ECC Based Lightweight Cybersecurity Solution For IoT Networks Utilising Multi-Access Mobile Edge Computing

Eric Gyamfi
School of Computer Science
University College Dublin
Dublin, Ireland
Email: eric.gyamfi@ucdconnect.ie

James Adu Ansere
College of Internet Engineering
Hohai University
Changzhou, China
Email: jaansere@hhu.edu.cn

Lina Xu
School of Computer Science
University College Dublin
Dublin, Ireland
Email: lina.xu@ucd.ie

***Abstract*—The Security of the Internet of Things (IoT) has gained great attention recently due to the increased cyber-threats in those systems. IoT technologies have many use cases and real-life applications and the IoT devices have been widely produced by industries. However, the security issue of IoT devices has not been fully resolved, leaving those devices exposing to cyber-threats. IoT end devices are normally resource constraint, which makes the implementation of traditional security solutions extremely hard if not impossible. The emergence of IoT-Edge computing technologies can grant the IoT devices the ability to overcome the local resource constraint problem. The current industrial revolution (Industry 4.0) requires IoT devices to be secured in its data transmission, and protected from network Intrusions. Since many IoT devices reply on the unsecured Internet as a means for data transmission, there is an urgent need to provide a public key cryptographic technique to protect the end-to-end transmission between those IoT devices. In this paper, based on the Elliptic Curve Cryptographic (ECC) technique, we have proposed a lightweight asymmetric security solution to enhance secured transmission of data through utilising the IoT-Edge computing architecture. We also have successfully embedded our lightweight cryptography on the edge, and the IoT device. The experimental results has shown that the proposed lightweight ECC security system can provide better practice when implemented in the IoT-Edge environment.**

I. Introduction

Internet of things (IoT) is novel paradigm that allows smart devices connectivity for information exchange through the uses of internet infrastructure. IoTs have numerous applications that has progressively penetrated into in our daily activities. It was estimated that, by 2020, the IoT devices will get to 50 billion [1] for industrial automation, health monitoring and smart transportations. However, the mobile IoT network is facing cybersecurity challenges due to its high-density network size and security vulnerability. Most of the security vulnerabilities are exploited due to flaws in design, execution, process and internal mechanism [2], [3]. The IoT-Edge and its data exchange can be organised into three main layers as shown in our proposed design in Figure 1.

- LAYER I: The first Layer consists of the sensor that detects and measure raw data from the environments they are installed. The sensors collect data according to user configuration and specification.
- LAYER II: The edge when configured on the IoT system, enhance it to perform data processing and filtering of data before they are sent over to remote servers. Recently, modern IoT devices consist of their own embedded network systems typically IEEE IPv6 Low-powered Wireless Personal Area Network (6LoWPAN), Routing Protocol for Low-Powered Lossy Networks (RPL), and Mobile Ad-hock Networks (MANET) [4] which does not require external gateway modules.
- LAYER III: In this Layer, data is received from the IoT gateway and further processed. This section is normally equipped with higher resources that can process, perform analytics and store data beyond the second section.

Elliptic-Curve Cryptography (ECC) has been investigated as new approach to mitigate security attacks in IoT networks [5], [6]. Elliptic Curve Cryptography (ECC) is an asymmetric encryption technique that is used in securing data transmission over public network by exchanging public key. Cryptography is a science used to secure information. Before, RSA was one of the most widely used public key Encryption before the total emergence and implementation of ECC came to being [7]. The security of ECC depends on the Elliptic Curve Discrete Logarithm Problem (ECDLP). Due to breakthroughs on algorithms for solving its underlying complex problem, the length of RSA's operands has increase to 3072-bits for a security level of 128-bits which can be achieved with 256-bits for the same security level with ECC. Since the security strength of ECC depends much on the curve, the National Institute of Standard and Technology (NIST), and International Organisation for Standardization (ISO) have provided safe ECC curves that enhance creation of secured cryptographic Encryption [8]. ECC offer an IT robust solution in terms of data transmission confidentiality, data authenticity and reliability, and non-repudiation [9], [10]. The Diffie-Hellman key exchange allows principal communication security over public network by employing key exchange(Public/Private) [11]. In this paper,

