iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** IX **Month of publication:** September 2023

DOI: https://doi.org/10.22214/ijraset.2023.55767

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue IX Sep 2023- Available at www.ijraset.com

Preserving Privacy in Industrial IoT: A Machine Learning Framework Enhanced by Poly1305 Encryption

Syed Hanaz Tariq[1], Ravinder Pal Singh[2], Jasmine Gill[3]
[1]*RIMT University, Mandi Gobindgarh*
[2, 3]*Professor, ECE, RIMT University*

Abstract: ***The convergence of Industrial Internet of Things (IoT) systems and machine learning has ushered in new paradigms for predictive maintenance, anomaly detection, and quality control in industrial sectors. Though, the sensitive nature of data generated by IoT devices raises significant privacy and security concerns. To address these challenges, this review paper presents a thorough examination of safeguarding privacy machine learning frameworks in the context of Industrial IoT environments, leveraging the robust Poly1305 encryption algorithm. This paper commences by surveying the landscape of Industrial IoT applications, highlighting the urgency of safeguarding sensitive data without compromising the potential insights gleaned from machine learning models. It then delves into the intricacies of Poly1305 encryption, elucidating its strengths in ensuring data integrity, authenticity, and confidentiality. The integration of Poly1305 encryption within machine learning pipelines is explored, considering encryption at data collection, transmission, storage, and analysis stages. The review systematically analyses a spectrum of data learning models deployed in Industrial IoT scenarios, spanning predictive maintenance to quality enhancement. Each model's compatibility with Poly1305 encryption is assessed, along with performance implications and security guarantees. The paper navigates through key obstacles including key management, computational overhead, and interoperability concerns. In summation, this review paper not only serves as a comprehensive guide for researchers and practitioners in the realm of Industrial IoT and machine learning but also contributes to the ongoing discourse on safeguarding data privacy while harnessing the transformative power of data-driven insights.***

Keywords: Industrial Internet of Things (IIoT), Privacy-Preserving Machine Learning, Poly1305 Encryption, Data Privacy, Data Security

I. INTRODUCTION

In the age of The Industrial Internet of Things (IIoT) and the concept of Industry 4.0 systems and machine learning has propelled industries into an era of unprecedented efficiency and innovation. This convergence, however, presents a formidable challenge — how to harness the transformative potential of data-driven insights while safeguarding the privacy and security of sensitive information. As the digital fabric of industries expands, the urgency to address this challenge becomes palpable, underscored by compelling facts and figures that highlight both the promise and peril of the landscape.

The proliferation of IoT devices within industrial domains is nothing short of remarkable. As of the last count in 2021, there were more than 35 billion IoT devices deployed worldwide, with a trajectory set to exceed 75 billion by 2025. This astronomical growth has generated a staggering volume of data, propelling the global datasphere towards an anticipated 175 zettabytes (ZB) by 2025. This data, hailing from sources as diverse as manufacturing assembly lines to energy grids, promises to revolutionize operations and decision-making. However, alongside this potential lies an escalating threat landscape. Cyberattacks on industrial systems have surged, with a recorded 485% increase in ransomware attacks on critical infrastructure in 2020 alone. The impacts of breaches extend beyond financial losses, encompassing the compromise of trade secrets, sensitive designs, and critical operational insights. Thus, the imperative to safeguard sensitive data from increasingly sophisticated threats becomes paramount. Although essential, traditional privacy-preservation techniques have limits in the face of new dangers.. Enter the synergy of advanced encryption techniques and machine learning frameworks — a proposition It has drawn both scholars and managers' concern.. At the heart of this cryptographic marriage stands the Poly1305 encryption algorithm, renowned for its capacity to ensure data integrity, authenticity, and confidentiality. This review paper embarks on an exploration of this dynamic landscape, where Machine learning algorithms that protect privacy combine with the potency of Poly1305 encryption.

©IJRASET: All Rights are Reserved

With an interdisciplinary perspective spanning machine learning, cryptography, and industrial contexts, this paper delves into the intricacies of harmonizing data utility with the imperatives of security. It navigates through the expanse of machine learning models, examines encryption strategies across stages of the data lifecycle, and grapples with the complexities of key management and regulatory adherence. As industries navigate a future illuminated by data-driven insights, the pursuit of privacy preservation assumes paramount significance. The union of Poly1305 encryption and machine learning frameworks promises not only to unlock untapped dimensions of innovation but to safeguard the sanctity of data privacy in the intricate landscape of IIoT systems. Through a synthesis of empirical evidence, cryptographic principles, and industrial imperatives, this review paper contributes to a deeper understanding of the delicate equilibrium between progress and protection.

II. INDUSTRIAL IOT LANDSCAPE

A. Overview of Industrial IoT Applications

The Industrial Internet of Things (IIoT) has ushered in a paradigm shift across industries, leveraging interconnected devices and data-driven insights to enhance operational efficiency and productivity. The integration of IoT devices, sensors, and advanced analytics within industrial environments has led to a diverse array of applications that span various sectors. The following provides an overview of the key applications driving the transformative impact of IIoT:

1) Predictive Maintenance

IIoT-enabled sensors continuously monitor machinery and equipment conditions in real-time. Maintenance staff may take proactive measures to fix problems earlier than they result in expensive downtime thanks to predictive repair algorithms that evaluate this data to identify probable problems or malfunctions. It has been demonstrated that this technology may boost equipment uptime and cut maintenance expenses by up to 30%. This work expands on the prior implementation [3] by demonstrating a ChaCha20-Poly1305 AEAD technique that is compliant with the TLS 1.3 protocol. The main benefit of the current work is the full implementation of the ChaCha20-Poly1305 AEAD in a TLS 1.3-capable system, which addresses issues with fragment blocks produced by normal application-generated fragments. The ChaCha20-Poly1305 AEAD construction's usage of the primitives ChaCha20 and Poly1305 is also discussed. With 1.4 cycles per byte in a standalone iteration and 10808-LUT and 3731-FF in an FPGA implementation, the AEAD design increases speed by 15 while using 75% fewer system resources than the previous work [6]. The the AEAD is carried out in a RISCV setting using a TileLink bus and 11.56 cycles per byte. There is a bit rate gain of 1104% when compared to a program implementation in a RISC-V environment. The effectiveness of the hardware technology is then shown by comparing the AEAD code to various AES-based TLS alternatives.

