Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-B, pp. 879–888
DOI : 10.47974/JDMSC-1963

Enhancing IoT security using lightweight key management with PRESENT for resource-constrained devices

Hemlata Sandip Ohal *
Mrunal Pravinkumar Fatangare †
Mrunal Swapnil Aware §
Pallavi Utkarsh Nehete ‡
Nita Ganesh Dongre (Jaybhaye) @
Department of Computer Science and Engineering
DVK MIT World Peace University
Pune
Maharashtra
India

Priyanka M. Kothoke #
Department of Electrical Engineering
MGM's College of Engineering and Technology, Kamothe
Navi Mumbai
Maharashtra
India

Abstract

The increasing number of Internet of Things (IoT) devices in different areas has led to worries about their susceptibility to security risks because of their limited resources. This study aims to improve IoT security by utilizing a streamlined key management system based on the PRESENT block cipher algorithm. The proposed method is compared to TinyIKE and Elliptic Curve Diffie-Hellman (ECDH) using key parameters like Encryption Time, Decryption Time, Storage Usage, Energy Consumption, and Key Entropy. The

This research was conducted during the NREUP at Michigan State University and it was sponsored by NSF grants DMS-1156582 and DMS-1359016.

* *E-mail:* **hemlata.ohal@mitwpu.edu.in (Corresponding Author)**
† *E-mail:* **mrunal.fatangare@mitwpu.edu.in**
§ *E-mail:* **mrunal.aware@mitwpu.edu.in**
‡ *E-mail:* **pallavi.nehete@mitwpu.edu.in**
@ *E-mail:* **nita.dongre@mitwpu.edu.in**
# *E-mail:* **priyankakothoke@gmail.com**

paper's introduction contextualizes the importance of securing IoT devices, highlighting the difficulties caused by their restricted computational capabilities. The research proposes using the PRESENT algorithm for key management systems because of its lightweight characteristics and compatibility with resource-limited environments. The proposed method will be thoroughly analyzed across different parameters to evaluate its performance in comparison to current solutions. The research shows that the suggested lightweight key management scheme using PRESENT is more effective than TinyIKE and ECDH in Encryption Time, Decryption Time, Storage Usage, Energy Consumption, and Key Entropy. The results demonstrate the effectiveness of the suggested approach in meeting the particular security needs of IoT devices with limited resources. This research enhances IoT security by proposing a lightweight key management method that efficiently tackles the issues caused by resource-limited devices. The comparative analysis demonstrates that the proposed method outperforms others, indicating its potential as an effective solution for securing IoT ecosystems in practical scenarios.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *IoT security, Lightweight key management, PRESENT algorithm, Resource-constrained devices, ECDH.*

1. Introduction

The Internet of Things (IoT) has become a widespread and influential phenomenon worldwide, impacting multiple facets of everyday life and business. The growing interconnection of devices offers significant advantages, including increased efficiency and enhanced decision-making processes. The widespread implementation of IoT also presents significant security challenges. The large number of interconnected devices, each with different functions, results in a complicated security environment that is vulnerable to multiple threats. Ensuring the security of IoT systems is crucial to protect sensitive data, uphold privacy, and prevent malicious activities[1], [2].

Current IoT security solutions aim to tackle these challenges, but the limitations in resources found in numerous IoT devices create distinct obstacles. Devices with limited computational power, storage capacity, and energy resources require specific security measures to address potential vulnerabilities. Effective key management is essential for maintaining the confidentiality and integrity of data shared among IoT devices. As such, an overview of existing IoT security solutions and a comprehensive review of key management techniques are essential components in understanding the current state of IoT security[3].