978-1-7281-1796-6/19/$31.00 ©2019 IEEE

we generate our public and private key using ECC curve and Diffie-Hellman key exchange. The edge computing is another promising area that provide larger space and higher computational power for the IoT system. It gives the IoT power to overcome the limited resources and constraints by performing all the require computation at the edge point. In this paper, we examine the cybersecurity in IoT and propose an efficient Lightweight security enhancement with ECC technique for IoT networks configured with IoT-Edge. The technique was implemented and tested with an Azure IoT edge platform connected to a Linux Docker on IoT device. Our contributions in this paper are summarised as follow:

- We investigated cybersecurity threats scenario, and the lack of solution for securing data exchange in IoT networks.
- We propose an energy-efficient algorithm to achieve a reliable security enhancement using Lightweight ECC with the IoT-Edge, and maximise security of data transmission in IoT networks without third-party attacks.
- It is also our aim to identify what a lightweight ECC, and the ability to implement the method without compromising on the standard strength of security in of ECC
- Finally, we validated the proposed techniques and our results are compared with traditional ECC deployed on PC.

The rest of this paper is organised as follows. In Section II, we present the related works. In Section III, we investigate the secured data exchange between IoT devices. Section IV presents the proposed techniques, thus, implementation of ECC encryption and decryption in IoT edge and Traditional PC. In Section V, we evaluate the proposed technique performance by simulations, and Section VI draws the paper conclusion.

II. Related Work

We can define Lightweight cryptography as been the method of implementing security (cryptography) by considering the resource constrained nature of the device. Many lightweight techniques have been proposed to facilitate a mutual shared keys authentication and establishment among the two entities using gateway node. In PriAuth, entities are encrypted to certify secrecy and privacy [12] for patients health monitoring and evaluation using wearable sensors. However, the key exchange protocol has been adopted to safeguard keys security because of its computational complexity and power constraints [13]. The user anonymous key authenticity and establishment approach to boost symmetric cryptosystem operations in wireless sensor networks was proposed [14]. This was to prevent the intruders to interfere the security of a connected network. In pervasive computing settings, the digital publication copyright is a critical concern for data protection. Digital rights management (DRM) technology has been proposed to mitigate such challenges [15]. Generally, DRM as a software restricts the accessibility of its content usage for protection, authorisation, and distribution for efficient data encryption and security [16]. In IoT networks, sensor nodes can be employed in insecure and hostile environments, and making IoT network security a major issue in recent times [17]. The authors in [18] proposed employed the bilinear pairing to design a certificateless encryption technique using EC over the ring for enhancing security and efficiency for large number factoring in RSA. Moreover, in [19], the proposed scheme secures the random oracle model for the problem of intractable factoring of large number, to protect the data transmission privacy and integrity among the sensor node in IoT network and gateway node. A hybrid security cloud algorithm was proposed to eliminate the expired content. This algorithm audits and increases the prediction of malicious node actions for the duration of data transfer. However, the cloud server replication reduces the EC-Schnorr performance established encryption systems. To avoid the duplication in the cloud server, a blooming filter was integrated into EC-Schnorr encryption system to efficiently advance the security performance [20]. In IoT networks with mobile edge computing technique, data transmissions need the security upgrade to avoid interruption from unauthorised users. In general, symmetric and asymmetric key-based cryptography mechanism, ensuring efficient security is a topmost priority for data transfer among IoT devices [21]. Several existing works offer a comprehensive study on confidentiality and authenticity of data transmission to improving cryptosystem performances in IoT networks, such as flexible authentication, privacy-preservation and encryption algorithms to improve data transfer security [22]. Few of research works seek to enhance security in IoT networks, particularly on cybersecurity efficiency for IoT networks with mobile edge computing technique. This paper provides the enhancement of data transfer integrity and security based on Lightweight ECC data key protection technique.

III. Proposed Method

A. System Architecture

It has been noted that, improving the performance, the size or the energy consumption of IoT device to accommodate the ECC should not affect (mitigate or compromise) the design of the IoT device. We therefore controlled this issues by implementing our method along with an IoT edge platform. The Fig. 1 shows the design and implementation of our proposed solution. Layer I and Layer II are connected together through a locally internal arrangement; while the connection between the Layer II and Layer III is typically cloud-based and the communication is through public Internet. Most of computation such as the public and private key generation were done at the Server side to reduce the ECC algorithm to a lightweight on the IoT-Edge. The variation in technology is causing a lot of changes in security implementation. Therefore, the ability of our security method to change when a the IoT device is under attack was a major factor to us in our design. The architecture gives the user the flexibility to generate and use new key pairs at any point. Different ECC curves can also be implemented without any modifications in the security component on the IoT-Edge. In another word, one of the biggest advantages of this technology is that, changing the key size will not require new IoT devices, but only need to update the key on the IoT-Edge. Based on this design, when

