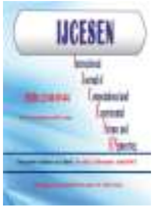
International Journal of Computational and Experimental Science and ENgineering
(IJCESEN)

Vol. 11-No.1 (2025) pp. 1452-1469
http://www.ijcesen.com



ISSN: 2149-9144

Research Article

Comparative Study of Lightweight Encryption Algorithms Leveraging Neural Processing Unit for Artificial Internet of Medical Things

Puthiyavan Udayakumar[1]*, R. Anandan[2]

[1]Research Scholar, Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu 600117, India;
* **Corresponding Author Email:** puthiyavanputhiyavan@gmail.com - **ORCID:** 0009-0004-5449-4568

[2] Department of Computer Science and Engineering, Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu 600117, India;
Email: anandan.se@velsuniv.ac.in - **ORCID:** 0000-0001-5461-1040

Article Info:

DOI: 10.22399/ijcesen.1259
Received : 11 January 2024
Accepted : 04 March 2025

Keywords :

Lightweight Encryption,
AIoMT,
NIST,
PRESENT,
Security,
Medical Data Security.

Abstract:

The Artificial Internet of Medical Things (AIoMT)enables a new generation of medical devices with real-time data analytics, remote patient monitoring, and tailored medicine. This interconnected landscape also facilitates cyberattacks targeting sensitive and critical patient information. Cryptography is one Method of ensuring secure data transmission. IoT networks have boosted the concept of lightweight cryptography since IoT devices have limited resources, including power, memory, and batteries. These algorithms are designed to protect data efficiently while utilizing minimal resources.

The research presents a comparative study of lightweight encryption algorithms evaluated by the National Institute of Standards and Technology (NIST) for suitability in securing data on AIoMT devices. Here, we analyze the Functional and Non-Functional characteristics of leading contenders. The value proposition of this research is to address the need to secure critical, sensitive patient information on AIoMT devices. The evaluation is performed using Raspberry Pi AI Kit, integrated with an M.2 HAT+ board and a Hailo-8L accelerator module; the Method adopted is a systematic literature review. Eight Models adopted AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE; ML models adopted and trained and verified against each of the eight NIST lightweight encryption algorithms and every model assessed with key performance indicators such as precision, recall, F1-score, and accuracy.

1. Introduction

Due to rapid advancements in the Internet of Things, AIoMT devices, such as wearable health monitors and connected medical equipment, have the potential to drastically improve patient treatment and the quality of healthcare delivery [1]. AIoMT devices have the potential to revolutionize healthcare [2]. However, digital technologies and increased connectivity pose new privacy and security threats.

As a result of these interconnected devices, enormous amounts of sensitive patient data are created, archived, and transferred, making AIoMT a significant concern. Electronic Health Records and other AIoMT applications require the protection of a wide range of patient information, including names, addresses, and medical conditions, from unauthorized access or misuse. The healthcare sector has grown significantly vulnerable to cyber threats like ransomware attacks. The IT infrastructure supporting AIoMT systems is often targeted in these attacks.

It is challenging to ensure the privacy and security of AIoMT. Due to their lack of security, innovative medical devices and wearables are frequently susceptible to hacking and data breaches. The healthcare profession and patients need to be made aware of the security and privacy implications of AIoMT, making them more susceptible to social engineering attacks [3,4].

Researchers and industry experts have proposed many solutions to address these challenges. One way to handle these problems is to implement a lightweight and efficient security protocol that can be easily incorporated into AIoMT devices without compromising their performance or functionality. Along with deploying robust access control mechanisms, encryption methods, and intrusion detection systems(IDS), AIoMT networks and their sensitive data can also be protected.

In addition, it is crucial to adopt an end-to-end security and privacy framework for AIoMT, including technical and organizational measures. As part, healthcare professionals will be trained on AIoMT security best practices, implement secure data storage and transmission practices, and establish clear data governance policies.

Security and privacy must remain top priorities in the AIoMT ecosystem. Future trends in this field include applying cutting-edge AI techniques for threat detection and response and including blockchain technology for data integrity and traceability.

With the AIoMT, medical devices and software applications can communicate with various healthcare IT systems. Protecting sensitive health data has become increasingly complex as this technology is increasingly integrated into healthcare. AIoMT poses unique challenges because of the heterogeneity of devices, the need for real-time performance, resource constraints, and users' mobility.The AIoMT [5] represents the convergence of medical devices and applications with network technology, enabling patient monitoring, diagnostics, and therapy to move beyond the confines of traditional healthcare facilities. From fitness trackers to insulin pumps, connected devices have enabled personalized medicine, remote monitoring, and data-driven diagnostics.Because AIoMT devices handle sensitive and personal health data, cybercriminals see them as lucrative targets. With the growth of AIoMT, cybersecurity has become a pressing concern. In the event of a successful breach, patient privacy could be compromised, and patient safety could be jeopardized, especially when critical devices are compromised.

Moreover, AIoMT introduces unique cybersecurity challenges:

- Diverse Ecosystem: Unlike traditional IT systems, the AIoMT ecosystem consists of many devices with varying computational capacities, making a one-size-fits-all security approach infeasible.
- As new threats emerge, many medical devices may become vulnerable due to their long operational lives.
- Medical industries are heavily regulated, and non-compliance can have significant legal and financial repercussions.
- A seamless and secure interoperability is essential when devices from different manufacturers must communicate.

It is about protecting unauthorized access in the AIoMT landscape and securing patients' health and devices' reliability. As AIoMT resumes to grow, robust, adaptive, and extended cybersecurity measures will be needed to assure patient safety and data privacy.

Due to their rapid growth, AIoMT devices are increasingly promising to improve patient care, disease management, and treatment effectiveness in healthcare. Wearables for monitoring vital signs, pacemakers, insulin pumps, and in-home medical equipment can all be used to manage chronic diseases. Since AIoMT devices collect sensitive medical data, robust security measures are necessary. In contrast to traditional encryption algorithms, AIoMT devices with limited processing power and battery life are usually incompatible with conventional algorithms because they require significant computational resources.

In this research, we probe the leading lightweight encryption candidates evaluated by NIST and analyze their suitability for diverse AIoMT applications. Lightweight encryption algorithms are crucial to securing data on AIoMT devices, balancing security and efficiency.

The rapid development of the AIoMT has transformed healthcare by enabling remote monitoring, real-time data collection, and personalized care. In complement to security and privacy concerns, the integration of these connected medical devices, referred to as the Internet of Medical Things, has also created substantial challenges [6-11].

Data Breaches: Health information is susceptible and valuable, making it a prime target for cyberattacks. Unauthorized access can expose patients to financial fraud, identity theft, and loss of patient trust.

Data breaches in the AIOMT refer to incidents where unauthorized individuals gain access to sensitive patient data. This can include personal identifying information, health history, and even real-time health data from connected devices.

The value and sensitivity of health data make AIoMT devices and systems attractive targets for hackers and other malicious actors. They may use various methods to breach the data, such as malware, phishing, ransomware, or exploiting device vulnerabilities.

It is well known that the health insurer Anthem was breached in 2015 [6], an example of an AIoMT data breach. In this case, hackers hacked Anthem's system. They stole information on more than 78.8 million people, including their names, birth dates, social security numbers, healthcare ID numbers, homes, email addresses, and income information. Even though this example does not involve a medical device, it illustrates the importance of health data and the potential scale of data breaches in the healthcare industry.

St. Jude Medical (now Abbott Laboratories) pacemakers, which are connected to the internet for monitoring purposes, were found to have vulnerabilities in 2017 [7]. As a result, the FDA recalled approximately half a million devices to install a critical security patch after hackers could deplete the device's battery or administer incorrect pacing or shocks, endangering patients' lives.

There is a potential risk to patient privacy and health in AIoMT due to these data breaches.

Device Vulnerabilities: Many AIoMT devices were not initially designed with robust security features in mind. As a result, they can be prone to cyberattacks, device spoofing, and physical tampering.

Device vulnerabilities in the AIoMT refer to the weaknesses in the design, implementation, or exploitation of connected medical devices for unauthorized access, manipulation of device operation, or compromise of data security.

Various reasons may lead to these vulnerabilities, such as inadequate security controls, outdated hardware and software, insecure APIs and interfaces, and a lack of encryption.

A notable example is the vulnerabilities discovered in the insulin pumps manufactured by Medtronic in 2019 [12]. The FDA has issued a warning regarding certain Medtronic MiniMedTM insulin pumps, which are vulnerable to cyberattacks.

