International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 12– No. 47, April 2025 – www.ijais.org

Analyzing Message Authentication Methods and Security Standards in Communication among IoT Devices

Nguyen Thi Phuong Bac
Hanoi University of Mining and Geology
18 Vien street, Duc Thang ward, Bac Tu Liem district, Hanoi, Vietnam

Nguyen Duy Huy
Hanoi University of Mining and Geology
18 Vien street, Duc Thang ward, Bac Tu Liem district, Hanoi, Vietnam

Tran Trung Chuyen
Hanoi University of Mining and Geology
18 Vien street, Duc Thang ward, Bac Tu Liem district, Hanoi, Vietnam

ABSTRACT
The rapid expansion of the Internet of Things (IoT) has led to an increasing number of interconnected devices, raising concerns about the security and privacy of data communication. This study analyzes various message authentication methods and security standards employed in IoT device communication to identify their strengths, weaknesses, and opportunities for improvement. The state-of-the-art message authentication techniques, such as symmetric and asymmetric cryptography, digital signatures, and light-weight authentication protocols are fully reviewed. Additionally, the most common security standards and protocols, focusing on the context of message authentication are also examined, and provide a detailed overview of their usage, advantages, and disadvantages. The findings emphasize the importance of selecting appropriate authentication methods and security standards considering IoT applications' specific requirements and constraints, including computational capacity, energy consumption, and latency. Furthermore, we propose recommendations for enhancing the security of IoT communication and discuss potential research directions in developing novel authentication techniques and security standards tailored to the unique challenges of the IoT ecosystem.

Keywords
IoT security, authentication protocols, communication, message authentication, cryptography, data privacy.

1. INTRODUCTION
Internet of Things (IoT) applications are becoming increasingly prevalent, with devices connecting and exchanging data to offer various services. Secure communication between IoT devices is essential to protect user privacy and data integrity. This paper analyzes and compares multiple message authentication methods and security standards employed in IoT communication. It also provides recommendations for selecting suitable authentication methods and security standards and discussing potential future research directions in IoT security.

2. LITERATURE REVIEW AND PROPOSALS

2.1 Message Authentication Methods in IoT
Symmetric Cryptography:

Symmetric algorithms, like AES, use a single secret key for encryption and decryption, ensuring data confidentiality and integrity in IoT communication [1]. The following Fig1 illustrates how AES encryption and decryption function at a basic level:

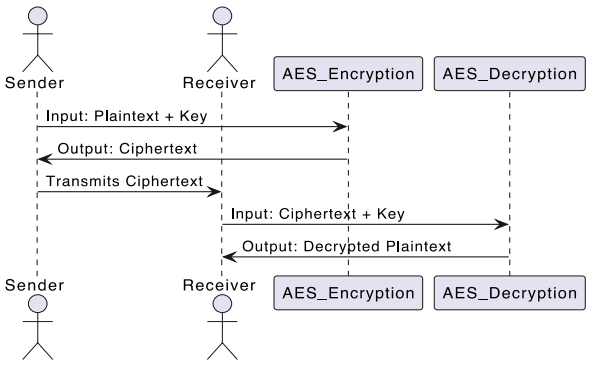

Fig 1: Basic AES encryption and decryption process with a single secret key

Symmetric algorithms offer efficiency and simplicity, making them suitable for resource-constrained IoT devices [2]. However, they face key management and distribution challenges and need more scalability in large-scale IoT networks [3]. Researchers have explored lightweight symmetric encryption algorithms, such as ChaCha20 [4] and TEA [5], and secure key exchange protocols, like the Diffie-Hellman key exchange [6].

Advantages:

• Efficiency: Symmetric encryption algorithms are generally faster and consume fewer computational resources than asymmetric algorithms, making them suitable for IoT devices with constrained resources.

• Simplicity: Symmetric algorithms use a single key for encryption and decryption, simplifying key management and distribution.

Disadvantages:

• Key management and distribution: Securely distributing and managing the secret key among multiple IoT devices can be challenging, as the key needs to be securely exchanged and stored.

• Scalability: In large-scale IoT networks, the number of keys required grows exponentially with the number of devices, increasing complexity in crucial management.

