IPTEK The Journal of Technology and Science, 34(3), 2023 (e/pISSN:2088-2033, 0853-4098)

DOI: 10.12962/j20882033.v34i3.16830 | Received 19 May, 2023; Revised 19 May, 2023; Accepted 30 May, 2024

ORIGINAL RESEARCH

ENCRYPTION OF INTERNET OF THINGS CONSTRAINED DEVICE FOR DIGITAL ENVELOPE : A SYSTEMATIC LITERATURE REVIEW

Isa Mulia Insan | Febriliyan Samopa*

[1]Department of Information Systems, Sepuluh Nopember Institute of Technology, Surabaya, Indonesia, Surabaya, Indonesia

Correspondence

Email: iyan@is.its.ac.id

Present Address

Magister Tower, Jl Informatika No. 10, Surabaya 60111, Indonesia

Abstract

Not only the exchange of information between IoT devices but integration between IoT devices and cloud servers has also brought IoT to a higher level. Security is the main problem for IoT devices with limited resources for exchanging information. Digital envelopes are one method that uses encryption to secure data. However, limited resources on constrained devices necessitate selecting the proper encryption. This systematic literature review (SLR) was conducted on 11 of 43 studies that have used encryption algorithms for IoT devices. In addition to using the algorithm, it will also explain the device used and the safety factor. A suitable encryption algorithm for the digital envelope has been found. In addition, Some of the safety factors, IoT devices, and specifications are also shown.

KEYWORDS:

Internet of things, Encryption, Digital envelope, Constrained device.

1 | INTRODUCTION

In the growing Internet of Things (IoT) era, many devices are connected to the Internet and exchange information. The exchange of information between IoT devices and integration between IoT devices and cloud servers have brought IoT to a higher level. Higher computing capabilities from cloud servers are used to calculate data that IoT devices have obtained. IoT device's function is fetching and sending data from the environment. Low-end or constrained devices are IoT devices with energy efficiency, small size, and mobility support[1]. Of the several constrained devices on the market, Arduino is the most popular device to use[2] [3] [4]. Constrained devices are suitable for collecting data in the real world.

Security is a significant concern for constrained devices with limited resources[5]. One of the critical security services in implementing the Internet of Things concept is authentication[6]. The number of devices that are connected raises suspicion about connected devices. It is crucial to ensure the identity of each sender and recipient[7]. In addition, messages sent via the protocol can be important assets that must be protected and managed correctly[8],[9]. To deal with this, what needs to be done is to

use a security scheme that can provide the right security services. In the X800 document, the International Telecommunication Union has defined five security service categories Authentication, Access Control, Data Confidentiality, Data Integrity, and non-repudiation. In addition to these five categories, the International Telecommunication Union defines one property availability. Digital envelopes are a security method that uses encryption to secure data. Digital envelopes are a straight forward, applicable way of reducing bandwidth overhead in encryption[10]. Proper encryption is required for constrained devices to implement digital envelopes on constrained devices. Therefore it is necessary to review the literature for selecting encryption algorithms that can be used on constrained devices. This proposal will propose an encryption algorithm suitable for constrained devices to increase the security of sending and receiving data on Internet of Things devices. This proposal will provide insight into selecting a secure encryption algorithm capable of running on limited devices with limited resources. The proposed solution will also help overcome the challenges of implementing secure communication for Internet of Things devices using constrained devices.