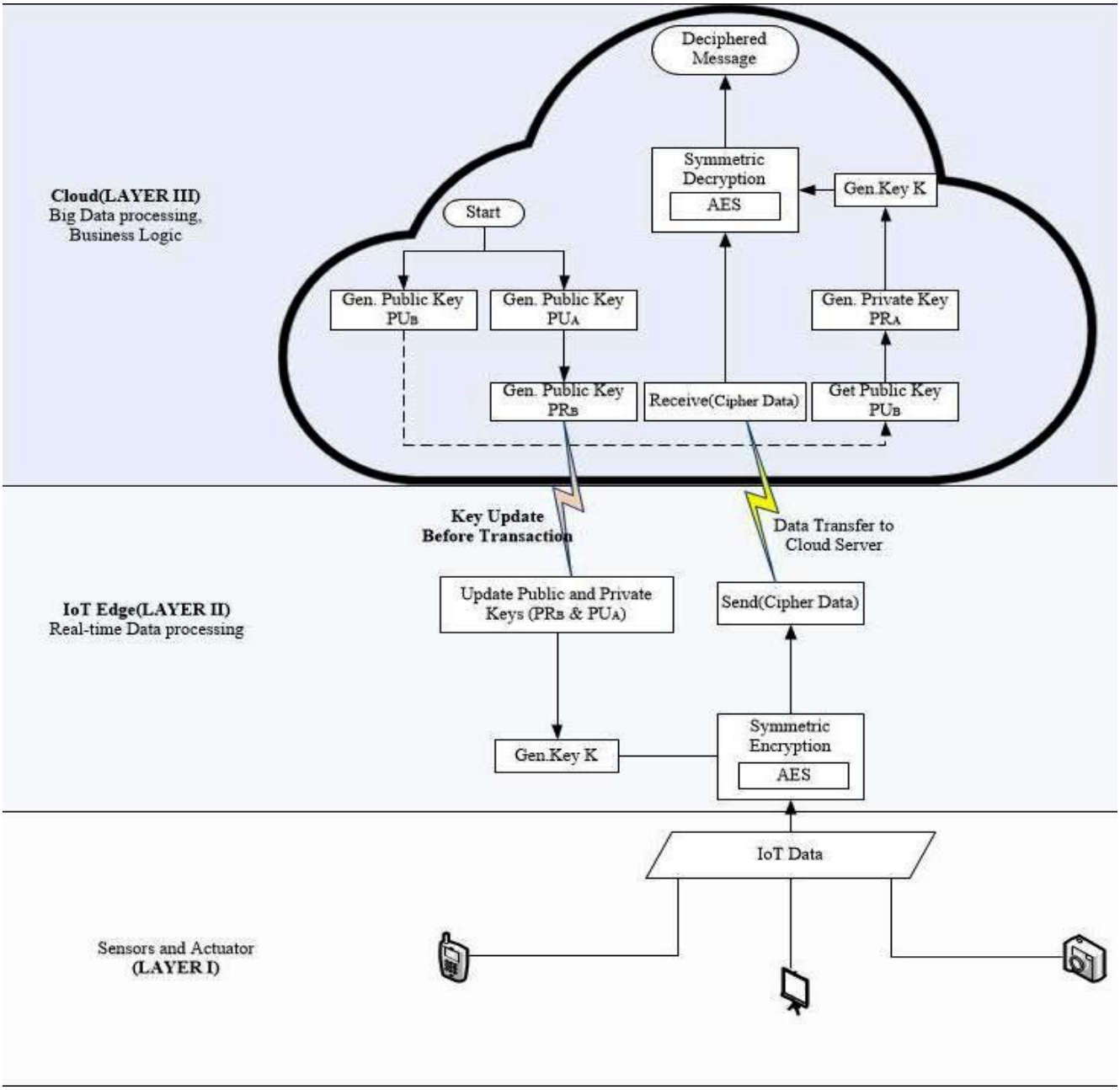

Fig. 1. Diagram of Lightweight ECC in IoT-Edge and Cloud Server

the security requirements and standards for the IoT devices is outmoded, it will be convenient for the user to switch to a more advanced ECC curve. Different keys can be used on different IoT devices, sharing information with the same cloud server.

