JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

DESIGN AND EVALUATION OF LIGHTWEIGHT CRYPTOGRAPHIC PROTOCOLS FOR SECURING IOT ENABLED SMART INFRASTRUCTURE

KRITENDRA SINGH, MRS. NEETA BHUSAL SHARMA

ASSISTANT PROFESSOR

SRMU, LUCKNOW

Abstract: *The dynamic surge of IoT-based smart infrastructures (smart grids, smart healthcare systems, and ndustrial IoT) have introduced new opportunities and threats never faced before. The high computational, memory and energy requirements make conventional crypto-graphic solutions inappropriate on a resource constrained devices despite their great security. This paper outlines the design and analysis of a light cryptographic protocol that relies on Elliptic Curve Cryptography (ECC) in order to safely exchange keys, PRESENT algorithm in order to securely encrypt and SPONGENT algorithm in order to verify integrity.*

Keywords: *IoT security, Lightweight cryptography, Smart infrastructure, Elliptic Curve Cryptography (ECC), PRESENT cipher, SPONGENT hash, Energy-efficient protocols*

I. Introduction

A. Background and Motivation

The proliferation of the Internet of Things (IoT) has revolutionized modern infrastructures, opening up the possibilities to build smart cities, intelligent healthcare systems, connected transportation, and advanced industrial automation. These IoT-enabled smart infrastructures are increasingly in charge of delivering critical services, from energy management in smart grids to patient monitoring in health care.

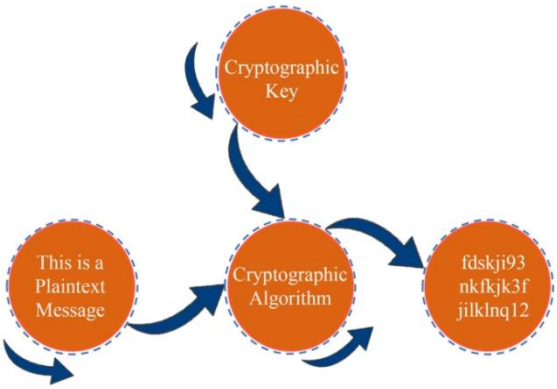

Figure 1: Encryption and decryption process using a key

B. Problem Statement

Traditional cryptographic algorithms such as RSA and AES are commonly used in order to secure data in traditional computing systems. Yet, these algorithms were never designed for lightweight devices that have to manage performance with a limited set of resources. Applying such algorithms in IoT scenarios frequently leads to excessive energy usage, high latency times, and issues with scalability, which are directly at odds with the operational requirements of smart infrastructures.

C. Research Objectives

This work aims to design and evaluate lightweight cryptographic protocols designed for IoT-enabled smart infrastructures. The specific objectives are threefold:

- To propose a cryptographic protocol or amend current lightweight schemes to address the special requirements of IoT devices.
- To test the designed protocol against conventional and lightweight benchmarks in terms of computational overhead, memory usage, and energy efficiency.

D. Contribution of the Paper

The contribution of this paper is as follows:

- The design of a cryptographic protocol for constrained IoT devices with low computational complexity.
- A detailed comparative analysis of the proposed scheme with benchmark protocols that exist.

E. Paper Organisation

The following is the structure of the rest of this paper. Section II is a review of the current research efforts into lightweight cryptographic techniques as well as literature gaps. The system model, attacker assumptions, and problem formulation are defined in Section III.

II. Literature Review

A. IoT Security Requirement

Internet of Things (IoT) is a massive system of interconnected gadgets that, together, create, refine, and share information in the fields of smart grids, healthcare, industrial automation, and intelligent transportation [1]. Sensitivity of data and critical nature of service in these infrastructures lead to strong security mechanisms being a necessity. Four fundamental security requirements are always present as themes in the literature: confidentiality, integrity, authentication and availability.

In the absence of a strong authentication, there are malicious actors capable of spoofing devices and transmitting malicious commands [2]. Availability promotes the continuous access of resources and services and defends against denial of service attacks that have the potential to cripple critical infrastructure.

