مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

Enhanced Data Security in IoT-Cloud Communication: Using Lightweight Cryptography Approach

Anaam Ghanim Hilal [1*], Mehdi Ebady Manaa[2]

1 College of Information Technology, University of Babylon, anaamgh.net.msc@student.uobabylon.edu.iq, Hilla,Iraq.
2 College of Information Technology, University of Babylon, It.mehdi.ebady@itnet.uobabylon.edu.iq, Hilla,Iraq.

*Corresponding author email: anaamgh.net.msc@student.uobabylon.edu.iq; mobile: 07814758916

تحسين أمن البيانات في اتصال إنترنت الأشياء – السحابة: باستخدام نهج التشفير الخفيف الوزن

انعام غانم هلال[1]*, مهدي عبادي مانع[2]

1 كلية تكنولوجيا المعلومات، جامعة بابل،anaamgh.net.msc@student.uobabylon.edu.iq، بابل، العراق

2 كلية تكنولوجيا المعلومات، جامعة بابل،anaamgh.net.mscIt.mehdi.ebady@itnet.uobabylon.edu.iq، بابل، العراق

Accepted: **23/8/2023** **Published:** **31/12/2023**

ABSTRACT

Background:

The Internet of Things (IoT) is expanding swiftly and producing a lot of data that needs to be securely stored. Although cloud computing is a useful method for storing IoT data, a lot of data is exposed to security risks and has a significant latency when it is sent from IoT devices to the cloud.

Materials and Methods:

The proposed work implements an authentication phase and encryption techniques between IoT devices and the cloud in order to address security challenges in IoT-Cloud computing systems. The client-side Elliptic Curve Diffie-Hellman (ECDH) protocol is used by the system to generate a shared secret key that is used to encrypt sensor data using the lightweight encryption method (SPECK). The encrypted data is additionally authenticated using a hashing process, guaranteeing its veracity and accuracy. On the server side, decryption processes are performed using the same encryption algorithms.

Results:

The results in the last read with data size 9198 Byte show that the system increased the Entropy value to 7.594 and the execution time will be 173 millisecond , and the Throughput is 53.16 .

Conclusion:

The obtained results of the proposed system are a good value in terms of the performance evaluation parameters such as encryption and decryption time, throughput, and entropy, which makes this algorithm more efficient and more secure.

Key words: Data security, Internet of things, Cloud computing, Lightweight algorithm, SPECK

\

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

1. INTRODUCTION

The Internet of Things (IoT) is a paradigm in which things having sensors, actuators, and processors interact with one another in order to accomplish a useful task[1]. Technology in the Internet of Things (IoT) is expanding quickly; by 2025, 75 billion connected devices are projected. IoT applications for smart environments, industry, and healthcare are just a few of the many options. These devices produce a lot of data, which conventional storage systems and processing platforms might not be able to handle. Therefore, managing and analyzing the data generated by IoT devices requires identifying appropriate solutions that rely on vast resource pools, such cloud computing.[2].

Cloud computing is powerful platform for delivering applications over the Internet or a private network. Cloud is The following technology is seen as being used in data processing and retrieval. These tools support data management and processing across a range of services and deployment patterns. Users are given the option to lease services in a certain range when receiving cloud services from cloud computing providers under a leased service delivery model. Today's big data situation calls for cloud data storage, which offers customers the same level of ease as on-premises devices. As a result, cloud computing is now being deployed centrally on a worldwide scale and is becoming a necessary component of IoT data processing[3].

In the context of the Internet of Things Huge amounts of data being transported through wireless networks to public cloud computing platforms, which raises a number of security concerns. IoT devices typically use wireless channels to send data across public networks, putting them susceptible to security problems including malicious attacks and data theft. IoT information security is therefore a significant concern that requires cutting-edge technologies to secure the system[4].

Encryption is the best way to safeguard information and data in many formats, such as files, images, and papers. The use of encryption is essential. By utilizing a mathematical technique to transform plain text into an unintelligible format, encryption can prevent illegal access and change[5].

