Ingénierie des Systèmes d'Information
Vol. 27, No. 4, August, 2022, pp. 637-643
Journal homepage: http://iieta.org/journals/isi

Analysis and Validation of Lightweight Authentication Algorithm

Pritam Salankar[1*], Vinay Avasthi[1], Ashutosh Pasricha[2]

[1] School of Computer Science, University of Petroleum and Energy Studies, Dehradun 248007, India
[2] Schlumberger, South Delhi 110067, India

Corresponding Author Email: p.salankar@gmail.com

https://doi.org/10.18280/isi.270414

Received: 9 April 2022
Accepted: 8 August 2022

Keywords:
IoT, CoAP, DTLS, lightweight mutual authentication, ROT 18, validation, simulation

ABSTRACT

The Constrained Application Protocol (CoAP) is extensively used in several industrial Internet of Things (IoT) applications. Using heavy-weight algorithms is not feasible in resource-constrained IoT environments, and lightweight solutions are vulnerable to security attacks. The trade-off between computing cost and security strength plays a significant role in deciding the right solution. Therefore, developing a lightweight security mechanism with a higher security level is paramount. Therefore, a lightweight authentication with Two-way Encryption for Secure Transmission in CoAP Protocol (LATEST) was proposed to achieve secure data transfer with a lightweight security mechanism. The proposed LATEST ensures high confidentiality and integrity against modification, impersonation, and replay attacks. Security analysis and validation tests are performed with the help of validation tools to measure the strength of the proposed LATEST mechanism. Testing and validation proved that the performance and security level improved significantly.

1. INTRODUCTION

Recently, the Internet of Things (IoT) has supported a broad range of smart applications by enabling the connection between tiny sensing devices that utilize advancements in information and communication technologies [1-3]. The Constrained Application Protocol (CoAP) is a reliable and lightweight protocol designed for the constrained IoT lossy network environment. CoAP includes many capabilities essential for IoT, such as resource observation and discovery, congestion control mechanism, and REST (Representational State Transfer) architecture. The successful deployment of massive IoT devices for smart applications relies on secure data transmissions. IoT devices are resource constrained and deployed at low-power lossy networks with limited physical security. Thus, these networks are vulnerable to attacks that lead to significant setbacks in real-world deployments. The core content for providing CoAP security in various IoT smart applications is cryptography, a technique of secure communications. The first line of defense applied in cryptography is generating a secure key and sharing it. The existing symmetric and asymmetric encryption schemes solve the main security issues induced by the application-layer attacks. Before implementing any lightweight algorithm for IoT in any industrial application, it is essential to prove the algorithm is lightweight and at the same time, it does not compromise security. In this paper, the authors tested and validated the claim that the proposed LATEST [4] is secure and efficient by using tool-based security analysis.

2. CoAP SECURITY CONCEPTS

The main security requisites in the IoT situation are availability, lightweight solution, authentication confidentiality, privacy integrity [5-7], and resource limitations [8, 9]. It is shown in Figure 1.

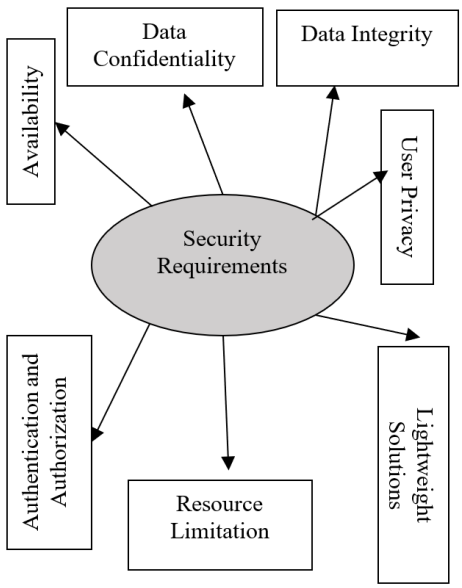

Figure 1. CoAP security requirements

Table 1 shows different symmetric and asymmetric security methods with the type of security they provide.

