Enhancing Secure Cryptography for Sustainable IoT Applications through Artificial Intelligence and Machine Learning

Ms. Kritika Purohit , Research Scholar, Career Point University, Kota
Dr. A.K. Sharma, Research Supervisor, Career Point University, Kota

Abstract

The Internet of Things (IoT) has revolutionized modern digital infrastructure by connecting billions of devices across domains such as healthcare, smart cities, industrial automation, and transportation. However, the rapid growth of IoT networks has also introduced significant security challenges due to the limited computational power, memory, and energy resources of many connected devices. Traditional cryptographic techniques provide essential security services, but their implementation in resource-constrained environments often results in increased computational overhead and reduced efficiency. Artificial Intelligence (AI) and Machine Learning (ML) have emerged as promising technologies for enhancing IoT security by enabling intelligent threat detection, adaptive authentication, dynamic key management, and real-time security monitoring. In addition to strengthening cybersecurity, these technologies can optimize resource utilization and support sustainable IoT operations by reducing unnecessary computational and energy consumption. This paper reviews the role of AI and ML in improving cryptographic security for sustainable IoT applications. It discusses key security challenges, examines recent advancements in AI-assisted cryptographic mechanisms, and proposes the Adaptive Intelligent Cryptographic Engine (AICE), a conceptual framework that integrates lightweight cryptography with intelligent security techniques. The study highlights the potential of AI-driven cryptographic solutions to develop secure, scalable, and energy-efficient IoT ecosystems capable of addressing future cybersecurity demands.

Keywords: Internet of Things (IoT), Artificial Intelligence, Machine Learning, Cryptography, Cybersecurity, Sustainable IoT, Lightweight Security.

1. Introduction

1.1 Background and Motivation

The Internet of Things (IoT) has revolutionized the way devices communicate and exchange information, creating a highly connected digital ecosystem that spans healthcare, transportation, manufacturing, agriculture, and smart city applications. By enabling real-time data collection and intelligent decision-making, IoT technologies have significantly improved operational efficiency and automation across various sectors [1], [2]. As organizations increasingly rely on connected devices to support critical operations, the importance of securing these systems has become more evident than ever. Despite its numerous advantages, IoT introduces a wide range of security challenges. Most IoT devices are designed with limited computational resources, restricted memory, and constrained battery capacity, making the deployment of traditional security mechanisms difficult [3], [4]. Furthermore, the large number of interconnected devices and the diversity of communication protocols increase system complexity and create multiple points of vulnerability. These weaknesses can be exploited through cyberattacks such as unauthorized access, data manipulation, malware infections, botnet

attacks, and distributed denial-of-service (DDoS) attacks [5], [8]. Cryptography serves as the foundation of secure communication in IoT environments by protecting sensitive information from unauthorized access and ensuring data integrity and authenticity. Conventional cryptographic techniques, including RSA, AES, and Elliptic Curve Cryptography (ECC), have been widely adopted because of their strong security capabilities. However, these algorithms often require considerable computational power and energy resources, which may not be suitable for lightweight IoT devices operating under strict resource constraints [3], [10]. Consequently, researchers have focused on developing security solutions that can provide strong protection while maintaining efficiency and minimizing resource consumption.

In recent years, Artificial Intelligence (AI) and Machine Learning (ML) have emerged as promising technologies for addressing complex cybersecurity challenges. Unlike traditional rule-based security systems, AI-powered approaches can learn from historical data, recognize abnormal behavior patterns, and adapt to evolving threats in real time [6], [7]. Machine learning techniques have shown significant potential in areas such as intrusion detection, anomaly detection, intelligent authentication, and automated threat response [11], [12]. When integrated with cryptographic mechanisms, these technologies can enhance security by enabling adaptive key management, dynamic encryption strategies, and predictive threat analysis. Alongside security concerns, sustainability has become a key consideration in IoT development. The growing number of connected devices contributes to increased energy consumption and computational demands, making energy-efficient security solutions essential for long-term deployment. Intelligent security mechanisms supported by AI and ML can optimize cryptographic operations, reduce unnecessary processing overhead, and improve resource utilization without compromising protection levels [14], [15]. Such capabilities are particularly important for battery-powered devices that are expected to operate continuously for extended periods. Given these challenges and opportunities, the integration of Artificial Intelligence, Machine Learning, and cryptographic technologies offers a promising approach for building secure and sustainable IoT ecosystems. This paper explores the role of AI and ML in enhancing cryptographic security for IoT applications, reviews existing research developments, examines current challenges, and proposes a conceptual framework that combines lightweight cryptography with intelligent security mechanisms. The objective is to highlight how AI-assisted cryptographic solutions can strengthen cybersecurity while supporting the sustainability requirements of next-generation IoT networks.

1.2 Problem Statement

The rapid adoption of Internet of Things (IoT) technologies has brought remarkable improvements in connectivity, automation, and real-time data processing. However, this growth has also created new security challenges that continue to evolve alongside the increasing complexity of IoT networks. While cryptography remains one of the most effective methods for protecting data and ensuring secure communication, many existing cryptographic solutions were not originally designed for devices with limited processing power, memory, and battery life.

To overcome these limitations, researchers have developed lightweight cryptographic techniques that require fewer computational resources. Although these approaches improve efficiency, they often operate using fixed security parameters and predefined rules. In practice, IoT environments are highly dynamic, with devices constantly joining, leaving, and exchanging data across different networks. As cyber threats become more sophisticated, static security mechanisms may struggle to provide the level of protection required in real-world

deployments. Another challenge lies in managing cryptographic keys across large-scale IoT systems. Many current solutions depend on centralized management approaches, which can become vulnerable if a single component is compromised. In addition, IoT devices remain exposed to a variety of attacks, including malware, unauthorized access, botnet activity, firmware exploitation, and attacks that target weaknesses in cryptographic implementations. These threats can affect both the security and reliability of IoT services. At the same time, sustainability has become an important concern. Security mechanisms should not only protect devices and data but also operate efficiently without placing unnecessary demands on energy and computational resources. This is particularly important for battery-powered devices that are expected to function continuously for months or even years without maintenance.

