УДК 621.391.3

Dulia O.O. (Igor Sikorsky Kyiv Polytechnic Institute)
PhD **Minochkin D.A.** (Igor Sikorsky Kyiv Polytechnic Institute)

DOI: https://doi.org/10.17721/2519-481X/2021/73-07

METHODS OF THE PUBLIC-KEY BASED AUTHENTICATION IN THE INTERNET OF THINGS

The Internet of Things (IoT) is a modern paradigm where everyday objects are interconnected and communicate with each other over the Internet. IoT facilitates the direct integration of physical objects with the cyber world through intelligent sensors, RFID tags, smartphones and wearable devices. IoT networks offer a variety of application areas, covering environmental monitoring, healthcare, smart cities, military aviation, and intelligent transportation systems. The number of devices open to the public network is gradually increasing; devices have a direct interaction with the physical world to collect data. Currently, one of the most debatable problems in the development of post-NGN communication networks is the problem of identifying the Internet of Things devices. Modern anonymization methods and the supposed large number of Internet of Things devices connected to the public communications network make modern communication systems vulnerable to intruders. The vulnerability of security consists in the impossibility of authentication of the Internet of Things devices, which opens the possibility for attackers to manufacture counterfactual physical and virtual products.

This situation requires secure solutions to prevent private information leakage and malicious activation through peer-to-peer authentication and secure data transfer between IoT nodes and servers. However, the existing structure and IP-based IoT primitives are not fully developed with resource-constrained IoT devices (such as power consumption, computational resource, communication ranges, RAM, FLASH, etc.). As a result, lighter solutions are needed to ensure security on IoT devices with limited resources.

Objective is to create a public-key based authentication method for IoT system that will be more optimized and secure than methods which already used for the Internet of Things. During the work process most of the existing methods of the public-key based authentication have been analyzed. Based on this analysis was proposed an authentication method that combines existing methods with improved cryptography algorithm.

Keywords: IoT, Interent of Things, authentication, cryptography, public-key, internet.

Introduction. The Internet of Things (IoT) is a modern paradigm where everyday objects are interconnected and communicate with each other over the Internet. IoT facilitates the direct integration of physical objects with the cyber world through intelligent sensors, RFID tags, smartphones and wearable devices [1]. IoT networks offer a variety of application areas, covering environmental monitoring, healthcare, smart cities, military aviation, and intelligent transportation systems. The number of devices open to the public network is gradually increasing; devices have a direct interaction with the physical world to collect data.

Currently, one of the most debatable problems in the development of post-NGN communication networks is the problem of identifying the Internet of Things devices. These problems are stipulated by the impossibility of detection and control of IP devices by modern methods used to find devices in the public communications network (PCN). Modern anonymization methods and the supposed large number of Internet of Things devices connected to the PCN make modern communication systems vulnerable to intruders. The vulnerability of security lies in the impossibility of authentication of the Internet of Things devices, which opens the possibility for attackers to manufacture counterfactual physical and virtual products.

This situation requires secure solutions to prevent private information leakage and malicious activation through peer-to-peer authentication and secure data transfer between IoT nodes and servers. However, the existing structure and IP-based IoT primitives are not fully developed with

resource-constrained IoT devices (such as power consumption, computational resource, communication ranges, RAM, FLASH, etc.) [2]. As a result, lighter solutions are needed to ensure security on IoT devices with limited resources.

Formation of the problem. There are several types of public-key based authentication methods that can be used for IoT devices but we should relay to the fact that IoT devices are really resources limited. The methods of authentication with large mathematical operations can cause the IoT device or sensor to malfunction. And it's a really big problem since the sensor needs to do a high resource loading operation before each data sending to the server and while it will be doing this the main data processing will be blocked which leads to losing data.

By analyzing existing public-key based authentication methods we need to find the best solution that can be applied to IoT devices depending on the limitations. This method should have a high security level and be lightweight.