2.1 IoT characteristics and CoAP security challenges

There are several security challenges in IoT applications as compared to the traditional model. The following are the security challenges in IoT applications.

- IoT devices are small in size, and their battery resources are limited.

- Limited memory capacities do not allow a strong and effective security scheme to be implemented.
- Moreover, most encryption calculations require high calculation and memory power.

The IoT technologies have become pervasive in several smart applications and an integral part of human life. The IoT consists of Internet-enabled tiny sensors and has improved the lifestyle of humans. The IoT applications use those devices to monitor the environment, communicate with each other, and react to changes in their environment [1-3]. Mostly, these IoT devices apply CoAP to communicate at the application layer [10]. With the rapid development of IoT and its usage among more people to acquire various services, IoT users face emerging network security challenges [11, 12]. The core content of the IoT security system is cryptography. The characteristics of IoT are listed in Table 2.

Table 1. CoAP security concepts

Technique	Type	Security Services Offered
Block Cipher	Symmetric	Authentication, Data Confidentiality, and Data Integrity
Stream Cipher		Authentication, Data Integrity, and Data Confidentiality
Hash Function		Authentication and Data Integrity
MAC		Authentication and Data Integrity
Authenticated Cipher		Authentication, Data Integrity, and Data Confidentiality
Public-Key Encryption	Asymmetric	Data Confidentiality, Authentication, and Data Integrity
Digital Signature		Data Integrity, Authentication, and Non-repudiation

Table 2. IoT Characteristics

IoT Characteristics	Explanation
Interconnectivity	The network entities are connected to global information and infrastructure
Things-related services	Integrity, Data confidentiality, authentication, authorization, and non-repudiation
Heterogeneity	The devices can interact with others in different networks
Dynamic changes	The network topology is changed frequently because of the number of devices and their mobility
Scalability	The number of devices and network areas improves the network scalability

2.2 CoAP security and DTLS

The DTLS provides a security mechanism for CoAP over IoT applications. It is based on the TLS in the provision of security which is demonstrated in Figure 2.

Initially, the first layer is called the request/response layer, which is responsible for RESTful paradigm implementation. It allows message interchanges asynchronously among CoAP clients and servers with the support of unicast and multicast communications. It is designed for retransmitting lost packets and for maintaining communication reliability. There are four types of messages in CoAP: non-confirmable (NON), Confirmable (CON), reset (nack), and Acknowledgement (ACK). For reliable CoAP communication over UDP, Confirmable messages are used. It explores the piggyback technique for sharing the Acknowledgement (ACK) message. Furthermore, most CoAP applications apply the Datagram Transport Layer Security (DTLS) for security purposes. The DTLS offers authentication, key exchange, and protection of communication between legal entities. However, it does not ensure communication security always in IoT environments. The existing DTLS/CoAP works mostly apply symmetric or asymmetric encryption schemes and attempt to improve the security of CoAP.

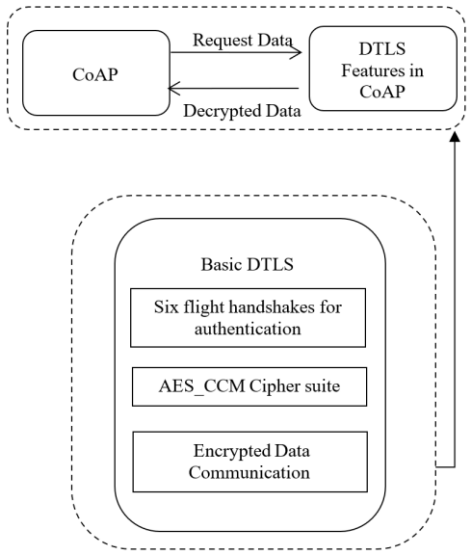

Figure 2. Basics of DTLS/CoAP

The second layer describes the DTLS/CoAP operation as mentioned below, along with the drawbacks.

1) The DTLS/CoAP architecture exchanges six flight handshake messages between IoT devices. It is not feasible for resource-restricted IoT networks.

