Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Secure Authentication Scheme for CoAP for Communication on Internet of Things (IoT)

Mohammad Reza Hosenkhan [1], Binod Kumar Pattanayak [2]
[1] *Faculty of Information and Communication Technology, Universite des Mascareignes, Mauritius. Email: rhosenkhan@udm.ac.mu*
[2] *Department of Computer Science and Engineering, Institute of technical education and Research, Siksha 'O' Anusandhan Deemed to be University, Bhubaneswar, Odisha, India. Email: binodpattanayak@soa.ac.in*

ARTICLE INFO

Received: 28 Dec 2024

Revised: 21 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

Security issues have arisen when billions of resource-constrained devices that connect to the Internet via the Internet of Things (IoT). This research emphasizes enhancing communication security in IoT systems using the Constrained Application Protocol (CoAP) by introducing a lightweight authentication method. The proposed approach utilizes a lightweight AES-based block cipher and dynamic one-time passkey generation for secure client device authentication. The technique was executed and verified in a simulated IoT environment utilizing resource-limited devices. Experimental findings indicate that the proposed authentication approach incurs a negligible authentication time overhead (~18 ms) and exhibits low resource usage, rendering it highly appropriate for limited situations. The model's resilience against surveillance, replay attacks, and man-in-the-middle attacks is further verified by security assessments. The findings validate the importance of the suggested strategy in improving secure communication inside IoT networks.

Keywords: IoT, CoAP, Lightweight Block Cipher, Security, Authentication.

INTRODUCTION

Internet of Things (IoT) system encompasses a large number of heterogeneous resource-constrained wireless devices that are connected to the global Internet and communicate among themselves autonomously [1]. Experts predict that the number of devices connected to the IoT environment may reach approximately 75 billion by the year 2025. Taking into consideration the dimension of IoT systems, security imposes a major challenge for communication on IoT. The heterogeneity of IoT environment leads to varieties of vulnerabilities during communication among the devices. In order to ensure secure communication on IoT environment, various security measures have been addressed by the researchers worldwide [2]. One of the major issues in security provisioning on IoT is the problem of device authentication. In addition to it, the process of communication needs to be protected from the malicious attackers. Security provisioning in IoT devices can be achieved using cryptographic algorithms. Further, the wireless devices that are constrained with limited storage cannot implement complex cryptographic algorithms. Hence, lightweight block ciphers can be useful for implementation of cryptographic algorithms for efficient authentication of IoT devices during communication. In this work, we implement lightweight AES based block cipher for encryption/decryption and the observed results justify the improvement in secure communication of IoT devices [3].

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

IoT Architecture

The protocol architecture of IoT is depicted in Fig.1 [4].