Due to the constrained resources of IoT devices, lightweight cryptography has been created to lower hardware and software implementation costs. The main objective of lightweight cryptography is to lower implementation costs for both software and hardware due to the complexity of the computations required for conventional cryptography. It is designed for use in rapidly expanding applications that heavily rely on hardware with limited resources[6]. several symmetric algorithms, have been utilized to secure the data during transmission. In this work, we will focus on SPECK lightweight encryption algorithm.

2. RELATED WORK

In [7] The authors suggested a cryptographic method for enhancing cloud computing security based on an improved Blowfish algorithm and elliptic curves. By using elliptic curve cryptography for the key and blowfish for data encryption, performance and security are both improved. The security of your data is ensured by using MD5-based digital signatures, as suggested. It is feasible to show a general improvement by comparing the performance of the solution with that of AES, DES, 3DES, and RSA. The recommended method is typically more efficient in terms of throughput, memory use, and runtime when compared to other alternatives.

In [8] The author suggests a brand-new encryption technique called Enhanced Modern Symmetric Data Encryption (EMSDE) to protect data in an Internet of Things (IoT) environment that uses the cloud. To make sure that the final encrypted text is uncrackable by malevolent users, EMSDE uses a 64-bit block and eight rounds of encryption. According to the findings, EMSDE has a security rating of 90% compared to DES's 78% and Blowfish's 84%, making it more secure than previous encryption methods. Furthermore, both during encryption and decryption, the suggested methodology is quicker than currently used encryption methods.

In [9] To enhance the security performance of IoT environments against various assaults, the authors suggested utilizing the LWC-ABE (Lightweight Cryptography-Attribute-Based Encryption) technique. IoT servers and devices may experience a bottleneck as a result of the method's utilization of numerous trusted authority environments to boost security. The suggested LWC-ABE method's high expressiveness, which enables access policy modifications and broad attribute domains, is one of its benefits. The simulation results show that the suggested method speeds up encryption and decryption compared to traditional methods for multiple users and various message sizes. With an encryption time of 0.000835s and a decryption time of 0.000310s, the numerical results of the proposed method demonstrate a significant increase in the performance of encryption and decryption times. This shows that the suggested approach is effective.

In [10] the hybrid lightweight cipher approach suggested by the authors to boost data security in IoT-based healthcare systems. To provide safe data transfer, the suggested technique makes use of the Present and Tea encryption algorithms, ECC authentication, and key generation technologies. The system enhances security while lowering network latency, making the most use of channel resources, and maintaining network performance. The study indicated that overall, the packet loss rate was decreased by 3.835 percentage points, resulting in a mean throughput of 68.74475 kbps for the payload, a mean latency of 17.158 seconds.

In [11] The authors suggest a cryptographic strategy that combines two different types of encryption to increase cloud security. The New Effective Light-Weight Cryptographic Method (NELC), which uses a symmetric key technique to encrypt data with a block encryption size of 8–16 bytes and a key size of 8–16 bytes, offers the first layer of protection. The multiplicative homomorphic property of the RSA algorithm provides an additional level of security for the data it stores. By fusing Network substitution-permutation (S.P.) characteristics with elements of the Feistel structure, the N.E.L.C. algorithm creates confusion and diffusion, increasing the difficulty of encryption. The algorithm also uses sequential processing, exclusive or (XOR), not (Ex-NOR), and other fundamental Boolean operations. The method utilizes mathematical operations to produce random data and confuse the receiver throughout each cryptographic round. The proposed solution reduces the number of iterations in the algorithm to 7, with each iteration requiring 32 bits of cryptographic data to function and therefore conserving energy. Experiments show that implementing the proposed method significantly speeds up the encryption process while also reducing its memory size and execution time.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652
info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

3. Materials and Methods

A. Methods

Speck Algorithm which was created in 2013 by the National Security Agency (NSA) as a family of block blades that are thin and symmetrical. The algorithm was designed to provide secure cryptography in situations with limited resources, where standard cryptography methods would not function effectively. The Speak and Simon method has been extensively tested and has been proven to be secure. It is also more flexible compared to other lightweight ciphers. This algorithm relies on basic operations like AND, OR, and XOR, which can be executed even on devices with limited resources, making it adaptable and effective in the future[12]. The primary objective of the Speak algorithm is to ensure safety in constrained devices. It has a strong reputation for having quick execution times, security, and using simple operations[13].