2 | DIGITAL ENVELOPE

One method of protecting messages using encryption and authentication is digital envelopes. Digital envelopes are used to use symmetric and asymmetric encryption when encrypting extensive data[11]. Digital envelopes also aim to avoid attacks when data exchange occurs.[12] Even if an unauthorized person snoops on the message, authenticated people can only open the actual message. The first step in implementing the envelope, the plaintext, is encrypted using symmetric encryption to become ciphertext. Each time sent, the sender will generate a new random message key which will be used to encrypt the message. To open the message, it needs the same random key that was generated earlier. Next, the random key is encrypted using asymmetric encryption with the recipients public key. Finally, the encrypted ciphertext and random key are sent together to the recipient. To open the message, the recipient needs to decrypt the received random key using the recipients private key to derive a plain text key from the symmetric method used in the message encryption. The plaintext key is used to unlock the sent ciphertext. An example of implementing a digital envelope is when Alice wants to send a message to Bob. For every message sent, the sender needs to generate a random key that will be used as a symmetric key. Alice generates a random key which is used as a symmetric key. Furthermore, the message is encrypted using the symmetric key that has been created. The owned symmetric key is encrypted using Bobs public key (asymmetric encryption). Finally, the ciphertext is obtained as an encrypted message and a symmetric key. To open the message, Bob first needs to decrypt the symmetric key. The symmetric key is decrypted using Bobs private key. The symmetric key obtained is used to decrypt the ciphertext, which contains messages from Alice. A digital envelope based security scheme can be seen in Figure 1 for more details.

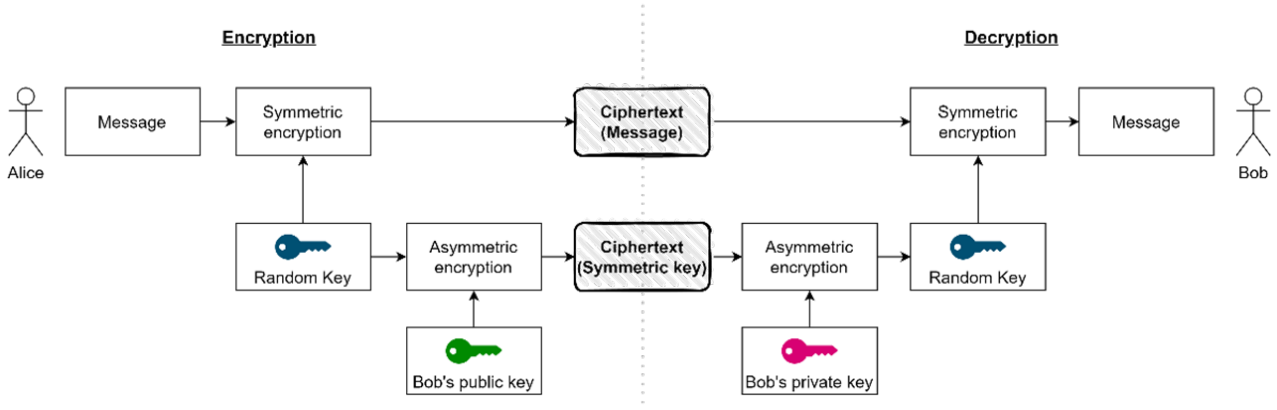


FIGURE 1 Signal strength meter.

3 | METHOD

In a study conducted in SLR, six steps can be done regardless of field, discipline, or perspective[13]. (1) defining the research question, (2) determining the required characteristics of primary studies, (3) retrieving a sample of potentially relevant literature, (4) selecting the pertinent literature, (5) synthesizing the literature, and (6) reporting the results.

1. Defining the research question.
   The first step that needs to be done is to determine the research question. This SLR will be conditioned to answer research questions that have been defined.

2. Determining the required characteristics of primary studies.
   After obtaining the formulation of the problem in the research conducted, the next step is to determine inclusion and exclusion before searching. Inclusion and exclusion are used to set the limits of the literature review so that the criteria from the search results are as expected.

3. Retrieving a sample of potentially relevant literature.

   The next stage is to take samples of potentially relevant literature to the research. The database used will be explained. The keywords used for the search are also mentioned.

4. Selecting the pertinent literature.
   At this stage, the inclusion and exclusion that have been defined in the literature that has been obtained are applied. A list of studies and a brief explanation is shown at this stage.

5. Synthesizing the literature.
   At this stage, the required information is taken from the selected paper. Relevant data needed is described narratively in this section.

6. reporting the results.
   The last is to report the results of the literature review that has been carried out.

4 | RESULT AND DISCUSSION

This section will explain the discussion of the results of the literature review that has been carried out. The results of the discussions that have been carried out have been adjusted to be able to answer the research questions that have been set.