Asymmetric Cryptography:

Asymmetric algorithms, such as RSA, use a public-private key pair to ensure data confidentiality and integrity in IoT communication [7]. The following Fig2 illustrates the basic RSA encryption and decryption process:

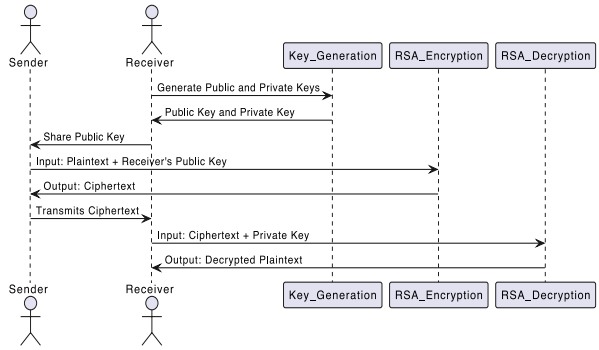

Fig 2: Basic RSA encryption and decryption process using a public-private key pair

Asymmetric algorithms offer simplified key management and distribution, non-repudiation, and increased security [2], [3], [8]. However, they are computationally complex and require larger key sizes [4], [9]. Researchers have investigated various asymmetric algorithms, like ECC [10] and Lattice-based cryptography [11], and novel key management schemes for IoT, such as PKI [12] and identity-based cryptography [13].

Advantages:

• It simplified key management and distribution.

• Digital signatures provide non-repudiation.

• Increased security with separate encryption and decryption keys.

Disadvantages:

• Higher computational complexity and less suitable for resource-constrained IoT devices.

• Larger key sizes, increasing storage and transmission overhead.

Digital Signatures:

Digital signatures, used for authentication and data integrity in IoT communication, involve signing a message with a private key and verifying it with the sender's public key. The following Fig 3 illustrates the basic functioning of a digital signature scheme:

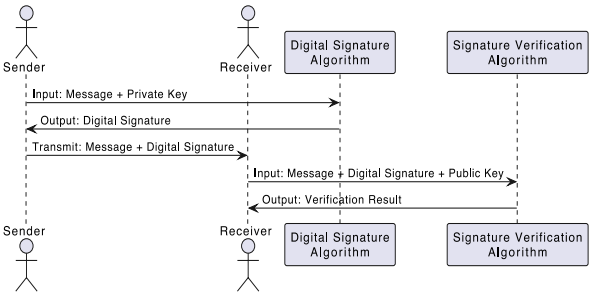

Fig 3: Digital Signature and Verification Process

Digital signatures provide authentication, integrity, and non-repudiation but can be computationally expensive and require proper key management [14]. Researchers have explored lightweight digital signature al- algorithms, such as ECDSA [15] and LDSA [16], and secure key management schemes, like PKI [12] and certificate-less public key cryptography [13].

Advantages:

• Authentication and integrity: Ensures data authenticity and integrity through the sender's private and corresponding public keys.

• Non-repudiation: Provides non-repudiation since the sender cannot deny sending the signed message.

Disadvantages of digital signatures:

• Performance: Computationally expensive algorithms may pose challenges for re-source-constrained IoT devices.

• Key management: Proper management and distribution of public keys are crucial for digital signature schemes to function correctly

Lightweight Authentication Protocols:

Lightweight authentication protocols, such as LEAP [17] and SLAP [18], are designed for IoT environments, catering to IoT devices' unique requirements and constraints. These protocols ensure security and privacy while minimizing overhead compared to traditional methods.

IoT Device Security Analysis 5:

Researchers emphasize balancing security and resource efficiency in these protocols [19], [20].

Advantages:

• Resource-efficient: Reduces computational complexity, energy consumption, and communication overhead for resource- constrained IoT devices.

• Scalability: Accommodates large-scale IoT networks, enabling secure communication between many devices.

Disadvantages:

• Security-performance trade-offs: May sacrifice some security features to achieve resource efficiency, potentially increasing vulnerability to attacks.

• Customization: Implementing these protocols may require tailoring to the specific IoT application, adding complexity to the development process

2.2 Security Standards and Protocols in IoT

This section provides an overview of the most prevalent security standards and protocols utilized in IoT device communication, focusing on the context of message authentication. We explore each standard and protocol's usage, advantages, and disadvantages [21], [22].