2) Since packets get fragmented into 27-byte, it may lead to loss of data and delay in CoAP communication.

3) It is possible to make multiple copies of the same "ClientHello" messages and unnecessarily transmit them to a server. It tends to be a Denial-of-Service attack for the server. The DoS attack in DTLS/CoAP architecture consumes more resources in both bandwidth and battery.

4) The 32 bytes request message is used in DTLS/CoAP. The 32 bytes of the packet header in IoT tends to have large packet size, buffer overflow, and network congestion. If congestion occurs in the communication, the data packets are delayed, or only a few fragments are received at the server in a packet. The malicious nodes can misuse this process. Thus, a strong and lightweight authentication and security scheme needs to be developed for CoAP. Moreover, interactions between CoAP and DTLS are given in Figure 3.

The main issues associated with the DTLS/CoAP are the necessity of exchanging handshake messages. Packets get fragmented into27-byte, and a large number of small packets lead to data loss and CoAP communication delay [13]. Another main concern associated with the DTLS protocol is the likelihood of sending multiple hello messages and DOS attacks against the server. The risk of a DoS attack in DTLS/CoAP architecture consumes more CPU and battery

inputs. Large numbers of small-size packet transmissions in IoT incur packet congestion. If a blockage occurs at the communication, the gateway may obtain the delayed packet or limited fragments in a packet. In such a scenario, the gateway needs the smart sensors to resend the packets.

It tends to energy consumption, network collision, unnecessary communication delay, and packet retransmission. Thus, it is essential to incorporate the important features of DTLS in CoAP as a replacement for using DTLS in a separate channel.

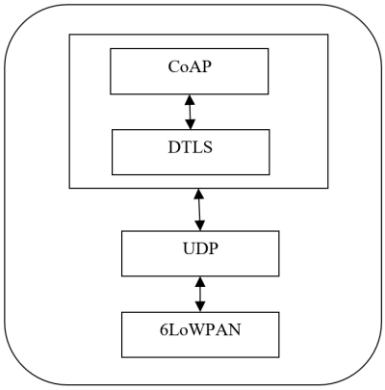

Figure 3. CoAP and DTLS communication

3. SCOPE AND MOTIVATION

Today the IoT is an emerging technology due to the enormous growth of the communication field. The interconnected devices in the IoT environment are steadily mounting. Recently, the CoAP has received much attention in research for several smart IoT applications from medical to industry since the CoAP meets the requirements of resource-constrained IoT communication. The increased presence of IoT devices in human lives tends to inherent security issues. Especially, application-dependent functions are implemented on the application layer, so a major level of security is necessary for CoAP. The CoAP is widely used in intelligent transportation systems. An intelligent transportation system controls the traffic data and monitors the transportation networks for evaluation purposes instead of controlling the vehicles by their driver. The IoT-enabled intelligent transportation system gathers real-time data from various vehicle sensors and provides a traffic route direction without delay.

In such applications, providing a secure closed environment is not possible, so the impact of attacks on CoAP for degrading the performance of those applications is high. Thus, the proposed work plans to develop a mutual and lightweight security scheme for CoAP as per the smart IoT application requirements.