4.1 | Defining the research question

Many encryption methods can be applied to digital envelopes. However, not all encryption methods suit digital envelopes on IoT constrained devices. Thus, the problem formulation in this research is What encryption scheme can be adopted for digital envelopes on IoT constrained devices.

4.2 | Determining the required characteristics of primary studies

In this section, the inclusion and exclusion criteria are determined. Inclusion and exclusion are used to set the limits of the literature review so that the criteria from the search results are as expected. The specified inclusion and exclusion criteria are as follows:

- Inlusion
  - Research on security schemes using encryption for sending Internet of Things data
  - Research Year in the last five years (2019-2023)
  - The database used is Google Scholar.

- Exceptions
  - Non-English language

4.3 | Retrieving a sample of potentially relevant literature

The next stage is to take samples of potentially relevant literature to the research. The database used for this literature sampling is Google Scholar. Google Scholar has covered conferences and journals such as IEEE Xplore, Science Direct, Springer, and others. The search keywords were encryption security schemes for Internet of Things constrained devices. The search results obtained from Google Scholar amounted to 17.200 articles. From these articles, articles related to the desired encryption algorithm are taken. Based on research [14], some lightweight symmetrical algorithms for IoT are AES, PRESENT, RC5, HEIGHT, and TEA. Meanwhile, lightweight asymmetric algorithms for IoT are RSA and ECC.

4.4 | Selecting the pertinent literature

The inclusion and exclusion defined in the literature obtained in the previous stage are applied at this stage. After applying inclusion exclusion, 43 studies were obtained. Of the 43 studies carried out in depth analysis. From the analysis results, 11 studies were reviewed for this study. Four studies for research implement a security scheme using symmetric encryption. Meanwhile, seven studies implement a security scheme using asymmetric encryption. For more details, the list of studies reviewed is written in Table 1 .

4.5 | Synthesizing the literature

At this stage, the required information is taken from the selected paper. Several studies have proposed encryption algorithms that can be applied to IoT. Research [15]. has proposed an authentication method using the AugPAKE and PRESENT algorithms. When the message is transferred to the broker, it is encrypted with AugPAKE. While at the broker, the message is already encrypted using PRESENT. Other studies have proposed encryption using RC5 [16] and AES [17], [18] as a lightweight authentication method in IoT. The downside of symmetric encryption is that the key used to encrypt and decrypt is the same, so the key needs to be regenerated each time a message is sent to maintain security. The thing is, exchanging a new key each time a key is generated isnt easy. A list of reviewed symmetric encryption studies are shown in Table 2

An asymmetric encryption algorithm is used to overcome key exchange in symmetric encryption. RSA is an asymmetric encryption algorithm that has guaranteed security. A study [19] has used the RSA encryption algorithm for a smart IoT environment. The researchers designed an RSA based authentication system for a networked smart IoT environment using advanced industry standard (NIST) level 4. However, implementing the RSA Algorithm is resource intensive. So it is not suitable for use on constrained devices. A list of reviewed symmetric encryption studies is shown in Table 2 There are also studies using other asymmetric encryption, such as Diffie Hellman [20], ElGamal [21], and Cramer-shoup [22]. Hybrid cryptography has been proposed using the Twofish and Diffie Hellman key exchanges [20]. The following research proposes cryptosystem and biometric information based on user passwords for cloud based IoT applications based on system security for cloud based [21]. Subsequent research proposes a system that allows nodes to perform integrity verification. The devices used in the implementation are not constrained by limited resources [22].

Apart from RSA, elliptic curve cryptography (ECC) has also been adopted in IoT [23]–[25]. Other studies argue that the proposed s0cheme uses ECC and simple operations to make the proposed authentication protocol light and secure [23]. The research proposes an authentication protocol to secure communication between devices based on ECC [24]. Experiences and lessons learned during the development of IoT security applications using ECDH have been documented in research [25].

4.6 | Reporting the results

This section will report the literature review results, provide a descriptive overview of the reviewed literature, and discuss the findings.

