Tikrit Journal of Engineering Sciences (2023) 30 (4): 153-158
DOI: http://doi.org/10.25130/tjes.30.4.16

IRAQI Academic Scientific Journals

College of Engineering

ISSN: 1813-162X (Print); 2312-7589 (Online)

Tikrit Journal of Engineering Sciences

available online at: http://www.tj-es.com

TJES Tikrit Journal of Engineering Sciences

An End-to-End Security Scheme for Protection from Cyber Attacks on Internet of Things (IoT) Environment

Ahamd Khader Habboush [a*], Bassam Mohammed Elzaghmouri [b], Binod Kumar Pattanayak [c], Saumendra Pattnaik [c], Rami Ahmad Haboush [b]

a Department of Computer Networks, Faculty of Information Technology, Jerash University, Jerash, Jordan.
b Department of Computer Science, Faculty of Information Technology, Jerash University, Jerash, Jordan.
c Department of Computer Science and Engineering, Institute of Technical Education and Research, Siksha 'O' Anusandhan Deemed to Be University, Bhubaneswar Odisha, India.

Keywords:

IoT; Security; Cyber Attacks; Encryption Scheme.

ARTICLE INFO

Article history:

Received	24 June	2023
Received in revised form	13 Aug.	2023
Accepted	03 Oct.	2023
Final Proofreading	18 Nov.	2023
Available online	15 Dec.	2023

Citation: Habboush AK, Elzaghmouri BM, Pattanayak BK, Pattnaik S, Haboush RA. **An End-to-End Security Scheme for Protection from Cyber Attacks on Internet of Things (IoT) Environment**. *Tikrit Journal of Engineering Sciences* 2023; **30**(4): 153-158.
http://doi.org/10.25130/tjes.30.4.16

Corresponding author:

Ahamd Khader Habboush

Department of Computer Networks, Faculty of Information Technology, Jerash University, Jerash, Jordan.

Abstract: The Internet of Things (IoT) technology has recently emerged as a potential global communication medium that efficiently facilitates human-to-human, human-to-machine, and machine-to-machine communications. Most importantly, unlike the traditional Internet, it supports machine-to-machine communication without human intervention. However, billions of devices connected to the IoT environment are mostly wireless, small, hand-held, and resourced-constrained devices with limited storage capacities. Such devices are highly prone to external attacks. These days, cybercriminals often attempt to launch attacks on these devices, which imposes the major challenge of efficiently implementing communications across the IoT environment. In this paper, the issue of cyber-attacks in the IoT environment is addressed. An end-to-end encryption scheme was proposed to protect IoT devices from cyber-attacks.

نظام أمني شامل للحماية من الهجمات السيبرانية على بيئة إنترنت الأشياء (IoT)

احمد خضر حبوش [١]، بسام محمد الزغموري [٢]، بايوند كومار باتانايك [٣]، ساومندرا باتانايك [٣]، رامي احمد حبوش [٢]
[١]قسم شبكات الحاسوب/ كلية تكنولوجيا المعلومات/ جامعة جرش/ جرش-الأردن.
[٢]قسم علوم الحاسوب/ كلية تكنولوجيا المعلومات/ جامعة جرش/ جرش- الأردن.
[٣]قسم علوم وهندسة الكمبيوتر/ معهد التعليم الفني والبحوث/ جامعة سيكشا "أو" أنوساندان/ بوبانسوار أوديشا- الهند.