B. The Diffie-Hellman ECC

The algorithm used in this paper consist of a lightweight implementation of ECC based on the Diffie-Hellman key exchange technique and Advance Encryption Standard (AES). The AES has been well accepted since it is computationally impossible for an adversary to obtain the transmitted content without the key. In symmetric encryption modeling, Plain text D is encrypted with a key K to produce ciphertext D'. The same key K is required by the receiving party to decipher the encoded information.

$$D' = Encrypt(K, D) \; and \; D = Encrypt(K, D') \quad (1)$$

In the asymmetric encryption, there are two pair of keys, Public key PU and Private key PR.

$$Y = Encrypt(PU, X) \; and \; X = Decrypt(PR, Y) \quad (2)$$

OR

$$Y = Encrypt(PR, X) \; and \; X = Decrypt(PU, Y) \quad (3)$$

Fig. 2. Structure of Proposed Method

To implement ECC base on Diffie-Hellman technique, a prime number q and an integer a that is a primitive root of q is known by the IoT edge and the remote server. The IoT-Edge selects a random integer $X_A < q$ and computes

$$Y_A = a^{X_A} mod\, q \tag{4}$$

The Server also randomly select $X_b < q$ and compute

$$Y_B = a^{X_B} mod\, q \tag{5}$$

Therefore IoT-Edge computes encryption Key K as

$$K = (Y_B)^{X_A} mod\, q \tag{6}$$

and the server also compute the encryption Key K as

$$K = (Y_A)^{X_B} mod\, q \tag{7}$$

The two keys K are identical since they can be proved by the rule of modular arithmetic as;

$$K = (Y_B)^{X_A} mod\, q \qquad [IoT - EdgeKey] \tag{8}$$

$$= (a^{X_B} mod\, q)^{X_A} mod\, q \tag{9}$$

$$= (a^{X_B})^{X_A} mod\, q \tag{10}$$

$$= a^{X_B X_A} mod\, q \tag{11}$$

$$= (a^{X_A})^{X_B} mod\, q \tag{12}$$

$$= (a^{X_A} mod\, q)^{X_B} mod\, q \tag{13}$$

$$K = (Y_A)^{X_A} mod\, q \qquad [ServerKey] \tag{14}$$

IV. Experiment and Result

A. Testbed Development

The following steps outline the process used in implementation of our technique.

1) IoT Edge Configuration: The Raspberry pi3 B+ was used as a testbed for the configuration of Azure IoT edge. The step-by-step configuration of the Azure IoT Edge and the Docker can be found on the Microsoft Azure website [23]. We also used the Visual Studio Code (VSCode) as a code editor on our Design platform. We established a connect between our IoT-Edge device and remote PC with Core (TM) i5 2.50GHz processor and 8.0GB running Microsoft Windows 10 professional X64 configured as our Remote Server.

2) Proposed Solution Implementation: Two sets of public, and private keys were generated from ECC Standard curves (BrainpoolPrime and NIST curves) based on 256-bits and 512-bits key size. The key exchange process was initiated by updating the IoT-Edge with $[PU_A, PR_B]$, and $[PU_A, PR_B]$ was used by the cloud server to generate Key K. We used K in each sides as encryption and decryption using AES with 10 different sets of data. Each of the experimental data were executed 1000 times continuously in both encryption and decryption method on the IoT-Edge, IoT device and the server. Figure 2 shows the data flow, encryption, and decryption process across the various section of our design. Sensor data is encrypted with low key at the IoT device level before it is transferred to the IoT-Edge. This ensures basic security since internet service is still used. The IoT-Edge receives the generated Public Keys from the cloud (Remote Server), extract and updates the various IoT devices accordingly. It also performs Higher standard of encryption and decryption to ensure maximum security. The Remote server perform Key generation base on supplied curve, update the various keys, perform encryption and decryption. The results obtained are shown in the next section.