Analysis of previous studies. One of the first examples of symmetric cryptography is presented in [3]. A symmetric-key system is used to provide confidentiality of messages in transmission, storing, and processing. The symmetric-key algorithm performs the operations of encryption/decryption based on a single key that is shared by two or more parties. Unlike [3 - 4] argues that there is a difficulty in symmetric cryptography; unsecure delivery of the key from the encoder to the decoder(s) can introduce a security risk. Anyone who gains access to the symmetric key can access/modify/send the message without the recipient's knowledge that the message has been modified.

Authors in [4] argue that the symmetric key algorithms are quite efficient, but the key distribution is difficult to IoT end devices. The key distribution requires a secure connection between the key distribution server and the IoT nodes. Public-Key Cryptography (PKC) and asymmetric cryptography are two effective ways of providing confidentiality and authentication.

The author of [5] has also found that this method of cryptography is difficult for IoT end devices. However, researchers have concluded that the RSA is a relatively slow algorithm for encryption however it is commonly used to pass encrypted shared keys for symmetric key cryptography. Since RSA encryption is an expensive operation, in IoT it is rather used in combination with symmetric cryptography.

As we know from [6] in the IoT environment, the general public-key problem is the requirement of an authenticated exchange of public keys. The PKI consists of components to securely distribute public keys and is widely used in the traditional Internet. The most important aspect of the PKI is a trusted third party who signs the identifier of an entity with its private key.

But PKI also has cons, as reported by [7] and [8], when PKI comes to very resource-constrained devices in the IoT, for most current deployments there is either no security at all or security that is based on shared keys or pins/passwords. It means that the risk of hacker attacks and eavesdropping is huge. As we are getting more and more dependent on the IoT, this risk is not acceptable.

Security in IoT implementations must be a critical component either during the device design and manufacturing phase or during the initialization phase or a product update. Previous studies indicate that there is no method of public-key-based authentication which will fit best in all situation, it depends on the performance of the devices. All of these methods, presented in the review, have pros as well as cons. The purpose of the study is to find a way to combine symmetric and asymmetric cryptography in order to achieve the best results, so that we can compensate for different method's shortcomings. Theoretically, this combined method will have good security enough in most cases and will fit most Internet of Things end devices.

Main part. Symmetric encryption (Fig. 1) is used to ensure the confidentiality of the message during its transmission, storage, and processing [3]. The symmetric key algorithm performs encryption/decryption operations based on a single key used by two or more parties. The difficulty in symmetric cryptography is the secure delivery of the key from the encoder to the decoder, which can create a security risk. Anyone who accesses the symmetric key can access/modify/send the message without the recipient knowing that the message has been modified. To address these issues, public-key encryption has been developed.

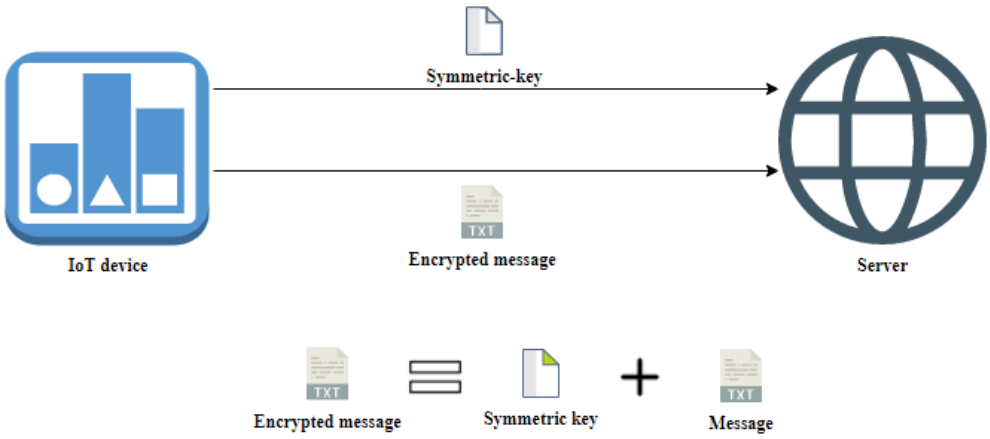

Figure 1 - Authentication method with symmetric cryptography

In symmetric-key encryption, the secret key S, the text message T and the encrypted text E of have the same length. For example, in AES 128 (Advanced Encryption Standard), the length of S, T, E is 128 bits (16 bytes), and encryption and decryption operations consist of XORing, permutations, bit offset, and linear mixing functions, which are performed in a known order. In general, the original plain text is divided into several blocks of fixed length:

$$E_i = Encrypt\ (S, T_i) \tag{1}$$

The weakness of symmetric cryptography is that the same blocks of plain text lead to the same cipher blocks. This is especially important for packages with a known format and a repeating pattern in the payload. To introduce randomness into cipher blocks and make decryption attacks difficult, you can use a Cipher Block Chaining (CBC), where before encoding each block of plain text is an exclusive operation (XORed) with the previous cipher block [9].

Asymmetric encryption or Public-Key cryptography (Fig. 2) always uses two different keys - private and public [10]. However, they are always generated as a linked pair. The private key always remains with the sender, while the public key is transmitted over an insecure channel to the receiving party [4]. The public key can be used to encrypt messages that can only be decrypted with the associated private key. The private key can generate an electronic signature that allows the recipient to uniquely identify the sender using the associated public key.

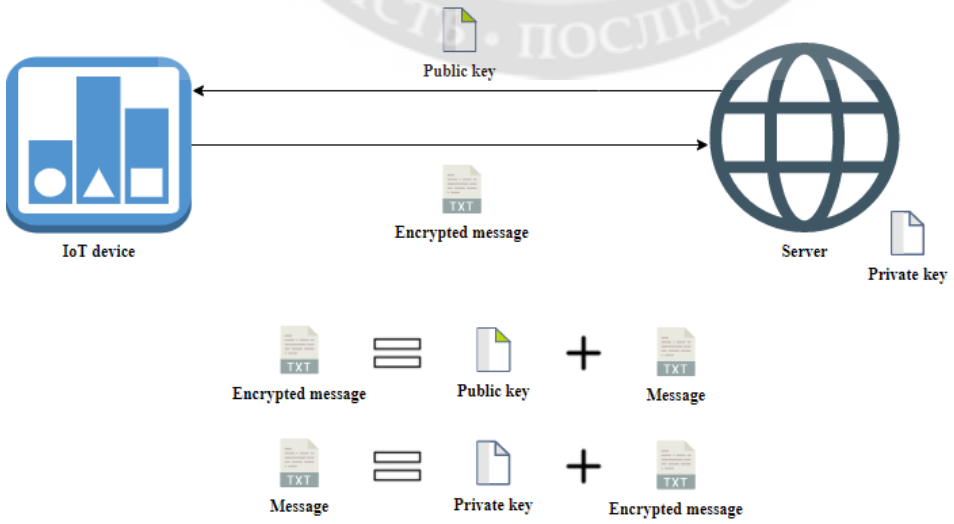

Figure 2 - Authentication method with asymmetric cryptography

Symmetric key algorithms are quite efficient, but key transfer is quite complex for IoT end devices. Key distribution requires a secure connection between the key distribution server and the IoT nodes. Public-key cryptography (PKC) is an effective way to ensure confidentiality and authentication [4]. Unlike symmetric encryption, asymmetric encryption is based on the idea of using one-way mathematical functions. They should be as simple as possible to calculate, but it is very difficult for them to do the reverse calculation. Since the constant increase in computing power improves the ability of computers to compute complex reversing functions, keys must be of appropriate length for proper security. Currently, 2048-bit keys such as RSA 2048 are classified as secure. Since encryption and decryption rates decrease as key lengths increase, asymmetric methods are only practical for processing small amounts of data.

As we see from [5] it also has been found that this method of cryptography is difficult for IoT end devices. It's because of a relatively slow speed of The RSA algorithm for encryption and that's the reason why it is commonly used to pass encrypted shared keys for symmetric key cryptography. Since RSA encryption is an expensive operation, in IoT it is rather used in combination with symmetric cryptography.