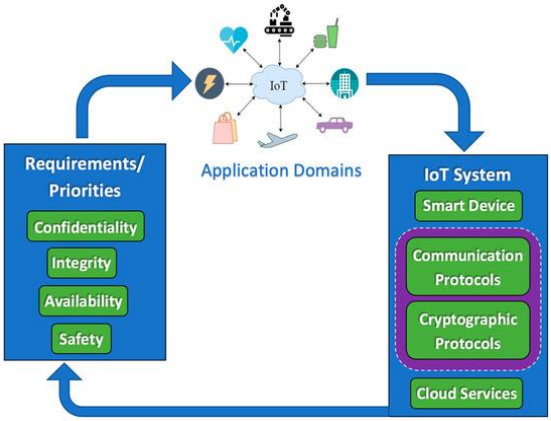

Figure 2: IoT applications have different requirements in terms of the CIA triad, in addition to safety

There is also a tendency of IoT devices to experience low bandwidth and poor wireless connectivity, and protocol stack has to be designed with low communication overhead [3].

B. Existing Lightweight Cryptographic Protocols

Researchers are coming up with a plethora of lightweight cryptographic solutions to the strict resource limit of IoT. These are basically divided into block ciphers, hash functions and lightweight public key schemes.

Block Ciphers:

Many lightweight cryptographic protocols are the offspring of block ciphers because they are efficient in symmetric key encryption. Algorithms including PRESENT, LED, SIMON and SPECK have shifted to first line. PRESENT is a 64bit block cipher designed to be hardware friendly and provide a trade off between security and efficiency [4].

Hash Functions:

SPONGENT takes advantage of sponges construction, where the state size is smaller hence the memory used is also smaller, and PHOTon is designed to consume as small as possible in hardware. They both have a smaller resource footprint than other common hash methods like SHA-2, and thus are well suited to resource-constrained IoT devices [5].

Lightweight Public Key Schemes:

Key exchange and authentication still require the use of public-key cryptography, however, classical algorithms such as RSA are not feasible in the IoT because of their high computational value. As an alternative, Lightweight public key solutions have become the de facto standard to Elliptic Curve Cryptography (ECC). ECC provides the same level of security as RSA with much smaller key sizes and thus computations and communications overhead are considerably reduced. Besides the ECC, post-quantum lightweight schemes like the lattice-based cryptography are also under consideration in their future-proof security [6]..

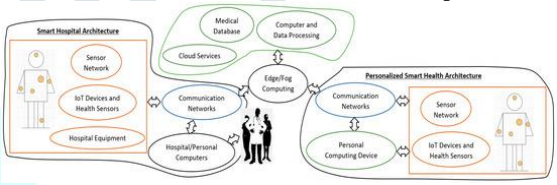

Figure 3: IoT-based healthcare environment

C. Security in Smart Infrastructure

The inclusion of IoT in smart infrastructure makes lightweight cryptographic protocols even more important. Security requirements differ from domain to domain, but have common limitations that are imposed by resource-limited devices and critical operational needs.

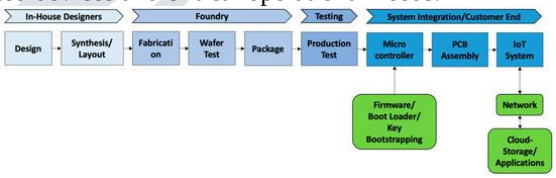

Figure 4: The different stages of hardware security

Smart Grids:

Smart grids are the combination of sensors, smart meters, and control systems that help to optimize energy production and consumption. The data exchanged is sensitive, since adversaries could potentially manipulate meter readings, disrupt demand response mechanisms, or blackout large areas [7].

Smart Healthcare:

The IoT in the healthcare sector is applied in wearable devices used as sensors to constantly track the health of patients and transmit data to the healthcare system, as well as implantable medical devices. Confidentiality breaches may lead to the exposure of private health records whereas the integrity and authentication errors may endanger the life of a patient [8].

Industrial IoT (IIoT):
Industrial systems are taking advantage of IoT to preemptively maintain and automate manufacturing processes and control [9].

Security Breaches Case Studies:
Weakness of unsecured devices is evidenced by documented attacks, including the Mirai botnet attack, that used unsecured IoT devices to execute massive distributed denial of service (DDoS) attacks. In the same manner, proof-of-concept attacks on smart meters have demonstrated the factors through which the assailants can manipulate the information to gain financial gain [10].