الخلاصة

برزت تكنولوجيا إنترنت الأشياء (IoT) مؤخرًا كوسيلة اتصال عالمية محتملة تعمل على تسهيل الاتصالات بين البشر، ومن إنسان إلى آلة، ومن آلة إلى آلة بكفاءة. والأهم من ذلك، أنها، على عكس الإنترنت التقليدية، تدعم الاتصال من آلة إلى آلة دون تدخل بشري. ومع ذلك، فإن مليارات الأجهزة المتصلة ببيئة إنترنت الأشياء هي في الغالب أجهزة لاسلكية وصغيرة ومحمولة باليد ومحدودة الموارد ذات سعات تخزين محدودة. مثل هذه الأجهزة معرضة بشدة للهجمات الخارجية. في هذه الأيام، يحاول مجرمو الإنترنت في كثير من الأحيان شن هجمات على هذه الأجهزة، مما يفرض التحدي الأكبر المتمثل في تنفيذ الاتصالات بكفاءة عبر بيئة إنترنت الأشياء. تتناول هذه الورقة مسألة الهجمات السيبرانية في بيئة إنترنت الأشياء. تم اقتراح نظام تشفير شامل لحماية أجهزة إنترنت الأشياء من الهجمات السيبرانية.

الكلمات الدالة: إنترنت الأشياء، حماية، هجمات سيبرانية، نظام التشفير.

1.INTRODUCTION

Over the years, the global Internet has been the principal communication medium for people globally. The diversity of its applications has made it extremely popular among people from various fields of application, from business enterprises to educators, healthcare professionals, and industry personnel. However, the traditional Internet cannot facilitate autonomous communication of connected devices. Further enhancement of the global Internet, often termed the Internet of Things (IoT), considered the future Internet, could successfully establish autonomous communication among billions of smart wireless resource-constrained devices connected to the IoT environment [1]. As experts reveal, in 2025, 30 billion smart devices will be connected to the IoT environment. The heterogeneity and resource-constrained features of such IoT devices make them extremely vulnerable to external attacks launched by malicious attackers [2]. Hence, it becomes essential to devise robust security mechanisms for ensuring secure communication among the devices connected to the IoT environment. The services provided by IoT are useful in real-time and essential from various operational points of view. Manufacturers, supply chain organizers, and various utility companies mostly rely on IoT services, often called operational technology (OT). An Industrial Control System (ICS) necessarily extends this operational technology. The underlying architecture of ICS is depicted in Fig.1. The basic components of ICS are firmware, microcontroller, battery/power, internal memory, external storage, motion sensors, connectivity stack, protective services, and authentication services. Firmware represents a read-only memory that supports low-level control over the ICS hardware components. The microcontroller is the central component of ICS, i.e., a processor necessary for running the software. Battery stores the required power to support operating the ICS and receive power from external sources. Internal memory is used for storing the relevant programs and the data. External storage is used to store the necessary information for an extended period. Such information includes the IoT device location, the connected devices, and user data [3]. Motion Sensors represent a combination of hardware and software to track the device's movement. The connectivity stack is intended to provide network connectivity, such as Wi-Fi, Bluetooth, and Zigbee. Authentication Services enable the IoT device to verify and validate its users. The Protective Services are responsible for protecting the device from possible external attacks.

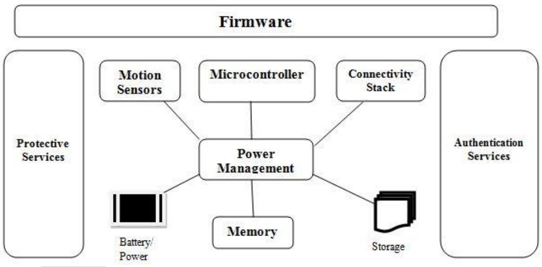

Fig.1 Architecture of Industrial Control System.