Recent developments in Artificial Intelligence (AI) and Machine Learning (ML) offer promising opportunities to address these challenges. AI-driven systems can learn from network behavior, identify unusual activities, and adapt security responses based on changing conditions. However, most existing research focuses either on cryptographic protection or AI-based threat detection as separate areas. There is still limited research on how these technologies can be combined into a unified framework that simultaneously improves security, efficiency, and sustainability. Therefore, there is a growing need for intelligent security solutions that integrate AI and ML with lightweight cryptographic mechanisms. Such an approach could enable IoT systems to respond more effectively to emerging threats, optimize resource usage, and maintain strong security without compromising device performance. Developing such a framework is essential for supporting the secure and sustainable growth of future IoT ecosystems.

1.3 Objectives of the Study

The primary aim of this study is to explore how Artificial Intelligence (AI) and Machine Learning (ML) can enhance cryptographic security while supporting the sustainability requirements of Internet of Things (IoT) environments. To achieve this aim, the study focuses on the following objectives:

1. **To review and analyze existing research** on the application of AI and ML techniques in IoT security, with particular emphasis on their role in strengthening cryptographic mechanisms.
2. **To examine the major security, performance, and sustainability challenges** associated with current cryptographic implementations in resource-constrained IoT devices and networks.
3. **To investigate the potential of AI-driven approaches** for improving key management, threat detection, authentication, and other cryptographic functions within IoT ecosystems.
4. **To propose a conceptual framework** that integrates lightweight cryptographic techniques with AI and ML technologies to provide secure, efficient, and adaptive protection for IoT applications.
5. **To compare AI-enhanced cryptographic approaches with traditional security methods** in terms of security effectiveness, resource utilization, scalability, and energy efficiency.
6. **To identify existing research gaps and emerging challenges** that may influence the future development of intelligent and sustainable IoT security solutions.
7. **To provide recommendations for future research** aimed at developing secure, scalable, and energy-efficient cryptographic frameworks capable of addressing the evolving requirements of next-generation IoT environments.

These objectives contribute to a better understanding of how intelligent technologies can strengthen cryptographic security while ensuring the long-term sustainability and reliability of IoT systems.

1.4 Paper Organization

The remainder of this paper is organized as follows. Section 2 presents the background of the study and reviews the existing literature related to IoT security, cryptography, and the application of Artificial Intelligence and Machine Learning in cybersecurity. Section 3 discusses the major security, performance, and sustainability challenges associated with cryptographic implementations in IoT environments. Section 4 examines various AI and ML techniques that can be utilized to strengthen cryptographic security and improve threat detection capabilities. Section 5 introduces a conceptual framework that integrates lightweight cryptography with intelligent security mechanisms for resource-constrained IoT devices. Section 6 provides a comparative discussion of traditional and AI-enhanced cryptographic approaches, with particular emphasis on security effectiveness, resource utilization, and sustainability considerations. Section 7 highlights existing research gaps, challenges, and potential directions for future work. Finally, Section 8 summarizes the key findings of the study and presents the concluding remarks.

2. Background and Related Work

2.1 IoT Architecture and Security Layers

The Internet of Things (IoT) ecosystem consists of a large number of interconnected devices that work together to collect, transmit, and process data. To better understand how security challenges arise within these systems, IoT architecture is commonly divided into three layers: the perception layer, the network layer, and the application layer. Each layer plays a different role in the overall system and faces its own set of security concerns. The **perception layer** serves as the foundation of the IoT environment. It includes sensors, actuators, RFID tags, and other smart devices that interact directly with the physical world. Since many of these devices are deployed in open or remote locations, they are often exposed to physical attacks, device manipulation, and unauthorized access. In addition, their limited processing power and memory make it difficult to implement complex security mechanisms, leaving them more vulnerable to potential threats [3], [8]. The **network layer** is responsible for transferring data between devices, gateways, and cloud platforms. Because information continuously flows through this layer, it becomes a frequent target for cyberattacks. Attackers may attempt to intercept communications, alter transmitted data, or impersonate legitimate devices through techniques such as eavesdropping, replay attacks, and man-in-the-middle attacks [4], [5]. If these threats are not properly addressed, the reliability and trustworthiness of the entire IoT system can be compromised. The **application layer** provides the services and interfaces that allow users to interact with IoT

systems. This layer includes mobile applications, cloud services, monitoring platforms, and data analytics tools. Security issues at this level often involve unauthorized access, data leakage, weak authentication mechanisms, and software vulnerabilities. Since many IoT applications handle sensitive personal or organizational information, protecting data at this layer is equally important [9], [10]. These security challenges demonstrate that protecting IoT systems requires a comprehensive approach rather than relying on a single security mechanism. Cryptography plays a crucial role by safeguarding data during transmission and storage while ensuring confidentiality, integrity, and authentication. However, implementing cryptographic solutions in IoT environments is not always straightforward. Many devices operate with strict limitations on power consumption and computational resources, making traditional security mechanisms difficult to deploy efficiently.

To address these challenges, protocols such as Datagram Transport Layer Security (DTLS) and the Constrained Application Protocol (CoAP) have been adapted for IoT environments. Although these protocols provide important security features, they can still place a noticeable burden on highly constrained devices. As a result, researchers have increasingly explored intelligent and adaptive approaches that combine cryptographic techniques with Artificial Intelligence (AI) and Machine Learning (ML) to achieve stronger security while maintaining efficiency and sustainability. This growing need for adaptive security forms the foundation for the integration of AI and ML into modern IoT cryptographic frameworks.