Table 3. Comparison of the existing authentication schemes

Ref.	Name	Techniques	Type	Advantages	Limitations
[14]	A lightweight authentication mechanism	ECC and packet compression	Asymmetric	It reduces the overhead and energy consumption	It does not handle the key exchange overhead
[15]	Two Way Authentication	RSA	Asymmetric	It minimizes memory overhead and end-to-end latency.	High computational complexity
[16]	Lightweight security scheme	Hashing and XoR operations	-	It provides the low computational and memory cost	It can ensure data privacy only to trusted entities
[17]	Unclonable Function (PUF) based authentication protocol	ECC	Asymmetric	The ElGamal cryptosystem ensures CoAP security	It has to change the hardware for its applicability
[18]	The lightweight mutual authentication protocol	ECC	Asymmetric	It provides an access control mechanism and reliable authentication.	High computational cost
[19]	A lightweight mutual authentication scheme	AES	Symmetric	It protects the network from resource exhaustion, and DoS attacks eavesdropping, and key fabrication	Sybil attack cannot be detected
[20]	Mutual authentication scheme	Hash-Based Authentication	Symmetric	It reduces the number of message exchanges	A possibility for capturing node and key information leakage to attackers is high
[21]	Lightweight authentication and key agreement scheme	Signcryption	Symmetric	It attains the user anonymity and non-repudiation successfully	It is not suitable for non-legalized users
[22]	User authentication and anonymity scheme	ECC	Asymmetric	Reduced computational cost	It does not handle the key exchange overhead
[23]	Multi-factor authentication protocol	ECC	Asymmetric	It successfully maintains the efficiency of mutual authentication and forwards secrecy	
[24]	An improved challenge-response mechanism	New Scheme	Symmetric	It provides a secure session key agreement process	It does not protect the network against DoS attacks, impersonation attacks, and plaintext attacks
[25]	Two-level session key-based authentication mechanism	AES	Symmetric	It protects the network against replay, channel, forward, key regeneration attacks, and DoS	It fails in considering the inter-cluster key freshness and key sharing scenarios.

4. LITERATURE SURVEY AND RELATED WORK

Various works are studied and reviewed for the existing authentication scheme. Table 3 provides a detailed comparison of the existing authentication schemes.

Several secure authentications and data encryption schemes are developed for CoAP under a resource-restricted IoT environment. Many systems implement authentication schemes for lightweight security. The existing schemes face issues related to the exchange of keys, complexity of operations, advance key sharing, high computational cost, and vulnerability to new and complex attacks.

5. RESEARCH GAP

The CoAP has no built-in security scheme, so the malicious devices target the weak points of IoT to catch hold of the system [26]. The entered malicious devices start a security threat and privacy violation. Several device authentications and data encryption schemes have been developed and applied for securing CoAP communication over resource-restricted IoT devices. Most of them implement identity authentication and cryptography to achieve security [27-29]. The research gaps are discussed under three dimensions. The general research gaps in CoAP security schemes, the problems associated with the DTLS-CoAP security schemes, and existing schemes that apply AES among various symmetric encryption schemes. The general gaps in the existing research works are discussed as follows.

- As of now, a few of them have been designed with complex operations for securing the IoT CoAP communication model.
- They either apply asymmetric or symmetric encryption schemes. The later technique lacks in eliminating the disadvantages of key sharing in the early stage.
- The asymmetric method does not require performing the advanced key sharing. However, this method consumes more calculation costs than the symmetric encryption technique.
- The utilization of keys with a long lifetime and intricate computations of this type of cryptography algorithm make them non-viable for IoT devices due to their limited memory and restricted battery resources.

Therefore, there is a need to develop an effective method to lightweight those existing security schemes and make them suitable for IoT devices. Hence, these solutions fail for IoT devices. Hence, there is a need for a lightweight security solution.

Notably, the CoAP protocol failed to provide protected communication between the end devices and the server due to the tiny and resource-restricted IoT devices.

The problems associated with the DTLS-CoAP security schemes are listed as follows.

- Even though DTLS-CoAP provides security, it requires abundant resources for IoT devices.
- The DTLS lacks in consideration the resources constraint nature of IoT devices.

Most of the existing schemes apply AES among various symmetric encryption schemes. Those schemes face the following issues.

- The symmetric encryption schemes apply the same key for both encryption and decryption for a long time. If insecure authentication is processed, it may expose the key that will hamper the security of both server and client.
- The differential or linear cryptanalysis methods in AES can deduce the overall key since the original key-generated words are related. The biased inputs in the key space of AES create a space to observe the differences between the words in the cipher text.

Frequent handshake request messages to IoT devices may tend to a DoS attack. An attacker could send numerous "ClientHello" messages to a server, and the network fails. Thus, the work proposed by the author claims to improve IoT security using lightweight algorithms, reducing its complexity.