B. Results

The graphs Fig. 3 and 4 show the results obtained from the IoT-Edge, and the IoT device(RaspberryPi 3B+). The y-axis in the graphs in Fig. 3 represent time in Milliseconds while the x-axis represents the size of data used in experiment. The results show that, on PC, IoT device, and IoT-Edge, the encryption times are higher than the decryption times. The results from the NISTprime curves in both 256-bits and 512-bits responded differently as compared to the BrainpoolPrime curve. In each of the experiments, the results from the ioT-edge shows that the execution time from 21KB to 673KB are very close. The execution time began to rise sharply after the 637KB. This shows that further increase in the data size will require higher execution time and resources. The overall execution rate on the IoT-Edge during the encryption using 512-key size was 51.82% better than the performance on a Server and IoT device. The 256-bits key size encryption process in IoT-Edge out-performed our other platforms by 33.43%. Moreover, the IoT-Edge case has showed 34.85% better performance during the decryption process using the 256-key size. Lastly, the performance of the IoT-Edge case during the decryption

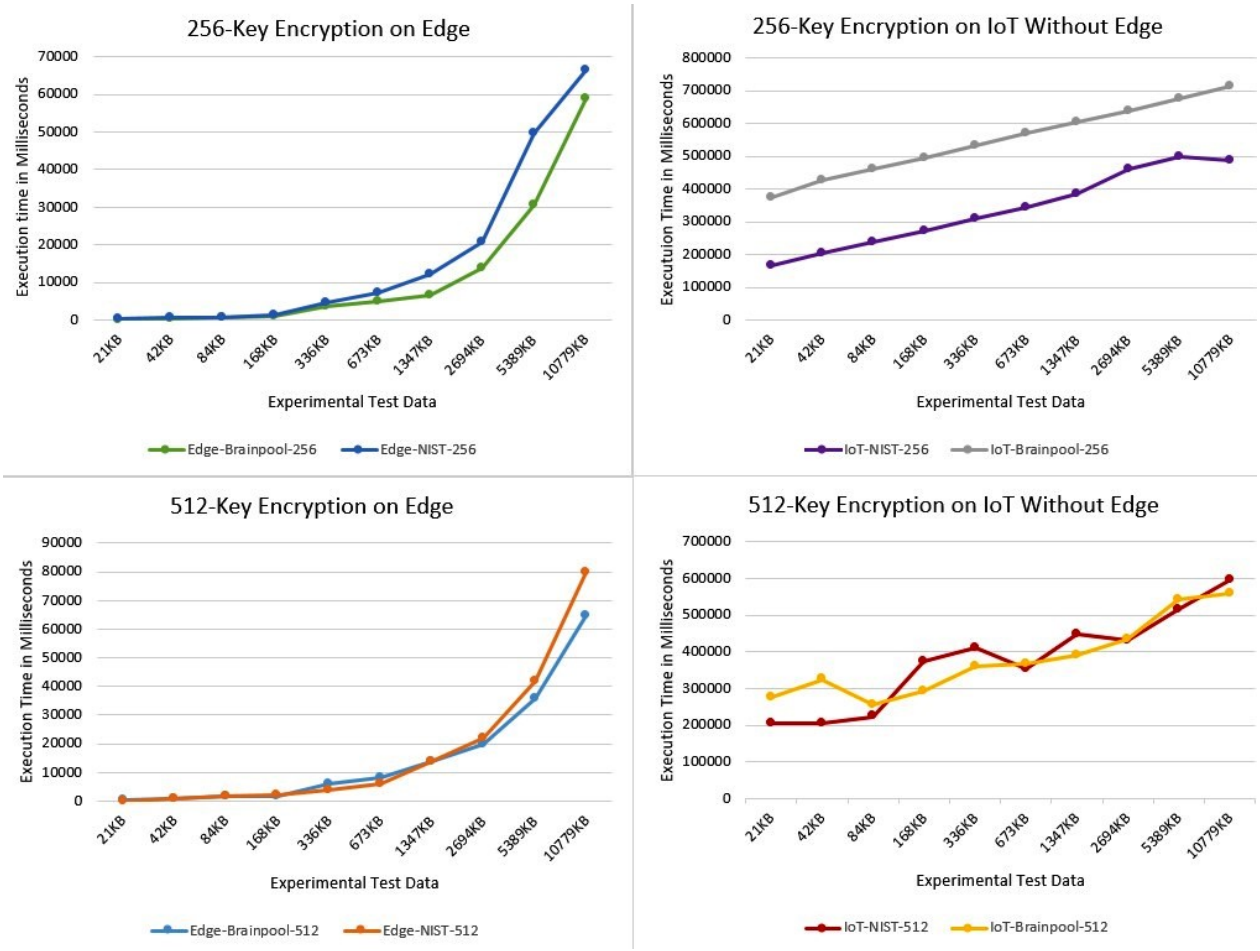

Fig. 3. Results of Encryption using IoT-Edge and IoT device

stage was 51.32% better when using 512-key size in the BrainpoolPrime curves. From our review, limited research has been done on the implementation of security for IoT using Edge Computing concept. The results obtained show clearly that the IoT-Edge solution is beneficial and advancing since it can provide additional resources to enhance the security protection the resource constraint IoT devices. Scaling down the ECC technique to a lightweight gives the IoT more computational power to also perform other operations along with the data exchange security. According to our knowledge, no