2.2 Classical Cryptography in IoT: Limitations

Cryptography is a fundamental component of IoT security, protecting data from unauthorized access and ensuring secure communication between connected devices. Traditional cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) have been widely used because of their proven security and reliability. However, applying these algorithms directly to IoT environments is often challenging due to the limited resources available on many IoT devices. Unlike conventional computers and servers, IoT devices typically operate with restricted processing power, limited memory, and constrained energy resources. As a result, executing computationally intensive cryptographic operations can significantly affect device performance and battery life. Even symmetric encryption techniques such as AES, which are generally considered efficient, may introduce noticeable processing overhead when implemented on highly constrained devices. Similarly, public-key cryptographic mechanisms such as RSA and ECC require additional computational effort for key generation, encryption, decryption, and digital signature operations, making them less suitable for low-power IoT environments.

To overcome these challenges, manufacturers often incorporate dedicated cryptographic hardware into devices. While hardware-based security can improve performance and reduce processing delays, it also increases device complexity, production costs, and energy consumption. For large-scale IoT

deployments involving thousands or even millions of devices, these additional costs can become a significant concern. These limitations highlight the need for security solutions that can provide strong protection while minimizing resource consumption. Consequently, researchers have focused on developing lightweight cryptographic techniques that are better suited to the unique requirements of IoT systems.

2.3 Lightweight Cryptography Standards

The growing demand for secure and resource-efficient IoT systems has led to significant research efforts in the field of lightweight cryptography. Unlike traditional cryptographic algorithms, lightweight cryptographic techniques are specifically designed to operate effectively on devices with limited computational capabilities, memory, and power resources. Recent developments in lightweight cryptography have produced several algorithms capable of providing strong security while reducing processing and energy requirements. Among these, ASCON has gained considerable attention because of its efficient design and suitability for constrained environments. Other lightweight cryptographic schemes, including GIFT-COFB, ELEPHANT, and TinyJAMBU, have also demonstrated promising results in terms of balancing security, performance, and resource efficiency. Although lightweight cryptographic algorithms reduce computational overhead, they do not completely eliminate the challenges associated with securing dynamic IoT environments. Different devices and applications often have varying security requirements, network conditions, and resource limitations. As a result, selecting the most appropriate cryptographic configuration for a given situation remains a complex task. This is where Artificial Intelligence (AI) and Machine Learning (ML) can provide additional value. AI-driven systems can analyze device behavior, network conditions, and potential threats in real time, enabling more intelligent security decisions. Machine learning techniques can assist in optimizing cryptographic parameters, detecting abnormal cryptographic activities, and adapting security mechanisms according to changing operational requirements. By combining lightweight cryptography with intelligent decision-making capabilities, IoT systems can achieve stronger security while maintaining efficiency and sustainability. This integration of AI, ML, and lightweight cryptography represents an important step toward developing secure, adaptive, and energy-efficient IoT ecosystems capable of addressing the challenges of future connected environments.

2.4 AI and ML in Security: Prior Contributions

Over the past decade, Artificial Intelligence (AI) and Machine Learning (ML) have become increasingly important tools in the field of cybersecurity. As cyber threats continue to evolve in complexity and scale, traditional security approaches that rely on fixed rules and signatures often struggle to keep pace. This has encouraged researchers to explore intelligent systems that can learn from data, identify unusual behavior, and respond to threats more effectively. Machine learning techniques have already demonstrated considerable success in areas such as intrusion detection,

malware identification, and anomaly detection. Instead of relying solely on predefined attack signatures, these systems can recognize patterns in network traffic and detect suspicious activities that may indicate an ongoing attack. This capability is particularly valuable in IoT environments, where thousands of devices generate large volumes of data and security events every second.

Recent advances in deep learning have further improved the ability of security systems to detect sophisticated attacks. Models such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have shown promising results in analyzing network behavior and identifying previously unseen threats. Their ability to learn complex relationships within data makes them especially useful for detecting attacks that may bypass conventional security mechanisms. The influence of AI and ML is also becoming visible in cryptographic research. Rather than being used solely for attack detection, intelligent algorithms are now being explored for improving authentication methods, strengthening key management processes, and identifying weaknesses in cryptographic implementations. Researchers have also investigated how machine learning can help detect side-channel attacks and support more adaptive security strategies. Another area that has attracted significant attention is federated learning. Unlike traditional machine learning approaches that require data to be collected in a central location, federated learning allows devices to collaborate in training a model while keeping their data locally stored. This approach aligns well with the privacy and security requirements of IoT systems, where sensitive information is often distributed across numerous devices and locations. Overall, existing research suggests that AI and ML can offer much more than automated threat detection. Their ability to learn from experience, adapt to changing conditions, and support intelligent decision-making makes them promising technologies for enhancing the security and resilience of future IoT ecosystems.

2.5 Sustainability in IoT Security

As IoT technologies continue to expand across homes, industries, healthcare systems, and smart cities, discussions around security are increasingly accompanied by concerns about sustainability. The growing number of connected devices means that even small increases in energy consumption can have a significant impact when multiplied across millions or billions of devices. For many IoT devices, energy is one of the most valuable resources. Sensors and embedded systems are often expected to operate for long periods without battery replacement or maintenance. In such environments, security mechanisms must be carefully designed to provide adequate protection without placing excessive demands on device resources. Cryptographic operations play an essential role in securing IoT communications, but they can also consume a considerable portion of a device's computational and energy resources. Complex encryption processes, authentication procedures, and key management operations may affect battery life and overall system performance, particularly in highly constrained devices. This challenge has led to growing interest in the concept of sustainable or green IoT. The goal is not only to create secure systems but also to ensure that those systems use resources efficiently and

responsibly. Researchers have explored various approaches, including energy-aware communication protocols, efficient hardware designs, and intelligent resource management techniques. Artificial Intelligence and Machine Learning offer additional opportunities to support these efforts. By continuously analyzing system behavior and operating conditions, AI-driven security mechanisms can make smarter decisions about when and how security operations should be performed. Instead of applying the same level of protection at all times, intelligent systems can adapt security measures according to the current risk level, helping to reduce unnecessary processing and energy consumption. In this way, AI and ML contribute not only to stronger cybersecurity but also to the long-term sustainability of IoT ecosystems. As the number of connected devices continues to grow, developing security solutions that are both effective and energy-efficient will become increasingly important for ensuring the reliability and scalability of future IoT applications.