The vulnerabilities allowed a malicious entity to wirelessly connect to a nearby insulin pump, change its settings, or control its delivery. These alterations could lead to hypoglycemia if additional insulin is delivered or hyperglycemia if not enough is given. In worst-case scenarios, these conditions could even lead to patient death. In response to these vulnerabilities, Medtronic recalled the affected insulin pumps and offered a replacement with a newer and more secure model.

Device vulnerabilities in the AIoMT may have real-world implications, as demonstrated in this case. Security measures, regular software updates, and proactive monitoring are essential for identifying and remediating vulnerabilities before they can be exploited.

Data Integrity: The quality and accuracy of medical data are crucial in healthcare. Any unauthorized modification can have severe implications on patient diagnosis and treatment.

Data integrity in the AIoMT refers to maintaining health data's accuracy, consistency, and reliability throughout its entire lifecycle. It also involves safeguarding the data against unauthorized modification and deletion, as well as making sure that it is not tampered with prior to transmission or storage.

Data integrity is important in life science as it presently influences medical decisions and patient care. Incorrect, incomplete, or out-of-date data can lead to misdiagnosis, delayed treatment, or wrong treatment, potentially endangering patient lives.

The 2015 Hospira Symbiq Infusion System case demonstrates the importance of data integrity [9]. Subject to restrictions from the U.S. Food and Drug Administration, unauthorized users could control the device and change the dosage of the infused drugs remotely.

The concern was that an attacker could alter the infusion pump's configuration or control drug delivery. If the drug dose data were tampered with, it could lead to over- or under-infusion of critical patient therapies. Given the severity of the situation, the FDA recommended that healthcare facilities stop using the Symbiq Infusion System and transition to other infusion systems as soon as possible.

This case illustrates the severe implications when data integrity is compromised in AIoMT devices. A fundamental part of AIoMT security is ensuring data integrity, which demands suitable safeguards such as cryptographic rules, secure networking communications protocols, hardy access control, and proactive/reactive monitoring.

User Privacy: When AIoMT devices are not adequately managed, they can continuously collect personal and health data, invading privacy. The data can reveal sensitive information about a user's lifestyle and health conditions [13].

Within the AIOMT, an individual's right to control their personal and health-related information is called their right to privacy. In addition to primary identifiers such as name and area time, AIoMT devices also collect health information such as heart rate, blood pressure, and glucose levels, often in real-time.

It can infringe on user privacy in various ways, including unauthorized data sharing, data breaches, or even legitimate uses for marketing or research they did not consent to.

Users can record and share their exercise activities with their friends via the Strava fitness app, an example of privacy concerns in AIoMT. Even though this isn't strictly a medical device, health-related data can pose privacy concerns. During the release of a global heatmap of Strava users' activities in 2018, military bases and patrol routes were inadvertently revealed. Despite the anonymized data and no individuals being directly identified, the incident raised serious privacy concerns. Implementing data anonymization techniques, rigorous access controls, and informed consent procedures are crucial for deploying strong privacy policies and safeguards in AIoMT. Furthermore, it emphasizes educating users about AIoMT's privacy implications.

Interoperability and Standardization: The need for standardization regarding security protocols among AIoMT devices from different manufacturers can lead to loopholes in the system.

In the AIOMT, interoperability and standardization are standardized ways to communicate, exchange, and interpret data from many devices and systems. Despite this, the AIoMT ecosystem often presents difficulties due to its broad range of devices, manufacturers, protocols, and data formats.

Fragmented care, redundant tests, and rising healthcare costs related to a lack of interoperability have improved healthcare efficiency, enabled data-driven decision-making, and provided integrated and coordinated services.

The AIoMT relies on standardization to define uniform protocols for device communication, data exchange, and privacy. In order to make AIoMT devices and systems interoperable, compatible, and reliable, standardization is essential. If there are no security vulnerabilities, interoperability is hampered, and scalability is compromised, security vulnerabilities may occur.

While EHRs are not AIoMT devices themselves, they are a crucial component of the larger health IT system, which includes AIoMT. As a result, interoperability is often required in healthcare organizations that use EHR systems from multiple vendors. Thus, healthcare providers or hospital departments might need help to access a patient's health record seamlessly.

The challenges associated with standardization can be seen in wireless infusion pumps, which can communicate with various systems, such as electronic health records, medication administration systems, and other medical equipment. These systems often have to communicate more effectively because they need standard communication protocols and data formats. This can lead to operational inefficiencies, errors, and security vulnerabilities.

Standards-based technologies must be adopted, foster stakeholder collaboration, and promote industry-wide standards in the AIoMT.

Data Encryption: Encryption of health data at rest and in transit can be challenging due to the diverse range of devices and transmission methods in AIoMT.

The AIOMT uses data encryption to convert plaintext data into an encoded version that can only be decoded and read by those with the decryption key. Encryption protects sensitive health data when it is inferred over the network or stored in an edge device; it is shielded from unauthorized access.

However, implementing robust data encryption in the AIoMT can be challenging due to various factors. These can include the computational limitations of small AIoMT devices, the overhead of encryption on the device's battery life, the need for real-time or near-real-time communication, and the diversity of devices and transmission protocols.

It was pointed out in the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) cybersecurity advisory in 2016 that inadequate encryption poses a serious threat. A medical syringe infusion pump from Hospira (now owned by Pfizer) transmits drug administration data unencrypted, leaving it vulnerable to eavesdropping and tampering, according to the advisory.

A hacker could modify the pump's data, generating it to administer the wrong doses, which could be deadly, if they acquired access to the hospital's network.

A robust encryption strategy is essential in AIoMT, as shown by this example. A fundamental part of protecting sensitive health data is encryption, despite the challenges, and strategies such as lightweight encryption algorithms, secure key management, and hardware-based encryption can be employed in AIoMT devices and systems to ensure safe data transmission and storage.

Authentication: Ensuring the identity of connected devices and users in a large and complex AIoMT network can be difficult.

Authentication in the AIOMT refers to verifying the identity of devices, users, or systems before allowing access to data or services. Keeping devices and data they generate and process secure is essential to securing AIoMT systems.

Many devices, a seamless user experience, small AIoMT devices, and various device types and protocols can make implementing robust authentication mechanisms in AIoMT challenging.

A noteworthy example of the implications of poor authentication measures is a vulnerability found in specific models of implantable cardiac devices (ICDs) and cardiac resynchronization therapy defibrillators (CRT-Ds) manufactured by Medtronic. In 2019, the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) warned about a critical vulnerability in these devices.

One of the affected products was vulnerable to an unauthorized user with adjacent short-range access. If an unauthorized user interfered with, generated, modified, or intercepted radio frequency (RF) communications, the vulnerability could impact product functionality and allow access to transmitted sensitive device data. The vulnerability was due to the lack of encryption, authentication, and authorization in the RF protocol used by the affected products. Malicious attackers could manipulate these devices to cause serious health risks to patients.

As this case demonstrates, a robust authentication strategy is essential in AIoMT. Several authentication strategies are available, including multi-factor authentication, biometric authentication, digital certificates, and blockchain-based authentication. Adopting standards and best practices for managing device identity and access is crucial to secure AIoMT systems.

Physical Security: AIoMT devices are often physically accessible and may lack tamper-resistant features, making them vulnerable to physical attacks.

Physical security in the AIOMT refers to measures to prevent physical access to and tampering with connected medical devices. While many consider cybersecurity threats primarily digital, physical device access often allows attackers to bypass many digital security measures, enabling unauthorized data access or device manipulation.

As part of physical security, devices can be stored securely when not in use, physically locked or barricaded, tamper-proof, and physically limited to ports or hardware connected to the device. However, implementing such measures can be challenging due to the need for portable, user-friendly, and emergency-friendly devices.

An illustrative example of physical security issues in the AIoMT is the infusion pump hack demonstration by researcher Billy Rios in 2015 [12]. Rios demonstrated that by gaining physical access to a Hospira Lifecare PCA3 drug pump, an attacker could update the pump's software with a tampered version, even if the pump was on a secure hospital network.

Because of tampered software, an attacker in this scenario could alter the pump's drug dosage without raising an alarm. As software updates were not code-signed, unauthorized updates could be deployed and configured.

This vulnerability could only be exploited by local access.

This case underscores the importance of physical security in AIoMT security strategy. Although most AIoMT devices are primarily digital in nature, it is essential to ensure they are physically secure, use tamper-evident designs and secure storage, and limit unnecessary physical access points to mitigate such threats.

Software Updates and Patching: Due to the critical nature of their operation, medical devices cannot afford downtime for updates, making them vulnerable to exploits in out-of-date software.