TABLE 1 List of research

Title	Journal or Conference	Tahun
MQTT PRESENT: Approach to secure internet of things applications using MQTT protocol[15]	International Journal of Electrical and Computer Engineering	2021
Application of RC5 for perangkat IoT in Smart Transportation System[16]	International Conference on Modeling, Simulation and Applied Optimization	2019
IOT Security Using AES Encryption Technology based ESP32 Platform[17]	International Arab Journal of Technology	2021
Reliability and availability of IOT devices in resource constrained environments[18]	International Journal of Quality and Reliability Management	2021
An RSA based Authentication system for Smart IoT Environment[19]	IEEE International Conference on High Performance Computing and Communications	2019
Secure Data Exchange Between Nodes in IoT Using Twofish and DHE[20]	International Conference on Cyber Security and Internet of Things	2019
ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications[21]	The Institution of Engineering and Technology	2019
Lightweight fog centric auditing scheme to verify integrity of IoT healthcare data in the cloud environment[22]	Concurrency and Computation: Practice and Experience	2021
Resource-Constrained IoT Authentication Protocol	International Conference on Future Data and Security	2019
An ECC Based Hybrid Scheme for Device to Server and Device to Device Communications[23]		
ECC based inter device authentication and authorization scheme using MQTT for IoT networks[24]	Journal of Information Security and Applications	2019
An Enhanced Mutual Authentication Scheme Based on ECDH for IoT Devices Using ESP8266[25]	International Conference on Communication Software and Networks	2019

4.6.1 | Encryption

From the results of the literature review that has been obtained, several symmetric encryption algorithms are AugPake, PRESENT, and AES. Compared to other encryption, AES has been used on constrained devices[18]. While the asymmetric encryption that will be used is Elliptic Curve Cryptography (ECC)[25] or Elliptic-curve Diffie Hellman (ECDH). The ECDH scheme has generated shorter, more secure shared keys suitable for IoT devices. Implementation of ECDH as a shared key algorithm can be combined with the symmetric encryption algorithm that has been mentioned or combined with Twofish[20] or with a lightweight encryption algorithm like AES[18]. From the literature conducted, several safety factors were mentioned in the study. Some of the factors mentioned are privacy[16],[17],[19],[20],[22],[23],[24],[25], confidentiality[17],[19],[20],[24],[25], integrity[15],[19],[20],[24],[25], authentication[15],[21],[24], access control[19], Non-repudiation[19], reliability[17] and availability[18]. one way to prove the security of the security scheme used is to carry out an attack[15]. Threat like eavesdropping attacks, MITM attack, replay attack, node capturing the attack used to test the security of a security scheme[15].

4.6.2 | Device

Various devices have been used in the studies that have been reviewed. However, not all devices used are constrained devices. Constrained devices are devices that have limited resources. Despite having limited resources, constrained devices have advantages in energy efficiency, small size, and mobility support[1]. Carsten Bormann has classified constrained devices into three classes 0,1, and 2. Classes 0 and 1 have minimal resources, making running OS on those devices impossible. While Class 2 has sufficient resources to run the OS, quite heavy protocols can also run on these devices. Details of the classification of constrained devices that have been classified by Carsten Bormann et al. are shown in Table 3 . The first device used was an FPGA using Quartus Prime Lite Edition version 18[16]. From the minimum specifications required to run Quartus Prime Lite Edition version 18, the device used for implementation is not constrained. The FPGA in this study is used to implement the RC5 Algorithm

TABLE 2 Research with symmetric encryption security scheme

Research	Security Factor	Encryption	Constrained device
[15]	Authentication, Integrity	AugPake and PRESENT	No
[16]	Privacy	RC5	No (Quartus Prime Lite Edition version 18)
[17]	Privacy, and confidentiality	AES	No (ESP32)
[18]	Reliability and availability	AES	Yes and No (Arduino Nano and Raspberry pi)
[19]	Confidentiality, Integrity, Access control, Non-repudiation, and Privacy	RSA	No (Mobile device)
[20]	Privacy, Confidentiality, Diffie-Hellman key Exchange (Asymmetric)	Twofish (Symmetric) and (Not Spesific)	No
[21]	Authentication	ElGamal	No (Mobile Device)
[22]	Privacy	Cramer Shoup	No (Computer)
[23]	Privacy	ECC	No (Not spesific)
[24]	Privacy, Confidentiality, Authentication, and Integrity	ECC	No (AVISPA and ACPT)
[25]	Privacy, Confidentiality, and Integrity	ECC	Yes (ESP8266)