3. Key Challenges in IoT Cryptography

3.1 Resource Constraints

One of the biggest obstacles to implementing strong security in IoT environments is the limited capability of many connected devices. Unlike laptops, servers, or smartphones, IoT devices are often designed to be small, low-cost, and energy efficient. Sensors used in agriculture, healthcare monitoring devices, smart home appliances, and industrial equipment frequently operate with minimal memory, modest processing power, and limited battery life. These limitations create a difficult balance between security and performance. While encryption and authentication are essential for protecting sensitive information, they also require computational resources. Running complex cryptographic operations repeatedly can consume valuable energy and processing capacity, which may affect device responsiveness or shorten battery life. In practical deployments, organizations often face the challenge of determining how much security a device can support without compromising its primary functionality. As IoT continues to expand into increasingly resource-constrained environments, security solutions must become smarter and more adaptive. Rather than applying the same level of cryptographic protection to every device and situation, future systems will need to adjust security measures according to available resources, operational requirements, and perceived risk levels.

3.2 Scalability and Key Management

Security becomes significantly more complex as the number of connected devices increases. A small IoT deployment may consist of only a few devices, but modern smart cities, industrial systems, and healthcare networks can involve thousands or even millions of interconnected endpoints. Managing cryptographic keys across such large environments is a major challenge. Every secure communication session depends on the proper generation, distribution, storage, and renewal of cryptographic keys. As the network grows, performing these tasks manually becomes unrealistic. At the same time, relying entirely on centralized key management systems may create security risks, as a single point of failure

can affect a large portion of the network. This challenge highlights the importance of automation. Intelligent systems capable of monitoring device behavior and automatically managing key lifecycles could significantly improve both security and efficiency. By reducing human intervention and responding dynamically to changing conditions, AI-driven approaches offer a practical path toward managing security on a scale.

3.3 Evolving Security Threat

Cybersecurity is not a static field, and neither are the threats faced by IoT systems. Attackers continuously develop new techniques to bypass existing defenses, exploit vulnerabilities, and gain unauthorized access to devices and networks. Security mechanisms that are effective today may become insufficient as new attack methods emerge. This issue is particularly challenging in IoT environments because many devices remain deployed for years and may not receive regular security updates. Updating cryptographic settings or deploying new security policies across large and diverse device populations can be difficult, costly, and sometimes impractical. As a result, there is a growing need for security solutions that can adapt to changing circumstances. Machine learning technologies offer a promising approach by enabling systems to learn from previous incidents, recognize suspicious behavior, and respond to emerging threats without relying solely on predefined rules. Such adaptability is becoming increasingly important as IoT ecosystems continue to grow in size and complexity.

3.4 Vulnerability to Side-Channel Attack

Not all attacks target weaknesses in cryptographic algorithms themselves. In many cases, attackers attempt to gather information from the way cryptographic operations are performed. By observing characteristics such as power consumption, processing time, or electromagnetic emissions, it may be possible to infer sensitive information without directly breaking the encryption algorithm. For resource-constrained IoT devices, defending against these attacks can be particularly difficult. Protective mechanisms often require additional processing and energy, which may not be feasible for devices already operating under strict resource limitations. Recent research suggests that AI and ML can contribute to more effective defenses by identifying unusual patterns associated with side-channel attack attempts. Instead of relying exclusively on predefined protection mechanisms, intelligent systems can continuously monitor device behavior and detect potential threats as they occur, providing an additional layer of security.

3.5 Interoperability and Protocol Diversity

Another challenge arises from the highly diverse nature of IoT ecosystems. Devices from different manufacturers often use different communication technologies, security standards, and networking protocols. A single IoT deployment may involve Wi-Fi, Bluetooth Low Energy, Zigbee, LoRaWAN, MQTT, CoAP, and several other technologies operating simultaneously. While this diversity enables

flexibility and broad connectivity, it also complicates security management. Ensuring that devices communicate securely across different protocols is not always straightforward, and inconsistencies in security implementations can create opportunities for attackers. Maintaining a consistent level of protection across such heterogeneous environments remains an ongoing challenge. AI-driven monitoring systems can help by providing a broader view of network activity, identifying security gaps, and supporting more coordinated security management across different technologies and platforms. In summary, the challenges associated with IoT cryptography extend far beyond the selection of encryption algorithms. Issues related to resource limitations, large-scale key management, evolving threats, side-channel vulnerabilities, and protocol diversity continue to shape the future of IoT security. Addressing these challenges will require security solutions that are not only strong and reliable but also intelligent, adaptive, and capable of operating efficiently in resource-constrained environments.