Domain	Incident / Case Study	Exploited Vulnerability	Impact	Lessons Learned
Smart Grid	Ukraine Power Grid Attack (2015)	Weak authentication and a lack of intrusion detection	Large-scale blackout affecting 225,000 customers	Stronger cryptographic protection and monitoring of control commands are essential
Smart Meters	Smart meter fraud (documented in multiple EU deployments)	Unencrypted or poorly protected meter-to-utility communication	Manipulated consumption data, financial losses	End-to-end encryption and lightweight authentication mechanisms are critical
Healthcare IoT	Johnson & Johnson insulin pump advisory (2016)	Insecure wireless communication (unencrypted RF signals)	Potential remote manipulation of insulin dosage	Secure lightweight encryption and device authentication are required in medical IoT
Industrial IoT	Stuxnet (2010) – although targeted at ICS	Default passwords and weakly protected PLCs	Physical damage to centrifuges in Iranian nuclear facilities	Critical infrastructures require lightweight but robust security tailored to industrial devices
General IoT	Mirai Botnet (2016)	Default credentials in consumer IoT devices	Large-scale DDoS attacks are disrupting Internet services	Secure authentication and mandatory key rotation should be enforced

Table 1: Case Studies of Security Breaches in Smart Infrastructure

D. Comparative Analyses in Literature

Many studies were carried out concerning the comparison of the performance of lightweight cryptographic protocols in various IoT applications [11]. Measures of energy use, latency, throughput, memory usage, and error resiliency (eg, Root Mean Square Error - RMSE) are common subjects of study.
The findings are frequently presented in a table so as to be clear. A common trend is that of efficiency vs. security strength: low-energy-use protocols can be susceptible to strong cryptanalysis, and highly-secure protocols require more computational effort [12].

The stability of protocols in the presence of a noisy or unreliable communications channel is another novel subject of analysis. Measures like RMSE have found more widespread use in the assessment of the performance of cryptographic schemes in the real world where packet loss and interference are high.

E. Literature Gap

Regardless of the excessive amount of development, there are certain serious gaps evident in the existing literature and the given study attempts to fill them.

First, lightweight cryptographic protocols have not been experimented in real IoT testbeds. Simulations or theoretical research are intensively used in many studies that are not necessarily representative of the limitations and performance trade-offs of actual IoT systems [13].

Second, in most of the works that have been proposed, formal verification of the proposed lightweight algorithms has not been made. Security properties such as secrecy, authenticity or resistance to replay attacks can be mathematically proven using formal systems such as ProVerif, AVISPA or BAN logic [14].

III. System Model and Problem Statement

A. System Architecture

The IoT-enabled smart infrastructure of this study has three major layers: end devices, gateways, and cloud/edge servers. End devices are resource-constrained sensors, actuators, and smart meters deployed in various domains such as healthcare, smart grids, and industrial environments [17].

B. Attacker Model

Such threats may cause disturbances to energy distribution in smart grids, the fabrication of medical data in healthcare, or production in industrial systems. The model, therefore, calls for protocols that ensure resistance to passive and active intrusions [18].

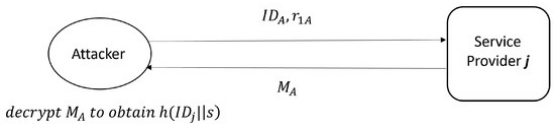

Figure 6: Attacker registration as a normal user

C. Design Constraints

IoT devices are limited in smart infrastructure due to limited CPU capacity, memory availability, and battery life. These limitations prohibit the use of computationally heavy cryptographic algorithms [19]. Additionally, in many deployments, the wireless links used have low bandwidth, which requires the protocols to have minimal communication overhead. Scalability is another limitation because infrastructures can contain thousands of interconnected devices.

D. Problem Definition

The research problem is to design lightweight cryptographic protocols that will provide for secure communication between devices, gateways, and servers while following the resource constraints. The goal is to achieve confidentiality, integrity, and authentication with minimal computational, memory, and energy overhead to enable secure and sustainable IoT-enabled smart infrastructure.