existing work has been done on implementing ECC on IoT-Edge. Therefore, we have implemented the proposed lightweight ECC solution assisted by IoT-Edge as described in Section. IV-A. All the results obtained were measured during the encryption and decryption process excluding the public and private key generation as well as the key update process. Our Lightweight ECC on the IoT-Edge performed better with both 256-byte and 512-bits key size across the experimental data supplied as compared with running the same algorithm on independent.

V. Conclusion

In order to solve cyber-security problems over IoT devices, in this paper, we have proposed a novel lightweight ECC based solution to improve transmission security in IoT-Edge environment. This proposed solution has greatly reduced the complexity of the traditional algorithms, such as ECC and AES, and therefore significantly reduced the running time for heavy encryption. Due to the reduction in running time and resource demands, such a solution is highly appreciated on resource constraint IoT devices operating in an Edge enabled network. A real world testbed has been conducted and the experimental results has demonstrated a promising improvement over the traditional solutions.

The experimental results has demonstrated a promising improvement over the traditional solution.

References

[1] J. Rivera and R. van der Meulen, "Gartner says the internet of things installed base will grow to 26 billion units by 2020," *Stamford, conn., December*, vol. 12, 2013.

[2] D. Schatz, R. Bashroush, and J. Wall, "Towards a more representative definition of cyber security," *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, p. 8, 2017.

[3] C.-H. J. Wu and J. D. Irwin, *Introduction to computer networks and cybersecurity*. CRC Press, 2016.

[4] L. Zhou and H.-C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Network*, vol. 25, no. 3, 2011.