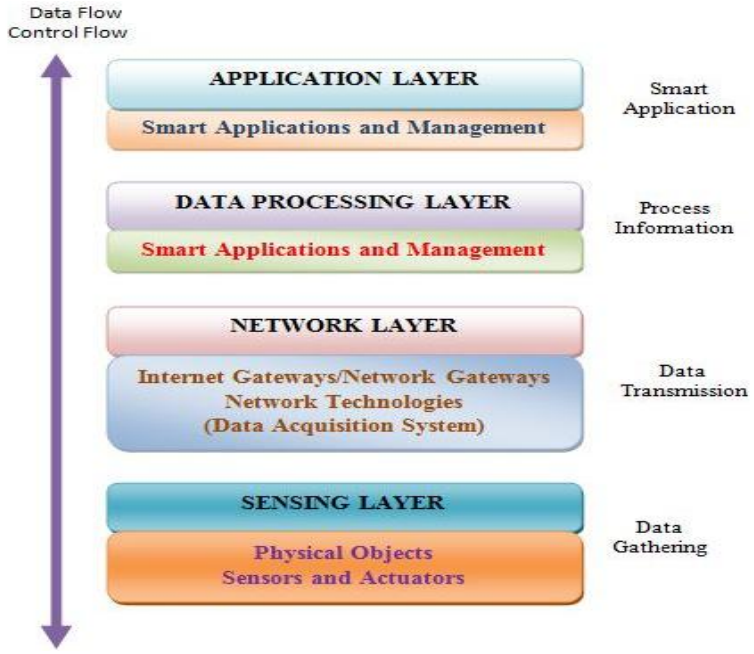

Fig.1: 4-Layer IoT Architecture

It comprises of four different layers, namely, sensing layer, network layer, data processing layer and application layer. The sensing layer represents the lowermost layer in the protocol stack of the IoT ecosystem. It encompasses various sensors and actuators. The sensors are necessary for collecting information from the environment with respect to the underlying application. For example, an environment monitoring IoT system would require data about the environment such as air pollution level, CO_2 level etc. [4]. Similarly, a IoT based agricultural monitoring system may require data about various characteristics of a plant [5]. The actuators are meant for taking necessary actions as required following sensing and analyzing of data. The network layer is responsible for transmitting the sensed by sensors data to the IoT ecosystem via gateways. The network layer incorporates data acquisition system (DAS) that deals with data aggregation and conversion if necessary (e.g., conversion of analog data to digital form). The gateways also perform the tasks of malware protection and data filtering. Data processing layer represents the basic processing unit of a IoT ecosystem. Here, received from network layer data are analyzed and pre-processed before being sent to the data centers from where the specific applications can access the pre-processed and analyzed data. The uppermost layer in the IoT protocol stack is the application layer that supports the user applications which enable the users to use the relevant data from the cloud or data centers.

IoT Security Issues and Challenges

A IoT ecosystem comprising of billions of heterogeneous devices is vulnerable to various threats from malicious users. The IoT security issues and challenges are detailed below [6].

- **Vulnerabilities:** IoT systems are very often prone to vulnerabilities for the reason that the IoT devices have limited computing capabilities and do not have any in-built security mechanism to get protected against the vulnerabilities.
- **Malware:** Irrespective of the fact that the IoT devices possess limited computing capacity, still they can be infected by malware. The most frequently encountered malware is the *IoT botnet malware*.
- **Cyberattacks:** Infected and hijacked IoT devices are very often used by the malicious attackers for distributed-denial-of-service (DDoS) attacks and also as a mean for attacking more devices in the network.

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Information Theft:** Since the IoT devices during communication are exposed to the global network environment, there arises a higher probability of the identity as well as the personal information of a user being exposed that can be accessed by the malicious users.
- **Device Misconfiguration:** Negligence in security provisioning as well as weak user login credentials make the device prone to external threats with a higher probability.
- **Authentication:** Every IoT device is assigned with a unique radio frequency identifier (RFID) for its identification in the network. Furthermore, during communication, it is necessary that the data must reach the desired user for which authentication becomes essential.

In this work, we address the issue of authentication by virtue of designing a secure model using cryptographic algorithms.

COAP ARCHITECTURE

Constrained Application Protocol (CoAP) represents an application layer communication protocol in the IoT protocol stack. It represents a two-layer protocol that is depicted in Fig.2 [7].

Fig.2: CoAP Architecture

The two layers are Message layer and Request/Response layer. The messages layer here deals with User Datagram Protocol (UDP) and asynchronous switching and, the request/response layer is responsible for dealing with request/response messages that primarily refers to the communication procedure within the IoT environment.

Message Layer Model

Message layer model in CoAP operates with four types of messages, namely, CON (confirmable), NON (non-confirmable), ACK (acknowledgement) and RST (reset).

Reliable Message Transport: In this procedure, a client sends a CON message to the server in anticipation to which the server sends back a ACK message to the client and on receiving ACK message, the communication can resume (Fig.3). In case, the server fails to process the message from the client, it replaces ACK by an RST message following which the connection is terminated.

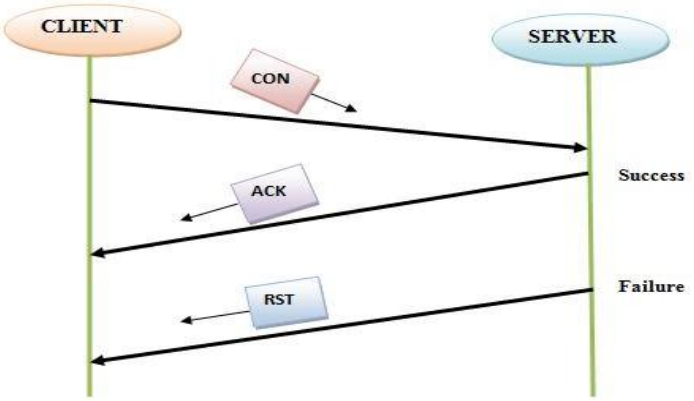

Fig.3: Reliable Message Transport

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Unreliable Message Transport: In this procedure, the client sends a NON message and if the server successfully processes the message, then no ACK is sent back and the communication can resume after this. But, if the server fails to process the message, it sends back an RST message to the client following which the connection is terminated (Fig.4).