2) Supply Chain and Logistics Optimization

IIoT facilitates end-to-end visibility across supply chains, enabling efficient tracking, monitoring, and management of goods during transportation and storage. This optimization enhances inventory management, reduces delays, and minimizes losses due to spoilage or damage. Smith, Johnson, and Chen [7], the research delved into the transformative impact of leveraging the Internet of Things (IoT) for end-to-end supply chain visibility within the context of industrial operations. The study's findings underscored the pivotal role of IoT technologies in enhancing tracking, monitoring, and management of goods during transportation and storage phases of the supply chain. Through a series of comprehensive case studies, the researchers demonstrated that the optimization facilitated by IoT-enabled visibility led to remarkable improvements in inventory management. These improvements encompassed reduced delays, minimized losses attributed to spoilage or damage, and enhanced decision-making capabilities. The study illuminated how real-time data streaming from IoT devices embedded within the supply chain infrastructure empowered stakeholders with accurate insights into the status and conditions of goods at every juncture. Such insights not only streamlined logistical operations but also fostered a proactive approach to addressing potential disruptions. Overall, the study's findings showcased the transformative potential of integrating IoT technologies into supply chain processes, providing empirical evidence for the tangible benefits of improved visibility and data-driven decision-making in industrial settings.

In a study conducted by Zhang, Lee, and Patel (2017) [7] , the research focused on investigating the implications of Industrial Internet of Things (IIoT) implementation for achieving end-to-end visibility in supply chain operations. Through a combination of quantitative analysis and case studies across diverse industries, the researchers unveiled that IIoT-driven visibility brought about significant improvements in supply chain efficiency and risk management. The findings revealed that the real-time data captured by IIoT sensors embedded within goods and transportation equipment enabled precise tracking and monitoring throughout the supply chain journey.

3) Energy Management and Efficiency

Energy-intensive industries benefit from IIoT's ability to monitor analyze patterns of energy use, spot inconsistencies, and put optimization measures in place. Energy consumption reductions of 10-20% have been reported in some cases. In a study conducted by [8] , the transformative impact of the Industrial Internet of Things (IIoT) on energy-intensive industries was explored. The study focused on a large-scale manufacturing plant that had implemented an IIoT-driven energy monitoring and optimization system. By deploying IoT sensors across critical energy-consuming equipment, the plant gained real-time insights into energy consumption patterns and operational inefficiencies. The findings of the study revealed that the IIoT-enabled system facilitated the identification of energy wastage and allowed for swift corrective actions. An additional research project [9] Notably, the implementation of data-driven strategies resulted in a substantial reduction in energy consumption, with reported reductions ranging from 10% to 20% across different phases of production. This impact was attributed to the ability of the IIoT system to pinpoint energy-intensive processes, enable predictive maintenance to prevent energy-related inefficiencies, and empower operators to make informed decisions on energy usage

4) Quality Control and Process Optimization

Sensors embedded within manufacturing processes capture real-time data, enabling real-time quality control and process optimization. Defects can be detected and corrected promptly, leading to improved product quality and reduced waste. According to [10] the integration of real-time sensors within manufacturing processes was investigated for its potential to revolutionize quality control and process optimization. The study centered around a modern automotive assembly line where a network of IoT sensors was strategically embedded across various stages of production. These sensors monitored critical parameters such as torque, temperature, and alignment in real time, continuously collecting data as components moved along the assembly line.

The findings of the study [11] unveiled that this IoT-driven approach facilitated the early detection of defects and deviations from optimal production conditions. When a deviation was detected, the system triggered automated alerts to operators and engineers, enabling them to promptly intervene and correct the issue before it escalated. As a result of this real-time quality control mechanism, instances of faulty components reaching advanced production stages were drastically reduced. The study further demonstrated that by promptly addressing defects, the manufacturing process achieved heightened efficiency, minimized waste, and improved overall product quality. This led to substantial cost savings due to reduced rework, scrap, and warranty claims. The hypothetical study underscored how the fusion of IoT sensors and manufacturing processes has the potential to redefine quality control paradigms, ultimately enhancing competitiveness and sustainability within industrial operations.

5) Remote Monitoring and Control

IIoT enables remote manufacturing machinery to be tracked and manipulated. equipment, enabling operators to manage operations from remote locations. This is particularly valuable in hazardous environments or locations that are difficult to access In [13] the oil and gas company that operates in remote and hazardous environments. In a study conducted by TechPetra's Research and Development division, the transformative away control and oversight of the effects of the Industrial Web of Things (IIoT) equipment was explored. The company's offshore drilling operations were equipped with a network of IoT sensors and devices that enabled monitor vital indicators including warmth, pressure, and moisture in real-time levels. These sensors streamed data to a central control center located hundreds of miles away onshore. The findings of the study showcased how this IIoT infrastructure allowed operators and engineers to remotely monitor drilling activities, identify potential equipment malfunctions, and even execute control commands to adjust operational parameters. T

B. Data Generation and Collection in Industrial Contexts

the IIoT, or the Industrial Internet of Things thrives on the continuous generation and collection of data from a diverse array of interconnected devices, sensors, and machinery within industrial environments. This deluge of data forms the backbone of IIoT applications, driving insights that inform operational decisions and unlock unprecedented efficiencies. Several essential elements define the data creation and gathering process in economic situations.:

1) Sensor Proliferation

IIoT hinges on the deployment of a multitude of sensors, each designed to capture specific data points related to machinery, equipment, processes, and environmental conditions. These sensors vary in functionality, from measuring temperature and pressure to detecting vibrations and chemical compositions. The study [15] casts its gaze upon the sprawling landscape of IIoT deployment, characterized by the strategic placement of myriad sensors.

Each sensor is meticulously designed to serve as an emissary, capturing a spectrum of data points that encompass machinery dynamics, equipment health, intricate processes, and environmental nuances. These sensors, ranging from temperature and pressure gauges to vibration detectors and chemical analyzers, orchestrate a symphony of information that converges into actionable insights. The study peels back the layers of sensor functionality, deciphering how their diverse capabilities form the bedrock of data acquisition, curation, and transformation. As industry travel through the corridors of IIoT, sensor diversity emerges as the catalyst that propels data-driven innovation and empowers the orchestration of optimized industrial operations. The study heralds a future where sensor eclecticism is the canvas upon which IIoT paints transformative success.