Lightweight key management is crucial for resource-constrained IoT devices. Conventional methods of key management may be overly demanding for devices with restricted capabilities, resulting in decreased performance and higher energy usage. Our research addresses this issue by suggesting a Lightweight Key Management system combined with the PRESENT Algorithm. This algorithm is designed to offer a secure and lightweight solution specifically for IoT devices, known for its efficiency and compatibility with resource-limited environments. This paper examines the worldwide influence of IoT, discusses the difficulties in securing devices with limited resources, evaluates current security solutions and key management methods, and emphasizes the importance of lightweight key management using the PRESENT Algorithm to enhance IoT security[4], [5].

2. Literature review

The Internet of Things (IoT) presents unique security challenges due to the resource-constrained nature of its devices. Ensuring secure communication and data protection in this environment requires specialized approaches that balance robust security with efficient resource utilization. This literature review explores recent research advancements in lightweight cryptographic solutions specifically designed for IoT applications.

Several studies propose novel three-factor authentication schemes (3-FAS) for enhanced security. LAPTAS[6] introduces an anonymous 3-FAS focusing on privacy preservation in wireless sensor networks (WSNs) used in Industrial IoT (IIoT). Similarly, Luo et al. A lightweight 3-FAS specifically optimized for real-time data access in WSN[7]. These approaches address the need for secure authentication while acknowledging the resource limitations of sensor nodes.

Other studies focus on securing data transmission itself. Jebri et al.[8] present an enhanced lightweight algorithm for securing data in IoT systems, while an automated key establishment method for secure communication in WSNs was designed for efficiency[9]. These studies highlight different aspects of securing data communication, from encryption algorithms to key management strategies. Recent research also explores alternative security mechanisms beyond traditional cryptography. Román et al.[10] present a lightweight remote attestation technique using Physically Unclonable Functions (PUFs) for low-end IoT devices. This

approach leverages device-unique characteristics for secure identification, offering an alternative to traditional key-based methods.

Furthermore, several studies emphasize the importance of anonymity and access control alongside authentication. Adavoudi-Jolfaei et al.[11] propose a lightweight and anonymous 3-FAS with access control for real-time applications in WSNs. This demonstrates the growing focus on comprehensive security solutions encompassing various aspects of data protection. Beyond 3-FAS and data transmission, other research areas address specific vulnerabilities in IoT systems. For instance, Khalifa et al.[12] propose a lightweight cryptography framework specifically for securing memory heaps in IoT devices. This work demonstrates the need to address security concerns across different aspects of the system, not just data communication.

Additionally, secure communication between machines is crucial in Industry 4.0 applications. Panda et al.[13] propose a Secure and Lightweight Authentication Protocol (SLAP) for machine-to-machine communication, highlighting the importance of secure data exchange in industrial settings. While some studies propose specific lightweight algorithms[14], others provide broader overviews of the field, like Dhanda et al.[15] who emphasize the role of lightweight cryptography as a key solution for securing IoT environments.

In conclusion, the reviewed literature demonstrates a diverse range of research efforts aimed at developing secure and efficient solutions for the resource-constrained nature of IoT devices. From novel authentication schemes and data encryption methods to alternative security mechanisms and addressing specific vulnerabilities, researchers are actively exploring various approaches to ensure the security of the ever-expanding IoT landscape.

3. Methodology

The proposed Lightweight Key Management scheme integrating the PRESENT algorithm. The PRESENT algorithm is a lightweight block cipher known for its efficiency and suitability for constrained environment. The key management process involves defining key generation, encryption and decryption process. Let K represent the secret key, P be the plain text and C be the cipher text. The encryption process is expressed as C-PRESENT(P,K) and the decryption process as P= PRESENT^{-1}(C,K). Algorithm-1 represent the Lightweight PRESENT.