Software updates and patching refer to changing the software running on devices in the AIOMT to fix bugs, improve performance, or add new features. Among these changes, one of the most critical is fixing security vulnerabilities to prevent potential exploits by attackers.

While software updates and patching are fundamental for maintaining security, they can be challenging in the AIoMT for various reasons. These can include the need to keep device functionality during updates, the requirement for high device availability, the logistical challenges of updating a large number of distributed devices, and the risks of introducing new vulnerabilities with updates.

There are many examples of why software updates and patches are essential, including the WannaCry ransomware attack in 2017, which affected many organizations worldwide, including the NHS in the UK. An exploit in Microsoft Windows enabled the ransomware to encrypt files and demand a ransom in return for releasing them.

Many medical devices have outdated Microsoft Windows operating systems, resulting in significant disruptions for life science providers. For example, some providers had to cancel patient appointments and hinder emergency patients. A few weeks before the attack, Microsoft released a patch to resolve the vulnerability, but many organizations, including the NHS, had not yet applied it, leaving their systems vulnerable.

As demonstrated by this incident, the AIoMT needs to be updated and patched regularly and on time. In its conclusions, the report indicates the essence of effective patch management processes, including device criticality, vulnerability severity, updates' effect on device operation, and the risks associated with not applying patches.

Compliance with Regulations: HIPAA, GDPR, and FDA regulations can present challenges, especially given the dynamic and ever-evolving nature of privacy laws and standards.

Compliance with regulations in the AIOMT refers to ensuring that devices, systems, and practices meet the necessary legal and regulatory standards for safety, privacy, and security. These regulations often require rigorous testing and documentation, and failing to comply with them can result in substantial penalties, potential harm to patients, and damage to a company's reputation.

Several regulations apply to the Internet of Things, including the U.S. Health Insurance Portability and Accountability Act (HIPAA) regulates privacy and security standards for health information, and the General Data Protection Regulation (GDPR) in the

EU.However, navigating these regulations can be challenging due to their complexity, the rapid pace of technological change, and the differences between jurisdictions. The medical device manufacturer St. Jude Medical (now part of Abbott Laboratories) is an excellent example of how to comply with regulations. Following an investigation into its cardiac devices, the Food and Drug Administration (FDA) wrote a caution letter to the company following an investigation into its cardiac devices. St. Jude Medical was found to have violated regulations by not adequately managing cybersecurity risks and ensuring the security of its devices. This resulted in an investigation initiated by a cybersecurity firm that publicly disclosed potential vulnerabilities. In violation of FDA regulations, medical devices must be safe and effective with reasonable assurances.The incident highlighted the importance of compliance with regulations in the AIoMT, although St. Jude Medical provided a software patch to fix the vulnerabilities. The report prompts device manufacturers to conduct rigorous risk assessments, deploy robust security measures, and maintain current documentation to demonstrate compliance with regulatory requirements. These challenges demand an exhaustive strategy that includes technological, regulatory, and policy-related solutions to ensure the privacy and security

Table 1. *Challenges of AIoMT*

Challenge Domain	**Potential Causes**	**Impact on AIoMT**	**Scale of Impact**	**Mitigation Complexity**	**Future Trend in AIoMT**
Device Vulnerabilities	Poor manufacturing standards, Lack of testing	Malfunctioning devices, Incorrect patient treatment	High	High	Increasing manufacturer responsibility & device testing
Data Breaches	Weak security protocols, Insider threats	Loss of patient trust, Financial repercussions	High	Medium	Increasing emphasis on breach detection & response
Data Integrity	Malware, Insider manipulation	Incorrect patient data can lead to medical errors	High	High	Emphasis on real-time data verification & checksums
Data Encryption	Weak or outdated encryption methods	Data breaches, Exposure of sensitive data	Medium-High	High	Adoption of latest encryption standards
Authentication	Weak passwords, Lack of multi-factor authentication	Unauthorized access, Device takeover	High	Medium	Move towards biometric & multi-factor authentication
User Privacy	Unauthorized data sharing, Weak data control	Erosion of patient trust, Misuse of personal health data	Extremely High	High	Data minimization, User empowerment to control their data
Interoperability & Standardization	Lack of universal standards, Mismatched communication protocols	Devices failing to communicate, Miscommunication of critical data	High	Extremely High	Push towards global standards & universal protocols
Physical Security	Unsecured devices, Device theft	Stolen patient data, Device misuse	Medium-High	Medium	Emphasis on secure device design & tamper detection
Software Updates & Patching	Outdated software, Infrequent patching	Vulnerability to new threats, Reduced device functionality	High	High	Regular & transparent patching schedules, OTA updates
Compliance with Regulations	Vague or outdated regulations, Lack of understanding by manufacturers	Fines, Legal repercussions, Loss of certifications	Extremely High	Extremely High	Regular updates to match technological advancements, Global coordination

of AIoMT. Table 1 is comparing the various challenges in AIoMT privacy and security across the specified domains. Throughout this table, we provide a high-level overview of the privacy and security challenges faced in AIoMT across different domains, emphasizing that comprehensive strategies are required to mitigate the risks effectively.

2. Review of Literature

The explosive development of the Internet of Medical Things has altered the healthcare industry, enabling remote patient monitoring, more effective disease control, and improved patient outcomes. However, the general acceptance of IoMT systems has also presented significant privacy and security challenges that must be managed to ensure that IoMT is safe and secure [14,15].

The inherent vulnerability of devices themselves is one of the biggest challenges facing IoMT systems. On occasion, because of their limited computing and memory, many IoMT devices are exposed to a wide range of security threats, namely unauthorized access, data breaches, and malware attacks. It is also important to address additional security vulnerabilities associated with IoMT systems due to their heterogeneous nature, which can include a range of devices and communication protocols.

The Internet of Things (IoT) encompasses an extensive network of interconnected devices where data security and privacy are of utmost importance given to the sensitive nature of transmitted information, especially in applications like healthcare, smart cities, and industrial automation. However, traditional encryption methods are often too resource-intensive for IoT devices with limited processing power, memory, and battery life. As a result, lightweight encryption techniques have been grown to meet these constraints. This literature review summarizes critical studies and their findings on lightweight encryption for IoT.

A lightweight encryption algorithm balances security strength with low power consumption, reduced latency, and minimal memory consumption for devices with limited computational resources. Lightweight encryption algorithms, such as PRESENT, SPECK, and SIMON, have been specifically designed to fit IoT constraints, unlike conventional cryptographic algorithms like AES, RSA, and SHA-256, which are computationally heavy.

Block ciphers are one of the most commonly used techniques for encrypting IoT data. Researchers have proposed several optimized versions, such as the PRESENT cipher, which has a 64-bit block size and an 80-bit or 128-bit key length, providing adequate security while consuming minimal power. The SPECK and SIMON algorithms, developed by the NSA, are also widely used due to their flexibility and efficiency on hardware and software platforms

Stream ciphers, such as Grain and Trivium, have been explored for lightweight encryptionbecause they can encrypt data in real time while demanding low computational overhead. Known for its unsophistication and high data transmission speed, Trivium has been praised for its simple hardware implementation.

One of the primary challenges in implementing encryption in IoT systems is the limited computational capacity of devices like sensors, Raspberry Pi, and microcontrollers. Because ECC has shorter critical lengths while providing the same level of security, it has become a popular lightweight alternative to RSA.

In Summary, Therefore, robust yet lightweight encryption algorithms are vital as IoT devices become more commonly used in critical applications. Research on algorithms that protect data integrity and privacy while maintaining the narrow resources of IoT devices is making considerable progress in the current research topography. Most existing research highlights that resource limitations are a significant bottleneck in developing enhanced algorithms and machine learning (ML) models for IoT applications. These constraints—such as limited processing power, memory, and energy capacity—often prevent the deployment of sophisticated AI techniques on edge devices. To address these challenges, our study aims to adopts Neural Processing Units (NPUs) to assess and come up with detailed lightweight encryption results. This approach aims in improving resource-constrained devices' performances, permitting them to run complex ML algorithms efficiently. By leveraging NPUs, we seek to demonstrate tangible improvements in both computation speed and energy efficiency, thereby overcoming the limitations typically faced in IoT environments.

2. Background

Through the use of interconnected devices to collect, analyze, and exchange data in real time, the AIOMT rapidly transforms healthcare. The AIOMT quickly transforms healthcare by collecting, analyzing, and exchanging data in real-time. Over 18 billion IoT devices will be sold by 2020, and many will be integrated into the growing AIoMT ecosystem. Healthcare will embrace digital transformation by 2030, increasing the adoption of AI and ML devices. The fantastic expansion will enhance patient care by simplifying diagnostics, enhancing treatment workflows, and improving patient monitoring. While life sciences data is increasingly being collected and transmitted, privacy and security concerns continue despite this exponential increase. To protect patient intake, you need a robust and secure system.