6. PROPOSED METHODOLOGY OF LIGHTWEIGHT AUTHENTICATION

An advanced level of security is essential for CoAP [6]. An external network interface connected through the application layer, such as insecure web and cloud interfaces, paves the way for entering the attacks. To solve those issues, the acceptance of authentication is prominent. An identity authentication provides access to only the authorized users, thereby minimizing attacks such as the Man-in-the-Middle, the impersonation, the reply, and the Sybil attack is possible. Thus, the research proposed by the author focuses on developing lightweight authentication mechanisms for CoAP in the IoT environment. The author develops an authentication mechanism, such as LATEST [3], for improving the adaptability of CoAP to security-critical applications.

6.1 Implementation and simulation tools

One of the important implementation tools is Contiki OS, which is a Linux-based open-source operating system. It helps in stimulating the networks with low-powered devices using a simulator. It allows IPV4 and Ipv6 Stack implementation and supports 6loWPAN, COAP, and RPL. It also supports different radio mediums. It makes a wireless connection among multiple sensor devices and packet transmissions among them. The back-end configuration tools are discussed as follows.

- **Virtual machine:** It virtualizes the network nodes and their connections. It codes the main functionality of a physical computer.
- **Ubuntu:** It is a Linux distribution, and it is based on Debian.
- **Cooja simulator:** It can simulate the network with Contiki OS by creating a virtual machine environment on Ubuntu.
- **Default Radio:** The default radio medium for implementing the network with low-power devices is ContikiMAC.
- **Network Mechanisms:** It provides TCP/IP stack for IPn6 networking, the IPv6 stack for IPv6 networking, and the Rime stack for customized lightweight networking protocols.

6.2 Performance evaluation

The proposed method validates the authenticity of the proposed LATEST mechanism using the Contiki operating system and Cooja simulator. The performance is compared to the existing mutual authentication information and the

LATEST mechanism [3]. In Cooja, the nodes are wismote mode, and the border router is Z1-Mote mode. The network area used in the simulation is 100 X 100 m^2, deployed with one border router, one server, and 28 client nodes. The range of the communication of every node is 50 m. The interval of the message transmission is 10 sec. with127 bytes and the transport layer is configured with UDP. The propagation model is the UDGM. The performance metrics are delay, energy consumption, and overhead. The performance metrics proposed in this scheme are Message Size Overhead, Delay, and Energy Consumption.

6.3 Simulation results for the proposed LATEST

The simulation results for our proposed LATEST and mutual authentication schemes by comparing delay, overhead, and energy consumption in the same scenario of 30 node topology are given in Table 4.

Table 4. Comparative results

Metric	Proposed Scheme, LATEST	Existing Scheme, Mutual Authentication
Delay (Seconds)	1.637	2.383
Energy Consumption (Joules)	1.410	1.453
Message Size Overhead (Bytes)	13.77	17.02

The first performance metric is the delay in communication. The proposed system significantly reduces the delay by reducing the delay of authentication and secures communication processes. The nodes in an IoT network are built with restricted battery power. Thus, the energy consumption metric is important in the lightweight security design, and due to the complexity of the proposed scheme, it is almost equal to the existing system. Thus, the energy consumption is very close. Finally, the message size overhead metric reveals the lightweight of the proposed authentication scheme in the network.

6.4 Validation of the results

In this section, the above results are validated**.** Several tools are used in the performance evaluation process to validate the above results. Those are listed below:

(1) Virtual machine: It helps in virtualization /emulation of the computer system. Virtual machines are built based on computer architectures, providing the main functionality of a physical computer.

(2) Ubuntu 2.0.0: It is a Linux distribution, and it is based on Debian.

(3) Contiki OS: It is an open-source operating system, and it is used in networking.

(4) Cooja simulator: It can simulate the network with multiple sensor devices and wireless communication among them. ContikiOS is run in a virtual machine environment with the Ubuntu 16.04 LTS system.

In the experimental scenario, simulation is performed as follows:

(1) Installing the Contiki OS on a virtual box machine.

(2) Implementing 30 numbers of nodes.