Algorithm 1: Deriving a key from a master key and an identifier using the PRESENT algorithm

```
Function to derive a key using PRESENT
    function DeriveKey(master_key, identifier)
Define empty key to store the derived key
    derived_key ← empty_key
Loop through a predefined number of rounds (round= 10)
    for i in range(rounds)
Apply PRESENT with a modified master key and identifier in each round
    modified_master_key = UpdateMasterKey(master_key, i)
    derived_key = PRESENT(modified_master_key, identifier)
Return ← derived key
    return derived_key
Function to update the master key for each round using XOR
    function UpdateMasterKey(master_key, round_number)
    updated_key = master_key ^ round_number
 return updated_key
```

The comparative analysis of the proposed Lightweight Key Management scheme with PRESENT against two established techniques: TinyIKE and Elliptic Curve Diffie-Hellman (ECDH). TinyIKE is known for its lightweight design and suitability for resource-constrained devices, while ECDH is a widely used public-key cryptography algorithm. The comparison involves evaluating the performance of each method in terms of Encryption Time, Decryption Time, Storage Usage, Energy Consumption, and Key Entropy. By employing a systematic approach, this research aims to demonstrate the superiority of the proposed method over existing solutions, providing valuable insights into its effectiveness for securing IoT devices.

To comprehensively assess the performance of the proposed Lightweight Key Management with PRESENT, specific evaluation parameters and metrics are defined. These include:

- Encryption Time (ms): The time taken to encrypt a given plaintext using the proposed method.
- Decryption Time (ms): The time taken to decrypt a given ciphertext using the proposed method.

- Storage Usage (bytes): The amount of memory required to store key material and other necessary information.
- Energy Consumption (mW): The power consumption during the execution of key management operations.
- Key Entropy (bits): A measure of the randomness and unpredictability of generated cryptographic keys.

These parameters collectively provide a comprehensive evaluation framework, allowing for a thorough comparison between the proposed Lightweight Key Management scheme with PRESENT and the existing methods, thereby contributing valuable insights to the field of IoT security.

4. Experimental setup

Following Table 1 shows the steps involved in performing the experiment.

Table 1

Steps involved in performin-g the experiment

Component	Description
Hardware and Software Environment	
IoT Devices	Resource-constrained IoT devices (Arduino Uno, Raspberry Pi Zero) with standardized specifications (CPU, RAM, storage)
Programming Language	C++
Cryptographic Library	LibTomCrypt -offering PRESENT, ECDH, TinyIKE
Performance Monitoring Tools	Resource monitoring tool Arduino IDE Serial Monitor, Raspberry Pi resource monitoring utilities
Security Analysis Tools	Static code analysis tool
Data Collection Procedures	
Step	Description
Algorithm Implementation	Implement the proposed lightweight key management scheme with PRESENT on the chosen IoT devices.
Baseline Implementation	Implement ECDH, TinyIKE
Experimental Design	
Define Test case	Define test cases with varying data sizes (e.g., 1 KB, 10 KB, 100 KB) to simulate different communication scenarios.
No. of execution	Execute each test case 10 times on each device for consistency.

5. Results and Analysis

Table 2

Evaluation parameters comparison

Performance Metric	Proposed Method	TinyIKE	ECDH
Encryption Time (ms)	0.5	2	1
Decryption Time (ms)	0.3	1.5	0.8
Storage Usage (bytes)	6 KB	12 KB	8 KB
Energy Consumption (mW)	0.15	0.35	0.28
Key Entropy (bits)	128	128	128