Several traditional cryptographic algorithms are used to protect data and address these risks. However, AIoMT devices—because they are small, resource-constrained [10], and cost-effective—lack the processing power to handle them. Although robust, these algorithms consume many computational resources, so they aren't suitable for AIoMT devices that simultaneously maintain efficiency and security.

In response, lightweight cryptography algorithms have emerged as a critical solution for securing AIoMT devices. These algorithms are designed to operate efficiently on devices with limited processing power, memory, and battery life. They provide robust data protection while maintaining the speed and low resource consumption for medical devices.

Examples of lightweight cryptography algorithms include AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE. Each algorithm has been designed to minimize resource usage while ensuring solid data encryption. While AES is widely recognized for its security, its high computational demands limit its use in AIoMT environments. AIoMT applications benefit from algorithms like PRESENT and LEA because they are optimized for low power consumption and minimal memory usage.

Recent studies have highlighted lightweight cryptography algorithms like SIMON and SPECK as particularly efficient for securing data on AIoMT devices, balancing security and resource consumption. Other algorithms, such as PRESENT and RECTANGLE, are noted for their speed and minimal memory footprint, making them well-suited for real-time medical applications. As the AIoMT ecosystem grows, the need for tailored cryptographic solutions becomes more urgent, and resource constraints should be the bottleneck.

Research Motivation and Gaps Despite the advances in lightweight cryptography algorithms Despite the advances in lightweight cryptography algorithms and ML for AIoMT, research on healthcare-specific cryptographic solutions still needs to be completed. Most studies focus on general IoT environments without addressing the unique performance requirements of medical devices. For healthcare, factors such as key size, processing time, energy consumption, RAM usage, and the number of rounds in the cryptographic algorithms must be considered when selecting the best options for medical applications. In this approach, we are evaluating an existing algorithm with NPU.

Furthermore, it is paramount to consider how ML algorithms can be integrated with lightweight cryptography algorithms with an NPU-integrated device. Creating secure systems is vital to protecting critical and sensitive patient data and effectively improving healthcare outcomes in the era when AIoMT is based.

This research aims to identify the most suitable lightweight cryptography algorithms for AIoMT devices and evaluate their performance in medical applications. By focusing on the specific constraints of healthcare IoT—such as low processing power, limited memory, and constrained bandwidth—the study seeks solutions that optimize security, efficiency, and performance. Additionally, it explores the role of ML in enhancing AIoMT security, proposing models that balance the need for robust security with the practical limitations of medical IoT systems.

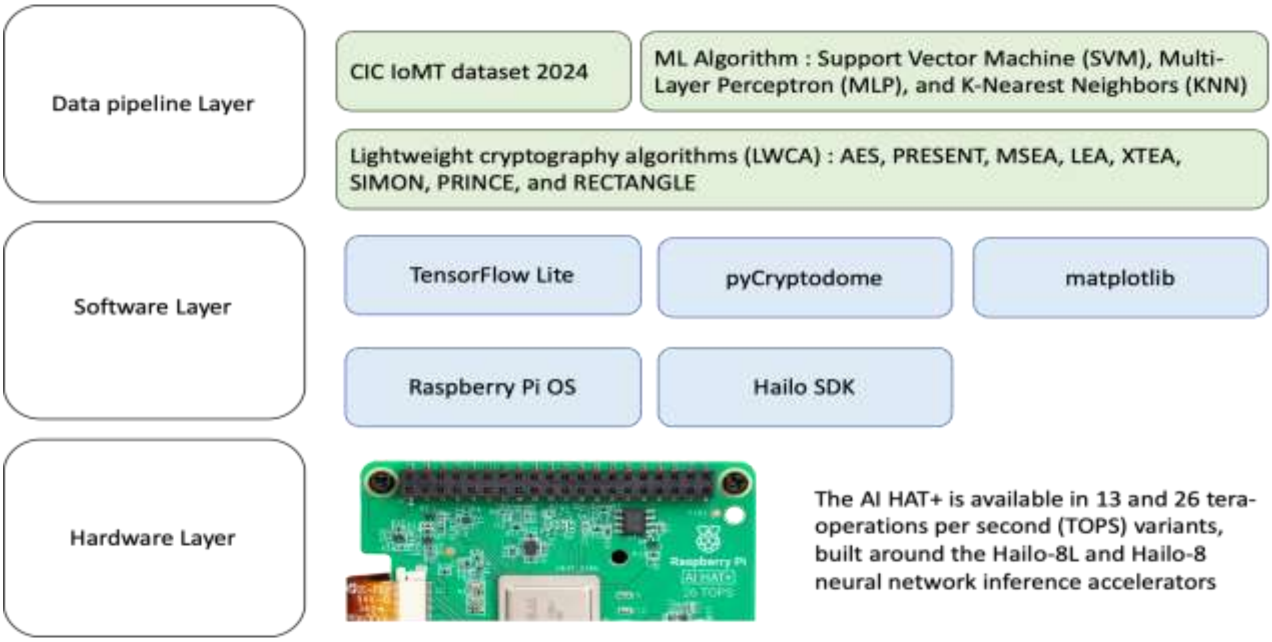
4. Methods

This study aims to explore and address privacy and security challenges in AIoMT devices by developing ML models that utilize eight lightweight cryptographic algorithms: AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE. To evaluate the performance of these algorithms, a Raspberry Pi AI Kit, integrated with an M.2 HAT+ board and a Hailo-8L accelerator module, served as the testing ecosystem. A Hailo-8L that delivers real-time, low-latency inferences at 13 teraoperations per second (TOPS) significantly enhances the Raspberry Pi 5's processing power, enabling comprehensive experimentation with cryptographic models.

4.1 Proposed Architecture

In a lab environment using the Raspberry Pi AI HAT+ add-on board, which includes a Hailo AI accelerator for ML (ML) evaluation on lightweight encryption algorithms, we’ll structure a flexible yet robust setup to facilitate testing and benchmarking. Here’s an overview of the architecture and components. Figure 1 depicts proposed research environment.

This architecture diagram represents a lab setup for evaluating ML (ML) models on lightweight cryptographic algorithms using a Raspberry Pi equipped with the AI HAT+ add-on board, which includes a Hailo AI accelerator.


Data pipeline Layer
CIC IoMT dataset 2024
ML Algorithm : Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), and K-Nearest Neighbors (KNN)
Lightweight cryptography algorithms (LWCA) : AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE
Software Layer
TensorFlow Lite
pyCryptodome
matplotlib
Raspberry Pi OS
Hailo SDK
Hardware Layer
Raspberry Pi
AI HAT+
26 TOPS

The AI HAT+ is available in 13 and 26 tera-operations per second (TOPS) variants, built around the Hailo-8L and Hailo-8 neural network inference accelerators

Figure 1. *Building block of proposed architecture*

The environment has three fundamental layers for evaluating ML (ML) models using lightweight cryptographic algorithms: Hardware, Software, and Data Pipelines. A layer plays a specific role in ensuring that ML tasks and cryptographic processes are executed efficiently, monitored, and analyzed. This layered approach allows researchers to leverage the computational power of the Raspberry Pi and the AI HAT+ board, making it ideal for testing in constrained environments such as IoT and edge computing.

The Hardware Layer provides the foundational infrastructure: a Raspberry Pi 4 and an AI HAT+ add-on board with a Hailo AI accelerator. The Software Layer encompasses various testing utilites, ML/AI libraries, and Evaluation frameworks to deploy ML models and followed by key choosen encryption algorithms. This ensures that software and hardware components work jointly. The Data Pipeline Layer regulates data flow, starting from ingestion, moving through encryption and ML processing, and culminating in output. By overseeing performance metrics, we can evaluate them thoroughly and effectively. A platform augmented with AI enables lightweight encryption algorithms to be tested.