The problem with using public-key cryptography is the certainty/proof that a certain public key is genuine. It is correct and belongs to the declared person or legal entity, and has not been changed or replaced by an attacker or a third party. The usual approach to solving the problem is to use a PKI in which one or more third parties, known as a Certification Authority (CA), certify ownership of the key pairs.

A Public-Key Infrastructure (PKI) (Fig. 3) is a set of roles, policies, and procedures required to create, manage, distribute, use, store, and revoke digital certificates, and manage public-key encryption [11]. In the IoT environment, a common public key problem is the requirement for authenticated public key exchange. PKI consists of components for reliable public key distribution. The most important thing in PKI is a trusted third party that signs the entity ID with its private key.

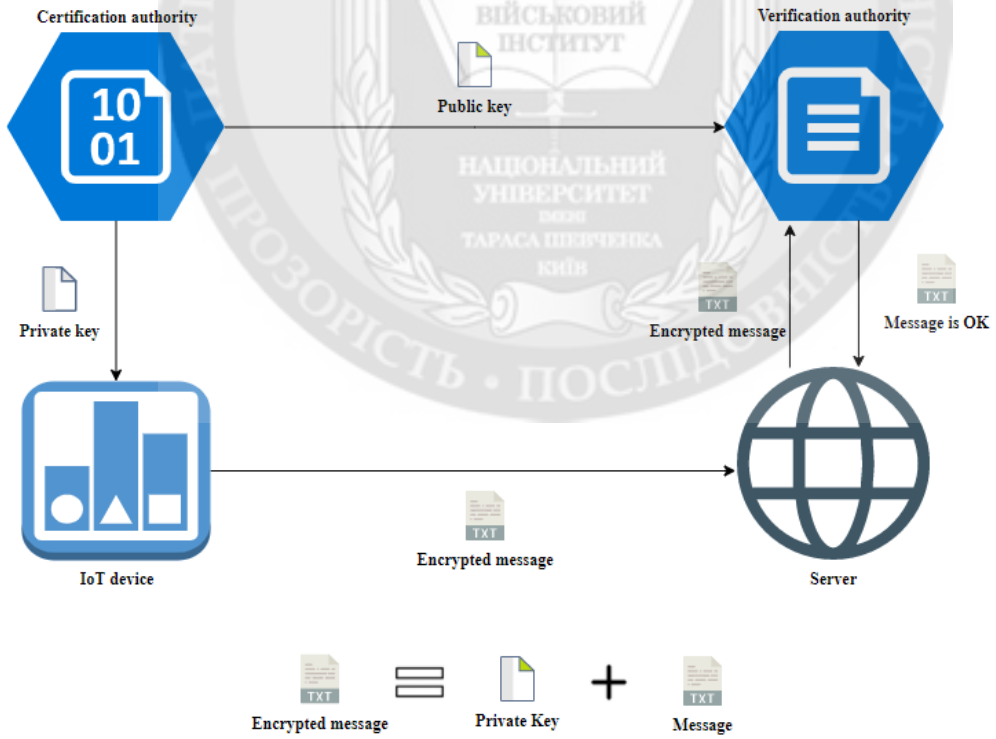

Figure 3 - Authentication method with public-key infrastructure

As we know from [6] in the IoT environment, the general public-key problem is the requirement of an authenticated exchange of public keys. The PKI consists of components to securely distribute

public keys and is today widely used in the traditional Internet. The most important part of the PKI is a trusted third party who signs the identifier of an entity with its private key.

But PKI also has cons, as reported by [8] and [12], when PKI comes to very resource-constrained devices in the IoT, for most current deployments there is either no security at all or security that is based on shared keys or pins/passwords. It means that the risk of hacker attacks and eavesdropping is huge. As we are getting more and more dependent on the IoT, this risk is not acceptable.

Proposed solution. We already know that symmetric cryptography has very good performance, which is exactly what we need to use it with resource-limited devices and sensors of the Internet of Things, but there is a drawback in the form of an insecure transmission of a single symmetric key. On the other hand, we have asymmetric cryptography, which has very good protection against hacking, but has algorithms that are difficult to calculate, which limits its use with devices of the Internet of Things. We propose a solution to combine these methods for maximum performance and security.