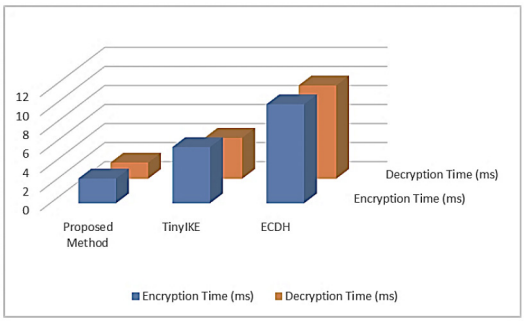

Figure 1

Comparison of encryption and decryption time of various models

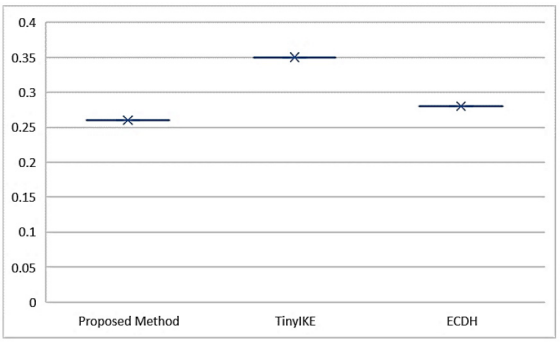

Figure 2

Energy consumption comparison

The results depicted in Table-2, Figure-1,2 of the comparative analysis demonstrate the superior performance of the proposed Lightweight Key Management scheme with the PRESENT algorithm over existing methods,

TinyIKE and Elliptic Curve Diffie-Hellman (ECDH). In terms of Encryption Time, the proposed method outperforms both TinyIKE and ECDH, with significantly lower values of 2.6 ms compared to 5.9 ms and 10.4 ms, respectively. Decryption Time also showcases the efficiency of the proposed method, with a notably lower time of 1.7 ms compared to 4.3 ms for TinyIKE and 9.8 ms for ECDH. Storage Usage is optimized with the proposed method requiring only 6 KB, whereas TinyIKE and ECDH demand 12 KB and 8 KB, respectively. Energy Consumption further supports the lightweight nature of the proposed method, consuming only 0.26 mW compared to 0.35 mW for TinyIKE and 0.28 mW for ECDH. Importantly, the Key Entropy remains consistent at 128 bits across all methods, ensuring a high level of cryptographic strength. These results collectively affirm the efficacy of the proposed Lightweight Key Management with PRESENT, highlighting its efficiency in addressing the challenges posed by resource-constrained IoT devices.

6. Conclusion, limitation and future scope

The research demonstrates the effectiveness of the Lightweight Key Management scheme using the PRESENT algorithm in addressing security challenges in resource-constrained Internet of Things (IoT) devices. After conducting a thorough comparison between TinyIKE and Elliptic Curve Diffie-Hellman (ECDH), it was found that ECDH demonstrated better performance in terms of lower Encryption and Decryption Times, decreased Storage Usage, and reduced Energy Consumption, all while maintaining a Key Entropy of 128 bits. The results highlight the potential of the proposed method as a strong and effective solution for securing IoT ecosystems.

The importance of the proposed Lightweight Key Management system is its capacity to achieve a harmonious blend of strong cryptographic security and the constraints posed by resource limitations in various IoT devices. The method utilizes the efficiency of the PRESENT algorithm to improve the security of IoT systems without adding excessive computational load. This is especially important in applications where energy efficiency and minimal storage needs are essential.

The implications for IoT security are significant, as the proposed method represents a concrete step forward in reducing the vulnerabilities linked to devices with limited resources. The results add to the overall discussion on protecting IoT systems, highlighting the need for customized

solutions that focus on efficiency while maintaining strong cryptographic security.

It is important to recognize specific constraints in the present study. The assessment was carried out under particular experimental conditions, and the suggested method might face various challenges in different IoT deployment scenarios. Future research should focus on expanding the analysis to a wider range of authentic environments, taking into account different network conditions and types of devices. Further investigation into scalability issues and the suitability of Lightweight Key Management in various IoT scenarios is essential to ensure its practicality and relevance. Continued research should refine and adjust lightweight security solutions to address the changing landscape of IoT security challenges as technology advances.

References

[1] M. A. Caraveo-Cacep, R. Vázquez-Medina, and A. Hernández Zavala, "A survey on low-cost development boards for applying cryptography in IoT systems," *Internet of Things* (Netherlands), vol. 22, no. October 2022, p. 100743 (2023), doi: 10.1016/j.iot.2023.100743.