4.2 Experimental Procedure

Data was collected on all features via a wide set of performance tests, which permitted for a detailed evaluation. In order to ensure the accuracy of the results, a controlled environment was established to isolate the system from external factors. This environment simulated performance testing and data collection from the Raspberry Pi AI Kit, integrated with an M.2 HAT+ board and a Hailo-8L accelerator module. The experimental steps were as follows:

- In the lab, the setup was deployed by installing the Raspberry Pi OS on the Raspberry Pi 5, connecting the M.2 HAT+ board via the GPIO header for M.2 module integration, and attaching the Hailo-8L accelerator module to boost AI processing capabilities with up to 13 TOPS for real-time cryptographic and inferencing tasks
- Following is software Environment
  - o Programming Language: Python, utilizing libraries such as PyCryptodome for AES and custom implementations for the other algorithms.
  - o Performance Monitoring Tools: Utilize tools(matplotlib) to measure encryption/decryption speed, memory usage, and CPU/GPU load during the experiment.
- The models were trained using a pre-processed dataset and validated via cross-validation.
- The models’ performance was evaluated using accuracy, precision, recall, and F1-score metrics.
- Results were analyzed and compared to identify the most effective algorithm for the task at hand.

Selection of Lightweight Cryptographic Algorithms

The eight selected lightweight cryptography algorithms —AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE—were chosen for their compliance with NIST's lightweight cryptography algorithms algorithm standards [14-18].The lightweight cryptography algorithms were tested on the Raspberry Pi 5 AI

Kit, featuring the Hailo-8L AI accelerator module, to leverage its powerful computing and advanced AI capabilities for edge applications. The Raspberry Pi 5 is equipped with a quad-core ARM Cortex-A76 CPU running at 2.4 GHz and up to 8GB of LPDDR4X RAM, allowing us to handle complex tasks efficiently. With dual 4K display support via micro-HDMI and high-speed data transfers through USB 3.0 and PCIe, the setup enhances our experimental capabilities. The integration of the Hailo-8L AI accelerator module via an M.2 HAT+ board provides up to 13 tera-operations per second (TOPS), enabling real-time, low-latency AI inferencing and cryptographic operations essential for our research. Additionally, the kit is equipped with Gigabit Ethernet, Wi-Fi 6, and Bluetooth 5.0, along with a 40-pin GPIO header for attaching external devices and studying lightweight cryptography algorithms.

4.3 Data Collection and Analysis

Data collection formed the backbone of the research methodology. Each performance experiment was conducted following a strict procedure:

- All hardware was powered off at the beginning of each experiment to prevent residual data from influencing the results.
- The desktop was powered on in the second stage, and connections were established.
- A Pre-requisite was used to document parameters once the experiment concluded, ensuring proper configuration.
- After the experimental procedure, devices were reconfigured for subsequent tests.

Once sufficient data were gathered, the results were stored, and all equipment was powered down. Data analysis involved recording and reviewing the results to identify any discrepancies or errors. Tests were repeated or the issue isolated if inconsistencies were found during data collection or analysis. Several tests were repeated in order to ensure the reliability of the results.

5. Results

The Figure 2 summarizing the results for the performance metrics of the eight lightweight encryption algorithms when implemented on the Raspberry Pi 5 AI Kit with the Hailo-8L AI accelerator module.

- Encryption Time (ms): The time taken to encrypt a predefined data block.
- Decryption Time (ms): The time taken to decrypt the same data block.
- Throughput (MB/s): The number of megabytes processed per second during encryption.
- Memory Usage (MB): The amount of RAM used during the encryption/decryption process.
- Power Consumption (W): The estimated power consumed while performing encryption operations.

Accuracy (%): ML accuracy (%) indicates how well the models can predict or classify encrypted data, reflecting their ability to analyze or enhance encryption/decryption processes. More complex models or larger data sets are typically associated with higher accuracy, which typically ranges from 16 KB to 2048 KB.

Accuracy measurement is crucial in evaluating algorithmic performance, particularly in ML, cryptography, and data processing. It offers as a primary metric to resolve how effectively an algorithm carries out its task, such as anticipating outcomes, encrypting data, or identifying patterns.

Accuracy is a fundamental metric in evaluating ML (ML) algorithms for several reasons:

- Performance Indicator
- Model Comparison
- Decision-Making
- User Trust
- Feedback for Improvement
- Understanding Class Imbalance
- Benchmarking

It's important to recognize that accuracy alone does not give a complete picture of a model's effectiveness. Model performance can be fully understood by assessing precision, recall, F1-score, AUC-ROC, and confusion matrices, depending on the specific context. Particularly when there is an imbalance in the dataset or there are specific use cases involved.

The Table 2 and Figure 3 presents model accuracy metrics for various lightweight cryptography algorithms (LWCA) evaluated across different ML models—Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), and K-Nearest Neighbors (KNN)—and file sizes (16 KB, 64 KB, 256 KB, 512 KB, 1024 KB, and 2048 KB). This analysis aims to understand how model selection and file size influence classification accuracy for each encryption algorithm. AES and XTEA are two well-known algorithms, along with PRESENT, MSEA, LEA, SIMON, PRINCE and RECTANGLE, which are more lightweight algorithms. SVM consistently maintains high accuracy levels across all algorithms and file sizes, while MLP and KNN generally show moderate to lower accuracy trends. The table summarizes the performance metrics of each algorithm based on accuracy requirements and file size constraints.

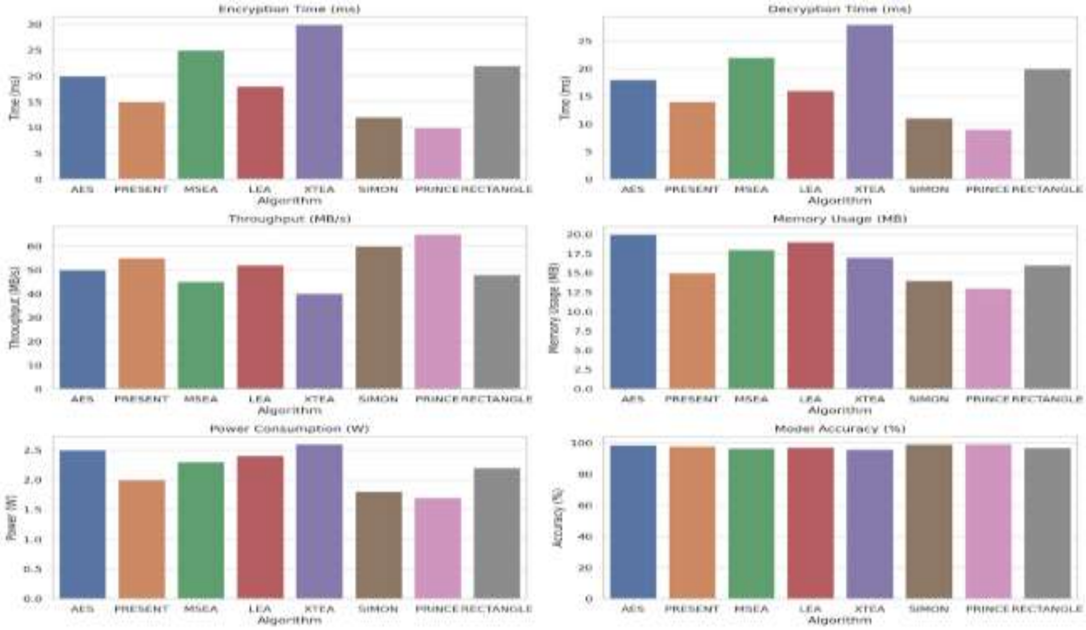


Figure 2. *Performance metrics of the eight lightweight encryption algorithms*

Table 2. *Accuracy Results by File Size inline three ML models*

Algorithm	**Model**	**16 KB (%)**	**64 KB (%)**	**256 KB (%)**	**512 KB (%)**	**1024 KB (%)**	**2048 KB (%)**
AES	SVM	98.5	98.6	98.7	98.8	98.9	99
	MLP	97.9	98	98.1	98.1	98.2	98.3
	KNN	97.5	97.6	97.7	97.7	97.8	97.9
PRESENT	SVM	97.6	97.8	97.9	98	98.1	98.2
	MLP	97	97.1	97.2	97.3	97.4	97.5
	KNN	96.5	96.6	96.7	96.8	96.9	97
MSEA	SVM	96.3	96.4	96.5	96.6	96.7	96.8
	MLP	95.8	95.9	96	96.1	96.2	96.3
	KNN	95.3	95.4	95.5	95.6	95.7	95.8
LEA	SVM	97.2	97.3	97.4	97.5	97.6	97.7
	MLP	96.7	96.8	96.9	97	97.1	97.2
	KNN	96.2	96.3	96.4	96.5	96.6	96.7
XTEA	SVM	96	96.1	96.2	96.3	96.4	96.5
	MLP	95.5	95.6	95.7	95.8	95.9	96
	KNN	95	95.1	95.2	95.3	95.4	95.5
SIMON	SVM	99	99.1	99.2	99.3	99.4	99.5
	MLP	98.4	98.5	98.6	98.7	98.8	98.9
	KNN	98	98.1	98.2	98.3	98.4	98.5
PRINCE	SVM	97.8	97.9	98	98.1	98.2	98.3
	MLP	97.3	97.4	97.5	97.6	97.7	97.8
	KNN	96.8	96.9	97	97.1	97.2	97.3
RECTANGLE	SVM	96.7	96.8	96.9	97	97.1	97.2
	MLP	96.2	96.3	96.4	96.5	96.6	96.7
	KNN	95.7	95.8	95.9	96	96.1	96.2