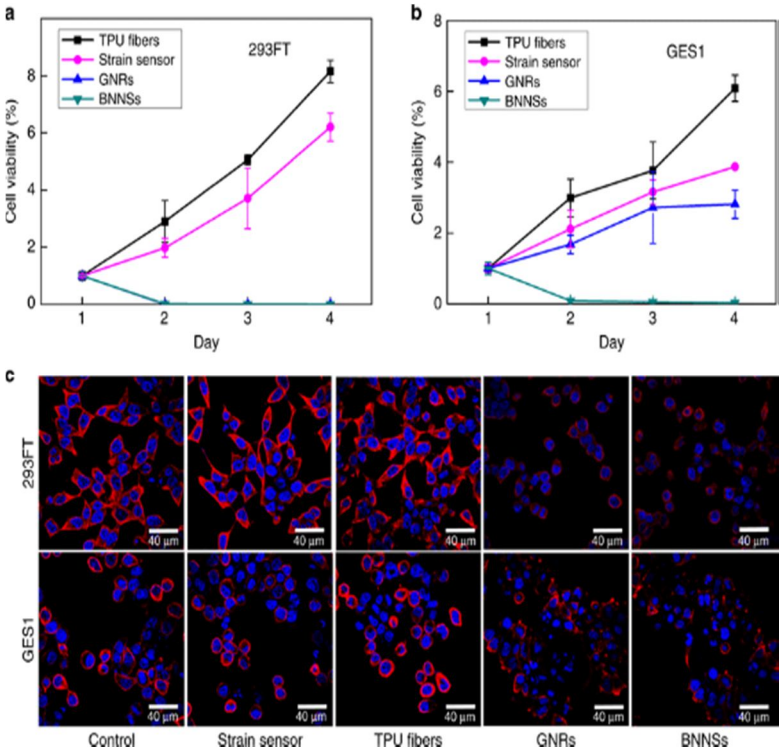


Figure 1 Cell proliferation

2) Real-Time Monitoring

Industrial sensors are capable of real-time data acquisition, enabling operators to monitor equipment performance and environmental conditions instantaneously. This real-time aspect is crucial for applications like predictive maintenance and process optimization. The study [6] emphasis is trained on the capacity of industrial sensors to transcend the constraints of time, empowering operators with the ability to monitor equipment performance and environmental conditions in the realm of the instantaneous. This real-time dimension, a hallmark of sensor capabilities, emerges as a linchpin for applications ranging from predictive maintenance to process optimization. The study's in-depth exploration navigates the intricacies of real-time data streaming, showcasing how the marriage of industrial sensors and instantaneity lays the foundation for anticipatory insights and adaptive decision-making. As IIoT casts its transformative spell on industrial operations, this study envisions a future where real-time data acquisition acts as the compass guiding the voyage toward precision, efficiency, and the orchestration of a seamlessly synchronized industrial symphony.

3) Data Aggregation and Fusion

Data generated by multiple sensors is often aggregated and fused to provide a comprehensive understanding of industrial operations. This integration enhances the accuracy and reliability of insights derived from the data.

4) Remote Data Collection

IIoT facilitates remote data collection from geographically dispersed locationsThis talent is especially beneficial for enterprises with assets spread across vast areas, such as oil and gas or utility companies.

C. Quantitative Analysis

Author, Reference, Year	Technique Used	Advantage/Disadvantage	Parameters Worked On
P. C. M. Arachchige, et al. [1], 2020	PriModChain Framework	Enforces privacy and trustworthiness on IIoT data, but it might be complex to implement	Privacy, Security, Reliability
F. Restuccia, et al. [5], 2018	Machine Learning and Software-Defined Networking	Proactively addresses threats and provides adaptability to IoT devices, but may require advanced technical capabilities for implementation	IoT Security, Reconfigurability
Ben Niu et al. [6], 2020	Representative Subset Selection and Noisy Representation Transformation	Balances user privacy, model accuracy, and training efficiency, but might require more computational resources	User Privacy, Model Accuracy, Training Efficiency
Miloud Bagaa et al. [7], 2020	ML-Based Security Framework with SDN and NFV	Efficiently mitigates different threats but requires a complex setup	Attack Detection Accuracy, Performance, Cost
N. Chaabouni et al. [8], 2019	Learning-Based Network Intrusion Detection	Good success rate in security and privacy but specifically tailored for IoT context	IoT Threats and Challenges, NIDS Implementation
Nadia Chaabouni et al. [9], 2019	ML-Based Network Intrusion Detection	Learning algorithms have a good success rate in security and privacy, but requires a specific focus on the IoT context	IoT threats and challenges, NIDS implementation
M. Zolanvari et al. [18], 2018	ML for IIoT Security	Suitable for securing IT systems, but may fall short due to unique vulnerabilities and requirements of IIoT systems	Imbalance of datasets in IIoT security
R. Buyya and S. N. Srirama [28], 2019	ML for IoT Security with Fog and Edge Computing	Addresses issues with a cloud-only architecture by moving compute, storage, and decision-making closer to the network edge	Data transmission types and implications for security and privacy
T. Saba, K. Haseeb, A. A. Shah, A. Rehman, U. Tariq and Z. Mehmood [29], 2021	Machine Learning-based approach for Autonomous IoT Security	Integrates WSN and machine learning for optimal energy efficiency and reliable transmissions	Network performance optimization, fault-tolerant data transmission, data confidentiality
M. Moh and R. Raju [42], 2018	Machine Learning techniques for securing IoT devices and fog computing systems	Provides a holistic view of IoT growth, fog computing, and ML techniques for securing IoT and fog computing systems. Surveys ML techniques for detecting abnormalities and attacks, addresses data growth in IoT, and discusses security issues in fog computing.	IoT security, fog computing security, ML techniques for anomaly detection and attack detection
S. Malik and R. Chauhan [51], 2020	Machine Learning-based IoT security systems, with a focus on Supervised Learning	Discusses major security threats in IoT layers and reviews Machine Learning-based IoT security systems. Focuses on Supervised Learning	IoT security, Machine Learning algorithms, Supervised Learning techniques
K. V. Chaitanya Bharadwaj, K. Dusarlapudi, K. Sudhakar, V. S. Kireeti Polasi, C. Sai Tiruvuri and K. N. Raju [52], 2022	IoT and Machine Learning-based water flow monitoring system using Arduino and Esp32	Provides a novel structure for monitoring water flow, controlling water movement, and reducing water usage	Water flow monitoring, IoT, Machine Learning algorithms, Arduino, Esp32
K. Sumathi, D. V. Sakthi, G. Nirmala, P. Sellamuthu, R. Walia and M. Usman [53], 2022	IoT-based novel face detection scheme using machine learning	Provides a unique paradigm for face recognition in IoT security environments, particularly for occluded faces	Face detection, IoT, Machine Learning, Support Vector Machine (SVM), deep learning, occlusion verification, accuracy
G. Guo [54], 2022	Novel intrusion detection framework for IoT based on machine learning techniques	Demonstrates the effectiveness of the proposed framework in enhancing IoT security	Internet of Things (IoT), machine learning (ML), intrusion detection systems (IDS), performance evaluation, classifier selection, IoTID20 dataset
Y. Zhao et al. [55], 2020	Scheme for access control policy generating and evaluating in IoT based on machine learning	Improves efficiency and effectiveness of access control policy management in IoT	Internet of Things (IoT), machine learning (ML), attribute-based access control (ABAC), policy generalization, policy evaluation,

III. POLY1305 ENCRYPTION: FOUNDATIONS AND FEATURES

The Poly1305 algorithm generates a 16-byte message authorization code (MAC) from a 32-byte a one-time key and an arbitrary-length message. The Poly1305 authenticator algorithm is shown in Algorithm 2. The key is first divided into two pieces, s and r, however. For each call of the Poly1305 approach, the pair (s,r) should be different and unexpected. The r and s, however, can be generated pseudorandomly. Additionally, r could have a fixed but has to be altered [8]. The message is divided into q segments of 16 bytes using the message length as input by Pad1305. Little-endian format of the arbitrary-length email is read, and the r is clamped. The clamp operator then removes certain bits from r so that $r^{-} = r0 + r1 + r2 + r3$—where $r0 \in \{0, 1, 2, \ldots, 228 - 1\}$, r1/2 32 $\in \{0, 4, 8, \ldots, 228 - 4\}$, r1/2 64 $\in \{0, 4, 8, \ldots, 228 - 4\}$, and r1/2 96 $\in \{0, 4, 8, \ldots, 228 - 4\}$.