TLS/SSL (Transport Layer Security/Secure Sockets Layer):

TLS/SSL are cryptographic protocols ensuring secure communication in IoT applications and protecting data confidentiality and integrity. They use symmetric and asymmetric encryption for secure connections and message exchange.

Advantages:

• Robust security: Offers encryption for data confidentiality and integrity and supports mutual authentication for verifying device and server identities.

Disadvantages:

• Resource-intensive: This may cause performance issues for resource-constrained IoT devices.

• Limited applicability: Incompatible with non-TCP-based protocols, restricting use in some IoT scenarios.

DTLS (Datagram Transport Layer Security):

DTLS, derived from TLS, provides secure communication for datagram-based transport protocols, such as UDP, maintaining TLS security benefits while adapting to connectionless protocols. It is helpful in IoT environments relying on connection-less transport protocols like CoAP over UDP.

Advantages:

DTLS retains TLS security and suits low-latency IoT scenarios where TCP isn't preferred.

Disadvantages:

DTLS can be resource-intensive for IoT devices and, due to datagram protocols, may need more reliable communication than TCP.

6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks):

6LoWPAN enables low-power IoT devices to communicate over IPv6 networks by adapting IPv6 packets for short-range wireless links. It includes link-layer encryption and authentication and supports higher-layer security protocols, like IPsec, for end-to-end network security.

Advantages:

• 6LoWPAN is designed for resource-constrained IoT devices, providing efficient low-power communication and IPv6 compatibility for end-to-end addressing.

Disadvantages:

• 6LoWPAN's security focuses on the link layer, requiring improvements for multi-hop communication. Implementing higher-layer security is challenging for con-strained devices due to computational requirements.

2.3 Analysis of Authentication Methods and Security Standards

This section analyzes various authentication methods and security standards employed in IoT device communication, considering their applicability, strengths, and weaknesses.

2.3.1 Symmetric and Asymmetric Cryptography

•Symmetric cryptography is fast and suitable for resource-constrained IoT devices but faces key distribution and management challenges, creating potential vulnerabilities.

•Asymmetric cryptography enhances security and simplifies key distribution but may be unsuitable for resource-constrained IoT devices due to computational intensity.

2.3.2Digital Signatures and Lightweight Authentication Protocols

•Digital signatures employ asymmetric cryptography to verify the authenticity and integrity of a message. They provide non-repudiation and help protect against man-in-the-middle attacks. However, digital signatures may only be suitable for some IoT scenarios due to their resource-intensive nature.

•Lightweight authentication protocols reduce computational and communication overhead while maintaining sufficient security. Explicitly designed for resource-constrained IoT devices, these protocols offer an attractive option for securing IoT communication. However, some lightweight protocols may sacrifice security features to achieve efficiency, potentially exposing IoT systems to attacks.

2.3.3 TLS/SSL, DTLS, and 6LoWPAN

• TLS/SSL ensures robust security for IoT communication, maintaining data confidentiality and integrity. However, its resource intensive nature may only be suitable for some IoT devices.

• DTLS extends the security benefits of TLS to connectionless transport protocols but shares similar performance drawbacks with TLS/SSL.

• 6LoWPAN suits resource-constrained IoT devices, offering efficient IPv6 communication. Its link-layer security may need enhancement for multi-hop communication, and implementing higher-layer protocols could be challenging.

2.3.4 Comparison and Discussion

Selecting IoT authentication methods and security standards depends on application needs and limitations. Symmetric cryptography and lightweight protocols suit resource-limited devices; asymmetric cryptography and digital signatures offer higher security but demand more resources. Weigh the pros and cons of security standards, considering application requirements like computational capacity, energy consumption, latency, and security needs.

Comparison of Authentication Methods:

Table 1 compares symmetric and asymmetric cryptography, digital signatures, and lightweight authentication protocols to better understand the differences between authentication methods. The comparison considers performance, computational complexity, bandwidth requirements, and security levels, helping readers choose a suitable authentication method for their IoT applications based on specific needs and constraints.