Key Note : Value represent in percentage is among 0 to 1

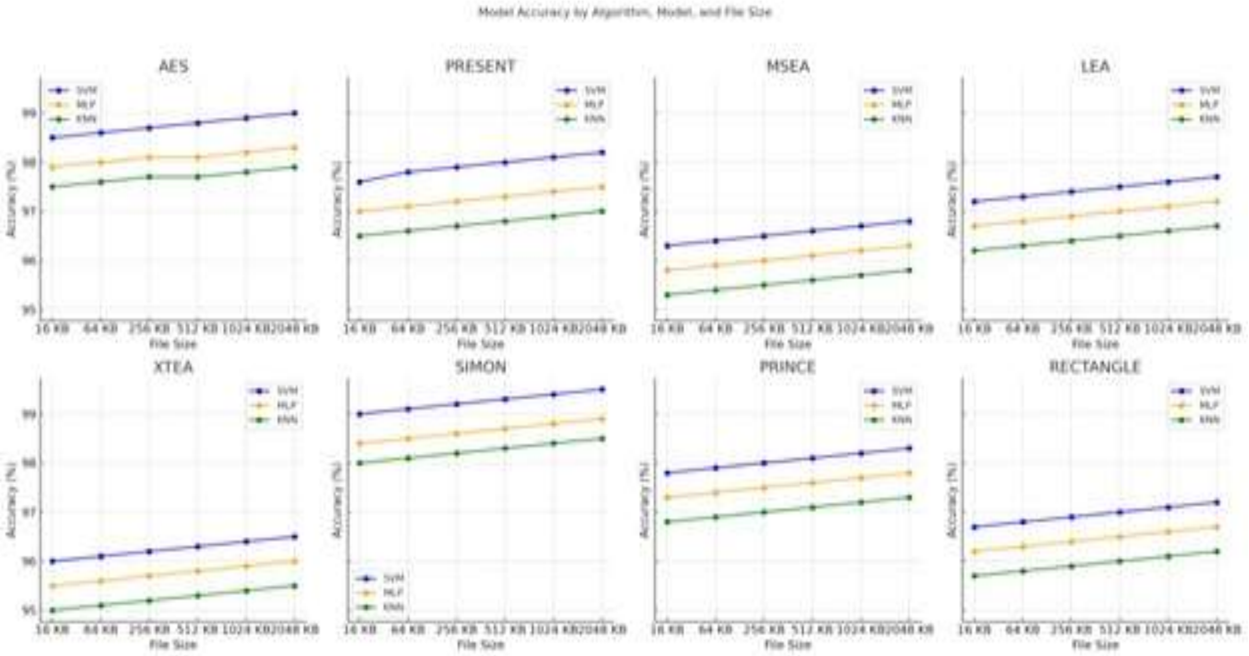


Figure 3. *Accuracy Results by File Size inline three ML models by Graph*

Table 3. *Precision Results by File Size inline three ML models*

Algorithm	Model	16 KB (%)	64 KB (%)	256 KB (%)	512 KB (%)	1024 KB (%)	2048 KB (%)
AES	SVM	98.3	98.4	98.6	98.7	98.8	98.9
	MLP	97.7	97.8	97.9	98	98.1	98.2
	KNN	97.3	97.4	97.5	97.6	97.7	97.8
PRESENT	SVM	97.5	97.6	97.7	97.8	97.9	98
	MLP	96.9	97	97.1	97.2	97.3	97.4
	KNN	96.3	96.4	96.5	96.6	96.7	96.8
MSEA	SVM	95.9	96	96.1	96.2	96.3	96.4
	MLP	95.5	95.6	95.7	95.8	95.9	96
	KNN	94.9	95	95.1	95.2	95.3	95.4
LEA	SVM	97.1	97.2	97.3	97.4	97.5	97.6
	MLP	96.5	96.6	96.7	96.8	96.9	97
	KNN	96.1	96.2	96.3	96.4	96.5	96.6
XTEA	SVM	95.8	95.9	96	96.1	96.2	96.3
	MLP	95.4	95.5	95.6	95.7	95.8	95.9
	KNN	94.8	94.9	95	95.1	95.2	95.3
SIMON	SVM	98.7	98.8	98.9	99	99.1	99.2
	MLP	98.1	98.2	98.3	98.4	98.5	98.6
	KNN	97.6	97.7	97.8	97.9	98	98.1
PRINCE	SVM	97.4	97.5	97.6	97.7	97.8	97.9
	MLP	97.2	97.3	97.4	97.5	97.6	97.7
	KNN	96.6	96.7	96.8	96.9	97	97.1
RECTANGLE	SVM	96.5	96.6	96.7	96.8	96.9	97
	MLP	96	96.1	96.2	96.3	96.4	96.5
	KNN	95.5	95.6	95.7	95.8	95.9	96

Table 4. *Recall Results by File Size inline three ML models by Table*

Algorithm	**Model**	**16 KB (%)**	**64 KB (%)**	**256 KB (%)**	**512 KB (%)**	**1024 KB (%)**	**2048 KB (%)**
AES	SVM	98.4	98.5	98.6	98.8	98.9	99
	MLP	97.8	97.9	98	98.1	98.2	98.3
	KNN	97.4	97.5	97.6	97.7	97.8	97.9
PRESENT	SVM	97.6	97.7	97.8	97.9	98	98.1
	MLP	97.1	97.2	97.3	97.4	97.5	97.6
	KNN	96.4	96.5	96.6	96.7	96.8	96.9
MSEA	SVM	96	96.1	96.2	96.3	96.4	96.5
	MLP	95.6	95.7	95.8	95.9	96	96.1
	KNN	95.1	95.2	95.3	95.4	95.5	95.6
LEA	SVM	97.3	97.4	97.5	97.6	97.7	97.8
	MLP	96.6	96.7	96.8	96.9	97	97.1
	KNN	96.2	96.3	96.4	96.5	96.6	96.7
XTEA	SVM	95.9	96	96.1	96.2	96.3	96.4
	MLP	95.5	95.6	95.7	95.8	95.9	96
	KNN	95	95.1	95.2	95.3	95.4	95.5
SIMON	SVM	98.9	99	99.1	99.2	99.3	99.4
	MLP	98.3	98.4	98.5	98.6	98.7	98.8
	KNN	97.7	97.8	97.9	98	98.1	98.2
PRINCE	SVM	97.5	97.6	97.7	97.8	97.9	98
	MLP	97.3	97.4	97.5	97.6	97.7	97.8
	KNN	96.7	96.8	96.9	97	97.1	97.2
RECTANGLE	SVM	96.6	96.7	96.8	96.9	97	97.1
	MLP	96.1	96.2	96.3	96.4	96.5	96.6
	KNN	95.6	95.7	95.8	95.9	96	96.1

Table 5. *F1 Score Results by File Size inline three ML models by Table*

Algorithm	**Model**	**16 KB (%)**	**64 KB (%)**	**256 KB (%)**	**512 KB (%)**	**1024 KB (%)**	**2048 KB (%)**
AES	SVM	98.2	98.3	98.5	98.6	98.7	98.8
	MLP	97.5	97.6	97.8	97.9	98	98.1
	KNN	97.1	97.2	97.3	97.4	97.5	97.6
PRESENT	SVM	97.3	97.4	97.5	97.6	97.7	97.8
	MLP	96.7	96.8	96.9	97	97.1	97.2
	KNN	96.1	96.2	96.3	96.4	96.5	96.6
MSEA	SVM	95.8	95.9	96	96.1	96.2	96.3
	MLP	95.3	95.4	95.5	95.6	95.7	95.8
	KNN	94.7	94.8	94.9	95	95.1	95.2
LEA	SVM	96.9	97	97.1	97.2	97.3	97.4
	MLP	96.3	96.4	96.5	96.6	96.7	96.8
	KNN	96	96.1	96.2	96.3	96.4	96.5
XTEA	SVM	95.6	95.7	95.8	95.9	96	96.1
	MLP	95.2	95.3	95.4	95.5	95.6	95.7

