SDN-based security framework for the IoT in distributed grid. In 2016 international multidisciplinary conference on computer and energy science (SpliTech). IEEE, 2016, 1-5.
14. Gollapalli VST. Enhancing disease stratification using federated learning and big data analytics in healthcare systems. *International Journal of Management Research and Business Strategy*. 2020; 10(4):19-38.
15. Suciu G, Suciu V, Martian A, Craciunescu R, Vulpe A, Marcu I & Fratu O. Big data, internet of things and cloud convergence–an architecture for secure e-health applications. *Journal of medical systems*. 2015; 39:1-8.
16. Gollapalli VST. Scalable Healthcare Analytics in the Cloud: Applying Bayesian Networks, Genetic Algorithms, and LightGBM for Pediatric Readmission Forecasting. *International Journal of Life Sciences Biotechnology Pharma Sciences*, 2020, 16(2).
17. Obaidat MA, Obeidat S, Holst J, Al Hayajneh A & Brown J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers. 2020; 9(2):44.
18. Ganesan T. Deep learning and predictive analytics for personalized healthcare: unlocking EHR insights for patient-centric decision support and resource optimization. *International Journal of HRM and Organizational Behavior*, 2020, 8(3).
19. Patil AS, Tama BA, Park Y & Rhee KH. A framework for blockchain based secure smart greenhouse farming. In Advances in Computer Science and Ubiquitous Computing: CSA-CUTE 17, 2018, 1162-1167. Springer Singapore.
20. Panga NKR & Thanjaivadivel M. Adaptive DBSCAN and Federated Learning-Based Anomaly Detection for Resilient Intrusion Detection in Internet of Things Networks. *International Journal of Management Research and Business Strategy*, 2020, 10(4).
21. Wu J, Ota K, Dong M & Li C. A hierarchical security framework for defending against sophisticated attacks on wireless sensor networks in smart cities. IEEE Access. 2016; 4:416-424.
22. Dyavani NR & Hemnath R. Blockchain-integrated cloud software networks for secure and efficient ISP federation in large-scale networking environments. *International Journal of Engineering Research and Science & Technology*, 2020, 16(2). https://ijerst.org/index.php/ijerst/article/view/614/558
23. Newaz AI, Sikder AK, Rahman MA & Uluagac AS. Healthguard: A machine learning-based security framework for smart healthcare systems. In 2019 sixth international conference on social networks analysis,

management and security (SNAMS). IEEE, 2019, 389-396.

24. Durai Rajesh Natarajan & Sai Sathish Kethu. Decentralized anomaly detection in federated learning: Integrating one-class SVM, LSTM networks, and secure multi-party computation on Ethereum blockchain. *International Journal of Computer Science Engineering Techniques*, 2019, 5(4).
25. Fathi R, Salehi MA & Leiss EL. User-friendly and secure architecture (UFSA) for authentication of cloud services. In 2015 IEEE 8th *International Conference on Cloud Computing*. IEEE, 2015, 516-523.
26. Nagarajan H & Kurunthachalam A. Optimizing database management for big data in cloud environments. *International Journal of Modern Electronics and Communication Engineering*, 2018, 6(1).
27. Sani AS, Yuan D, Jin J, Gao L, Yu S & Dong ZY. Cyber security framework for Internet of Things-based Energy Internet. Future Generation Computer Systems. 2019; 93:849-859.
28. Basani DKR & Aiswarya RS. Integrating IoT and robotics for autonomous signal processing in smart environment. *International Journal of Information Technology and Computer Engineering*, 2018, 6(2).
29. Manogaran G, Thota C, Lopez D & Sundarasekar R. Big data security intelligence for healthcare industry 4.0. In Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing. Cham: *Springer international publishing*, 2017, 103-126.
30. Gudivaka BR & Palanisamy P. Enhancing software testing and defect prediction using Long Short-Term Memory, robotics, and cloud computing. International *Journal of modern electronics and communication Engineering*, 2018, 6(1).
31. Kumar P, Braeken A, Gurtov A, Iinatti J & Ha PH. Anonymous secure framework in connected smart home environments. IEEE Transactions on Information Forensics and Security. 2017; 12(4):968-979.
32. Kodadi S & Kumar V. Lightweight deep learning for efficient bug prediction in software development and cloud-based code analysis. *International Journal of Information Technology and Computer Engineering*, 2018, 6(1).
33. Manogaran G, Thota C & Kumar MV. Meta Cloud Data Storage architecture for big data security in cloud computing. Procedia Computer Science. 2016; 87:128-133.