(3) Appending byte-break shift row transformation and restricted sequential round constant based add round keys in default AES.

The proposed security protocol with implemented cryptographic algorithms, such as Lightweight AES, is validated using Scyther, as shown in Figure 4.

The Scyther tool exploits its own language SPDL to describe protocols, roles, and parameters used. The security properties or protocol functions are given as claim events in SPDL. If not given, the Scyther can automatically generate the claim events. It is taken as input by the Scyther tool. The Scyther tool validates whether the claim events are maintained for the entire communication or not.

Using such a tool, the impact of Replay and DoS attacks can be identified. However, if an attacker traces the secret key of legitimate nodes, the malicious request messages, guessing, traceability, and data confidentiality-related attacks, may not be detected using the Scyther tool.

This is because the claim events generated for malicious traffic are similar to the legitimate ones (Figure 5).

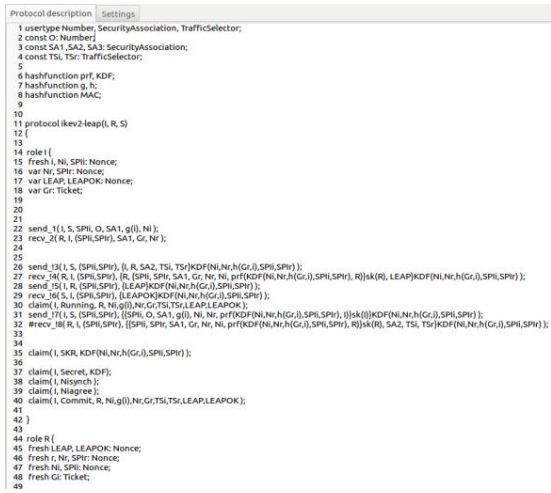

Figure 4. Scyther tool

Figure 5. Security protocol verification

After starting the verification process, a window appears. There are several rows and columns. Each row denoted one claim. The column fields are the name of the protocol, role, ID requirements, the request type parameter, state of an attack, and displaying graphic attack.

The protocol verifies under the criteria of claim, status, comments, and patterns.

Claim: It shows the individual process of the initiator, receiver, and server. Initiator performs hash functions, key derivation function, and generates the Nonce Values. Server functions depend on the results of initiator functions. After finishing the server operation, the output is sent to the receiver. It shows the final commit of the receiver side, either normal or attack.

Status: It helps to show the presence of attacks.

Comments: It is used to show the comments of attack. There are two types of comments: no attacks within bounds and at least n attacks, at most n attacks, and exactly n attacks.

Patterns: It shows the attack pattern of a network.

The following figures (Figure 6 and 7) show the presence of attack trace patterns for initiator, receiver, and server-side, and trace pattern.

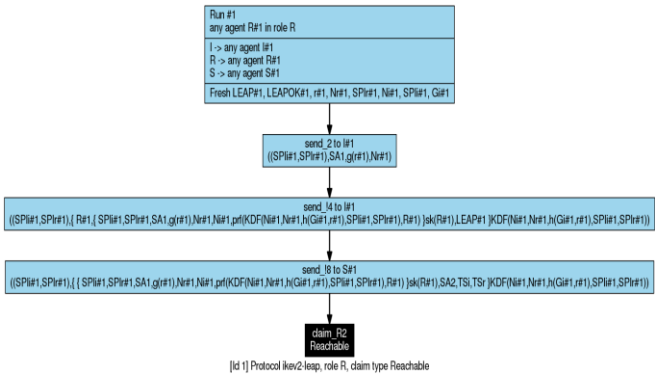

Figure 6. Presence of attacks

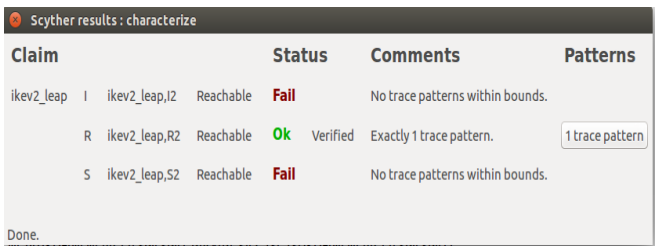

Figure 7. Trace pattern

7. CONCLUSIONS

A widely used application layer protocol is the CoAP. However, it is vulnerable to security and privacy threats over IoT applications. Most data encryption and user authentication schemes do not consider computation and communication costs. Hence, these solutions do not adapt well to resource-constrained IoT devices. To solve such issues, the proposed work has presented the LATEST scheme for resolving the authentication issues. The proposed scheme is successfully tested using simulation and security verification tools.