An IoT ecosystem comprises software developers, hardware engineers, network connectivity, platforms, data analysts, scientists, IT workers and managers, cybersecurity workers and managers, and Artificial Intelligence (AI) and Machine Learning (ML). It is necessary to create relevant IoT solutions, thereby managing various devices. Cybersecurity threats on IoT ecosystems, i.e., present a major challenge for efficient implementation of such systems, have increased over the years. The attackers may compromise sensitive information shared between communicating devices, leading to a communication failure. Hence, it needs a robust security mechanism to overcome such cybersecurity attacks. Furthermore, since IoT devices are extremely resource-constrained, implementing complex security algorithms is not viable. Cryptographic security algorithms can be very useful for such scenarios. Advanced Encryption Standard (AES) based cryptographic algorithms are widely used by researchers to provide security for lightweight IoT devices. In the present work, the AES-128 block cipher was used for key generation for security provisioning of the IoT systems. The present work focused on minimizing packet loss during communication between IoT devices using the AES-128-based security key generation scheme. The experimental results showed that 98% of packets are successfully communicated between the end user IoT devices. The remaining parts of the paper are organized as detailed below. Section 2 includes the aspects relating to IoT cybersecurity and associated issues and challenges. Related work about IoT cybersecurity is covered in Section 3. The proposed model is discussed in Section 4, and the analysis of experimental results is discussed in Section 5. Section 6 concludes the paper along with probable extensions suggested for future work.

2.IOT CYBERSECURITY

Cybersecurity issues have become a major concern for various enterprises, especially financial institutions. With a growing number of cybercrimes, relevant solutions for preventing such attacks become essential to protect the functionality and the enterprises' properties. Several cybersecurity threats that emerge from the improper development of IoT devices and lack of security provisioning are detailed below.

Service Disruption: results from manipulating an IoT device to make a desired service unavailable.

Data Theft: It refers to a situation where a malicious attacker may tend to improperly access the personal information of a user, such as a user account, addresses, and phone numbers.

Data or Service Manipulation: In such a case, the attacker may modify the settings of an IoT device, causing loss of service and damage to the device.

Non-compliance refers to the violation of regulations as imposed by the government designed to protect user's privacy.

Malicious attackers may also launch various malware activities to compromise the policies of various enterprises. A few probable solutions can be incorporated to overcome the issues and challenges related to cyber security in the IoT environment:-

1- Enhancement of device monitoring: Implementing intrusion detection systems (IDS) and security information and event management (SIEM) and sharing information among host devices significantly resolves cyber threats on IoT devices. As a result, it becomes feasible to profile the cyber attackers and get protected from possible attacks on the devices.

2- Addition of security features: Security features like encrypted stored and communicated information can ensure privacy. Also, powerful authentication schemes can be introduced to control the connections fully. The IoT traffic segmentation can assist in better management of the IoT traffic.

3- Compliance with IoT and ICS Standards: Various cybersecurity standards and necessary recommendations for the manufacturers of IoT devices have been published by the National Institute of Standards and Technology (NIST) that need to be complied with by enterprises to make the security system robust in any circumstance.

The present research paper focuses on the secure authentication of IoT devices using an end-to-end encryption scheme detailed in Section 4.