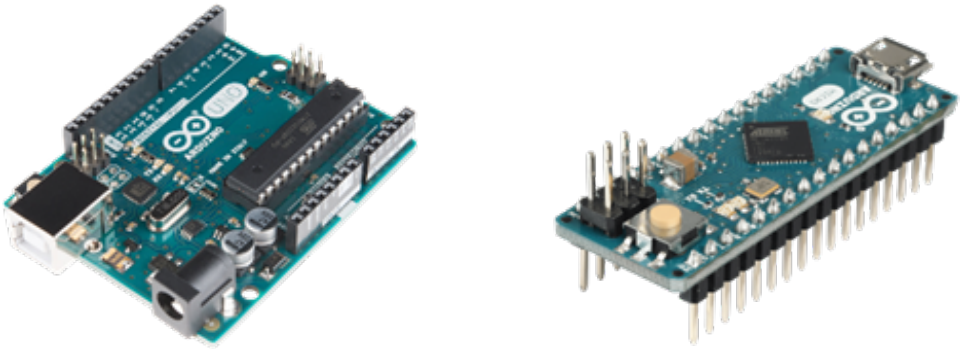
to determine the resources needed for research. The second device used is the ESP32[17]. The ESP32 specifications are 320 KiB RAM, and 448 KiB ROM, if paying attention to the classification[26], not a constrained device. The latest devices used in research that uses symmetric encryption are Arduino Nano and Raspberry Pi[18]. Arduino is an open-source electronic platform widely circulated in the market. Arduino is also easy to connect with plug-ins such as inputs, sensors, and lights. Arduino Nano specifications are 2 Kb SRAM and 32 Kb Flash Memory. At the same time, the second device used in this research is a Raspberry Pi with 4GB RAM specifications. Both devices were used for experiments by running AES-128 encryption on both devices.

TABLE 3 Classification of constrained devices[1], [26]

Spesification	Class 0	Class 1	Class 2
RAM	« 10 KB	10 KB	50 KB
Flash	« 100 KB	100 KB	250 KB
Real time operating system (RTOS) support	The device does not implemented on the device	RTOS may be	RTOS can operate
Communication protocol	No protocol stack planted, using gateways for communication	Can communicate with other devices without gateways help	Powered by protocol communications like HTTP

The following device is the device used to perform asymmetric encryption. The first device is a smartphone which is used in the two studies[19], [21]. The first study uses a smartphone to implement a security standard of NIST level 4 using microSD. MicroSD itself is widely used on smartphones[19]. The following research presents the ElGamal cryptographic and biometric information system and a user password-based authentication scheme for a cloud based IoT application called SAS Cloud. In this study,

smartphones were used because smartphones are commercial devices that are readily available and have biometric support[21]. The following device is a computer used to run the tools AVISPA[24]. AVISPA is a tool for verifying Internet security protocols, their security objectives, and associated threat models. The last device used is the ESP8266 which has built-in wifi capabilities. Mutual authentication improvements have been made using ECDH on curve25519[25]. The specifications of the ESP8266 are 64 KB of RAM and 4 MB of flash memory. Of the several devices mentioned, mobile devices and computers are the devices most frequently used. Arduino-constrained devices are devices that are quite popular for use in research[2]–[4]. Some examples of Arduino devices are shown in Figure 2 .



(a) (b)

FIGURE 2 Examples of IoT constrained devices a) Arduino Uno, b) Arduino Nano.