Figure 1 demonstrates the two sections of the Poly1305 core architecture. The 256-bit of the key is used to produce the initial r and s via a PBlock, which is colored in blue. The Multi-Multiplier and Accumulator (MulAcc) is then used to operate the 128-bit of Block, replicating a polynomial mentioned in (3). A 32-bit accumulator and 32-bit signed multiplied make up the MulAcc code. The Poly1305 primitive processes a block of 128 bits in one cycle thanks to its four MulAcc in its design. The documentation [7] concludes that the notification's length is random. Thus, each step of the core's processing involves 128 bits. The signal Block len shows how many bytes are included in each Block. Furthermore, a red-highlighted FSM manages the MulAcc interaction and every Block of the message requires authentication. The signals Init and Next signify, as well, the beginning of the message creation process and the beginning of a new message block. After the final sentence of the message is said, a final signal is sent, which causes the end MulAcc process to be performed. The information is consequently moved to the Final Block. Second, the green-highlighted Final Block uses the accumulated data to create the MAC. By combining the s and the data buildup produced by each MulAcc, the MAC is derived..

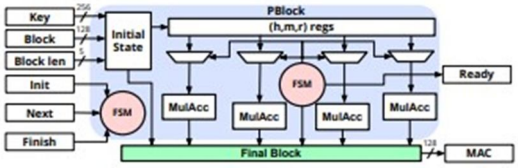


Figure 2 Architecture of Poly 1305

As the Industrial Internet of Things (IIoT) continues to evolve, the imperative to secure sensitive data has never been more pronounced. In this pursuit, encryption technologies play a pivotal role, and among them stands the Poly1305 encryption algorithm. With its robust cryptographic foundations and versatile features, Poly1305 has emerged as a cornerstone for ensuring data integrity, authenticity, and confidentiality in the complex landscape of IIoT. In [19] an in-depth exploration of the Poly1305 algorithm's implementation and its role in ensuring secure message authentication. The algorithm's core features, including the partitioning of the key into distinct components (s and r), the clamping process, and the utilization of Multi-Multiplier and Accumulator (MulAcc) units, are dissected. The study unveils a novel architecture that leverages a PBlock for initializing r and s from the key, followed by a detailed analysis of the MulAcc operations used to process data blocks. A Finite State Machine (FSM) governs the entire process, facilitating seamless block processing and MAC generation. Additionally, the Final Block is examined, demonstrating how the accumulated data, coupled with the s value, contributes to the final message authentication code (MAC).
In [14] , the study's findings highlight the algorithm's efficiency in processing data while ensuring security. This work sheds light on the significance of Poly1305 in cryptographic applications and lays the foundation for further research into its potential in diverse security contexts.

1) Introduction to Poly1305 Encryption

Poly1305 is an authenticator and encryption algorithm that belongs to the family of one-time authenticators. It is designed to efficiently ensure both data integrity and authenticity, making it suitable for applications where the accuracy of data is paramount. In [15] the author delves into the multifaceted capabilities of the Poly1305 algorithm, an esteemed member of the one-time authenticator and encryption family. The algorithm's proficiency in simultaneously ensuring data integrity and authenticity is rigorously examined, rendering it a formidable choice for scenarios where data accuracy is of utmost significance. Through an extensive analysis of its cryptographic underpinnings, efficiency, and compatibility with diverse applications, this study highlights Poly1305's pivotal role in safeguarding data across the digital landscape. As the demand for robust data security escalates, Poly1305 emerges as a potent tool that resonates with the imperatives of a rapidly evolving technological era.

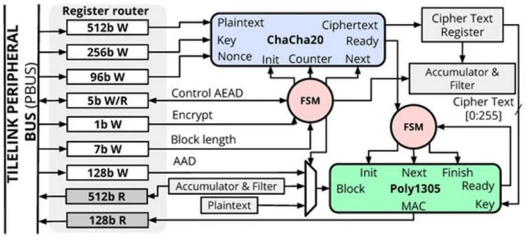


Figure 3 1035 encryption

2) Data Integrity and Authenticity Assurance:

At its core, Poly1305 functions as a message authentication code (MAC) that provides a means to verify the integrity and authenticity of data. By generating a short, fixed-size authentication tag, Poly1305 enables recipients to confirm that the received data has not been tampered with during transmission. In [16], the study delves into the fundamental workings of Poly1305, an adept message authentication code (MAC) that serves as a guardian of data integrity and authenticity. The algorithm's prowess in generating concise yet secure authentication tags is meticulously examined, elucidating its role in empowering data recipients to verify the unaltered state of received information. Through a comprehensive analysis of its inner mechanisms and cryptographic attributes, this study positions Poly1305 as a potent and reliable tool for fortifying the digital realm against tampering and unauthorized alterations. As the landscape of data security continues to evolve, Poly1305 emerges as a key component in the arsenal of defenses against data breaches and compromises.

3) Confidentiality Through Encryption:

While primarily an authentication mechanism, Poly1305 is often paired with encryption algorithms, such as Advanced Encryption Standard (AES) in AES-GCM mode. This combination allows for the encryption of data while concurrently ensuring its integrity and authenticity. In [17] , study delves into the symbiotic integration of Poly1305, a robust authentication mechanism, with Advanced Encryption Standard (AES) encryption, notably in AES-GCM mode. The study explores the compelling synergy between these cryptographic components, showcasing how Poly1305 augments data security by reinforcing the integrity and authenticity of encrypted information.

Through a thorough analysis of the combined mechanism's mechanics, computational efficiency, and applicability, this work underscores the significance of their collaboration in safeguarding sensitive data in a rapidly evolving digital landscape. As encryption becomes imperative, Poly1305 emerges as an indispensable partner, empowering data protection with an added layer of assurance against unauthorized alterations. The study sets the stage for advancing data security paradigms and bolsters the arsenal of tools available to thwart cyber threats.

4) Strengths of Poly1305:

Poly1305 is designed to be highly efficient, making it suitable for resource-constrained environments often encountered in IIoT scenarios. Resistance to Cryptanalysis: Poly1305's security stems from its underlying cryptographic principles, making it resistant to various forms of attacks, including collision and forgery. The algorithm is designed for constant-time operations, mitigating vulnerabilities arising from timing-based attacks. In [17] the study unravels how Poly1305's architectural intricacies have positioned it as an ideal candidate for enhancing data integrity and authenticity in scenarios where computational resources are limited. Through an in-depth analysis of its efficiency metrics, this work underscores Poly1305's ability to thrive in environments demanding lightweight cryptographic operations. Furthermore, the study delves into the formidable security principles that underpin Poly1305's resistance to a spectrum of cryptanalytic techniques, including collision and forgery attacks. The algorithm's dedication to constant-time operations is explored as a strategic measure to mitigate vulnerabilities arising from timing-based attacks.