8. FUTURE DIRECTIONS

In the future, the following directions should be considered to improve the efficiency and security of CoAP communication.

- The data analysis is crucial for deploying the security scheme on CoAP over IoT smart applications. The machine learning algorithms can analyze the data in the gateway itself. It can further enhance the security of the CoAP communication in various IoT applications. Evaluating the CoAP performance with various encryption schemes to identify the suitable encryption algorithms for CoAP under dynamic network scenarios.
- Analyzing the impact of further network metrics on the performance of the secure CoAP should be performed to improve the security scheme against different application-layer attacks.
- Along with the analysis, systematic validating and testing of all results before implementing any method for any industrial application with the help of a validation tool is very important with different attack scenarios and topologies.

ACKNOWLEDGMENT

I take this special opportunity and express my deep gratitude to the University of Petroleum and Energy Studies for their continuous support of this work. I am also thankful to all my colleagues who always encourage me in this work.

REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4): 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

[2] Gherbi, C. (2021). Internet of things and heterogeneous networks technologies: Concepts, challenges and perspectives. Ingénierie des Systèmes d'Information, 26(4): 403-408. https://doi.org/10.18280/isi.260408

[3] Tawalbeh, L.A., Muheidat, F., Tawalbeh, M., Quwaider, M. (2020). IoT Privacy and security: Challenges and solutions. Applied Sciences, 10(12): 4102. https://doi.org/10.3390/app10124102

[4] Salankar, P.S., Avasthi, V., Pasricha, A. (2020). Lightweight CoAP based authentication scheme by applying two-way encryption for secure transmission. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(6): 404-412. https://doi.org/10.35940/ijitee.E3017.049620

[5] Fenanir, S., Semchedine, F., Harous, S., Baadache, A. (2020). A semi-supervised deep auto-encoder based intrusion detection for IoT. Ingénierie des Systèmes d'Information, 25(5): 569-577. https://doi.org/10.18280/isi.250503

[6] Ferrag, M.A., Maglaras, L.A., Janicke, H., Jiang, J., Shu, L. (2017). Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks, 2017: 6562953. https://doi.org/10.1155/2017/6562953

[7] Hassan, W.H. (2019). Current research on internet of things (IoT) security: A survey. Computer Networks, 148: 283-294. https://doi.org/10.1016/j.comnet.2018.11.025

[8] Abdulghani, H.A., Nijdam, N.A., Collen, A., Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective. Symmetry, 11(6): 774. https://doi.org/10.3390/sym11060774

[9] Obaidat, M.A., Obeidat, S., Holst, J., Al Hayajneh, A., Brown, J. (2020). A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers, 9(2): 44. https://doi.org/10.3390/computers9020044

[10] Kabalci, Y., Kabalci, E., Padmanaban, S., Holm-Nielsen, J.B., Blaabjerg, F. (2019). Internet of things applications as energy internet in smart grids and smart environments. Electronics, 8(9): 972. https://doi.org/10.3390/electronics8090972

[11] Asghari, P., Rahmani, A.M., Javadi, H.H.S. (2019). Internet of Things applications: A systematic review. Computer Networks, 148: 241-261. https://doi.org/10.1016/j.comnet.2018.12.008

[12] Das, M.L. (2015). Privacy and security challenges in internet of things. In International Conference on Distributed Computing and Internet Technology, pp. 33-48. https://doi.org/10.1007/978-3-319-14977-6_3