In the proposed solution, asymmetric cryptography is used only once when communicating between IoT devices in order to encode a symmetric key. For asymmetric cryptography, the Elliptical curve cryptography (ECC) algorithm was chosen, which provides the smallest key size, which provides good performance for IoT devices. Symmetric cryptography will be used for the main communication between devices and the server, using asymmetric cryptography to encrypt the symmetric key, we get rid of the most important disadvantage of symmetric cryptography, namely, the secure transfer of the key from the device to the server. The general scheme of work of my solution is shown in the Fig 4.

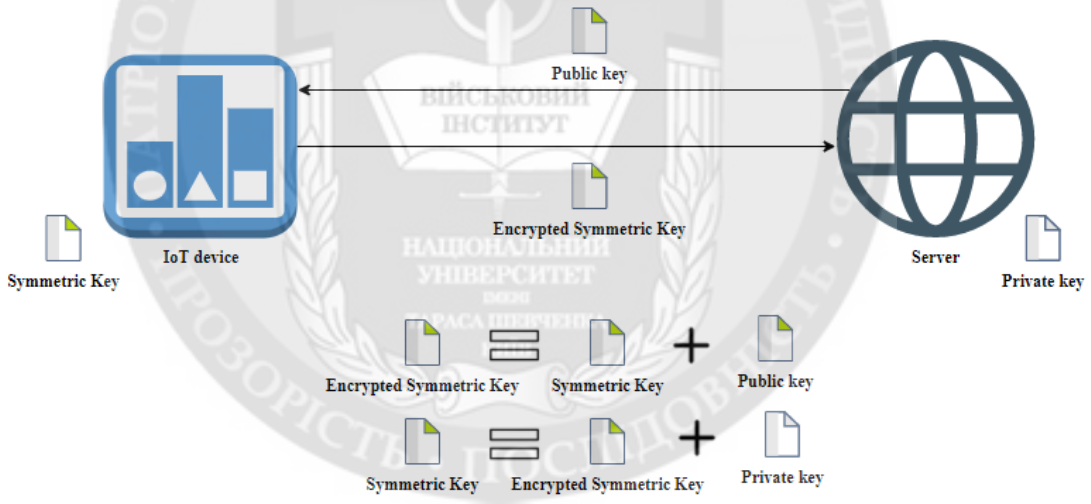

Figura 4 - Proposed solution, work algorithm

Conclusions. The proposed solution has good performance and is suitable for use in resource-limited devices and sensors of the Internet of Things, which is achieved by using asymmetric cryptography only for encrypting the symmetric key, as well as using the EEC algorithm, also the solution has required level of security, since the main drawback of symmetric encryption has been fixed. This solution can be used both for home devices and sensors as well as for industrial devices of the Internet of Things.

REFERENCES:

1. Zhao, Guanglei & Wang, Jingcheng & Luo, Jian & Long, Xiao & Si, Xianping. (2011). Applicability of Elliptic Curve Cryptography on Internet of Things. Energy Procedia. 11. 128-133. 10.1016/j.egypro.2011.10.220.

2. Singh, Deepti, et al. "A Secure IoT-Based Mutual Authentication for Healthcare Applications in Wireless Sensor Networks Using ECC." IJHISI vol.16, no.2 2021: pp.21-48. http://doi.org/10.4018/IJHISI.20210401.oa2

3. Rao U.H., Nayak U. (2014) Cryptography. In: The InfoSec Handbook. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4302-6383-8_8

4. Baldimtsi, F., Kiayias, A. and Samari, K. (2021), Watermarking public-key cryptographic functionalities and implementations: The case of encryption and signatures. IET Inf. Secur, 15: 205-222. https://doi.org/10.1049/ise2.12013

5. Z. Li, H. Zhao, X. Su and C. Wan, "Asymmetric Cryptography Based Unidirectional Authentication Method for RFID," 2018 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Zhengzhou, China, 2018, pp. 374-3743, doi: 10.1109/CyberC.2018.00073.