3.RELATED WORKS

A large spectrum of research work on cybersecurity can be observed. Ref. [4] proposed an approach to predicting security attacks using Hidden Markov Models (HMM), establishing an expert system operating on large network datasets. Here, HMM was used by the authors to distinguish among three states: security attacks, unsure, and no attacks. The authors split the dataset into three clusters. The experimental observations were extremely encouraging compared to other existing approaches. The Cyber Security Operations Centre (CSOC) is a necessarily horizontal technological process inherently responsible for managing various security-related activities, such as detecting and identifying security threats on devices, their management, coordination, and analysis. Further, cyber onboarding is the process of setting up the devices to make it possible for CSOC to track and manage the security threats on the device. CSOC and cyber onboarding have been used by [5] for the successful identification and management of security attacks incoming to a device. A cyber-0banking security framework has been proposed by the [6] and specifically focused on the cyber-attacks on financial institutions in the African region. The authors proposed boundary security and applied security approaches to protect from cyber-attacks. A detailed discussion of various issues related to IoT cybersecurity and regulations has been conducted by [7] to facilitate a better understanding of security threats on IoT devices. A cyber security testbed has been proposed by [8]. The authors relied on the existing testbeds and presented the work as a case study, thereby claiming the utility of such testbeds with experimental verifications. Various security threats, related issues, and challenges in the context of IoT-based environmental monitoring systems have been encompassed in the research work presented by [9], which helps security professionals explore various security aspects of IoT systems. Timely knowledge acquisition of information about various cyber-attacks and security threats is necessary to overcome such issues and keep them in view. Ref. [10] presented the design principles addressing the related issues and challenges of cyber threats in small-scale IoT projects. The integrated cyber supply chain platforms are often affected by various cyberattacks, imposing a major challenge for the organization in securing the data. This issue has been comprehensively addressed by [11]. The authors developed a capability maturity model to develop awareness regarding cyber-attack threats evolving around Industrial IoT (IIoT) enabled supply chain processes. Ref. [12] proposed a few recommendations to counter the threats to the UK Critical National Infrastructure (NIS) in the context of cyber security measures. A 32-bit AES encryption/decryption architecture for utilization in IoT infrastructure for security provisioning is addressed in [13]. The authors presented a low-cost architecture called LC-FRAES, which is fault-resilient and can be used for data path and key expansion unit sharing the resources between the encryption and decryption processes. An AES-based cryptographic algorithm for security provisioning in IoT communication using MQTT communication protocol has been proposed by [14]. An AES-based encryption/decryption keys were exchanged between the subscriber and the client through the broker device, which significantly enhanced the security aspect of the IoT communication. Identification of attacks in the IoT environment and mitigation of them using filtering and patches method has been proposed by [15]. The authors implemented an AES-based encryption mechanism, claiming that the proposed scheme could successfully address DoS attacks for many IoT devices and other miniature devices. Another AES-based encryption scheme for ensuring IoT security using the ESP32 module was proposed in [16]. In this approach, data are received by a card created and developed by the Espressif Systems (ESP32) module; then, it is encrypted and sent to the authorized receiver. AS claimed by the authors in their research work, this scheme was robust enough to provide security to IoT devices with minimal resources. A hardware representation of the AES algorithm for generating an encryption/decryption key for IoT security provisioning was proposed in [17]. It used an AES 128-bit block cipher to generate the encryption/decryption key that was robust enough to provide security for the IoT communication. A model based on AES-256 and Secure Hash Algorithm-256 (SHA_256) was proposed by [18] for IoT security provisioning. The data generated by IoT devices were encrypted using AES-256 with a symmetric key generated using SHA-256, and subsequently, ciphertext was created. Then, the created ciphertext was added to the MQTT at the security layer, which enhanced the security aspect of IoT communication using MQTT. An IoT model based on a Lightweight Intrusion Detection System (LIDS) has been proposed by [19]. It employed a deep learning strategy using a Multi-layer Perception (MLP) Network. LIDS provides higher-level security, thereby exhibiting high speed in detection, and can handle some of the MQTT communication protocol features. The proposed IoT model was tested over the MQTT dataset for training the model and its validation. The experimental results exhibited that the deep learning approach efficiency improved the intrusion detection accuracy for the proposed IoT model by 3-5% compared to other existing IoT models.

4. PROPOSED MODEL

In this paper, the secure authentication of devices on IoT was addressed. As depicted in Fig.2, the sending IoT device communicates with the receiver IoT device through a gateway acting as a broker. At the beginning of communication, the sender sends a control packet that holds the encryption/decryption key generated using Advanced Encryption Standard (AES) to the gateway that further forwards it to the authenticated receiver [19]. The control packet holds the RFID of the receiver. On receiving the packet, the receiver caches the key and then acknowledges it to the sender via the gateway. As a result, a presumably secure connection would be established between the desired sender and receiver devices. Then, the data communication session begins. Every data packet is routed through the gateway that verifies the destination address and then delivered to the authenticated receiver. On receiving the data packet, the receiver decrypts the received data using the key received initially and then caches the data. This process continues until the entire dataset is communicated to the receiver. It should be noted that since the data packets are encrypted, external hackers cannot access or modify them. After the data communication session is accomplished, the connection is terminated.