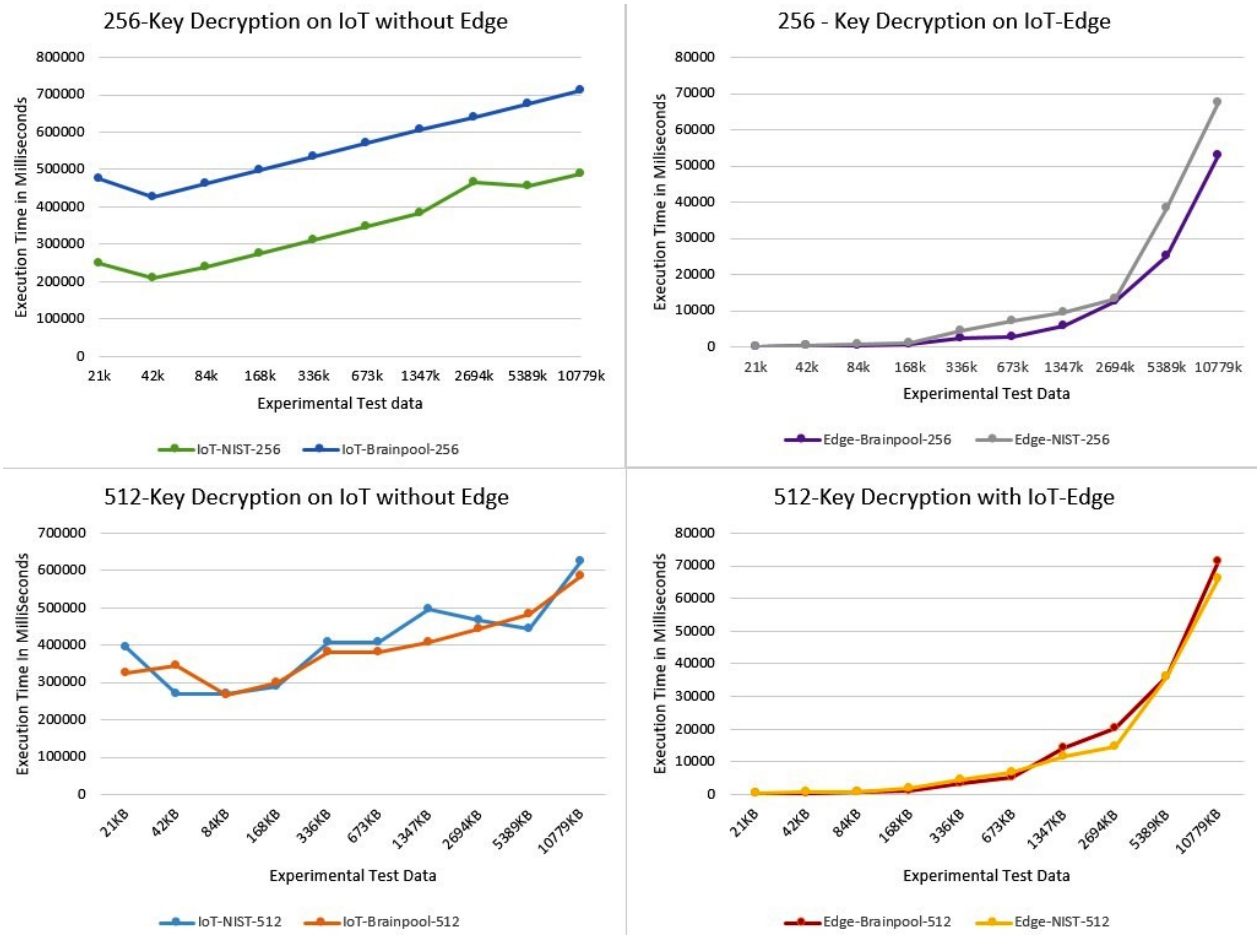

Fig. 4. Results of Decryption using IoT-Edge and IoT

[5] Z. Xiao, W. Song, Q. Chen *et al.*, "Dynamic resource allocation using virtual machines for cloud computing environment." *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1107–1117, 2013.

[6] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2386–2396, 2014.

[7] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[8] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, no. 2, pp. 147–159, 2011.

[9] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *IEEE transactions on parallel and distributed systems*, vol. 25, no. 2, pp. 468–477, 2014.

[10] Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, "Dynamic audit services for outsourced storages in clouds," *IEEE Transactions on Services Computing*, vol. 6, no. 2, pp. 227–238, 2013.

[11] E. Bresson, O. Chevassut, and D. Pointcheval, "Dynamic group diffie-hellman key exchange under standard assumptions," in *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2002, pp. 321–336.

[12] C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 357–366, 2016.

[13] A. G. Reddy, A. K. Das, E.-J. Yoon, and K.-Y. Yoo, "A secure anonymous authentication protocol for mobile services on elliptic curve cryptography," *IEEE Access*, vol. 4, pp. 4394–4407, 2016.

[14] J. Jung, J. Kim, Y. Choi, and D. Won, "An anonymous user authentication and key agreement scheme based on a symmetric cryptosystem in wireless sensor networks," *Sensors*, vol. 16, no. 8, p. 1299, 2016.

[15] A. Seki and W. Kameyama, "A proposal on open drm system coping with both benefits of rights-holders and users," in *Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE*, vol. 7. IEEE, 2003, pp. 4111–4115.

[16] H.-W. Yang, C.-C. Yang, and W. Lin, "Enhanced digital rights management authentication scheme based on smart card," *IET information Security*, vol. 7, no. 3, pp. 189–194, 2013.

[17] R. Guo, Q. Wen, H. Shi, Z. Jin, and H. Zhang, "Certificateless public key encryption scheme with hybrid problems and its application to internet of things," *Mathematical Problems in Engineering*, vol. 2014, 2014.

[18] H. Liu, Y. Zhou, and N. Zhu, "A novel elliptic curve scalar multiplication algorithm against power analysis," *Mathematical Problems in Engineering*, vol. 2013, 2013.

[19] Y. Chen, J.-F. Martínez, P. Castillejo, and L. López, "A privacy protection user authentication and key agreement scheme tailored for the internet of things environment: Priauth," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[20] V. Muthurajan and B. Narayanasamy, "An elliptic curve based schnorr cloud security model in distributed environment," *The Scientific World Journal*, vol. 2016, 2016.

[21] K. Yang, X. Jia *et al.*, "An efficient and secure dynamic auditing protocol for data storage in cloud computing." *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, 2013.

[22] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, no. 1, pp. 131–143, 2013.

[23] E. Bertrand, "Custom vision + azure iot edge on a raspberry pi 3," p. 1, 2018. [Online]. Available: https://azure.microsoft.com/en-us/resources/samples/custom-vision-service-iot-edge-raspberry-pi/