34. Bobba J & Prema R. Secure financial data management using Twofish encryption and cloud storage solutions. *International Journal of Computer Science Engineering Techniques*. 2018; 3(4):10–16.
35. Gehrmann C & Gunnarsson M. A digital twin based industrial automation and control system security architecture. IEEE Transactions on Industrial Informatics. 2019; 16(1):669-680.
36. Gollavilli VSB & Thanjaivadivel M. Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. *International Journal of Information Technology and Computer Engineering*. 2018; 6(4):77–85. ISSN 2347–3657.
37. Abed SE, Al-Shayeji M & Ebrahim F. A secure and energy-efficient platform for the integration of Wireless Sensor Networks and Mobile Cloud Computing. Computer Networks. 2019; 165:106956.
38. Nippatla RP & Palanisamy P. Enhancing cloud computing with eBPF powered SDN for secure and scalable network virtualization. *Indo-American Journal of Life Sciences and Biotechnology*, 2018, 15(2).
39. Abed SE, Al-Shayeji M & Ebrahim F. A secure and energy-efficient platform for the integration of Wireless Sensor Networks and Mobile Cloud Computing. Computer Networks. 2019; 165:106956.
40. Budda R & Pushpakumar R. Cloud Computing in Healthcare for Enhancing Patient Care and Efficiency. *Chinese Traditional Medicine Journal*. 2018; 1(3):10-15.
41. Garg S, Singh A, Kaur K, Aujla GS, Batra S, Kumar N, & Obaidat MS. Edge computing-based security framework for big data analytics in VANETs. IEEE Network. 2019; 33(2):72-81.
42. Vallu VR & Palanisamy P. AI-driven liver cancer diagnosis and treatment using cloud computing in healthcare. *Indo-American Journal of Life Sciences and Biotechnology*, 2018, 15(1).
43. Sengan S, Subramaniyaswamy V, Nair SK, Indragandhi V, Manikandan J & Ravi L. Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network. Future generation computer systems. 2020; 112:724-737.
44. Jayaprakasam BS & Hemnath R. Optimized microgrid energy management with cloud-based data analytics and predictive modelling. *International Journal of modern electronics and communication Engineering*. 2018; 6(3):79–87.
45. Rathore S, Kwon BW & Park JH. BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network. *Journal of Network and Computer Applications*. 2019; 143:167-177.
46. Mandala RR & Purandhar N. Optimizing secure cloud-enabled telemedicine system using LSTM with stochastic gradient descent. *Journal of Science and Technology*, 2018, 3(2).
47. Tao M, Zuo J, Liu Z, Castiglione A & Palmieri F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Generation Computer Systems. 2018; 78:1040-1051.
48. Garikipati V & Palanisamy P. Quantum-resistant cyber defence in nation-state warfare: Mitigating threats with post-quantum cryptography. *Indo-American Journal of Life Sciences and Biotechnology*, 2018, 15(3).
49. Mozzaquatro BA, Agostinho C, Goncalves D, Martins J, & Jardim-Goncalves R. An ontology-based cybersecurity framework for the internet of things. Sensors. 2018; 18(9):3053.
50. Ubagaram C & Mekala R. Enhancing data privacy in cloud computing with blockchain: A secure and decentralized approach. *International Journal of Engineering & Science Research*. 2018; 8(3):226–233.
51. Huang X, Craig P, Lin H & Yan Z. SecIoT: a security framework for the Internet of Things. Security and communication networks. 2016; 9(16):3083-3094.
52. Ganesan S & Kurunthachalam A. Enhancing financial predictions using LSTM and cloud technologies: A data-driven approach. *Indo-American Journal of Life Sciences and Biotechnology*, 2018, 15(1).
53. Bagaa M, Taleb T, Bernabe JB & Skarmeta A. A machine learning security framework for IoT systems. IEEE access. 2020; 8:114066-114077.
54. Musam VS & Kumar V. Cloud-enabled federated learning with graph neural networks for privacy-

preserving financial fraud detection. *Journal of Science and Technology*, 2018, 3(1).

55. Lounis A, Hadjidj A, Bouabdallah A & Challal Y. Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. Future Generation Computer Systems. 2016; 55:266-277.
56. Musham NK & Pushpakumar R. Securing cloud infrastructure in banking using encryption-driven strategies for data protection and compliance. *International Journal of Computer Science Engineering Techniques*. 2018; 3(5):33–39.
57. Sohal AS, Sandhu R, Sood SK & Chang V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Computers & Security. 2018; 74:340-354.