IV. Design of Lightweight Cryptographic Protocol(s)

A. Protocol Overview

It is suggested that the proposed lightweight cryptographic protocol will make the communication in IoT-based smart infrastructure secure, based on integrating three valuable functions, which are key exchange, encryption and authentication. The protocol begins with a default and lightweight key establishment procedure and this helps devices to share the session keys with the gateways or servers [20].

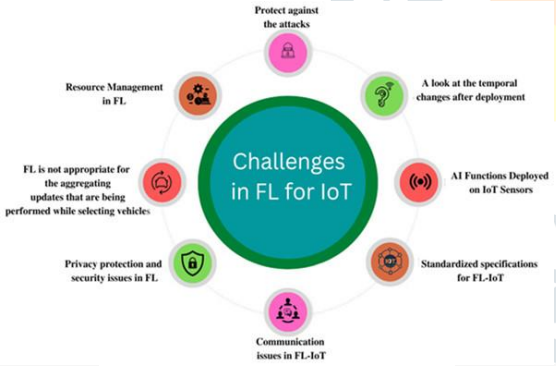

Figure 5: Challenges in FL-IoT

B. Cryptographic Primitives Used

The efficiency of the protocol is dependent on careful selection of the lightweight cryptographic primitives. A lightweight block cipher such as PRESENT or SPECK is used for symmetric encryption due to its low memory footprint and low gate equivalent requirements. For the data integrity and authentication purposes, a light-weighted hash Function, such as SPONGENT, is included that ensures very little computational overhead during the generation of the Message Authentication Code (MAC) [21].

C. Protocol Workflow

The protocol is based on the reduced workflow for communication:

- **Initialization:** Every IoT device comes pre-installed with an ECC key pair and a unique identifier. Gateways or servers maintain the public keys of the registered devices.
- **Key Exchange:** By this, the device that wants to start a communication sends the public key to the gateway in a light handshake. The gateway responds with its own public key, and a common session key is agreed on using the ECDH scheme.

D. Key Management Strategy

The protocol has a hybrid key management approach. ECC is utilized only at the time of initial exchange of keys and after that further communication is conducted with the help of symmetric key. This method significantly reduces energy and computation costs because operations that are symmetric are far lighter than those of public-key [22].

E. Light Weight Design Principles

The protocol design is based on three basic principles:

- **Energy-efficient operations:** The lightweight ciphers and hash functions save power, extending the battery life of devices.
- **Reduced computation overhead:** The hybrid scheme guarantees that resource-intensive public key operations are kept to a minimum while leveraging efficient symmetric cryptography to perform the frequent exchanges.
- **Security-robustness balance:** The combination of ECC, PRESENT, and SPONGENT allows confidential, integrity, and authentication without sacrificing efficiency. The design preserves resilience against eavesdropping, replay, and impersonation attacks while satisfying real-time requirements of smart infrastructures.

By combining these design elements, the proposed protocol provides a secure, scalable, and efficient protocol suited for IoT-enabled smart infrastructures.

V. Security Analysis and Formal Verification

A. Informal Security Analysis

The proposed lightweight cryptographic protocol is evaluated on common security requirements. Confidentiality is maintained by encrypting all the data packets with the PRESENT block cipher, which means that the adversaries cannot access the plaintext even if communication channels are monitored. Integrity is assured by using lightweight hash-based message authentication codes (MACs) based on SPONGENT. A

B. Formal Methods

To reinforce the guarantee of security claims, the protocol can be checked with formal verification tools. BAN Logic offers a framework to reason about the beliefs of entities in authentication protocols to confirm that both communicating parties believe that they share a fresh session key [24].