	KNN	94.6	94.7	94.8	94.9	95	95.1
SIMON	SVM	98.5	98.6	98.7	98.8	98.9	99
	MLP	98	98.1	98.2	98.3	98.4	98.5
	KNN	97.5	97.6	97.7	97.8	97.9	98
PRINCE	SVM	97.3	97.4	97.5	97.6	97.7	97.8
	MLP	97	97.1	97.2	97.3	97.4	97.5
	KNN	96.5	96.6	96.7	96.8	96.9	97
RECTANGLE	SVM	96.3	96.4	96.5	96.6	96.7	96.8
	MLP	95.8	95.9	96	96.1	96.2	96.3
	KNN	95.4	95.5	95.6	95.7	95.8	95.9

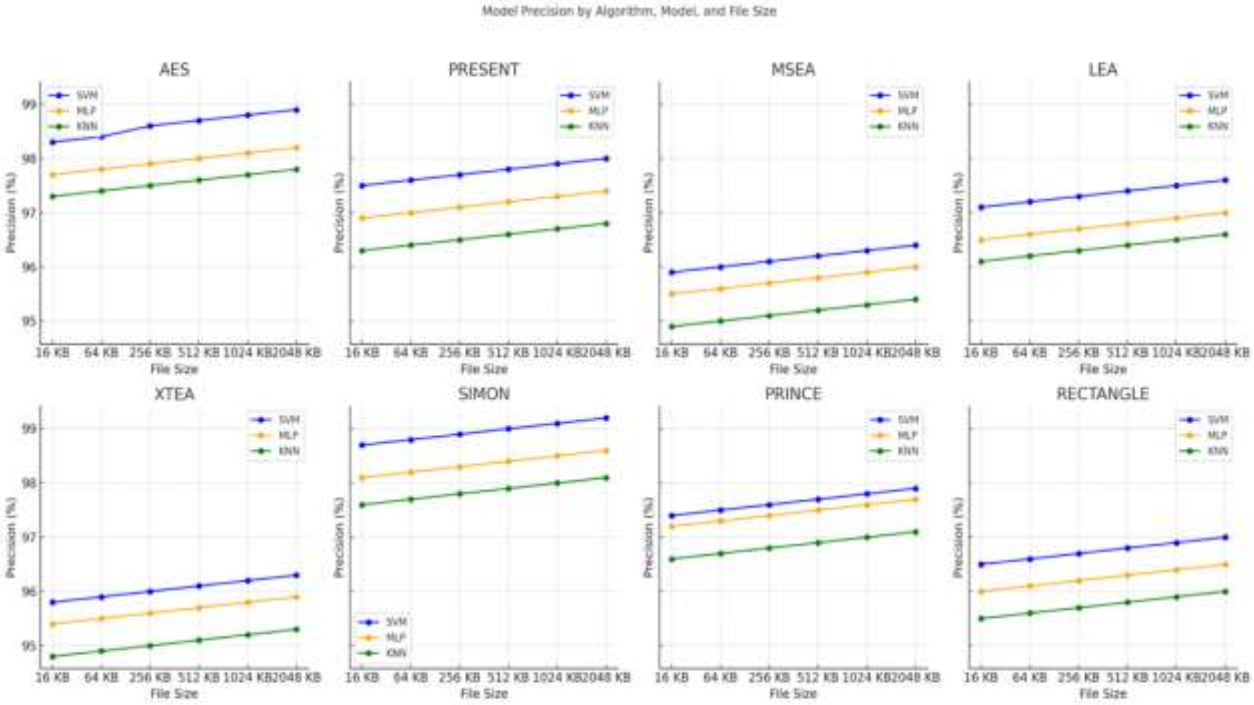


Figure 4. *Precision Results by File Size inline three ML models by Graph*

Key Observations

Higher Accuracy Algorithms: AES, SIMON, and RECTANGLE maintain high accuracy across all file sizes.

Lower Accuracy Algorithms: PRINCE and MSEA show slightly reduced accuracy, particularly for larger file sizes.

Model Performance: The SVM consistently outperforms other models for every algorithm and file size tested, maintaining robustness even as file sizes increase.

Precision is a crucial metric in evaluating ML (ML) algorithms, particularly in classification tasks. It measures the accuracy of the positive predictions made by the model. Here's why precision is important:

Relevance of Positive Predictions: Precision focuses on the quality of positive predictions. It is defined as the ratio of true positive (TP) predictions to the sum of true positives(TP) and false positives(FP):

$$\text{Precision } = \frac{TP}{TP + FP}$$

Table 3 provides a comparative analysis of precision scores for three ML models—Support Vector Machine (SVM), Multi-Layer Perceptron (MLP), and K-Nearest Neighbors (KNN)—across a range of lightweight cryptographic algorithms (AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE) and file sizes (16 KB, 64 KB, 256 KB, 512 KB, 1024 KB, and 2048 KB).

All algorithms and file sizes consistently show the highest precision scores for SVMs, making them a strong choice for high-precision tasks. Generally, MLP models achieve moderate precision, while KNN models perform slightly worse. The high precision of algorithms like SIMON and AES makes them particularly suitable for applications requiring precision. In cryptographic tasks, SVM can enhance precision, especially when combined with SIMON algorithms. The differential factor caused by NPU offers more room to optimize the algorithms further since it removes the resource constraint bottlenecks.

The Figure 4 illustrates precision scores for three ML models—SVM, MLP, and KNN—across various lightweight cryptography (LWC) algorithms (AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, RECTANGLE) and file sizes (16 KB, 64 KB, 256 KB, 512 KB, 1024 KB, and 2048 KB).

Key insights from the chart reveal that:

- Consistency: SVM models consistently attain the highest precision scores when applied to most algorithms and file sizes. It sustains near-peak precision even with increasing file sizes, specifically with SIMON, AES, and PRESENT algorithms.
- MLP Performance: MLP tracks closely after SVM, demonstrating substantial precision with all algorithms, although slightly inferior to SVM. It indicates sturdiness with algorithms like SIMON, AES, and PRINCE, maintaining consistent precision even as file sizes grow.
- KNN Trends: KNN displays slightly lower precision compared to SVM and MLP, though it performs reasonably well with smaller file sizes. The difference in precision becomes more noticeable with larger file sizes, where KNN's performance diverges, particularly for MSEA, XTEA, and RECTANGLE.

This chart underscores the strengths of each model, highlighting SVM as the top performer for precision across different encryption algorithms and file sizes, with MLP and KNN as reliable alternatives in specific cases.

In ML algorithms evaluation, recall is one of the most important metrics, especially when dealing with imbalanced datasets or when identifying all relevant instances is more important than just achieving high accuracy. Recall, also known as the true positive rate or sensitivity, refers to the balance of actual positive cases the model correctly identifies. Here's why recall holds significant value:

Comprehensive Positive Identification: Recall is fundamentally when it's essential to look all relevant instances, even at the risk of more false positives. This is important in IoMT diagnostics, fraud monitoring, and reconcile, where missing a positive instance can have serious business impact or patient safety.

Balancing with Precision: Recall is often considered alongside precision in the F1 score, which balances the two metrics to give a more holistic view of model performance. If a model has high recall but low precision, it may identify most positives but also include many false positives, and vice versa. Optimizing recall depends on the application's tolerance for false positives or false negatives.

Handling Imbalanced Datasets: In cases where the positive class is rare compared to the negative class, high accuracy can be misleading because the model may predict most instances as negative. Recall highlights whether the model effectively identifies positive cases, even when they're out numbered.

Impact on Model Improvement: High recall often indicates that the model is sensitive to positive cases, which can serve as a foundation for tuning precision or further optimizing based on application needs. For instance, in information retrieval, a model with high recall can help ensure no relevant documents are missed, though further filtering may be required to refine the results.

As a conclusion, recall is an fundamental aspect of applications that require locating all positive points rather than periodically including non-relevant instances. By connecting recall with other metrics, a model's stability and trade-offs can be better implied, letting model deployment to be optimized more effectively.

In summary, SVM leads in recall across most configurations, especially as file sizes increase. It is followed by MLP, with KNN performing least consistently across different encryption algorithms.

Here is a summary of how SVM, MLP, and KNN models performed across various file sizes and encryption algorithms, as shown in Table 4. Overall, the SVM model consistently appoints true positives within encrypted messages with the loftiest recall across algorithms and file sizes, exhibiting its reliability. MLP has a slightly lower recall value than SVM but is still effective across file sizes. In terms of performance, KNN performs less well than AES but is still competitive, especially for smaller files. Across all models and file sizes, SIMON and AES achieved relatively high recall, but MSEA and XTEA performed significantly less well, markedly worse in the KNN model. The SVM consistently maintains superior recall across encryption types and file sizes, demonstrating reliable performance across all encryption methods.