The process of communication is depicted in Fig.3.

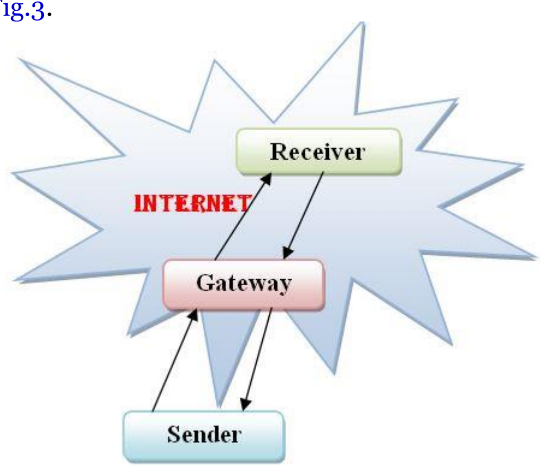

Fig.2 IoT Environment.

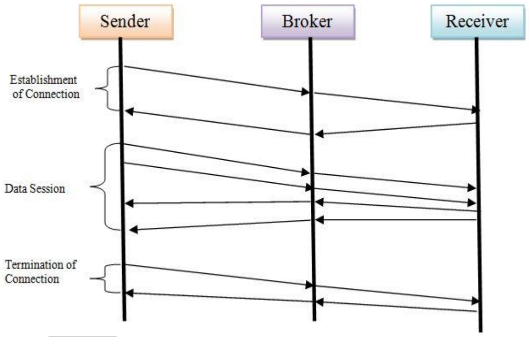

Fig.3 Data Communication on IoT.

In the present study, an AES 128 block cipher generated the encryption/decryption key [20]. Data communication was secure and faster because the encryption and decryption were conducted using the same key.

5.EXPERIMENTAL RESULT ANALYSIS

The simulation work has been conducted using a SimpleIoT Simulator implementing the MQTT communication protocol with two mobile devices as sender and receiver. AES 128 has been used to generate the encryption/decryption key, which was the same for encryption and decryption. The mobile devices were connected to the IoT broker using Bluetooth wireless. The results showed that 98% of data between the sender and receiver were securely communicated, with the data integrity maintained. The proposed encryption/decryption scheme was proven robust under any circumstances.

6.CONCLUSION AND FUTURE WORK

The IoT environment, being a heterogeneous environment, is often prone to cyber-attacks from external hackers. Among various other issues, proper authentication of IoT devices can significantly protect the IoT devices from cyber-attacks. In the present research work, an end-to-end encryption scheme was proposed to secure communication on IoT, protecting the environment from probable cyber-attacks. Although the AES 128 block cipher was used for key generation, the existing work can be extended by lightweight block ciphers, significantly enhancing the IoT system efficiency.

ACKNOWLEDGEMENTS

The authors are grateful for the financial support for this research by the Department of Computer Science and Computer Networks, Faculty of Information Technology, Jerash University, Jerash, Jordan.

REFERENCES

[1] Rath M, Pattanayak BK. **Technological Improvement in Modern Health Care Applications Using Internet of Things (IoT) and Proposal of Novel Health Care Approach**. *International Journal of Human Rights in Healthcare* 2019; **12**(2): 148-162.

[2] Ramlowat DD, Pattanayak BK. Exploring Internet of Things (IoT) in Education: A review. *Information Systems Design and Intelligent Applications*, 2019; 245-255.