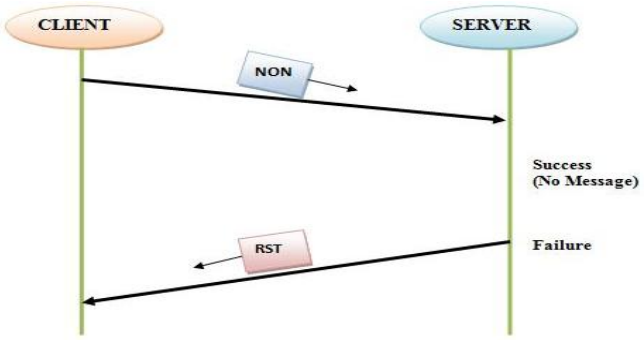

Fig.4: Unreliable Message Transport

Request/Response Layer Model

Piggy-backed Model: In this approach, the client sends a CON or NON message and immediately receives an ACK message in response to the CON message in both successful and failure situations that is depicted in Fig.5. As it can be observed from Fig.5, if the server processes the message successfully, then it sends the ACK message along with a success response token and in case of a failure, it sends an ACK message with a failure response code.

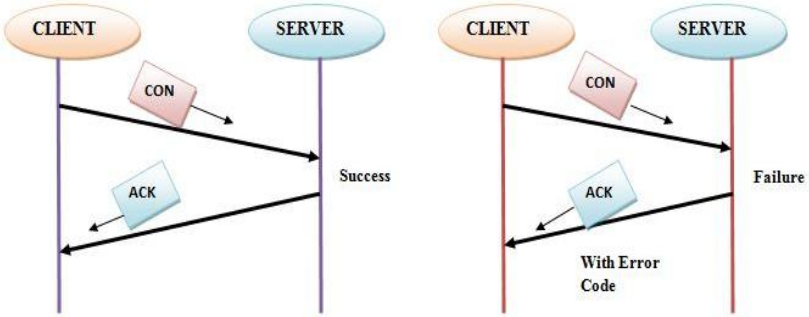

Fig.5: Exchange of Success and Failure Response Messages

***Separate Response Model*:** If a client sends a CON message which the server fails to response immediately, then the client repeats the CON message and on receiving the second CON message, the server sends back an empty ACK message to the client. When the server is ready, it sends a CON message to the client and the client in response sends back an ACK message to the server in order to confirm the CON message irrespective of whether it's a request or response message. This model is depicted in Fig.6.

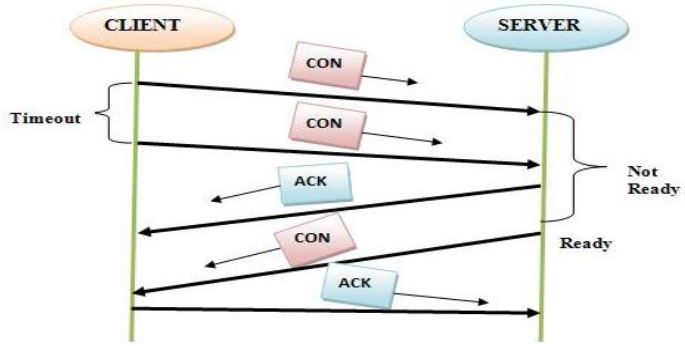

Fig.6: Get Request with A Separate Message

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

***Non-Confirmable Request and Response*:** In this procedure, the client sends a NON type message which need not be confirmed. However, the server in response to it, sends back a NON type message to the client (Fig.7).

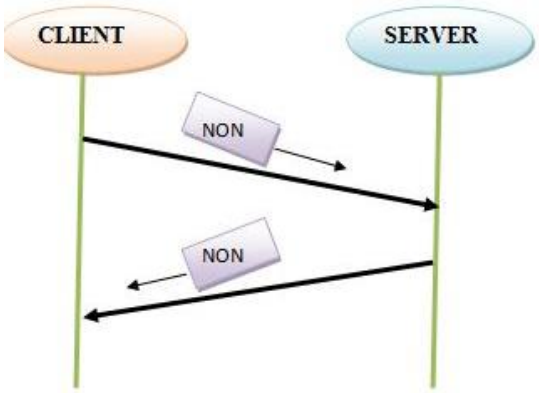

Fig.7: NON-Confirmable Request and Response

CoAP Message Format

The format of a CoAP message is shown in Fig.8 [8]. As it can be observed from Fig.8, the smallest in size CoAP message comprises of 4 bytes if version, tokens and options are omitted from it. The first 2 bits represent the version of CoAP. The messages are of two types: request and response. The next 2 bits refer to the type of message:

Request (00: CON and 01: NON)

Response (10: ACK and 11: RST)

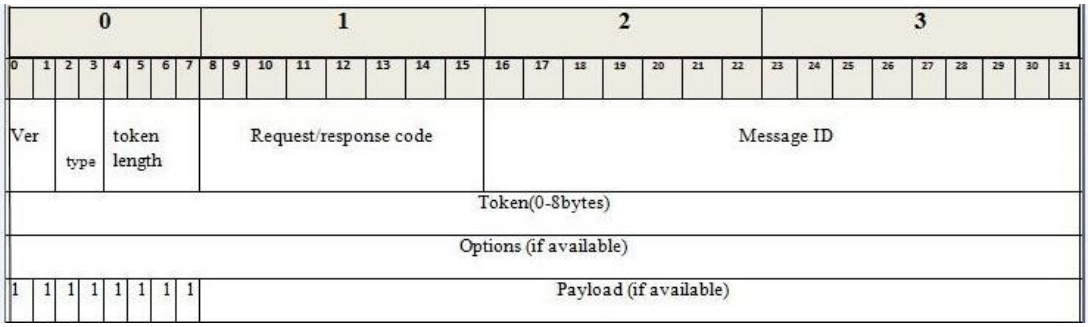

Fig.8: CoAP Message Format

The next 4 bits hold the length of the token field which may vary from 0 to 8 bytes. Then, the following 1 byte holds the request/response code. The next two bytes represent the message ID. The next field may hold 0 or more tokens up to 8 bytes followed by 0 or more options. Then follows one byte of 1's followed by the payload if available.

In this work, we use CoAP for communication between IoT devices and address the issue of authentication using cryptographic scheme.

RELATED WORK

Communication on IoT has been significantly challenging for the reason that a large spectrum of heterogeneous resource constrained wireless devices is connected to it that imposes a wide range of security threats and for effective communication, these security challenges need to be addressed. Significant amount of research work has been done in this direction by various researchers and scientists around the globe. The authors in [9] propose a strategy for CoAP security that uses Datagram Transport Layer Security (DTLS) mechanism wherein DTLS compression techniques sufficiently reduces the additional number of bits meant for security provisioning. A comprehensive analysis of various congestion control mechanisms for IoT environment has ben conducted by the authors in [10]. A security scheme for supporting the authentication procedure and access control on CoAP (AAC-CoAP) has been

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

proposed by the authors in [11] and as claimed by the authors, it improves the IoT security significantly. A security scheme having used TACACS+ has been proposed by the authors in [12] that additionally supports the process of authentication, access control as well as accounting. The experimental results justify its usage in compatibility with various IoT devices. An analysis of Distributed Denial of Service Attack that use Amplified Reflection (AR-DDoS) has been carried out by the authors in [13] and it was reported that AR-DDoS attacks often abuse CoAP running on an IoT environment and the results were found to be consistent. Interoperability between smart devices in IoT environment across multiple platforms presents a major challenge due to resource constraints that can be successfully overcome using AllJoyn framework. Design and implementation of an application that serves as a bridge between AllJoyn and CoAP networks has been conducted by the authors in [14]. It leverages advanced CoAP features and provides AllJoyn applications with a rich low-level interface in order to interact with multiple CoAP servers that host CoAP resources. The experimental results as claimed by the authors show that the said implementation extensively validates a real test case and has been proved to work effectively. Validation of CoAP in a low-power Personal Area Network (PAN) in order to determine the effectiveness of CoAP as an application protocol for IoT environment, has been conducted by the authors in [15]. CoAP being a powerful messaging protocol manages the communication between the resource constrained devices and the IoT environment. However, these constrained devices generate large number of messages that most often leads to congestion in the IoT environment. To address this issue, the authors in [16] devise an effective congestion control algorithm for CoAP that necessarily ensures effective network operation thereby providing effective usage of the network resources. The authors in [17] develop a secure IoT medical based on CoAP protocol for collecting data for COVID-19 identification thereby adding a security layer to CoAP protocol for encrypting data using AES algorithm. CoAP has been applied to a web-based remote-control platform by the authors in [18] that can be effectively used in public networks as well as large networks. Since CoAP relies on an unreliable transport layer protocol, that is UDP, loss-based congestion control algorithms are incorporated into CoAP in order to counter congestion. A TCP based congestion control algorithm, BDP-CoAP, has been proposed by the authors in [19] that is capable of mitigating congestion more effectively thereby improving the throughput of the network. CoAP has been used as the application layer protocol in a IoT healthcare remote monitoring system by the authors in [20]. Demand Response (DR) messaging protocols rely on HTTP application protocol on IoT environment for messaging services, but however, it is less effective for resource constrained devices. To overcome this issue, the authors in [21] propose CoAP-based DR messaging strategy that necessarily reduce network overhead significantly.