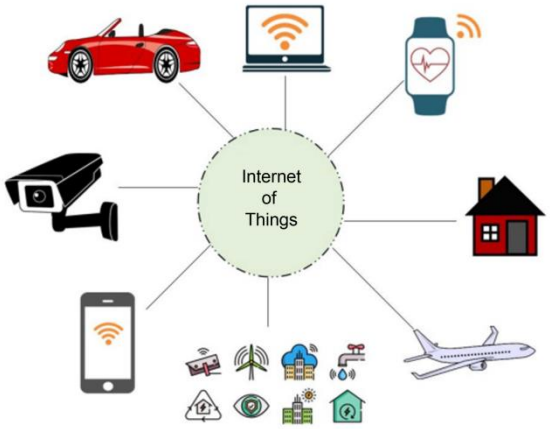

Figure 6: IoT application sectors

C. Threat Modeling and Evaluation

The adversary model is a model that assumes an attacker has full control over the communication channel, being able to intercept, modify, replay, or inject messages.

D. Proof of Security Properties

The protocol achieves a number of formally verifiable properties. Key secrecy is maintained because ECDH is guaranteed to only be derived by legitimate devices. Forward secrecy is achieved with periodic key refreshment, so that compromise of one session does not compromise future communications [26].

VI. Implementation and Experimental Setup

A. Test Environment

To assess the feasibility and efficiency of the proposed lightweight cryptographic protocol, implementation was performed on resource-limited IoT platforms representative of real-world smart infrastructures [27].

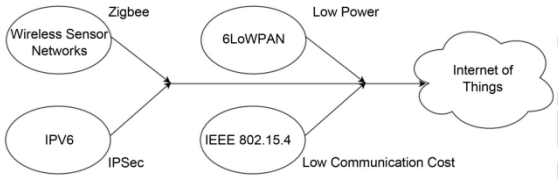

Figure 7: IoT background

B. Evaluation Metrics

The protocol was assessed on four primary metrics:

- **Computation time:** measured to assess the processing delay introduced by encryption, decryption, and authentication operations.
- **Memory usage:** both the consumption of memory (RAM and flash) was recorded to determine the suitability for constrained devices.

C. Benchmark Protocols for Comparison

Comparisons between such schemes enabled to determine the energy saving benefits, the latency and memory saving benefits and to establish the security properties as equal or higher than the traditional techniques [28].

VII. Results and Performance Evaluation

A. Experimental Results

The lightweight cryptography protocol was proposed and experimented with the real and simulated IoT environments. Findings indicate that the protocol is experiencing significant energy saving in comparison to conventional cryptographic schemes.

In terms of latency, the hybrid scheme added very little latency. The initial ECC-based key exchange took somewhat more computation time than symmetric-only, but subsequent symmetric operations were done with low latency.

B. Comparative Tables and Figures

Performance comparisons with benchmark algorithms described the advantages of the proposed scheme. Across key metrics, Table III summarises the results.

To complement tabular data, graphical results have been plotted. RMSE vs. SNR curves demonstrated the resiliency of the protocol under noisy communication channels with almost no error rates as compared to conventional schemes.

C. Observations

The findings point to evident trade-offs that are implemented by the suggested protocol. Although the use of the ECC-based key exchange has a small one-time cost, the benefits are high security assurances and effective symmetric operation thereafter. The encryption (PRESENT)-integrity (SPONGENT) combination ensures a trade-off between energy-efficiency and robustness that renders the protocol viable to long-term implementation in smart infrastructures.

VIII. Discussion

The analysis results indicate that the suggested lightweight cryptographic protocol is highly suitable in the context of smart infrastructure. This is scalable to thousands of devices with its low energy and memory needs and no computational or storage resource constraints [29].

A. Practical Implications

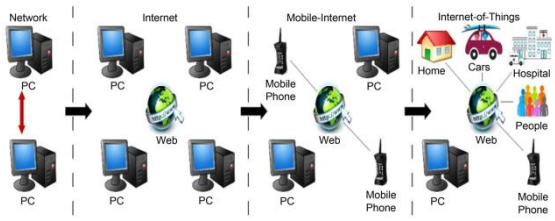

Figure 8: Evaluation of IoT

B. Strengths

The use of lightweight primitives provides reduced overhead compared with conventional algorithms, while the combination of ECC, PRESENT, and SPONGENT provides confidentiality, integrity, and authentication. The design is a balance between robust and practical, which allows for secure communication on ultra-constrained devices [30].

C. Limitations

Despite such advantages, there are some limitations. The evaluation was done on a small number of IoT boards which has limited the number of hardware we have tested.