4. AI and ML Techniques for IoT Cryptography

4.1 Machine Learning-Based Key Generation

The effectiveness of any cryptographic system largely depends on the quality of the keys used for encryption and authentication. In many IoT devices, generating truly random cryptographic keys can be challenging because of limited hardware capabilities and restricted entropy sources. Weak or predictable randomness may reduce the overall strength of the security system and create opportunities for attackers. Recent research has explored the use of Machine Learning (ML) techniques to improve key generation processes. Instead of relying solely on traditional random number generators, intelligent systems can utilize information collected from device-specific environmental conditions, such as sensor readings, signal variations, and operational behavior, to enhance entropy generation. This approach can help create cryptographic keys that are more unique and difficult to predict. Researchers have also investigated advanced techniques such as Generative Adversarial Networks (GANs) and Physical Unclonable Functions (PUFs) for strengthening device identity and authentication. PUFs are particularly attractive in IoT environments because they leverage natural manufacturing variations to generate unique device characteristics, making device cloning significantly more difficult.

.4.1.1 Integration of PUF and ML

Physical Unclonable Functions have gained considerable attention as a lightweight authentication mechanism for resource-constrained devices. Since every device possesses unique physical characteristics, PUFs can be used to generate device-specific responses for authentication purposes. However, studies have shown that certain PUF designs may become vulnerable when attackers collect a large number of challenge-response pairs and use machine learning techniques to model their behavior. To address this issue, researchers have proposed more complex PUF architectures and

intelligent monitoring mechanisms capable of detecting suspicious authentication patterns. By combining PUF technology with AI-based analysis, it is possible to improve both authentication reliability and resistance to modeling attacks.

4.2 Anomaly Detection and Intrusion Detection Systems

One of the most successful applications of AI and ML in cybersecurity is anomaly and intrusion detection. Traditional security systems often depend on predefined attack signatures, which can limit their ability to identify new or previously unseen threats. Machine learning techniques offer a more flexible approach by learning normal system behavior and identifying deviations that may indicate malicious activity. In IoT environments, anomaly detection systems can continuously monitor network traffic, device communications, and operational patterns to identify unusual behavior. Such anomalies may indicate attempts to manipulate cryptographic protocols, intercept communications, or gain unauthorized access to connected devices. Deep learning models, including Long Short-Term Memory (LSTM) networks, have demonstrated promising results because they can analyze temporal patterns and recognize subtle behavioral changes over time. These capabilities make them particularly useful for detecting sophisticated attacks that may otherwise remain unnoticed.

4.2.1 Federated Intrusion Detection

Privacy remains an important concern when deploying machine learning solutions in IoT networks. Traditional centralized approaches require large amounts of data to be collected and processed at a central location, which may introduce privacy and security risks. Federated learning offers an alternative approach by allowing devices to train machine learning models locally while sharing only model updates rather than raw data. This enables collaborative learning without exposing sensitive information. For sectors such as healthcare, industrial automation, and smart cities, federate learning provides an effective balance between security intelligence and data privacy.

4.3 Adaptive Cryptographic Protocol Selection

IoT devices often operate under changing conditions. Network quality, battery status, computational resources, and security requirements may vary significantly over time. Applying the same cryptographic configuration in every situation may therefore lead to inefficiencies or unnecessary resource consumption.

Artificial Intelligence can help address this challenge by supporting adaptive security decisions. Machine learning and reinforcement learning techniques can evaluate current operating conditions and recommend cryptographic settings that best balance security and performance requirements. For example, a device operating under normal conditions may use lightweight security mechanisms, while stronger protection can be activated when suspicious activity is detected. Such adaptive approaches allow security mechanisms to respond more effectively to changing environments while reducing unnecessary computational overhead.

4.4 Side-Channel Attack Detection and Mitigation

Side-channel attacks exploit information leaked during cryptographic operations, such as power consumption, timing behavior, or electromagnetic emissions. These attacks are particularly concerning for IoT devices because resource limitations often restrict the implementation of advanced defensive mechanisms. Machine learning techniques have shown potential in identifying side-channel attack attempts by analyzing operational patterns and detecting abnormal behavior. By continuously monitoring device activity, intelligent systems can recognize suspicious measurements or probing attempts that may indicate an ongoing attack. In addition, AI-driven optimization techniques can assist in designing more efficient countermeasures that balance security protection with resource consumption. This helps improve resilience against side-channel attacks without introducing excessive computational overhead.

4.5 AI-Driven Key Lifecycle Management

Managing cryptographic keys throughout their lifecycle is a critical aspect of IoT security. Tasks such as key generation, distribution, renewal, and revocation become increasingly difficult as the number of connected devices grows. Artificial Intelligence can support more efficient key management by analyzing device behavior and network conditions to determine when security actions should be performed. Intelligent systems can identify unusual patterns that may indicate compromised credentials and trigger appropriate security responses automatically. Such capabilities reduce administrative complexity while improving the ability of IoT systems to respond quickly to potential security incidents.

4.6 Lightweight Neural Cryptography

Another emerging area of research involves the application of neural networks within cryptographic systems. Researchers have explored whether neural models can support certain cryptographic functions such as key generation, randomness enhancement, and secure communication mechanisms. Although neural cryptography remains at an experimental stage and does not yet provide the same mathematical guarantees as conventional cryptographic algorithms, it offers an interesting direction for future research. Rather than replacing established cryptographic standards, current studies suggest that neural techniques may be more effective when used alongside traditional security mechanisms. Hybrid approaches that combine conventional cryptography with AI-assisted security functions appear particularly promising for IoT environments, as they can provide stronger adaptability while preserving the reliability and trust associated with established cryptographic methods. Overall, the integration of Artificial Intelligence and Machine Learning into cryptographic systems offers new opportunities for improving IoT security. From intelligent key management and adaptive encryption to anomaly detection and side-channel attack mitigation, these technologies have the potential to make future IoT ecosystems more secure, efficient, and sustainable.