Speck algorithm, which offers various block and key sizes to accommodate the user's hardware resources. This is in contrast to other lightweight ciphers that operate with fixed-size keys and blocks. The algorithm supports 10 different sizes depending on block size (2n) and key size (mn) resulting in 20 different sizes 10 for encryption and 10 for decryption, this flexibility allow the algorithm to be applied in both small embedded devices and sophisticated computer systems. Additionally, the Speck scheme includes a counter that is built into the algorithm. This improves the efficiency of the algorithm and guards against rotation and slide assaults. This means that the Speck algorithm is not only flexible, but also provides strong security features that make it a reliable choice for various applications[14]. The pseudo code of the SPECK algorithm is shown in algorithm 1

Algorithm 1: pseudo code of the SPECK encryption

```
Input: sensor data
Output: Encrypted data
Begin:
Step1: Generate a key.
Step 2: input data.
Step3: input values for α, β.
        Step 4: Split the input data block into two half : X, Y.
        Step5: For each round, apply the equation of encryption with the SPECK algorithm
        $R(x, y) = ((S^{-\alpha}$ x + y) ⊕ k, $S^{\beta}$ y Å ($S^{-\alpha}$ x + y) ⊕ k)
                can be described the equation of encryption as the following:
                Step 5.1: Apply the shifting α to X(left side) input data.
                    Step 5.2: Apply the Anding operation between the output of shifting X
                    with Y(right side), the result of this operation can be called X1
                    Step 5.3: XOR the X1 bit state with the round key Ki, the result of this
                    operation will be X2
                    Step 5.4: Apply the shifting β to Y input data.
                    Step 5.5: Apply the XOR operation between the output of shifting Y
                    with X2
          Step6: The 64-bit state is the output
      End
```

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com | ISSN: 2312-8135 | Print ISSN: 1992-0652

B. System Specifications

This approach involves the use of IoT devices like Raspberry Pi equipped with temperature, heartbeat rate, and oxygen sensors as the main data gathering points.

1. Raspberry Pi (RPi): is a fundamental building block due to its small size, affordability, processing power, and flexibility. The RPi is a computer that can be programmed that comes with built-in support for input/output ports and network connectivity, making it ideal for monitoring and controlling sensing devices in the proposed system. the model of raspberry pi used is version 3 B+ (ARD_000049).
2. Temperature Sensor: monitoring and identifying changes in body temperature. The model of this device used is DS18B20 Waterproof Digital Thermal Probe 1m.
3. A sensor of oxygen, a Heart rate sensor (Pulse sensor module): the measurement of the body's pulse or heart rate. The model of this device used is Pulse Ox meter (SPO2) Sensor MAX30100.

These devices are connected to a cloud computing platform type virtual private server (VPS) with CPU 2*2.6 GHz, RAM 4GB and Bandwidth 8TB, which acts as the central management and storage solution for the collected data by using HTTPs protocol.

4. THE PROPOSED APPROACH

The proposed approach is built on the SPECK algorithm, which is frequently used in encryption-related tasks. At the IoT sensor level, the SPECK approach is utilized to encrypt sensor values before they are sent to the cloud computing level. By doing this, the data are safeguarded and sent more securely. The flowchart for the suggested method is shown in Figure 1.