Table 1. Comparison of Authentication Methods in IoT

Authentication Methods	Performance	Computational Complexity	Bandwidth Requirements	Security Level
Symmetric Cryptography	High	Low	Low	Moderate
Asymmetric Cryptography	Moderate	High	Moderate	High
Digital Signatures	Moderate	High	Moderate	High
Lightweight Authentication	High	Low/Moderate	Low/Moderate	Moderate/High

Comparison of Security Standards:

Table 2 compares TLS/SSL, DTLS, and 6LoWPAN, considering performance, computational complexity, bandwidth requirements, and security levels, providing an overview of the security standards. This comparison helps readers evaluate each standard's pros and cons and select the most appropriate one for their IoT applications.

Table 2. Comparison of Security Standards in IoT

Security Standards	Performance	Computational Complexity	Bandwidth Requirements	Security Level
TLS/SSL	Moderate	High	Moderate	High
DTLS	Moderate	High	Moderate	High
6LoWPAN	High	Low/Moderate	Low	Moderate

2.4 Recommendations and Future Research Directions

This section recommends selecting appropriate authentication methods and security standards for IoT applications and discusses potential future research directions.

2.4.1 Selecting Authentication Methods and Security Standards

Selecting suitable authentication methods and security standards for IoT applications involves considering factors like computational capacity, energy consumption, latency requirements, and security needs. Here are some recommendations:

- Use symmetric cryptography and lightweight authentication protocols for resource-constrained devices to minimize overhead and energy consumption.

- For higher security and non-repudiation, consider asymmetric cryptography and digital signatures, noting increased computational demands.

- Select a security standard based on the communication protocol; e.g., use DTLS for connectionless transport protocols instead of TLS/SSL.

- Evaluate the scalability and key management ease for the chosen authentication method as they impact IoT system security.

- Regularly assess and update security measures against emerging threats and vulnerabilities.

2.4.2 Future Research in IoT Authentication and Security Standards

Possible research directions for IoT authentication and security include:

- Developing advanced lightweight cryptographic algorithms for IoT devices.

- Investigating novel key management and distribution schemes for IoT's unique challenges.

- Integrating machine learning and AI into authentication and security protocols.

- Assessing the impact of emerging technologies like quantum computing on security standards and developing quantum-resistant solutions.

- Conducting interdisciplinary research to gain insights into human factors affecting IoT security and integrating these findings into the design and development of security measures.

Exploring these areas can help advance IoT security and address changing needs, ensuring safety and reliability.

3. CONCLUSIONS

The increasing integration of IoT devices has heightened concerns regarding secure and reliable communication. This study has provided a comprehensive analysis of various message authentication techniques, including symmetric and asymmetric cryptography, digital signatures, and lightweight authentication protocols, alongside an evaluation of existing security standards. The findings highlight the trade-offs between security, computational efficiency, energy consumption, and latency, which are crucial considerations for IoT applications.

Selecting the appropriate authentication method is essential to ensuring data integrity and preventing unauthorized access in resource-constrained environments. While existing techniques offer varying levels of security and efficiency, challenges remain in achieving a balance between robustness and performance. To address these challenges, we propose several enhancements, including optimizing authentication protocols for low-power devices and improving cryptographic algorithms to reduce computational overhead while maintaining strong security guarantees.

Future research should focus on developing novel authentication mechanisms that cater to the unique constraints of IoT ecosystems. Additionally, refining security standards to accommodate emerging IoT applications will be essential for maintaining secure and scalable device communication. By adopting adaptive and context-aware authentication strategies, the IoT landscape can better mitigate security threats and support the continued growth of interconnected systems.

4. REFERENCES

[1] Halak, B., Yilmaz, Y., & Shiu, D. 2022. Comparative analysis of energy costs of asymmetric vs symmetric encryption-based security applications. IEEE Access, 10, 76707–76719.

[2] Saikumar, N., Krishnan, R.B., Meganathan, S., Raajan, N.R. 2016. An encryption approach for security

enhancement in images using key based partitioning technique. In: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), pp. 1-4. Nagercoil, India (2016). DOI: 10.1109/ICCPCT.2016.7530327.