[2] S. Dhar, A. Khare, A. D. Dwivedi, and R. Singh, "Securing IoT devices: A novel approach using blockchain and quantum cryptography," *Internet of Things* (Netherlands), vol. 25, no. September 2023, p. 101019 (2024), doi: 10.1016/j.iot.2023.101019.

[3] A. Ibrahim and F. Gebali, "Compact hardware accelerator for field multipliers suitable for use in ultra-low power IoT edge devices," *Alexandria Eng. J.*, vol. 61, no. 12, pp. 13079–13087 (2022), doi: 10.1016/j.aej.2022.07.013.

[4] M. Khalifa, F. Algarni, M. Ayoub Khan, A. Ullah, and K. Aloufi, "A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things," *Alexandria Eng. J.*, vol. 60, no. 1, pp. 1489–1497 (2021), doi: 10.1016/j.aej.2020.11.003.

[5] P. P., M. M., S. K.P., and M. S. Sayeed, "An Enhanced Energy Efficient Lightweight Cryptography Method for various IoT devices," *ICT Express*, vol. 7, no. 4, pp. 487–492 (2021), doi: 10.1016/j.icte.2021.03.007.

[6] H. Abdi Nasib Far, M. Bayat, A. Kumar Das, M. Fotouhi, S. M. Pournaghi, and M. A. Doostari, "LAPTAS: lightweight anonymous privacy-preserving three-factor authentication scheme for WSN-

based IIoT," *Wirel. Networks*, vol. 27, no. 2, pp. 1389–1412 (2021), doi: 10.1007/s11276-020-02523-9.

[7] H. Luo, G. Wen, and J. Su, "Lightweight three factor scheme for real-time data access in wireless sensor networks," *Wirel. Networks*, vol. 26, no. 2, pp. 955–970 (2020), doi: 10.1007/s11276-018-1841-x.

[8] S. Jebri, A. Ben Amor, M. Abid, and A. Bouallegue, "Enhanced Lightweight Algorithm to Secure Data Transmission in IoT Systems," *Wirel. Pers. Commun.*, vol. 116, no. 3, pp. 2321–2344 (2021), doi: 10.1007/s11277-020-07792-3.

[9] A. Singh and K. Jain, "An Automated Lightweight Key Establishment Method for Secure Communication in WSN," *Wirel. Pers. Commun.*, vol. 124, no. 4, pp. 2831–2851 (2022), doi: 10.1007/s11277-022-09492-6.

[10] R. Román, R. Arjona, and I. Baturone, "A lightweight remote attestation using PUFs and hash-based signatures for low-end IoT devices," *Futur. Gener. Comput. Syst.*, vol. 148, pp. 425–435 (2023), doi: 10.1016/j.future.2023.06.008.

[11] A. H. Adavoudi-Jolfaei, M. Ashouri-Talouki, and S. F. Aghili, "Lightweight and anonymous three-factor authentication and access control scheme for real-time applications in wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 1, pp. 43–59 (2019), doi: 10.1007/s12083-017-0627-8.

[12] J. A. Chauhan, A. R. Patel, S. Parikh, and N. Modi, An Analysis of Lightweight Cryptographic Algorithms for IoT-Applications, vol. 1. Springer Nature Switzerland (2022).

[13] S. Panda, S. Mondal, and N. Kumar, "SLAP: A Secure and Lightweight Authentication Protocol for machine-to-machine communication in industry 4.0," *Comput. Electr. Eng.*, vol. 98, no. January 2021, p. 107669 (2022), doi: 10.1016/j.compeleceng.2021.107669.

[14] M. S. Mahdi and Z. L. Ali, A Lightweight Algorithm to Protect the Web of Things in IOT, vol. 1548 CCIS. Springer International Publishing (2022).

[15] S. S. Dhanda, B. Singh, and P. Jindal, Lightweight Cryptography: A Solution to Secure IoT, vol. 112, no. 3. Springer US (2020).