5. Proposed Integrated AI-ML Cryptographic Framework

5.1 Framework Architecture

To address the security, scalability, and sustainability challenges identified in previous sections, this paper proposes an integrated framework called the Adaptive Intelligent Cryptographic Engine (AICE). The framework combines Artificial Intelligence (AI), Machine Learning (ML), and lightweight cryptographic techniques to provide a more adaptive and efficient security solution for IoT environments. The proposed framework consists of four interconnected layers that work together to enhance security while minimizing resource consumption. These layers include the Entropy Harvesting Layer, the Adaptive Protocol Layer, the Distributed Detection Layer, and the Lifecycle Management Layer. Rather than relying on fixed security policies, the framework continuously evaluates device conditions and network behavior to support intelligent security decisions. A key feature of the proposed architecture is its flexibility. Since IoT devices vary significantly in terms of processing power, memory, and energy availability, not all devices require the same level of security functionality. Therefore, the framework allows individual components to be deployed according to device capabilities. Resource-constrained devices can utilize only the essential security functions, while more capable edge devices and gateways can support advanced AI-driven operations.

5.2 Entropy Harvesting Layer

The first layer focuses on improving the quality of cryptographic randomness used in security operations. Strong cryptographic keys depend on high-quality random values, yet many IoT devices have limited sources of entropy due to their constrained hardware environments. To overcome this limitation, the proposed framework utilizes machine learning techniques to analyze information collected from available sensors and environmental conditions. Device-specific characteristics such as sensor readings, operational behavior, and environmental variations can serve as additional sources of randomness. By intelligently processing this information, the system can generate stronger and more unpredictable inputs for cryptographic key generation. This approach enhances the reliability of cryptographic operations while maintaining compatibility with lightweight IoT devices.

5.3 Adaptive Protocol Layer

IoT devices often operate under changing conditions, including variations in battery level, network quality, workload, and security requirements. Applying the same cryptographic configuration at all times may either waste resources or provide insufficient protection. The Adaptive Protocol Layer addresses this challenge by introducing intelligent decision-making into the security process. Using machine learning and reinforcement learning techniques, the framework continuously evaluates the current operating environment and selects the most appropriate cryptographic configuration for a given situation. For example, under normal operating conditions, lightweight security mechanisms may be

sufficient. However, if suspicious activity is detected or the perceived threat level increases, stronger cryptographic protection can be activated automatically. This adaptive behavior allows the system to maintain an effective balance between security, performance, and energy efficiency.

5.4 Distributed Detection Layer

The Distributed Detection Layer is responsible for identifying abnormal activities and potential security threats within the IoT network. Traditional security solutions often rely on centralized monitoring systems, which may introduce scalability and privacy concerns. In contrast, the proposed framework adopts a distributed approach that enables devices to participate in the security monitoring process. Machine learning models deployed on individual devices continuously observe communication patterns, authentication activities, and operational behavior. When unusual patterns are detected, the system generates alerts that can be analyzed at higher network layers. To further improve detection capabilities, the framework incorporates federated learning. This approach allows devices to collaboratively improve detection models without sharing sensitive raw data. As a result, the system benefits from collective learning while preserving privacy and reducing communication overhead.

5.5 Lifecycle Management Layer

Managing cryptographic keys throughout their lifecycle remains one of the most challenging aspects of large-scale IoT security. As the number of connected devices increases, tasks such as key generation, distribution, renewal, and revocation become increasingly complex. The Lifecycle Management Layer introduces AI-assisted decision-making to automate these processes. By analyzing device behavior, communication patterns, and security indicators, the system can determine when keys should be updated or when additional security measures may be required. Intelligent key management helps reduce administrative effort while improving responsiveness to potential security incidents. Instead of relying solely on predefined schedules, the framework adapts security actions according to real-time conditions, ensuring that protection mechanisms remain both effective and efficient. Overall, the proposed AICE framework demonstrates how AI and ML can be integrated with lightweight cryptographic mechanisms to create a security architecture that is adaptive, scalable, and sustainable. By combining intelligent decision-making with resource-aware security controls, the framework provides a practical foundation for securing future IoT ecosystems while addressing the limitations of conventional cryptographic approaches.

6. Comparative Analysis and Sustainability Assessment

6.1 Comparative analysis of Security Approaches

To understand the potential benefits of integrating Artificial Intelligence (AI) and Machine Learning (ML) with cryptographic mechanisms, it is useful to compare traditional IoT security approaches with lightweight cryptographic solutions and the proposed Adaptive Intelligent Cryptographic Engine (AICE) framework. Traditional cryptographic approaches provide strong security but often struggle in resource-constrained IoT environments due to their computational and energy requirements. Lightweight cryptographic algorithms improve efficiency and are better suited for constrained devices; however, they generally operate using fixed configurations and have limited ability to respond to changing threat conditions. In contrast, the proposed AICE framework introduces adaptability into the security process. By incorporating AI and ML techniques, the framework can support intelligent decision-making, dynamic threat detection, adaptive security policies, and automated key management. This enables the system to respond more effectively to evolving security challenges while maintaining efficient resource utilization. From a security perspective, AI-assisted cryptographic frameworks offer advantages in anomaly detection, behavioral monitoring, and proactive threat response. They also provide greater flexibility by allowing security mechanisms to adjust according to device conditions, network status, and perceived threat levels. These capabilities are difficult to achieve using conventional static security architectures.

6.2 Computational Overhead Considerations

Although AI-enhanced security mechanisms provide additional functionality, they also introduce some computational overhead. Machine learning models require processing resources for activities such as anomaly detection, behavioral analysis, and decision-making. Consequently, the integration of AI within IoT security frameworks must be carefully designed to avoid excessive resource consumption. Recent research suggests that lightweight machine learning models can be deployed effectively on modern IoT and edge devices without significantly affecting system performance. Functions such as adaptive protocol selection, intelligent key management, and anomaly detection can often be performed using compact models optimized for constrained environments. In the proposed AICE framework, computational overhead is minimized through a layered architecture in which more demanding analytical tasks can be delegated to edge gateways or intermediate processing nodes. This approach allows highly constrained devices to benefit from intelligent security services without bearing the full computational burden. Therefore, while AI integration introduces additional processing requirements, the resulting improvements in security awareness, automation, and adaptability may justify the modest increase in resource utilization.