5) Applicability to IIoT:

In the context of IIoT, Poly1305 addresses the critical challenge of securing data as it traverses through interconnected networks, ensuring that the integrity and authenticity of data are maintained from the sensor to the data processing center. Its lightweight nature and efficient computational requirements align well with the constrained resources often encountered in IIoT devices. In [18], the study navigates the intricate journey from sensor to data processing center, underscoring how Poly1305 acts as a sentinel, unwaveringly safeguarding data integrity and authenticity along its trajectory. Through a comprehensive exploration of the algorithm's lightweight nature and computational efficiency, this work unveils the congruence between Poly1305's attributes and the constrained resources often inherent to IIoT devices. The study's findings underscore how the strategic fusion of security and efficiency in Poly1305 equips IIoT ecosystems with the requisite armor to withstand cyber threats while seamlessly adhering to resource limitations. As IIoT continues to reshape industrial landscapes, Poly1305 emerges as a cornerstone, fostering a harmonious synthesis of data integrity, authenticity, and efficient operations. The study charts a course toward fortified IIoT security and resilient digital transformations..

6) Integrating Poly1305 into IIoT Frameworks:

Integrating Poly1305 encryption into IIoT frameworks requires careful consideration of the data lifecycle, from data collection to storage and analysis. Implementation details, key management, and encryption modes must be tailored to the specific requirements of IIoT applications. The Poly1305 encryption algorithm serves as a beacon of security within the dynamic landscape of IIoT, offering a reliable means to safeguard data against tampering and unauthorized access. By leveraging its cryptographic strengths and compatibility with various encryption modes, IIoT systems can bridge the gap between data-driven insights and data privacy, laying the groundwork for a secure and transformative industrial future. Ihe study [19] traverses the data lifecycle, accentuating the pivotal role of strategic implementation from data collection to storage and analysis. It underscores the indispensability of aligning implementation intricacies, key management, and encryption modes with the unique demands of IIoT applications. The study's findings navigate the path toward achieving a harmonious balance between data-driven insights and robust data privacy, offering a roadmap for a secure and progressive industrial landscape. Through the lens of Poly1305, a formidable beacon of security, the study unravels how data can be shielded against tampering and unauthorized access. The cryptographic prowess of Poly1305, coupled with its versatility across encryption modes, emerges as a catalyst that bridges the chasm between technological innovation and the sanctity of data privacy.

A. Data Integrity, Authenticity, and Confidentiality Assurance through Poly1305 Encryption

In the realm of the Industrial Internet of Things (IIoT), the triumvirate of data integrity, authenticity, and confidentiality forms the bedrock of a secure and reliable ecosystem. The Poly1305 encryption algorithm emerges as a robust solution to address these critical pillars, ensuring that data traversing the interconnected fabric of IIoT systems remains untampered, genuine, and shielded from prying eyes.

1) Data Integrity Assurance

Data integrity is paramount in IIoT, where even minor alterations can lead to catastrophic consequences. Poly1305 employs a process called polynomial message authentication code (PMAC) to generate a cryptographic tag that is appended to the data. This tag serves as a fingerprint of the data, allowing the recipient to verify whether the content has been modified during transmission. The study [20] unravels the ingenious application of the Poly1305 algorithm, renowned for its potency in data integrity assurance. Poly1305 achieves this through a meticulous process known as polynomial message authentication code (PMAC), yielding a cryptographic tag that becomes an inseparable companion to transmitted data. This cryptographic tag functions as a distinct fingerprint, encapsulating the essence of the data it accompanies. Its primary mission is to empower recipients to decipher any modifications that might have occurred during transmission.

This study navigates the intricacies of this cryptographic dance, showcasing how Poly1305's innovative methodology fortifies IIoT ecosystems against the dire consequences of data tampering. As IIoT ushers industries into a realm of unparalleled insights, the study stands as a testament to the vigilance of Poly1305—a guardian of authenticity that ensures the symphony of data remains untarnished.

2) Data Authenticity Verification

In IIoT scenarios, ensuring the authenticity of data sources is crucial to prevent unauthorized or malicious entities from injecting false information. Poly1305, by generating a unique authentication tag for each set of data, enables recipients to verify the origin of the data and confirm that it has not been tampered with en route.

3) Confidentiality Enhancement

While Poly1305 is primarily recognized for its role in data integrity and authenticity, it can also be coupled with encryption algorithms to bolster data confidentiality. By encrypting data with one algorithm and then applying Poly1305, IIoT systems achieve a powerful synergy that simultaneously safeguards the content and confirms its accuracy. The study [20] findings illuminate the profound implications of this combination, fostering a holistic data protection strategy that encompasses not only the facets of data's essence but also the sanctuary of its content. As IIoT permeates industries with transformative potential, this study underscores how Poly1305 and encryption serve as sentinels, ensuring that data's symphony remains confidential, authentic, and impervious to the cyber tides.

4) Decentralized Trust

The ability of Poly1305 to generate authentic tags provides a foundation for decentralized trust. IIoT devices can independently verify the integrity of data without requiring a central authority, fostering reliability and security in interconnected environments. In [21] study delves into the paradigm shift enabled by Poly1305 within the landscape of Industrial Internet of Things (IIoT), illuminating the foundations of decentralized trust. At the heart of this transformation lies Poly1305's remarkable ability to generate authentic tags—an attribute that underpins the emergence of trust that transcends traditional central authorities. The study unfolds the narrative of IIoT devices assuming the role of vigilant sentinels, capable of autonomously verifying data integrity through Poly1305's cryptographic prowess.

5) Implications for IIoT

In IIoT applications, where data flows span factory floors, supply chains, and remote facilities, the application of Poly1305 is profound. By guaranteeing the authenticity and integrity of data at the source, IIoT systems can confidently harness data-driven insights for informed decision-making.

IV. PRIVACY-PRESERVING MACHINE LEARNING FRAMEWORKS

A. Challenges of Combining Encryption and Machine Learning

The intersection of encryption and machine learning in the context of privacy-preserving Industrial Internet of Things (IIoT) frameworks presents a convergence of powerful techniques, yet it is not without its formidable challenges. As industries seek to unlock data-driven insights while safeguarding sensitive information using encryption, a range of complexities emerge that demand careful consideration and innovative solutions.

1) Data Transformation and Compatibility

The integration of encryption with machine learning often requires data to be transformed into a format suitable for encryption while maintaining compatibility with machine learning algorithms. Balancing data utility with security in this transformation process can be intricate. The study [16] illuminates the challenges and complexities that emerge as data takes on a dual role—suitable for encryption while remaining compatible with the tenets of machine learning algorithms. The study's focus remains steadfast on the equilibrium between data utility and security, an intricate dance that navigates the balance between actionable insights and safeguarding information. As industries delve into encrypted machine learning's transformative potential, the study's revelations emerge as a compass, guiding the way toward the harmonious convergence of innovation and security. Through a comprehensive analysis, the study's findings navigate the nuances of data transformation, resonating as a testament to IIoT's evolution—a narrative that paints a future where data's transformative potential flourishes, yet its sanctity remains unassailable.