5 | CONCLUSION

The more use of IoT technology, the more it is necessary to pay attention to technology security. The review results show that the factors that need to be considered and improved by using encryption are privacy, confidentiality, integrity, authentication, access control, non-repudiation, reliability, and availability. The digital envelope method is suitable for encrypting large data by taking advantage of symmetric and asymmetric encryption. Several encryptions that can be applied to digital envelopes on IoT constrained devices have also been obtained. For symmetric encryption, AES is the encryption that has been widely used on constrained devices. Meanwhile, Asymmetric encryption is ECDH. For symmetric encryption combined with ECDH, Twofish or other lightweight symmetric encryption such as AES can be used. Some of the devices used for research are mobile devices, computers, ESP8266, Arduino Nano, dan raspberry pi. For validation, AVISPA tools can be considered for use. In the future, we are planned to implement digital envelopes in IoT constrained devices to increase the safety factor of constrained devices.

ACKNOWLEDGMENT

CREDIT

References

1. Mike, O Ojo S, Giordano G, Procissi INS. A Review of Low-End, Middle-End, and High-End Iot Devices. IEEE Access 2018;6:70528–70554. https://ieeexplore.ieee.org/document/8528362.

2. Hari, Kishan Kondaveeti a N, Kumar Kumaravelu b S, Dayal Vanambathina b S, Ellison Mathe b S, Vappangi. A systematic literature review on prototyping with Arduino: Applications, challenges, advantages, and limitations. Computer Science Review 2021;40. https://www.sciencedirect.com/science/article/pii/S1574013721000046?via%3Dihub.

3. Weibao, Gao a b X, Luo b Y, Liu b Y, Zhao a Y, Cui. Development of an arduino-based integrated system for sensing of hydrogen peroxide. Sensors & Actuators Reports 2021;3:100045. https://www.sciencedirect.com/science/article/pii/

S2666053921000217?via%3Dihub.

4. Oscar, O Rodriguez-Diaz D, F Novella-Rodriguez E, Witrant E, Franco-Mejía. Benchmark for analysis, modeling and control of ventilation systems in small-scale mine. 2019 International Conference on Control & Automation & Diagnosis (ICCAD) 2020;3:1–6. https://ieeexplore.ieee.org/document/9037923.

5. Giuseppe Nebbione MCC. Security of IoT Application Layer Protocols: Challenges and Findings. Future Internet 2020;12:3:55. https://www.mdpi.com/1999-5903/12/3/55.

6. Panda, Prabhat Kumar C, Sudipta. A secure mutual authentication protocol for IoT environment. Journal of Reliable Intelligent Environments 2020;6:79–94. https://link.springer.com/article/10.1007/s40860-020-00098-y.

7. Chau D M Pham T, Dang K. A lightweight authentication protocol for D2D-enabled IoT systems with privacy. Pervasive and Mobile Computing 2021;74. https://www.sciencedirect.com/science/article/pii/S1574119221000559?via%3Dihub.

8. An, Braeken M, Liyanage A, Jurcut D. Anonymous Lightweight Proxy Based Key Agreement for IoT (ALPKA). Wireless Personal Communications 2019;106:345–364. https://link.springer.com/article/10.1007/s11277-019-06165-9.

9. Kai, Fan a H, Xu a L, Gao b H, Li a Y, Yang. Efficient and privacy preserving access control scheme for fog-enabled IoT. Future Generation Computer Systems 2019;99:134–142. https://www.sciencedirect.com/science/article/pii/S0167739X18323367?via%3Dihub.

10. Marco, Rasori M, La Manna P, Perazzo G, Dini. A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things. IEEE Internet of Things Journal 2022;9:8269 – 829. https://ieeexplore.ieee.org/document/9721417.

11. Farid, Akbar Siregar A, Rizka A, Siregar F. Analisis Perbandingan Algoritma NGG dan GGHN pada Frekuensi Hasil Enkripsi. Building of Informatics, Technology and Science (BITS) 2022;4:1860–1865. https://ejurnal.seminar-id.com/index.php/bits/article/view/1639.