[13] Nastase, L. (2017). Security in the internet of things: A survey on application layer protocols. In 2017 21st International Conference on Control Systems and Computer Science (CSCS), Bucharest, Romania, pp. 659-666. https://doi.org/10.1109/CSCS.2017.101

[14] Kumar, P.M., Gandhi, U.D. (2020). Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. The Journal of Supercomputing, 76(6): 3963-3983. https://doi.org/10.1007/s11227-017-2169-5

[15] Jan, M.A., Khan, F., Alam, M., Usman, M. (2019). A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems, 92: 1028-1039. https://doi.org/10.1016/j.future.2017.08.035

[16] Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F.B., Rodriguez, J., Bicaku, A., Bastos, J. (2017). A lightweight authentication mechanism for M2M communications in industrial IoT environment. IEEE Internet of Things Journal, 6(1): 288-296. https://doi.org/10.1109/JIOT.2017.2737630

[17] Wallrabenstein, J.R. (2016). Practical and secure IoT device authentication using physical unclonable functions. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), Vienna, Austria, pp. 99-106. https://doi.org/10.1109/FiCloud.2016.22

[18] Li, N., Liu, D., Nepal, S. (2017). Lightweight mutual authentication for IoT and its applications. IEEE Transactions on Sustainable Computing, 2(4): 359-370. https://doi.org/10.1109/TSUSC.2017.2716953

[19] Jan, M.A., Nanda, P., He, X., Tan, Z., Liu, R.P. (2014). A robust authentication scheme for observing resources in the internet of things environment. In 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, Beijing, China, pp. 205-211. https://doi.org/10.1109/TrustCom.2014.31

[20] Yoon, S., Kim, J. (2017). Mutual authentication scheme for lightweight IoT devices. In 2017, Eleventh International Conference on Emerging Security Information, Systems and Technologies.

[21] Liu, J., Ren, A., Zhang, L., Sun, R., Du, X., Guizani, M. (2019). A novel secure authentication scheme for heterogeneous internet of things. In ICC 2019-2019 IEEE International Conference on Communications (ICC), Shanghai, China, pp. 1-6. https://doi.org/10.1109/ICC.2019.8761951

[22] Li, C.T., Wu, T.Y., Chen, C.L., Lee, C.C., Chen, C.M. (2017). An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. Sensors, 17(7): 1482. https://doi.org/10.3390/s17071482

[23] Dhillon, P.K., Kalra, S. (2018). Multi-factor user authentication scheme for IoT-based healthcare services. Journal of Reliable Intelligent Environments, 4(3): 141-160. https://doi.org/10.1007/s40860-018-0062-5

[24] Mahmood, Z., Ning, H., Ghafoor, A. (2016). Lightweight two-level session key management for end user authentication in Internet of Things. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 323-327. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.78

[25] Li, X., Peng, J., Kumari, S., Wu, F., Karuppiah, M., Choo, K.K.R. (2017). An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Computers & Electrical Engineering, 61: 238-249. https://doi.org/10.1016/j.compeleceng.2017.02.011

[26] Shelby, Z., Hartke, K., Bormann, C. (2014). The constrained application protocol (CoAP). Internet Engineering Task Force (IETF) RFC-7252. http://dx.doi.org/10.17487/RFC7252

[27] Gharaibeh, A., Salahuddin, M.A., Hussini, S.J., Khreishah, A., Khalil, I., Guizani, M., Al-Fuqaha, A. (2017). Smart cities: A survey on data management, security, and enabling technologies. IEEE Communications Surveys & Tutorials, 19(4): 2456-2501. https://doi.org/10.1109/COMST.2017.2736886

[28] Eckhoff, D., Wagner, I. (2017). Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Communications Surveys & Tutorials, 20(1): 489-516. https://doi.org/10.1109/COMST.2017.2748998

[29] Yu, M., Zhuge, J., Cao, M., Shi, Z., Jiang, L. (2020). A survey of security vulnerability analysis, discovery, detection, and mitigation on IoT devices. Future Internet, 12(2): 27. https://doi.org/10.3390/fi12020027