58. Radhakrishnan P & Mekala R. AI-Powered Cloud Commerce: Enhancing Personalization and Dynamic Pricing Strategies. *International Journal of Applied Science Engineering and Management*, 2018, 12(1).
59. Xu Y & Helal A. Scalable cloud–sensor architecture for the Internet of Things. *IEEE Internet of Things Journal*. 2015; 3(3):285-298.
60. Nagarajan H & Kumar RL. Enhancing healthcare data integrity and security through blockchain and cloud computing integration solutions. *International Journal of Engineering Technology Research & Management*, 2020, 4(2).
61. Sridhar S & Smys S. Intelligent security framework for iot devices cryptography based end-to-end security architecture. In 2017 International Conference on Inventive Systems and Control (ICISC). IEEE, 2017, 1-5.
62. Gudivaka BR & Thanjaivadivel M. IoT-driven signal processing for enhanced robotic navigation systems. *International Journal of Engineering Technology Research & Management*, 2020, 4(5).
63. Medhane DV, Sangaiah AK, Hossain MS, Muhammad G & Wang J. Blockchain-enabled distributed security framework for next-generation IoT: An edge cloud and software-defined network-integrated approach. *IEEE Internet of Things Journal*. 2020; 7(7):6143-6149.
64. Chetlapalli H & Pushpakumar R. Enhancing accuracy and efficiency in AI-driven software defect prediction automation. *International Journal of Engineering Technology Research & Management*, 2020, 4(8).
65. Pirbhulal S, Samuel OW, Wu W, Sangaiah AK & Li G. A joint resource-aware and medical data security framework for wearable healthcare systems. Future Generation Computer Systems. 2019; 95:382-391.
66. Budda R & Mekala R. Cloud-enabled medical image analysis using ResNet-101 and optimized adaptive moment estimation with weight decay optimization. *International Research Journal of Education and Technology*, 2020, 03(02).
67. Wang T, Zhang G, Bhuiyan MZA, Liu A, Jia W & Xie M. A novel trust mechanism based on fog computing in sensor–cloud system. Future Generation Computer Systems. 2020; 109:573-582.
68. Vallu VR & Rathna S. Optimizing e-commerce operations through cloud computing and big data analytics. *International Research Journal of Education and Technology*, 2020, 03(06).
69. Pacheco J & Hariri S. IoT security framework for smart cyber infrastructures. In 2016 IEEE 1st International workshops on Foundations and Applications of self* systems (fas* w). IEEE, 2016, 242-247.
70. Jayaprakasam BS & Padmavathy R. Autoencoder-based cloud framework for digital banking: A deep learning approach to fraud detection, risk analysis, and data security. *International Research Journal of Education and Technology*, 2020, 03(12).
71. Patil R, Dudeja H & Modi C. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. Computers & Security. 2019; 85:402-422.
72. Mandala RR & Kumar VKR. AI-driven health insurance prediction using graph neural networks and cloud integration. *International Research Journal of Education and Technology*, 2020, 03(10).
73. Chadwick DW, Fan W, Costantino G, De Lemos R, Di Cerbo F, Herwono I & Wang XS. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future generation computer systems. 2020; 102:710-722.
74. Ubagaram C & Kurunthachalam A. Bayesian-enhanced LSTM-GRU hybrid model for cloud-based stroke detection and early intervention. *International Journal of Information Technology and Computer Engineering*, 2020, 8(4).
75. Khan MA, Quasim MT, Alghamdi NS & Khan MY. A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data. IEEe Access. 2020; 8:52018-52027.
76. Ganesan S & Hemnath R. Blockchain-enhanced cloud and big data systems for trustworthy clinical decision-making. *International Journal of Information Technology and Computer Engineering*, 2020, 8(3).
77. Chang V, Kuo YH & Ramachandran M. Cloud computing adoption framework: A security framework for business clouds. Future Generation Computer Systems. 2016; 57:24-41.
78. Musam VS & Purandhar N. Enhancing agile software testing: A hybrid approach with TDD and AI-driven self-healing tests. *International Journal of Information Technology and Computer Engineering*, 2020, 8(2).
79. Chang V & Ramachandran M. Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on services computing. 2015; 9(1):138-151.
80. Musham NK & Bharathidasan S. Lightweight deep learning for efficient test case prioritization in software testing using MobileNet & TinyBERT. *International Journal of Information Technology and Computer Engineering*, 2020, 8(1).
81. Mall S & Saroj SK. A new security framework for cloud data. Procedia computer science. 2018; 143:765-775.
82. Chang V & Ramachandran M. Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on services computing*. 2015; 9(1):138-151.