PROPOSED MODEL FOR IOT AUTHENTICATION

Our proposal pertains to a lightweight authentication model based on CoAP that facilitates secure communication in an IoT environment. The model implements a cryptographic technique requiring a client device to authenticate with the server using a dynamically generated one-time passkey before commencing communication. The client and server utilize a lightweight encryption method founded on the Advanced Encryption Standard (AES) with a 128-bit key length. AES-128 provides a robust equilibrium between security and computational performance, rendering it suitable for resource-limited IoT devices. The proposed framework enhances the resilience of IoT communication by regularly renewing the passkey and encrypting authentication exchanges, thereby mitigating risks such as replay attacks, unauthorized access, and man-in-the-middle assaults.

RESULT ANALYSIS

In an IoT-simulated environment, the proposed authentication model was implemented and validated. The experimental configuration included Raspberry Pi 3 Model B units, each featuring a 1.2 GHz quad-core processor and 1 GB of RAM. Communication was established using a Wi-Fi 802.11n network functioning at 2.4 GHz. The CoAP protocol stack was built on the Contiki operating system, and lightweight AES-based encryption techniques were created using Python. For a secure connection, 50 IoT devices were simulated in order to verify the model's efficacy. Each device utilized the CoAP protocol and implemented a lightweight block cipher-based authentication method before initiating a server connection.

Authentication Time Analysis

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The authentication time was calculated as the interval between a client's authentication request and the subsequent server acknowledgment. In the conventional CoAP configuration without any authentication method, the mean authentication duration was recorded as 50 milliseconds. On the other hand, the proposed model, which comprises lightweight AES-based authentication, demonstrated an average authentication time of 68 milliseconds. The implementation of the encryption process thus incurred an extra cost of around 18 milliseconds. Figure 9 illustrates that the proposed authentication approach slightly raises authentication time relative to regular CoAP. Nonetheless, the overhead will be satisfactory for a secure IoT connection. However, considering the significant enhancement in security offered by dynamic key generation and encryption, this slight increase in authentication duration is seen as acceptable for resource-limited IoT environments.

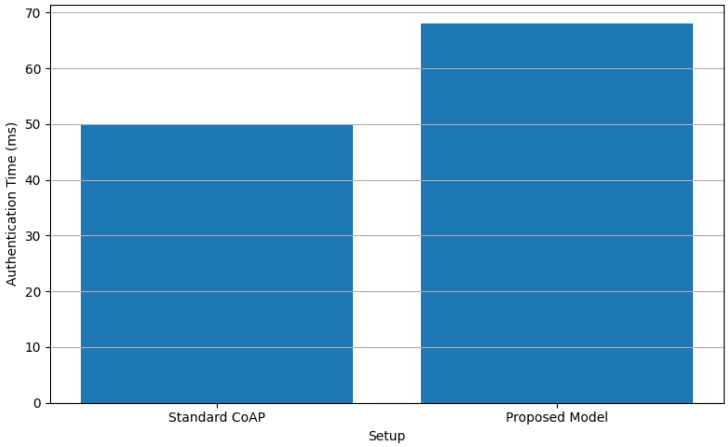

Figure 9: Comparison of Authentication Time

Usages of the Resources (CPU & RAM)

The effectiveness of the proposed authentication techniques was assessed by analyzing resource usage, such as RAM consumption and CPU utilization. In conventional CoAP connection without encryption, the average RAM use was roughly 23 KB, while CPU utilization was approximately 18%. Following the lightweight AES-based authentication implementation, RAM use climbed marginally to 27 KB, while CPU usage elevated moderately to 23%. The supplementary resource burden imposed by the encryption process is negligible and is comfortably within acceptable parameters for standard IoT devices. These results demonstrate that, despite enhanced security measures, the model retains a lightweight configuration, rendering it exceptionally appropriate for implementation in resource-limited settings where memory and processing capabilities are scarce. The comparison depicted in Fig. 10 indicates that the proposed model exhibits minimal resource consumption, confirming its viability for implementation in resource-limited IoT devices.