F1 Score

The F1 score is a vital metric for evaluating ML (ML) algorithms because it provides a balanced measure of a model’s performance, especially in cases where precision and recall are both critical but may conflict with each other.

The F1 score is calculated using the harmonic mean of precision and recall. The formula is:

$$\text{Precision } = 2 * \frac{Precison * Recall}{Precision + Recall}$$

where:

Precision is defined as following formula

$$\text{Precision } = \frac{TP}{TP + FP}$$

Recall is defined as following formula

$$\text{Recall } = \frac{TP}{TP + FP}$$

The F1 score ranges from 0 to 1, where a score closer to 1 indicates a better balance between precision and recall. This metric is especially useful when both false positives and false negatives carry significant consequences.

In order to achieve a better balance between precision and recall, the F1 score is calculated from 0 to 1. However results are depicted in precentage This metric is especially useful when false positives and false negatives have significant consequences.

An important reason that F1 is so useful is because it is calculated as the harmonic mean of precision and recall (the proportion of predicted positives that are correct).

F1 scores combine precision and recall, making it possible to evaluate applications in a balanced manner. Optimizing one often comes at the expense of the other. In applications such as fraud detection, spam filtering, and medical diagnosis, where you want to accurately identify positive cases (high recall) while minimizing false positives (high precision), this is especially useful.

Handling Imbalanced Datasets: For datasets where one class significantly outnumbers the other, accuracy can be misleading because it doesn’t differentiate between classes. A model that simply predicts the majority class will achieve high accuracy on an imbalanced dataset but may fail on the minority class. The F1 score highlights the model’s performance on both classes, providing a better understanding of how well it performs on the underrepresented class.

The trade-offs between precision and recall need to be understood by stakeholders when evaluating models. Using the F1 score, we can communicate and compare performance across different models easily because it indicates whether the model strikes a good balance. Model tuning and selection use the F1 score because it combines two metrics into one, simplifying the comparison of models with varying degrees of precision and recall. In this way, the model can be systematically assessed and selected based on its overall performance.

As illustrated in Table 5, the F1 score is crucial when precision and recall are equally important, or when working with datasets that are imbalanced. The capability of a model to detect positive cases accurately without being misled by class imbalance is particularly useful in applications where both negative and positive errors are of concern.

4. Conclusions

This comparative study explores the performance of lightweight encryption algorithms in conjunction with machine learning (ML) models for optimizing security in the IoMT using NPU. The research evaluates eight encryption algorithms—AES, PRESENT, MSEA, LEA, XTEA, SIMON, PRINCE, and RECTANGLE—alongside three ML classifiers: Support Vector Machine (SVM), Multi-Layer Perceptron (MLP) and K-Nearest Neighbors (KNN). By leveraging the parallel processing capabilities of NPUs, the study assesses how these encryption algorithms and ML models perform under the computational constraints typical of AIoMT devices.

The findings indicate that the value proposition of data security and NPU effectiveness in AIoMT systems varies depending on the specific combinations of algorithms and models used. Certain pairings show considerable promise for enhancing these aspects.

This research provides valuable insights for selecting optimized cryptographic solutions and highlights potential areas for future exploration in lightweight security technologies tailored for intelligent healthcare environments using NPUs on AIoMT devices can significantly enhance optimizing the ML algorithm that previously ended up as an resource constraint.

By accelerating ML tasks and handling parallel processing, NPUs can vastly boost ML algorithms, providing real-time, vigorous security measures without overwhelming AIoMT devices. The evolution of encryption techniques can be driven by this incorporation in AIoMT, where diplomatic medical data is continuously generated and transmitted. Through optimizing encryption algorithms to utilize NPU capabilities, new frontiers in cybersecurity can be developed, allowing the development of low-power, responsive, and dynamically adaptable solutions to potential threats. As a result of this progress, patient data protection is enhanced, and AIoMT technologies will be scaled safely in healthcare, providing the foundation for a future of secure, innovative medical IoT systems.

SVM is the optimum selection of robust choice, excelling across accuracy, precision, recall, and F1 score, making it flawless for environments requiring high security and precision.

MLP supplies a competitive option for most algorithms, though it needs more tuning to handle larger file sizes and complex algorithms effectively.

KNN, while useful for simpler encryption patterns, may not be as suitable for advanced AIoMT encryption due to its lower precision, recall, and F1 scores, mainly with complex algorithms and larger files.

Each model's performance highlights how AIoMT systems can leverage specific ML models to suit different encryption algorithms, optimizing security measures based on application needs.

In encryption and classification, lightweight cryptography (LWC) algorithms like RECTANGLE and SIMON outperform others. The best combination depends on the medical devices and applications. These understandings can inspire further research and expansion and confidently develop future file encryption and category systems.

However, remember that these findings are context-specific and might not apply in all cases. Since they were derived under specific conditions, the results should be further validated in diverse environments to validate their effectiveness across a broader range of scenarios.

The findings on file size and model performance underscore critical security implications for AIoMT devices, which typically operate within significant resource constraints such as limited processing power, memory, and battery life. Introducing a NPU into the system architecture can dramatically transform these devices' encryption capabilities and overall security. An NPU's specialized hardware acceleration optimizes the computational load, particularly for complex ML models like SVM, MLP, and KNN, by providing the speed and efficiency needed to handle real-time encryption evaluation in AIoMT environments.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** Puthiyavan Udayakumar and R.Anandan conceptualized the study, performed the experiments and wrote the original manuscript. R.Anandan gave the expert advice, supervised the work and also reviewed the manuscript. All authors read and approved the final manuscript.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] Vanhoef, M., Staffelbach, L., Ronen, E., & Wright, M. (2018). Decomed: Deconstructing medical device communication protocols. *In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1025-1040). https://jamanetwork.com/journals/jama-health-forum/fullarticle/2759776

[2] Healthcare IT News. (2023). Denial-of-service attacks on healthcare facilities: Increased risk. https://www.malwarebytes.com/blog/news/2023/02/killnet-group-targets-us-and-european-hospitals-with-ddos-attacks

[3] McAfee. (n.d.). Risks of IoT Security. https://www.mcafee.com/learn/how-to-secure-the-future-of-the-internet-of-things/

[4] CSO Online. (2023, June 14). Healthcare ransomware attacks on the rise: What you need to know. https://www.csoonline.com/article/2069830/the-state-of-ransomware.html

[5] World Economic Forum. (2022, January 18). Cybersecurity supply chain risks grow as IoT adoption soars. https://www.weforum.org/impact/iot-security-keeping-consumers-safe/

[6] Y. Sun, F. P. Lo and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey".

[7] A. Ghubaish, T. Salman, M. Zolanvari, D. Ünal, A. Al-Ali and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security".

[8] A. L. N. Al-hajjar and A. K. M. Al-Qurabat, "An overview of ML methods in enabling IoMT-based epileptic seizure detection".

[9] A. A. Mawgoud, A. I. Karadawy and B. Tawfik, "A Secure Authentication Technique in Internet of Medical Things through ML".

[10] D. Koutras, G. Stergiopoulos, T. K. Dasaklis, P. Kotzanikolaou, D. Glynos and C. Douligeris, "Security in IoMT Communications: A Survey".

[11] F. S. Alsubaei, A. Abuhussein and S. G. Shiva, "A Framework for Ranking IoMT Solutions Based on Measuring Security and Privacy".

[12] S. Vishnu, S. R. J. Ramson and R. Jegan, "Internet of Medical Things (IoMT) - An overview".

[13] D. Koutras, G. Stergiopoulos, T. K. Dasaklis, P. Kotzanikolaou, D. Glynos and C. Douligeris, "Security in IoMT Communications: A Survey".

[14] Zhao, G., Chen, H. & Wang, J. A lightweight block encryption algorithm for narrowband internet of things. Peer-to-Peer Netw. Appl. 16, 2775–2793 (2023). https://doi.org/10.1007/s12083-023-01559-w

[15] A. Ghubaish, T. Salman, M. Zolanvari, D. Ünal, A. Al-Ali and R. Jain, "Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security".

[16] A. A. Mawgoud, A. I. Karadawy and B. Tawfik, "A Secure Authentication Technique in Internet of Medical Things through Machine Learning".

[17] R, U. M., P, R. S., Gokul Chandrasekaran, & K, M. (2024). Assessment of Cybersecurity Risks in Digital Twin Deployments in Smart Cities. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.494

[18] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in IEEE Access, vol. 9, pp. 28177-28193, 2021,