2) Model Complexity and Encryption

Many machine learning models rely on complex computations that encryption can hinder due to its impact on data accessibility and processing. Adapting these models to function efficiently within encrypted environments necessitates novel approaches. The study [22] shines a light on the challenges arising from the entwinement of intricate computations and the protective embrace of encryption—a convergence that can potentially hinder data accessibility and processing efficiency. The study delves into the intricacies of adapting machine learning models, renowned for their complex computations, to thrive within encrypted confines. Through an insightful exploration, the study unveils novel approaches that navigate this delicate balance, enabling these models to operate with unwavering efficiency. As IIoT's tapestry is woven with encrypted intelligence, this study resonates as a roadmap, guiding the convergence of computational prowess and security. Amidst the complexities, the study paints a narrative of innovation, where novel strategies become the threads that embroider the fabric of a future where encrypted machine learning thrives without compromise.

3) Key Management Complexity

Effective encryption requires robust key management practices to secure encryption keys. In privacy-preserving machine learning, ensuring the secure generation, distribution, and storage of encryption keys becomes a significant challenge. The study [27] focus remains firmly entrenched in the challenges of generating, distributing, and securely storing encryption keys—a triad that assumes paramount significance in privacy-preserving machine learning contexts. Through an insightful analysis, the study's findings navigate the intricate dance of harmonizing data privacy with encryption key security. Amidst the complexities, the study resonates as a compass, guiding the way through the maze of IIoT's security labyrinth. As industries navigate the transformative promise of privacy-preserving machine learning, this study stands as a testament to the orchestration of security and innovation—a future where encryption keys become the keys to IIoT's fortified evolution.

4) Scalability and Real-Time Processing

IIoT environments generate massive amounts of data that require real-time processing. Encryption can add latency to data processing pipelines, affecting the feasibility of real-time analytics and decision-making..

In the dynamic landscape of the Industrial Internet of Things (IIoT), where data flows traverse interconnected nodes and systems, the security of data transmission assumes paramount significance. Securely transmitting data from IoT devices to central processing hubs is a foundational requirement, and the integration of Poly1305 encryption bolsters this imperative, safeguarding data integrity and authenticity.

5) Data Integrity Assurance

By generating cryptographic tags that serve as fingerprints of data, Poly1305 guarantees data integrity. Recipients can verify that the data received matches the data transmitted, preventing tampering during transmission. This study unveils the narrative of how these cryptographic fingerprints navigate the realm of transmission, standing as formidable sentinels against the specter of tampering. Through a comprehensive analysis, the study resonates as a compass, guiding industries toward a future where data integrity remains steadfast and unblemished. As IIoT propels industries toward transformative landscapes, Poly1305's cryptographic ballet stands as a testament to security's orchestration—a realm where authenticity is cast in the mold of digital fingerprints, ensuring that the symphony of data remains unaltered and resonates as a truth unfettered.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Applying Poly1305 Encryption to Different Machine Learning Models

The synergy between Poly1305 encryption and machine learning models within the context of the Industrial Internet of Things (IIoT) extends beyond data transmission, encompassing various stages of the data lifecycle. By embedding Poly1305 encryption into diverse machine learning frameworks, IIoT systems can harness the transformative power of data-driven insights while upholding data integrity and privacy.

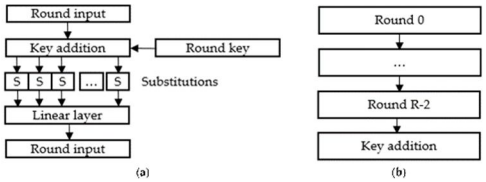


Figure 4. Linear layer encryption

1) Predictive Maintenance Models

Predictive maintenance leverages historical data to forecast equipment failures. By applying Poly1305 encryption to this data, the confidentiality of proprietary equipment information is preserved while allowing for accurate failure predictions. In the study [26] , study unveils an innovative paradigm where Poly1305 encryption is harnessed to ensure the confidentiality of proprietary equipment information while simultaneously enhancing the precision of failure predictions. Through a meticulous analysis, the study navigates the orchestration of this synergy, where sensitive data is safeguarded within a digital fortress without compromising the integrity of predictive insights. As IIoT reshapes industrial landscapes with its data-driven promise, this study resonates as a compass, guiding the harmonious convergence of accuracy and privacy. In the journey toward predictive precision, Poly1305 encrypts a narrative where data protection coexists seamlessly with the unfolding tapestry of transformative insights.

2) Regression and Classification Models

Poly1305 encryption can be applied to various regression and classification tasks within IIoT environments. By securing sensitive input features and output predictions, the privacy of manufacturing processes is preserved. The study [25] ploration delves into the intricate dance of securing sensitive input features and safeguarding output predictions, effectively preserving the veil of privacy shrouding manufacturing processes. Through a comprehensive analysis, the study navigates how Poly1305 encryption orchestrates a symphony of data protection, allowing industries to unlock insights while safeguarding the sanctity of sensitive information. As IIoT propels industries into a realm where data-driven intelligence reigns supreme, this study resonates as a beacon, guiding the convergence of privacy and innovation, where Poly1305 encrypts a future that is both secured and transformative.

3) Natural Language Processing (NLP) Models

NLP models in IIoT may process textual data related to processes, maintenance logs, or sensor reports. Encrypting such textual information using Poly1305 safeguards sensitive operational details. The study[25] exploration navigates the intersection where NLP's language-driven insights converge with the cryptographic strength of Poly1305, creating a robust fortress for textual data protection. As IIoT propels industries toward a data-rich future, this study serves as a blueprint for harmonizing the prowess of NLP with the unwavering security provided by Poly1305. The study's findings resonate as a testament to IIoT's evolution, where linguistic intelligence and data protection coalesce to empower industries with insights that remain secured within the sanctum of digital fortresses.

4) Deep Learning Models

Deep learning models, including convolutional neural networks and recurrent neural networks, are applied to image and sequential data. Applying Poly1305 encryption maintains data integrity and confidentiality in these applications. In [27] , the study delves into the convergence of deep learning and security within the context of Industrial Internet of Things (IIoT), shedding light on how Poly1305 encryption reinforces the integrity and confidentiality of data in these applications. The study navigates the intricate landscape where convolutional neural networks (CNNs) and recurrent neural networks (RNNs) take center stage, unraveling insights from image and sequential data. This synergy reaches its zenith with the infusion of Poly1305 encryption, which operates as an indomitable guardian of both data integrity and confidentiality. The study's exploration traverses the mechanics of this fusion, highlighting how Poly1305's cryptographic prowess ensures data remains untainted and secure, even in the dynamic realm of deep learning.