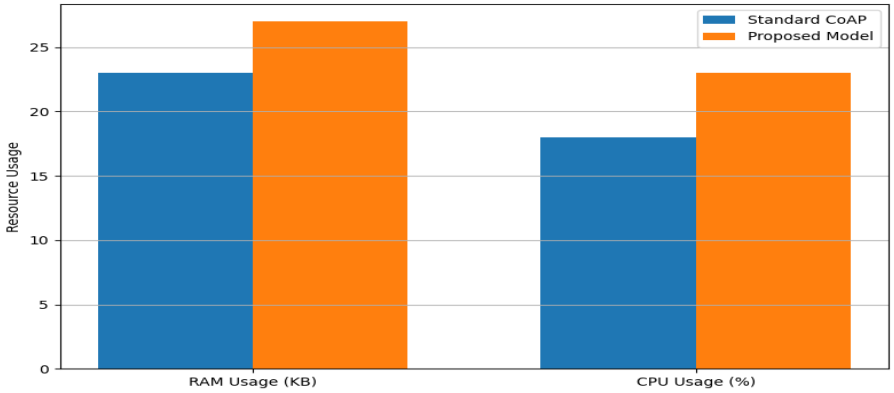

Figure 10: Comparative Analysis of Resource Utilization

Security Analysis

Journal of Information Systems Engineering and Management
2025, 10(44s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The proposed model's security efficacy was evaluated against several prevalent attack scenarios often seen in IoT environments. To mitigate replay attacks, the model utilizes a one-time passkey method that promptly invalidates previously used keys, preventing the reuse of old authentication credentials. The hazards of spying are reduced by encrypting session beginning signals, which prevents unauthorized interception and access to confidential information. Dynamic key generation on both the client and server sides markedly diminishes the threat of man-in-the-middle attacks by guaranteeing that authentication credentials remain non-static and unpredictable. The simulated findings affirm that the suggested approach offers robust resistance against various attacks, enhancing its appropriateness for safeguarding communication in IoT devices.

Comparative Analysis

A comparison was conducted between the proposed model and extant authentication schemes designed for CoAP-based IoT environments to obtain a more comprehensive understanding of the proposal's advantages. The AAC-CoAP model and TACACS+ security methodologies were specifically selected for assessment. AAC-CoAP provides considerable security enhancements but incurs significant communication costs, whereas TACACS+-based models exacerbate resource consumption, rendering them inappropriate for restricted IoT devices. The proposed lightweight AES-based architecture preserves a minimal resource footprint while providing robust dynamic authentication using one-time passkeys. Furthermore, the dynamic key updating in the proposed model offers an extra degree of security that is absent in static key-based methods. The proposed approach, as outlined in Table 1, attains an improved equilibrium among security robustness, computing efficiency, and applicability for practical IoT implementations.

Table 1: Comparative Analysis of Authentication Models for CoAP-based IoT Communication

Features	AAC-CoAP [11]	TACACS+ based CoAP [12]	Proposed Approach
Authentication Overhead	Moderate	High	Low
Resource Consumption	High	Very High	Low
Suitability for Constrained Devices	Limited	Poor	High
Key Refresh Mechanism	Static	Static	Dynamic (one-time keys)

CONCLUSION AND FUTURE WORK

In this research work, we propose a novel technique in order to strengthen the security of communication in IoT environment using IoT communication protocol Constrained Application protocol (CoAP). In a IoT-simulated environment, our proposed model exhibits robust security provisioning with a marginal higher authentication time as compared to standard CoAP. However, it is compensated by a stronger security support. The same approach can also be applied in future to various other IoT communication protocols.

REFERENCES

[1] Ramlowat D. D. and Pattanayak B. K., Exploring Internet of Things (IoT) in Education: A Review, Information Systems Design and Intelligent Applications, pp.245-255, Springer, 2019.