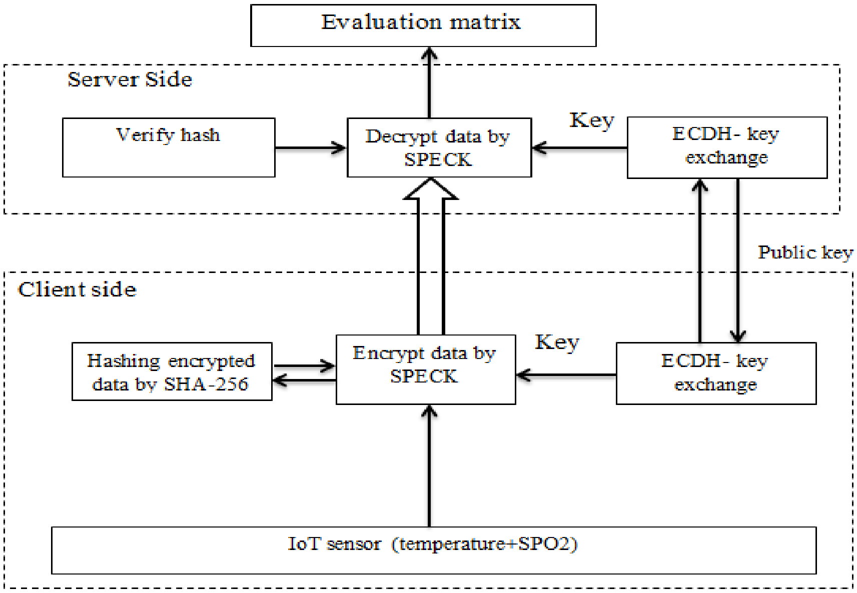

Figure 1. The flowchart of the proposed system

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

A. System implementation steps

1. Read sensor data: IoT sensors strategically placed in the environment gather essential information like oxygen saturation levels, temperature, and heart rate. A Raspberry Pi serving as a gateway receives this data and processes it before uploading it to the cloud. Real-time data processing and capture are made sure of in this step.
2. Key Exchange: Elliptic Curve Diffie-Hellman (ECDH) key exchange is used to enable secure communication between IoT devices and the cloud. Only IoT devices and the cloud have access to the shared secret key established by the ECDH protocol. The security of data transmission is increased by the use of this shared secret key for encryption and decryption.
3. Encryption: The sensor data is encrypted using SPECK lightweight encryption algorithm. The algorithm is designed for IoT environments, offering a high level of security while minimizing computational and energy costs. Encryption ensures that even if the data is intercepted during transmission, it remains secure and unreadable to unauthorized parties.
4. Digital signature: To protect the authenticity and integrity of the encrypted data, the SHA-256 digital signature algorithm is employed. This algorithm generates a unique signature that can only be reproduced by the original sender. It provides additional assurance that the data has not been tampered with during transit, maintaining data integrity.
5. Transmission: After encryption and digital signature, the data is sent from the IoT devices to the cloud server using a secure protocol such as HTTPS. HTTPS ensures the privacy and integrity of data during transit between the IoT devices and the cloud server, preventing unauthorized access or tampering.
6. Decryption: Upon reaching the cloud server, the encrypted data is decrypted using the shared secret key obtained through the ECDH key exchange. This step allows authorized parties, such as medical professionals or researchers, to access and analyze the data securely.
7. Store data: Finally, the decrypted data is stored in a secure location within the cloud for future reference and analysis. Storing data in a secure manner ensures that it remains accessible for long-term monitoring and research purposes while maintaining its confidentiality.

B. Evaluation Metrics

The proposed cryptosystem will be tested and evaluated using some assessment metrics, including:

1. Throughput

The greatest amount of data that can be delivered across an internet connection from source to destination in a specific amount of time is measured using this unit. Equation (1) is utilized to calculate the throughput[15].

$$Throughput = \left(\frac{Number\ of\ send\ data}{Time}\right) \quad \ldots.(1)$$

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

2. Execution Time

It is a measure of how long it takes for a system or application to complete a specific task. It is often used to evaluate the efficiency of a system or application. The execution time is calculated using Equation (2) [16].

$$Execution\ time = End\ Time - start\ Time \qquad \dots.(2)$$

3. Entropy

Entropy, which is used to define and measure the unpredictable nature of data, is the most significant indicator of information randomness. Its definition states that it is the projected average scale of information from the data following encryption. Equation (3) is utilized to calculate the entropy [17].

$$Entropy = -\sum_{i=0}^{m} pi\ log_2(pi) \qquad \dots..(3)$$

5. RESULTS AND DISCUSSION

The output of the suggested approach is based on the main network architecture derived from the IoT and cloud layers of cloud computing. The results are shown in Table (1) and Figure (2) based on 10, 100, and 1000 sensor readings with input data sizes of 90 Byte, 918 Byte, and 9198 Byte respectively, and it has the least execution time for the smallest input data size and number of sensor readings.