6.3 Sustainability and Energy Efficiency

Sustainability has become an important consideration in the design of modern IoT systems. With billions of devices expected to operate continuously across various applications, even small improvements in energy efficiency can have a significant cumulative impact. Conventional cryptographic systems often apply the same security configuration regardless of operating conditions. While this approach simplifies implementation, it may result in unnecessary energy consumption, particularly during periods of low risk or limited activity. In contrast, AI-driven security frameworks can make more informed decisions regarding when and how cryptographic operations should be performed. The proposed AICE framework supports sustainability by enabling adaptive security management. Machine learning algorithms can evaluate device conditions, communication requirements, and threat levels to determine the most appropriate security configuration at any given time. By avoiding unnecessary cryptographic operations and optimizing resource utilization, the framework has the potential to reduce energy consumption and extend device lifetime. Furthermore, the integration of intelligent security mechanisms with energy-aware IoT strategies such as edge computing, duty cycling, and energy harvesting can further improve overall system efficiency. These capabilities are particularly valuable for battery-powered devices deployed in remote or difficult-to-access locations. Consequently, AI-assisted cryptographic frameworks not only contribute to stronger cybersecurity but also support the broader goal of developing sustainable and environmentally responsible IoT ecosystems.

6.4 Privacy and Regulatory Considerations

As IoT networks continue to collect and process large volumes of data, privacy protection remains a critical concern. Security frameworks must ensure that sensitive information is protected while maintaining compliance with applicable data protection regulations. The proposed framework addresses this challenge through the use of distributed and privacy-preserving learning techniques. Federated learning allows devices to participate in collaborative model training without transmitting raw data to a central location. This approach reduces privacy risks while enabling continuous improvement of security models. In addition, intelligent security mechanisms should be designed according to principles of transparency, accountability, and data minimization. Such considerations are increasingly important as governments and regulatory bodies introduce stricter requirements for cybersecurity, privacy protection, and trustworthy AI systems. By combining strong cryptographic protection with privacy-aware AI techniques, the proposed framework supports both security and regulatory compliance, making it suitable for a wide range of IoT applications, including healthcare, industrial automation, and smart city environments. Overall, the comparative analysis suggests that integrating AI and ML with lightweight cryptography can provide significant advantages in terms of adaptability, automation, security awareness, and sustainability. While challenges related to implementation complexity and resource management remain, the proposed framework offers a promising direction for the development of future secure and sustainable IoT ecosystems.

7. Open Research Challenges and Future Directions

Although the integration of Artificial Intelligence (AI), Machine Learning (ML), and cryptographic techniques has shown significant potential for improving IoT security, several challenges remain unresolved. As IoT ecosystems continue to expand in scale and complexity, addressing these issues will be essential for developing security solutions that are not only effective but also reliable, sustainable, and trustworthy.

7.1 Security of AI-based Defense Mechanisms

While AI and ML can strengthen cybersecurity, they also introduce new vulnerabilities that traditional cryptographic systems do not face. Machine learning models can become targets of attack. For example, attackers may manipulate input data in a way that causes a model to make incorrect decisions, allowing malicious activities to bypass security controls. In IoT environments, where automated decision-making is increasingly used for threat detection and response, such vulnerabilities can have serious consequences. A compromised or misled security model may fail to detect attacks or generate inaccurate security recommendations. Therefore, improving the robustness of AI-driven security mechanisms remains an important area of research. Future studies should focus on developing more resilient learning models, secure training methodologies, and mechanisms for validating the reliability of AI-based security decisions.

7.2 Preparing for the post-Quantum Era

The rapid advancement of quantum computing has raised concerns about the long-term security of many existing cryptographic algorithms. Techniques that are currently considered secure may become vulnerable once large-scale quantum computers become practical. This challenge is particularly significant for IoT environments because many connected devices are expected to remain operational for years after deployment. Replacing or upgrading cryptographic systems on a large number of devices can be difficult and costly. As a result, researchers are actively exploring post-quantum cryptography as a future replacement for traditional public-key algorithms. However, many post-quantum algorithms require greater computational power, memory, and energy resources than current cryptographic solutions. Finding ways to deploy these algorithms efficiently on resource-constrained IoT devices remains a major research challenge. AI-assisted optimization techniques may provide valuable support in identifying suitable cryptographic configurations and managing the transition toward quantum-resistant security architectures.

7.3 Explainability and Transparency of AI Decisions

As AI becomes more involved in security management, understanding how decisions are made becomes increasingly important. Security administrators, system developers, and regulatory authorities often need clear explanations for why a particular threat was identified, why a cryptographic policy was modified, or why a device was classified as suspicious. Many advanced machine learning models, particularly deep learning architectures, operate as "black boxes," making their decision-making processes difficult to interpret. This lack of transparency can reduce trust in AI-driven security systems and complicate incident investigations. Future research should focus on developing explainable AI techniques that provide meaningful insights into security-related decisions. Improving transparency will not only increase trust in intelligent security systems but also support compliance with emerging regulatory requirements related to responsible and accountable AI deployment.

7.4 Secure and Trustworthy Federated Learning

Federated learning has emerged as a promising approach for privacy-preserving security analytics in IoT environments. By allowing devices to train models collaboratively without sharing raw data, federated learning helps protect sensitive information while enabling collective intelligence. Despite these advantages, several challenges remain. Since learning occurs across multiple devices, there is always the possibility that some participants may be compromised. Malicious devices could intentionally provide misleading information during the training process, affecting the accuracy and reliability of the global model. Developing federated learning frameworks that can tolerate malicious participants while maintaining efficiency remains an active area of research. Future solutions must balance security, privacy, computational cost, and communication overhead to ensure practical deployment in large-scale IoT systems.