6. Marino, Francesco & Moiso, Corrado & Petracca, Matteo. (2019). PKIoT: A public key infrastructure for the Internet of Things. Transactions on Emerging Telecommunications Technologies. 30. 10.1002/ett.3681.

7. Vulić, I., Prodanović, R., Vukčević, G., Sretenović, S. Trust Establishing Model in IoT using PKI and Timestamp. In: Konjović, Z., Zdravković, M., Trajanović, M. (Eds.) ICIST 2018 Proceedings Vol.2, pp.333-338, 2018

8. Won, Jongho & Singla, Ankush & Bertino, Elisa & Bollella, Greg. (2018). Decentralized Public Key Infrastructure for Internet-of-Things. 907-913. 10.1109/MILCOM.2018.8599710.

9. Baldimtsi, F., Kiayias, A., Samari, K.: Watermarking public-key cryptographic functionalities and implementations. ISC 2017, 173– 191 (November 2017)

10. El. Gamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. CRYPTO 1985., 10– 18 (1985)

11. Gope P. Hwang T. (2016). A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks.IEEE Transactions on Industrial Electronics, 63(11), 7124–7132. 10.1109/TIE.2016.2585081

12. Watro R. Kong D. Cuti S. F. Gardiner C. Lynn C. Kruus P. (2004, October). TinyPK: securing sensor networks with public key technology. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (pp. 59-64). ACM.10.1145/1029102.1029113

Дуля О.О., к.т.н., с.н.с. Міночкін Д.А.

МЕТОДИ АВТЕНТИФІКАЦІЇ НА ОСНОВІ ВІДКРИТОГО КЛЮЧА ДЛЯ СИСТЕМИ ІНТЕРНЕТУ РЕЧЕЙ

Інтернет речей (IoT) – це нова парадигма, де повсякденні об'єкти взаємопов'язані та спілкуються один з одним через Інтернет. IoT полегшує пряму інтеграцію фізичних об'єктів із кібер-світом за допомогою інтелектуальних датчиків, RFID-міток, смартфонів та носимих пристроїв. Мережі IoT пропонують різноманітні сфери застосування, охоплюючи моніторинг навколишнього середовища, охорону здоров'я, розумні міста, військову авіацію та інтелектуальні транспортні системи. Кількість пристроїв, відкритих для загальнодоступної мережі, поступово збільшується; пристрої мають безпосередню взаємодію з фізичним світом для збору даних. Наразі однією з найбільш дискусійних проблем розвитку мереж зв'язку пост-NGN є проблема ідентифікації пристроїв Інтернету речей. Сучасні методи анонімізації та передбачувана велика кількість пристроїв Інтернету речей, підключених до загальнодоступної комунікаційної мережі, роблять сучасні комунікаційні системи вразливими для зловмисників. Уразливість безпеки полягає в неможливості аутентифікації пристроїв Інтернету речей, що відкриває можливість зловмисникам виготовляти контрафактні фізичні та віртуальні продукти.

Ця ситуація вимагає безпечних рішень для запобігання втрати приватної інформації та зловмисної активації за допомогою одноранговоі аутентифікації та безпечної передачі даних між вузлами Інтернету речей і серверами. Однак існуюча структура та примітиви IoT на основі IP не повністю розроблені з урахованням можливостей пристроїв IoT з обмеженими ресурсами (такими як енергоспоживання, обчислювальний ресурс, діапазон зв'язку, RAM, FLASH тощо). Як

наслідок, потрібні більш легкі рішення для забезпечення безпеки пристроїв IoT з обмеженими ресурсами.

Мета полягає в тому, щоб створити метод аутентифікації на основі відкритого ключа для системи IoT, який буде більш оптимізованим і безпечним, ніж методи, які вже використовуються для Інтернету речей. У процесі роботи було проаналізовано більшість існуючих методів аутентифікації на основі відкритих ключів. На основі цього аналізу був запропонований метод аутентифікації, який поєднує існуючі методи з покращеним алгоритмом криптографії.

Ключові слова: IoT, Interent of Things, аутентифікація, криптографія, відкритий ключ, Інтернет.