Table (1): the result of the SPECK algorithm

No. of reads	Data Size in Byte	Encryption Time (ms)	Throughput (Byte/ ms)	Entropy
10	90	7	12.85	7.353
100	918	52	17.65	7.419
1000	9198	173	53.16	7.594

From table (1) notice that, As the data size increases, the encryption time generally increases. For example, with 10 reads and a data size of 90 bytes, the encryption time is 7 milliseconds. However, with 1000 reads and a data size of 9198 bytes, the encryption time increases to 173 milliseconds.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

The throughput varies with the data size. In general, as the data size increases, the throughput tends to decrease. For instance, with 10 reads and a data size of 90 bytes, the throughput is calculated as 12.85 bytes per millisecond. On the other hand, with 1000 reads and a data size of 9198 bytes, the throughput decreases to 53.16 bytes per millisecond.

The entropy values generally increase as the number of reads and the size of the data increase. For example, with 10 reads and a data size of 90 bytes, the entropy is 7.353. However, with 1000 reads and a data size of 9198 bytes, the entropy increases to 7.594.

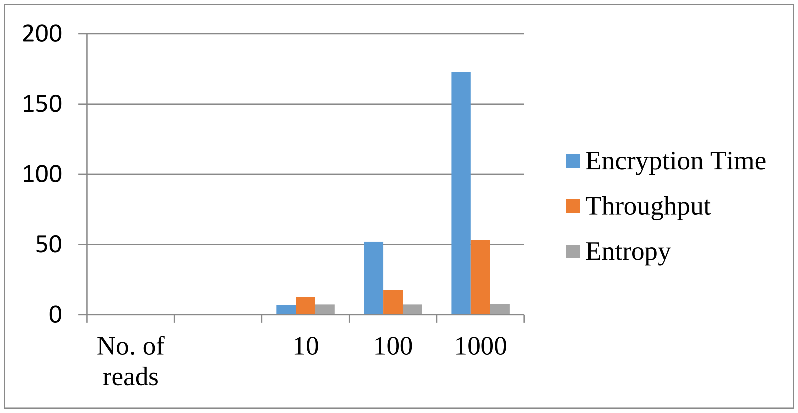

Figure 2: the result of the SPECK algorithm

In Table (2), a comparison is made between the proposed system and one of the previous works. The reference number [9] pertains to the algorithm named LWC-ABE, and the proposed algorithm is referred to as SPECK. The data size being considered is 100 bytes, and the corresponding encryption time in milliseconds is given for each algorithm. According to the data presented, the proposed SPECK algorithm demonstrates significantly faster encryption times (8 ms) compared to the LWC-ABE algorithm (157 ms), making it a more efficient option for this specific data size.

Table (2):A comparison between the proposed system and one of the previous works

Ref.no	Algorithm Name	Data size	Encryption Time(ms)
[9]	LWC-ABE	100 Byte	157
proposed	SPECK	100 Byte	11

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

6. CONCLUSION

Cloud computing and the Internet of Things (IoT) have been merged to provide clients with a wide range of services. Cloud computing, however, faces formidable challenges as the number of Internet-connected smart devices increases exponentially, especially for real-time and low-latency applications. One of the biggest problems with IoT and cloud computing is ensuring the security and privacy of the data being transmitted and stored. The suggested solution encrypts sensor data on the Raspberry Pi using the SPECK algorithm and the ECDH protocol in order to produce shard keys in a safe manner without the involvement of a third party. This helps defend against potential hacks and attacks on the sensitive data. Additionally, the system is assessed using metrics like execution time, throughput, and entropy to make sure to ensure that it is efficient and performs well in a real-world scenario. Overall, the proposed system is a promising solution for improving security and privacy in IoT and Cloud computing applications. The SPECK algorithm is fast and the randomize of encrypted data is high (Entropy value) that make this algorithm more efficient in IoT-cloud environment . For further study, we suggest hybrid lightweight cryptography algorithms for increased transmission speed and security.