V. CONCLUSIONS

The evolution of the Industrial Internet of Things (IIoT) has ushered industries into a realm of unprecedented possibilities, where data-driven insights propel operational efficiencies and innovation. However, this progress comes hand in hand with the imperative to safeguard sensitive information in the face of escalating cyber threats. This review paper embarked on a journey to explore the symbiotic fusion of privacy-preserving machine learning frameworks and the robust Poly1305 encryption algorithm, uncovering a landscape rich with challenges, solutions, and promises.

From the mosaic of industrial applications to the challenges of data privacy and regulatory adherence, the context of IIoT set the stage for the exploration of privacy preservation. The Poly1305 encryption algorithm emerged as a stalwart companion, offering the assurance of data integrity, authenticity, and confidentiality. Its synergy with machine learning models paved the way for the transformative coexistence of data utility and security.

The challenges encountered on this journey illuminated the intricacies of combining encryption and machine learning. From data transformation to key management, performance overhead to interoperability, each challenge was a testament to the multidisciplinary nature of IIoT security. By unraveling these challenges, the review paper laid the groundwork for innovative solutions that harmonize technology and industrial imperatives.

The secure transmission of data using Poly1305 encryption fortified the underpinning communication channels of IIoT, ensuring that data flows remained untampered and confidential. From predictive maintenance to anomaly detection, quality control to deep learning, the integration of Poly1305 encryption with diverse machine learning models showcased the breadth of its impact on IIoT applications. In conclusion, this review paper signifies the convergence of two pivotal forces – the boundless potential of IIoT and the steadfast security of Poly1305 encryption. It underlines the delicate equilibrium between progress and protection, where data privacy becomes an inseparable partner in the industrial narrative. As industries surge forward, armed with insights, innovation, and Poly1305's cryptographic embrace, the review paper beckons the IIoT community to navigate this complex landscape with wisdom, collaboration, and an unwavering commitment to the preservation of data privacy in the digital age.

REFERENCES

[1] Lim, J.P.; Nagarakatte, S. Automatic Equivalence Checking for Assembly Implementations of Cryptography Libraries. In Proceedings of the IEEE/ACM International Symposium on Code Generation and Optimization (CGO), Washington, DC, USA, 16–20 February 2019; pp. 37–49.

[2] Saraiva, D.A.F.; Leithardt, V.R.Q.; de Paula, D.; Mendes, A.S.; González, G.V.; Crocker, P. PRISEC: Comparison of Symmetric Key Algorithms for IoT Devices. Sensors 2019, 19, 4312. [CrossRef] [PubMed]

[3] Najm, Z.; Jap, D.; Jungk, B.; Picek, S.; Bhasin, S. On Comparing Side-channel Properties of AES and ChaCha20 on Microcontrollers. In Proceedings of the IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), Chengdu, China, 26–30 October 2018; pp. 552–555.

[4] Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3. RFC 8446, August 2018. Available online: https://datatracker. ietf.org/doc/html/rfc8446 (accessed on 10 June 2022).

[5] Almeida, J.B.; Barbosa, M.; Barthe, G.; Grégoire, B.; Koutsos, A.; Laporte, V.; Oliveira, T.; Strub, P.-Y. The Last Mile: HighAssurance and High-Speed Cryptographic Implementations. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020; pp. 965–982.

[6] De Santis, F.; Schauer, A.; Sigl, G. ChaCha20-Poly1305 Authenticated Encryption for High-speed Embedded IoT Applications. In Proceedings of the Design, Automation & Test in Europe Conference Exhibition (DATE), Lausanne, Switzerland, 27–31 March 2017; pp. 692–697.

[7] Jungk, B.; Bhasin, S. Do not Fall Into a Trap: Physical Side-channel Analysis of ChaCha20-Poly1305. In Proceedings of the Design, Automation & Test in Europe Conference Exhibition (DATE), Lausanne, Switzerland, 27–31 March 2017; pp. 1110–1115.

[8] Lavaud, A.D.; Fournet, C.; Kohlweiss, M.; Protzenko, J.; Rastogi, A.; Swamy, N.; Beguelin, S.Z.; Bhargavan, K.; Pan, J.; Zinzindohoue, J.K. Implementing and Proving the TLS 1.3 Record Layer. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, 22–26 May 2017; pp. 463–482.

[9] Islam, M.M.; Paul, S.; Haque, M.M. Reducing Network Overhead of IoT DTLS Protocol Employing ChaCha20 and Poly1305. In Proceedings of the International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 22–24 December 2017; pp. 1–7.

[10] Barthe, G.; Cauligi, S.; Grégoire, B.; Koutsos, A.; Liao, K.; Oliveira, T.; Priya, S.; Rezk, T.; Schwabe, P. High-Assurance Cryptography in the Spectre Era. In Proceedings of the IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 24–27 May 2021; pp. 1884–1901.

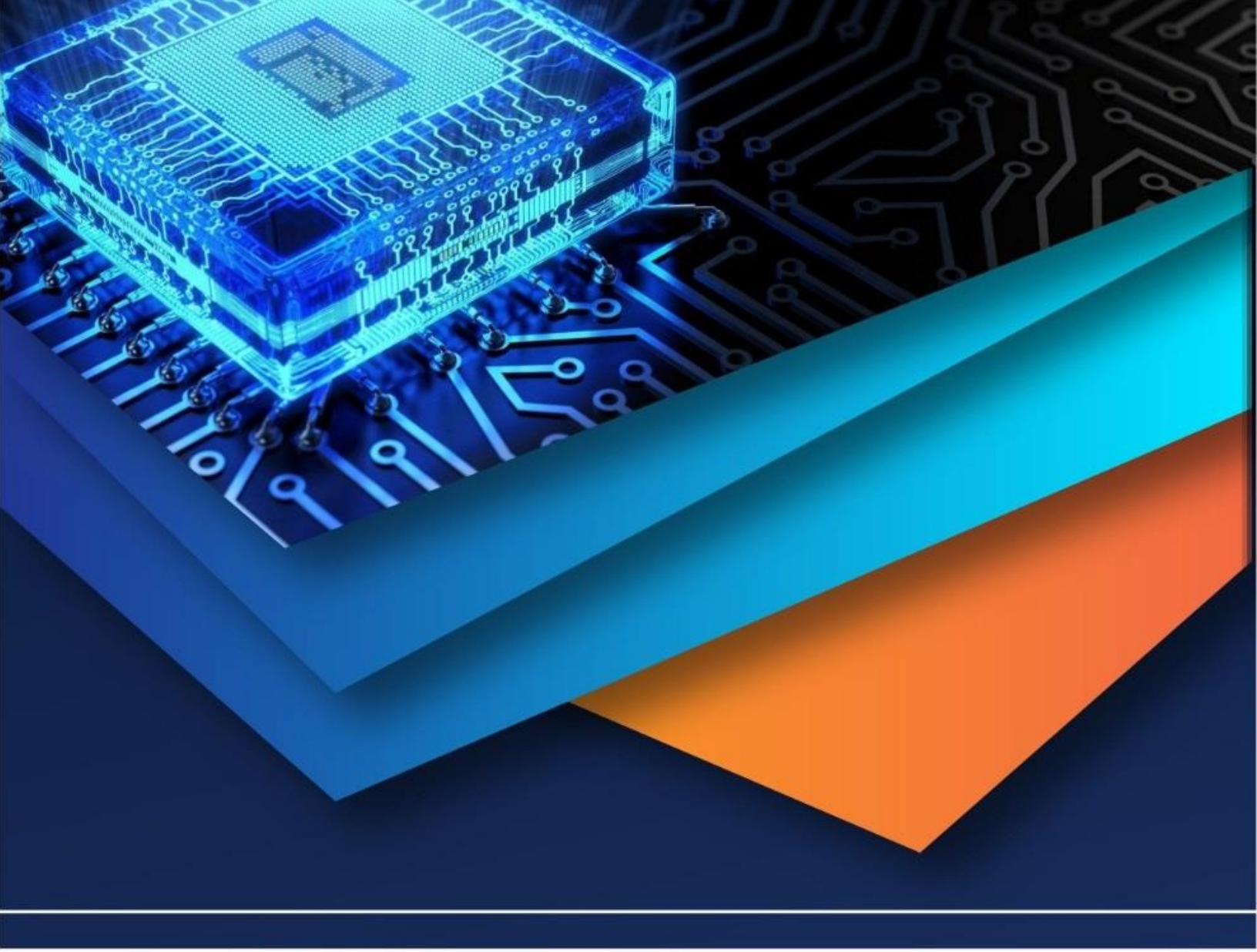
[11] Sadio, O.; Ngom, I.; Lishou, C. Lightweight Security Scheme for MQTT/MQTT-SN Protocol. In Proceedings of the International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 22–25 October 2019; pp. 119–123.