7.5 Standardization and Interoperability

The successful adoption of AI-enhanced cryptographic frameworks will depend heavily on the availability of widely accepted standards and interoperability guidelines. Currently, IoT ecosystems consist of diverse devices, communication protocols, and security mechanisms developed by different manufacturers and organizations. The absence of standardized approaches for integrating AI, ML, and cryptographic technologies may lead to fragmented implementations that are difficult to manage, evaluate, and secure. Establishing common frameworks, evaluation methodologies, and interoperability standards will therefore be essential for large-scale adoption. Collaboration among researchers, industry stakeholders, and standardization bodies will play a crucial role in addressing these challenges. Future efforts should focus on developing practical guidelines that ensure AI-assisted security solutions remain compatible, reliable, and trustworthy across diverse IoT environments.

8. Conclusion

The rapid growth of the Internet of Things (IoT) has created unprecedented opportunities for connectivity, automation, and intelligent decision-making across diverse application domains. However, this growth has also introduced significant security challenges, particularly in resource-constrained environments where traditional cryptographic solutions may not always be practical. Ensuring strong security while maintaining energy efficiency and system sustainability has therefore become a critical concern for researchers and practitioners. This paper examined the role of Artificial Intelligence (AI) and Machine Learning (ML) in enhancing cryptographic security for sustainable IoT applications. Through an extensive review of existing literature, the study highlighted the limitations of conventional cryptographic approaches and discussed how intelligent techniques can contribute to key generation, anomaly detection, intrusion prevention, adaptive security management, and secure key lifecycle management. The analysis indicates that AI and ML have the potential to make IoT security systems more adaptive, responsive, and capable of addressing evolving cyber threats.

To address the identified challenges, this paper proposed the Adaptive Intelligent Cryptographic Engine (AICE), a conceptual framework that integrates lightweight cryptography with AI-driven decision-making. The framework combines entropy enhancement, adaptive protocol selection, distributed threat detection, and intelligent key management within a unified architecture. By introducing adaptability into the cryptographic process, the framework aims to balance security requirements with the computational and energy limitations of IoT devices. In addition to improving cybersecurity, the study emphasized the importance of sustainability in future IoT deployments. Intelligent security mechanisms can support more efficient resource utilization by reducing unnecessary cryptographic operations and enabling context-aware security decisions. Such capabilities are particularly important as billions of IoT devices continue to be deployed across smart cities, healthcare systems, industrial environments, and critical infrastructure. Despite the promising potential of AI-assisted cryptographic systems, several challenges remain unresolved. Issues related to adversarial attacks on machine learning models, post-quantum cryptographic readiness, explainability of AI decisions, secure federated learning, and the lack of standardized implementation frameworks require further investigation. Addressing these challenges will be essential for ensuring reliability, trustworthiness, and large-scale adoption of intelligent security solutions. In conclusion, the convergence of AI, ML, and lightweight cryptography represents a promising direction for the future of IoT security. Rather than replacing traditional cryptographic mechanisms, intelligent technologies can complement and enhance existing security architectures by enabling greater adaptability, automation, and efficiency. As IoT ecosystems continue to evolve, the integration of intelligent and sustainable security frameworks will play a vital role in protecting connected devices, safeguarding sensitive data, and supporting the long-term growth of secure digital infrastructures.

References

1. Abadi, M., & Andersen, D. G. (2016). Learning to protect communications with adversarial neural cryptography. arXiv preprint arXiv:1610.06918.
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cybersecurity intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.
3. Doröz, Y., & Sunar, B. (2022). Accelerating fully homomorphic encryption in hardware. IEEE Transactions on Computers, 71(1), 213–227.
4. Ericsson Mobility Report. (2024). Connected devices outlook 2024–2030. Ericsson AB.
5. Gohr, A. (2019). Improving attacks on round-reduced Speck32/64 using deep learning. Advances in Cryptology – CRYPTO 2019, Lecture Notes in Computer Science, Vol. 11693, Springer.
6. Hameed, K., Khan, A., Ahmed, M., Lv, Z., & Amara Dinesh Kumar, S. (2023). AI-driven lightweight cryptography for IoT environments: A comprehensive survey. Internet of Things, 21, 100663.
7. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3, 678–708.
8. Maghrebi, H., Portigliatti, T., & Prouff, E. (2023). Breaking cryptographic implementations using deep learning techniques. Security, Privacy, and Applied Cryptography Engineering, Lecture Notes in Computer Science, Springer.
9. McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Agüera y Arcas, B. (2017). Communication-efficient learning of deep networks from decentralized data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS).
10. National Institute of Standards and Technology (NIST). (2023). NIST Lightweight Cryptography Standardization: ASCON. NIST Special Publication.
11. Raza, S., Trabalza, D., & Voigt, T. (2022). 6LoWPAN compressed DTLS for CoAP. IEEE 8th International Conference on Distributed Computing in Sensor Systems, 287–289.
12. Shafique, K., Khawaja, B. A., Sabir, F., Qazi, S., & Mustaqim, M. (2020). Internet of Things (IoT) for next-generation smart systems: A review of current challenges, future trends, and prospects for emerging 5G-IoT scenarios. IEEE Access, 8, 23022–23040.
13. Yao, Y., Chang, X., Mišić, J., Mišić, V. B., & Li, L. (2019). BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 6(2), 3775–3784.
14. Zeng, K., & Zhou, J. (2023). Federated learning for intrusion detection in IoT environments: Challenges and opportunities. IEEE Transactions on Information Forensics and Security, 18, 3520–3535.