[2] Hosenkhan R. and Pattanayak B. K., A Secured Communication Model for IoT, Information Systems Design and Intelligent Applications, pp.187-193 Springer, 2019.

[3] Hosenkhan R. and Pattanayak B. K., Security Issues in Internet of Things (IoT): A Comprehensive Review, New Paradigm in Decision Science and Management, pp. 359=369, Springer, 2020.

[4] Laha, S. R., Pattanayak B. K. and Pattnaik S., Advancement of Environmental Monitoring System Using IoT and Sensor: A Comprehensive Analysis, AIMS Environmental Science, Vol.9, No.6, pp.771-800, 2022.

[5] Laha, S. R., Pattanayak, B. K., Pattnaik, S., & Hosenkhan, M. R. (2024). Challenges associated with cybersecurity for smart grids based on IoT. In *Intelligent Security Solutions for Cyber-Physical Systems* (pp. 191-202). Chapman and Hall/CRC.

Research Article

[6] Dash, L., Pattanayak, B. K., Laha, S. R., Pattnaik, S., Mohanty, B., Habboush, A. K., & Al Smadi, T. (2024). Energy Efficient Localization Technique Using Multilateration for Reduction of Spatially and Temporally Correlated Data in RFID System. Tikrit Journal of Engineering Sciences, 31(1), 101-112.
[7] Chen X., Constrained Application Protocol for Internet of Things, 2022.
[8] https://en.wikipedia.org/wiki/Constrained_Application_Protocol
[9] Raza S., Trabalza D. and Voigt T., 6LoWPAN Compressed DTLS for CoAP, Proceedings of the 2012 8th International Conference on Distributed Computing in Sensor Systems, pp.287-289, 2012.
[10] Parween S. and Hussein S. Z., A Comprehensive Analysis of CoAP Based Congestion Control in IoT, Proceedings of the 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST-2021), pp.321-324, 2021.
[11] Obaidat M.A., Choong J. L. and Thakur K., A Secure Authentication and Access Control Scheme for CoAP-Based IoT, Proceedings of the 5th Conference on Cloud and Internet of Things (CIoT), pp.145-149, 2022.
[12] Khalil K., Elgazzar K.and Bayoumi M., A Security Approach for CoAP-Based Internet of Things Resource Discovery, Proceedings of the IEEE 6th World Forum on Internet of Things (WF-IoT), pp.1-6, 2020.
[13] Vasques A. T. and Gondim J. J. C., Amplified Reflection DDoS Attacks over IoT Reflector Running on CoAP, Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI), pp.1-6, 2020.
[14] Costa D., Mingozzi E., Tanganelli G. and Vallati C., An AllJoyn to CoAP Bridge, Proceedings of the IEEE 3rd World Forum on Internet of Things (WF-IoT), pp.395-400, 2016.
[15] Coetzee L., Oosthuizen D. and Mkhize B., An Analysis of CoAP as Transport in an Internet of Things Environment, Proceedings of IST-Africa 2018 Conference, pp.1-7, 2018.
[16] Ouakasse F. and Rakrak S., An Improved Adaptive CoAP Congestion Control Algorithm, International Journal of Online and Biomedical Engineering, February 2019, pp.96-98, 2019.
[17] FDIL E. L. M., HAIDI M. E. L., Bajit A., ELAIDI S., BARODI A. and Tamtaoui A., A New Constrained Protocol S-CoAP Applied to Optimize COVID-19 Medical IoT Intelligent and Security-Based Data Supervising Platform, Proceedings of the 2020 International Symposium on Advanced Electrical and Communication technologies, pp.1-6, 2020.
[18] Lee K. and Seol S., Applying CoAP for Real-Time Device Control over Public Networks, Proceedings of the 2018 International Conference on Electronics, Information and Communications (ICEIC), pp.1-2, 2018.
[19] Ancillotti E. and Bruno R., BDP-CoAP: Leveraging Bandwidth-Delay Product for Congestion Control in CoAP, Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), pp.656-661, 2019.
[20] Ugrenovic D. and Gardasevic G., CoAP Protocol for Web-Based Monitoring in IoT Healthcare Applications, Proceedings of the 23rd Telecommunications Forum (TELFOR 2015), pp.79-82, 2015.
[21] Son S. C., Lee H. and Lee B-T, CoAP-Based Lightweight Information Exchange Technique for Demand Response, Proceedings of the 2017 International Conference on Information and Communication Technology Convergence (ICTC), pp.973-975, 2017.