[3] Beevi, L. S., Merlin, G., & MoganaPriya, G. 2016. Security and privacy for smart grid using scalable key management. In 2016 international conference on electrical, electronics, and optimization techniques (iceeot) (pp. 4716–4721).

[4] Bernstein, D. J. 2008. Chacha, a variant of salsa20. In Workshop record of sasc (pp. 3–5).

[5] Wheeler, D.J., Needham, R.M.1995. TEA, a tiny encryption algorithm. In: Proceedings of the Second International Workshop on Fast Software Encryption. pp. 363-366. Springer, Heidelberg (1995).

[6] Diffie, W., & Hellman, M. 1976. New directions in cryptography. IEEE transactions on Information Theory, 22(6), 644–654.

[7] Rivest, R. L., Shamir, A., & Adleman, L. M. 1978. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126. DOI: 10.1145/359340.359342.

[8] Halak, B., Yilmaz, Y., Shiu, D.: Comparative Analysis of Energy Costs of Asymmetric vs Symmetric Encryption-Based Security Applications. IEEE Access 10, 76707-76719 (2022). DOI: 10.1109/ACCESS.2022.3192970

[9] Raza, S., Seitz, L., Sitenkov, D., & Selander, G. 2016. S3K: Scalable security with symmetric keys—DTLS key establishment for the Internet of Things. IEEE Transactions on Automation Science and Engineering, 13(3), 1270-1280. DOI: 10.1109/TASE.2015.2511301.

[10] Koblitz, N. 1987. Elliptic curve cryptosystems. Mathematics of computation, 48(177), 203–209.

[11] Regev, O.: Lattice-based cryptography. In: Proceedings of Advances in Cryptology-CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, vol. 26, pp. 131–141. Springer Berlin Heidelberg (2006). https://link.springer.com/content/pdf/10.1007/11818175_8.pdf

[12] Housley, R. 2004. Public key infrastructure (pki). John Wiley & Sons. Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ecdsa). International journal of information security, 1(1), 36–63.

[13] Anand, D., Khemchandani, V. L., & Sharma, R. K. 2013. Identity-based cryptography techniques and applications (a review). In Proceedings of the 5th international conference on computational intelligence and communication networks (pp. 343–348).

[14] Sultana, R., & Shahid, T. 2021. A Survey on Digital Signatures. International Journal of Recent Technology and Engineering, 9(4S2), 2599-2602. https://www.ijrpr.com/uploads/V2ISSUE2/IJRPR196.pdf

[15] Johnson, D., Menezes, A., & Vanstone, S. 2001. The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1, 36-63.

[16] Alnahawi, N., Schmitt, N., Wiesmaier, A., Zok, C.-M. 2023. Towards next generation quantum-safe eids and emrtds – A survey. ACM Transactions on Embedded Computing Systems.

[17] Amine Ferrag, M., Maglaras, L. A., Janicke, H., & Jiang, J. 2016. Authentication Protocols for Internet of Things: A Comprehensive Survey. arXiv e-prints, arXiv-1612. https://arxiv.org/abs/1612.07206.

[18] Aghili, S. F., Mala, H., Kaliyar, P., & Conti, M. 2019. SecLAP: Secure and lightweight RFID authentication protocol for Medical IoT. Future Generation Computer Systems, 101, 621-634. DOI: 10.1016/B978-0-12-819511-6.00016-9

[19] Saraiva, D.A.F.; Leithardt, V.R.Q.; de Paula, D.; Sales Mendes, A.; González, G.V.; Crocker, P. PRISEC. 2019. Comparison of Symmetric Key Algorithms for IoT Devices. Sensors 2019, 19, 4312. DOI: 10.3390/s19194312

[20] Gilbert, H., Robshaw, M., & Sibert, H. (2005). An active attack against HB+-a provably secure lightweight authentication protocol. Cryptology ePrint Archive, Report 2005/237. https://eprint.iacr.org/2005/237.pdf

[21] Salman, T., & Jain, R. 2019. A survey of protocols and standards for Internet of Things. arXiv preprint arXiv:1903.11549.

[22] Zeadally, S., Das, A. K., & Sklavos, N. 2021. Cryptographic technologies and protocol standards for Internet of Things. Internet of Things, 14, 100075. DOI: 10.1016/j.iot.2019.100075.