12. Mariem, Bouchaala C, Ghazel L, Saidane A. Revocable sliced ciphertext policy attribute based encryption scheme in cloud computing. International Conference on Engineering Research, Innovation and Education 2014;1-6. https://ieeexplore.ieee.org/document/8766597.

13. Christian, F Durach J, Kembro A, Wieland. A New Paradigm for Systematic Literature Reviews in Supply Chain Management. Journal of Supply Chain Management 2017;53:4:67–85. https://onlinelibrary.wiley.com/doi/10.1111/jscm.12145.

14. Saurabh, Singh P, Kumar Sharma S, Moon Y, Park JH. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Ambient Intell Humaniz Comput 2017;https://onlinelibrary.wiley.com/doi/10.1002/cpe.6450.

15. Mohamed, Sirajudeen Yoosuf A, R. MQTT-PRESENT: Approach to secure internet of things applications using MQTT protocol. International Journal of Electrical and Computer Engineering (IJECE) 2021;11:5:4577. https://ijece.iaescore.com/index.php/IJECE/article/view/25403.

16. Nawal, Alsaffar W, Elmedany H, Ali. Application of RC5 for IoT devices in smart transportation system. 2019 8th International Conference on Modeling Simulation and Applied Optimization (ICMSAO), IEEE 2019;11:1–4. https://ieeexplore.ieee.org/document/8880351.

17. Al, Mashhadani M S, M. IoT Security Using AES Encryption Technology based ESP32 Platform. International Arab Journal of Information Technology 2022;19 No. 2.

18. V, Bansod T, Khandekar K. Reliability and availability of IoT devices in resource constrained environments. International Journal of Quality and Reliability Management 2022;39:1648–1662. https://www.emerald.com/insight/content/doi/10.1108/IJQRM-09-2021-0334/full/html.

19. Majid, Mumtaz J, Akram L, Ping. An RSA based authentication system for smart IoT environment. Proceedings - 21st IEEE International Conference on High Performance Computing and Communications, 17th IEEE International Conference

on Smart City and 5th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2019 (2019) 2019;11. https://ieeexplore.ieee.org/document/8855549.

20. Bismark, Tei Asare K, Quist Aphetsi L, Nana. Secure Data Exchange Between Nodes in IoT Using TwoFish and DHE. in 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), IEEE 2019;p. 101–104. https://ieeexplore.ieee.org/document/9058353.

21. Tanmoy, Maitra M, S Obaidat D, Giri S, Dutta K, Dahal. ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications. IET Networks 2019;8, No. 5:289–298. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-net.2019.0004.

22. Mohamed, Sirajudeen Yoosuf A, R. Lightweight fog-centric auditing scheme to verify integrity of IoT healthcare data in the cloud environment. Concurr Comput 2021;33, No. 24:289–298. https://onlinelibrary.wiley.com/doi/10.1002/cpe.6450.

23. M C, Pham T, Nguyen LP, Dang TK. Resource-Constrained IoT Authentication Protocol: An ECC-Based Hybrid Scheme for Device-to-Server and Device-to-Device Communications. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2019;11814:446–466. https://link.springer.com/chapter/10.1007/978-3-030-35653-8_30.

24. Ankur, Lohachab K. ECC based inter-device authentication and authorization scheme using MQTT for IoT networks. Journal of Information Security and Applications 2019;46:1–12. https://www.sciencedirect.com/science/article/pii/S2214212618306513?via%3Dihub.

25. Anothay, Phimphinith X, Anping Q, Zhu Y, Jiang Y, Shen. An Enhanced Mutual Authentication Scheme Based on ECDH for IoT Devices Using ESP8266. 2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN), IEEE 2019;46:490–496. https://ieeexplore.ieee.org/document/8905268.

26. Bormann, Keranen E. Terminology for Constrained-Node Networks. Internet Engineering Task Force (IETF) 2019;46:490–496.

How to cite this article: Isa Mulia Insan, Febriliyan Samopa (2023), Encryption of Internet of Things Constrained Device For Digital Envelope : A Systematic Literatur Review, *IPTEK The Journal of Technology and Science*, .