[3] Internet Source: What Is IoT Cybersecurity?. Downers Grove, Illinois, US. Available from: https://www.comptia.org/content/articles/what-is-iot-cybersecurity

[4] Teoh TT, Nguwi YY, Elovici Y, Cheung NM, Ng WL. Analyst Intuition Based Hidden Markov Model On High Speed. *Temporal Cyber Security Big Data, Proceedings of the 13th International Conference on Neural Computation, Fuzzy Systems and Knowledge Discovery*, 2017;2080-2082

[5] Onwubiko C, Quazzane K. Cyber Onboarding is 'Broken'. *Proceedings of the 2019 IEEE International Conference on Cyber Security and Protection of Digital Services*,2019;1-13

[6] Mbelli TM, Dwolatzky B .Cyber Security a Threat to Cyber Banking in South Africa An approach to Network and application security. *Proceedings of the IEEE 3rd International Conference on Cyber Security and Cloud Computing*,2016;1-6.

[7] Sevis KN, Seker E. Cyber Warfare: Terms, Issues, Laws and Controversies, *Proceedings of the 2016 IEEE International Conference on Cyber Security and Protection of Digital Services*, 2016;1-9

[8] Frank M, Leitner M, Pahi T. Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education, *Proceedings of the 15th IEEE International Conference on Pervasive Intelligence and Computing 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress*,2017;38-46.

[9] Laha SR, Pattanayak BK, Pattnaik S. **Advancement of Environmental Monitoring System Using IoT and Sensor: A Comprehensive Analysis**. *AIMS Environmental Science* 2022; **9**(6) :771-800 .

[10] Skopik F, Filip S. Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators. *Proceedings of the 2019 IEEE International Conference on Cyber Security and Protection of Digital Services*, 2019;1-8.

[11] Isbell RA, Maple C, Hallaq B, Boyes H. Development of A Capability Maturity Model for Cyber Security in IIoT Enabled Supply Chains. *Living in the Internet of Things (IoT 2019)*, 2019;1-82019.

[12] Shukla M, Johnson SD, Jones P. Does the NIS Implementation Strategy Effectively Address Cyber Security Risks in the UK?, *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 2019;1-11.

[13] Sheikhpour S, Ko SB, Mahani AA. **Low-Cost Fault Attack Resilient AES for IoT Applications**. *Microelectronics Reliability* 2021; **123**: 114202.

[14] Swamy KSK, Sony G, Ram ChJ, Navven B. Harshita J. **Secure IoT Devices Using AES.** *Encryption Journal of Engineering Sciences* 2020;**11**(4):115-118

[15] Javed Y, Khan AS, Qahar A, Abdullah J. **Preventing DoS Attacks in IoT Using AES**. *Journal of Telecommunication, Electronic and Computer Engineering* 2017;**9**(3):55-60.

[16] Al-Mashhadani M, Sujja M. IoT Security Using AES Encryption Technology based ESP32 Platform. *The International Arab Journal of Information Technology* 2022;**19**(2):214-223.

[17] Nandan V, Rao RGS. **An Efficient AES Algorithm for IoT Based Applications**. *International Journal of Engineering and Advanced Technology*. 2019; **9**(1) :1939-1944.

[18] Ahamed J, Zahid Md, Omar M, Ahmad K. **AES and MQTT Based Security System in the Internet of Things**. *Journal of Discrete Mathematical Sciences and Cryptography* 2016; **22**(8) :1589-1598

[19] Mahmood MS, Al-Dabagh NB. **Improving IoT Security using Lightweight Based Deep Learning Protection Model**. *Tikrit Journal of Engineering Sciences* 2023; **30**(1)119–129

[20] Radanliev P, Roure DD, Cannady S, Montalvo RM, Nicolescu R, Huth M. Economic Impact of IoT cyber risk - Analysing Past and Present to predict the future developments in IoT risk analysis and IoT cyber insurance. *Living in the Internet of Things: Cybersecurity of the IoT* ,2018;1-9.

[21] Hosenkhan MR, Pattanayak BK. **An End-to-End AES Based Cryptographic Authentication Mechanism for Communication on Internet of Things (IoT) Using MQTT**. *Natural Volatiles and Essential Oils* 2021;**8**(3):29-33