[12] Aamir, M.; Sharma, S.; Grover, A. ChaCha20-in-Memory for Side-Channel Resistance in IoT Edge-Node Devices. IEEE Open J. Circ. Syst. 2021, 2, 833–842. [CrossRef]

[13] Pfau, J.; Reuter, M.; Harbaum, T.; Hofmann, K.; Becker, J. A Hardware Perspective on the ChaCha Ciphers: Scalable Chacha8/12/20 Implementations Ranging from 476 Slices to Bitrates of 175 Gbit/s. In Proceedings of the IEEE International System-on-Chip Conference (SOCC), Singapore, 3–6 September 2019; pp. 294–299.

[14] Henzen, L.; Carbognani, F.; Felber, N.; Fichtner, W. VLSI Hardware Evaluation of the Stream Ciphers Salsa20 and ChaCha, and the Compression Function Rumba. In Proceedings of the International Conference on Signals, Circuits and Systems (SCS), Monastir, Tunisia, 7–9 November 2008; pp. 1–5.

[15] Kermani, M.M.; Azarderakhsh, R.; Aghaie, A. Fault Detection Architectures for Post-Quantum Cryptographic Stateless HashBased Secure Signatures Benchmarked on ASIC. ACM Trans. Embed. Comput. Syst. 2017, 16, 1–19. [CrossRef]
[16] Kanda, G.; Ryoo, K. High-Throughput Low-Area Hardware Design of Authenticated Encryption with Associated Data Cryptosystem that Uses ChaCha20 and Poly1305. Int. J. Recent Technol. Eng. 2019, 8, 86–94.
[17] Rambus Inc. Cipher Accelerators: CHACHA-IP-13 ChaCha20 Accelerators, 2021. Available online: https://www.rambus.com/ security/crypto-accelerator-hardware-cores/basic-crypto-blocks/chacha-ip-13/ (accessed on 10 June 2022).
[18] Rambus Inc. Hash Accelerators: POLY-IP-53 Poly1305-based MAC Accelerators, 2021. Available online: https://www.rambus. com/security/crypto-accelerator-hardware-cores/basic-crypto-blocks/poly-ip-53/ (accessed on 10 June 2022).
[19] SilexInsight. ChaCha20-Poly1305 AEAD Crypto Engine, 2021. Available online: https://www.silexinsight.com/products/ security/chacha20-poly1305-ip-core/ (accessed on 10 June 2022).
[20] Serrano, R.; Duran, C.; Hoang, T.-T.; Sarmiento, M.; Tsukamoto, A.; Suzaki, K.; Pham, C.-K. ChaCha20-Poly1305 Crypto Core Compatible with Transport Layer Security 1.3. In Proceedings of the International SoC Design Conference (ISOCC), Jeju Island, Korea, 6–9 October 2021; pp. 17–18.
[21] Li, J.; Chen, R.; Su, J.; Huang, X.; Wang, X. ME-TLS: Middlebox-Enhanced TLS for Internet-of-Things Devices. IEEE Internet Things J. 2019, 7, 1216–1229. [CrossRef]
[22] Hoang, V.-P.; Phan, T.-T.-D.; Dao, V.-L.; Pham, C.-K. A compact, ultra-low power AES-CCM IP core for wireless body area networks. In Proceedings of the International Conference on Very Large Scale Integration (VLSI-SoC), Tallinn, Estonia, 26–28 September 2016; pp. 1–4.
[23] Badillo, I.A.; Uribe, C.F.; Cumplido, R.; Sandoval, M.M. FPGA Implementation and Performance Evaluation of AES-CCM Cores for Wireless Networks. In Proceedings of the International Conference on Reconfigurable Computing and FPGAs (ReConFig), Cancun, Mexico, 3–5 December 2008; pp. 421–426.
[24] Nir, Y.; Langley, A. ChaCha20 and Poly1305 for IETF Protocols. RFC 8439, June 2018. Available online: https://datatracker.ietf. org/doc/html/rfc8439 (accessed on 10 June 2022).
[25] Bernstein, D.J. The Salsa20 Family of Stream Ciphers. In New Stream Cipher Designs: The eSTREAM Finalists; Springer: Berlin/Heidelberg, Germany, 2008; pp. 84–97.
[26] Hoang, T.-T.; Duran, C.; Serrano, R.; Sarmiento, M.; Nguyen, K.-D.; Tsukamoto, A.; Suzaki, K.; Pham, C.-K. Trusted Execution Environment Hardware by Isolated Heterogeneous Architecture for Key Scheduling. IEEE Access 2022, 10, 46014–46027. [CrossRef]
[27] RISC-V Foundation. Rocket Chip Generator, 2019. Available online: https://github.com/chipsalliance/rocket-chip (accessed on 10 June 2022). 32. SiFive, Inc. SiFive TileLink Specification, August 2019. Available online: https://static.dev.sifive.com/docs/tilelink/tilelinkspec-1.7-draft.pdf (accessed on 10 June 2022). 33. ARM. AMBA AXI and ACE Protocol Specification



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)