IX. Conclusion and Future Work

This paper showed the design and evaluation for the light weight cryptographic protocols for IoT enabled smart infrastructures. The proposed scheme offered confidentiality, integrity and authentication using less energy, latency and memory overhead.

Future Work:

- Extend evaluation to IoT ecosystems with multiple, heterogeneous devices.
- Integrate AI-based adaptive security measures for dynamic threat detection.
- Test the protocol in real world deployments such as smart city and healthcare systems.
- Investigate post-quantum lightweight cryptography to guarantee long-term resilience from emerging computational threats.

X. References

[1] Dhanda, S.S., Singh, B. and Jindal, P., 2020. Lightweight cryptography: a solution to secure IoT. *Wireless Personal Communications*, *112*(3), pp.1947-1980.

[2] Rana, M., Mamun, Q. and Islam, R., 2020. Current lightweight cryptography protocols in smart city IoT networks: a survey. *arXiv preprint arXiv:2010.00852*.

[3] Samaila, M.G., Sequeiros, J.B., Simoes, T., Freire, M.M. and Inacio, P.R., 2020. IoT-HarPSecA: a framework and roadmap for secure design and development of devices and applications in the IoT space. *IEEE Access*, *8*, pp.16462-16494.

[4] Bhagat, V., Kumar, S., Gupta, S.K. and Chaube, M.K., 2023. Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications. *Concurrency and Computation: Practice and Experience*, *35*(1), p.e7425.

[5] Radhakrishnan, I., Jadon, S. and Honnavalli, P.B., 2024. Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices.*Sensors*, *24*(12), p.4008.

[6] Jan, S.U., Qayum, F. and Khan, H.U., 2021. Design and analysis of lightweight authentication protocol for securing IoD. *Ieee access*, *9*, pp.69287-69306.

[7] Khan, M.N., 2024. *Lightweight and post-quantum safe security solutions for IoT systems* (Doctoral dissertation, RMIT University).

[8] Shamala, L.M., Zayaraz, G., Vivekanandan, K. and Vijayalakshmi, V., 2021. Lightweight cryptography algorithms for internet of things enabled networks: An overview. In *Journal of Physics: Conference Series* (Vol. 1717, No. 1, p. 012072). IOP Publishing.

[9] Akram, M.W., Bashir, A.K., Shamshad, S., Saleem, M.A., AlZubi, A.A., Chaudhry, S.A., Alzahrani, B.A. and Zikria, Y.B., 2021. A secure and lightweight drones-access protocol for smart city surveillance.*IEEE Transactions on Intelligent Transportation Systems*, *23*(10), pp.19634-19643.

[10] Pandey, S. and Bhushan, B., 2024. Recent Lightweight cryptography (LWC) based security advances for resource-constrained IoT networks. *Wireless Networks*, *30*(4), pp.2987-3026.

[11] Abed, A.M. and Boyacı, A., 2020. A lightweight cryptography algorithm for secure smart cities and IOT.*Electrica*, *20*(2), pp.168-176.

[12] Roy, S., Das, D., Mondal, A., Mahalat, M.H., Sen, B. and Sikdar, B., 2022. PLAKE: PUF-based secure lightweight authentication and key exchange protocol for IoT. *IEEE Internet of Things Journal*, *10*(10), pp.8547-8559.

[13] Parmar, M. and Shah, P., 2023. Internet of things-blockchain lightweight cryptography to data security and integrity for intelligent application.*International Journal of Electrical & Computer Engineering (2088-8708)*, *13*(4).

[14] Jan, M.A., Khan, F., Mastorakis, S., Adil, M., Akbar, A. and Stergiou, N., 2021. LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. *IEEE transactions on green communications and networking*, *5*(3), pp.1202-1211.

[15] Rana, S., Mondal, M.R.H. and Kamruzzaman, J., 2023. RBFK cipher: a randomized butterfly architecture-based lightweight block cipher for IoT devices in the edge computing environment. *Cybersecurity*, *6*(1), p.3.

[16] Ali, Z., Chaudhry, S.A., Ramzan, M.S. and Al-Turjman, F., 2020. Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles.*IEEE Access*, *8*, pp.43711-43724.