Conflict of interests.

There are non-conflicts of interest.

References

[1] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” *J. Electr. Comput. Eng.*, vol. 2017, 2017, doi: 10.1155/2017/9324035.

[2] A. H. Aly, A. Ghalwash, M. M. Nasr, and A. A. A. El-Hafez, “Formal security analysis of lightweight authenticated key agreement protocol for IoT in cloud computing,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 24, no. 1, pp. 621–636, 2021, doi: 10.11591/ijeecs.v24.i1.pp621-636.

[3] M. Manna and M. Ali Mohammed A, “Data Encryption Scheme for Large Data Scale in Cloud Computing,” *J. Telecommun. Electron. Comput. Eng.*, vol. 9, no. 2–12, pp. 1–5, 2017.

[4] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” *Futur. Gener. Comput. Syst.*, vol. 78, pp. 964–975, 2018, doi: 10.1016/j.future.2016.11.031.

[5] M. Usman, I. Ahmed, M. I. Aslam, S. Khan, and U. A. Shah, “SIT: A Lightweight Encryption Algorithm for Secure Internet of Things,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 1, pp. 402–411, 2017, doi: 10.14569/IJACSA.2017.080151.

[6] M. Subhi Ibrahim, Y. Amer Abbas, and M. Hussein Ali, “Efficient hardware implementation for lightweight Loong algorithm using FPGA,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 30, no. 1, p. 451, 2023, doi: 10.11591/ijeecs.v30.i1.pp451-459.

[7] H. Abroshan, “A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography Algorithms,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 6, pp. 31–37, 2021, doi: 10.14569/IJACSA.2021.0120604.

[8] S. Alexander Suresh and R. Jemima Priyadarsini, “Design of Maintaining Data Security on IoT Data Transferred Through IoT Gateway System to Cloud Storage,” *Int. J. Comput. Networks Appl.*, vol. 9, no. 1, pp. 135–149, 2022, doi: 10.22247/ijcna/2022/211632.

[9] M. Jammula, V. M. Vakamulla, and S. K. Kondoju, “Hybrid lightweight cryptography with attribute-based encryption standard for secure and scalable IoT system,” *Conn. Sci.*, vol. 34, no. 1, pp. 2431–2447, 2022, doi: 10.1080/09540091.2022.2124957.

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

[10] A. S. Kadhim, A. H. Alazam, and N. F. Sahib, “A hybrid lightweight security approach in internet of things for healthcare application,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 6, pp. 3562–3569, 2022, doi: 10.11591/eei.v11i6.4417.

[11] F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, “A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing,” *Int. J. Intell. Networks*, vol. 3, no. April, pp. 16–30, 2022, doi: 10.1016/j.ijin.2022.04.001.

[12] A. D. Dwivedi, P. Morawiecki, and G. Srivastava, “Differential Cryptanalysis of Round-Reduced SPECK Suitable for Internet of Things Devices,” *IEEE Access*, vol. 7, pp. 16476–16486, 2019, doi: 10.1109/ACCESS.2019.2894337.

[13] L. Sleem and R. Couturier, “Speck-R: An ultra light-weight cryptographic scheme for Internet of Things,” *Multimed. Tools Appl.*, vol. 80, no. 11, pp. 17067–17102, 2021, doi: 10.1007/s11042-020-09625-8.

[14] A. Alkamil and D. G. Perera, “Towards Dynamic and Partial Reconfigurable Hardware Architectures for Cryptographic Algorithms on Embedded Devices,” *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3043750.

[15] A. N. Kadhim and M. E. Manaa, “Design an efficient internet of things data compression for healthcare applications,” *Bull. Electr. Eng. Informatics*, vol. 11, no. 3, pp. 1678–1686, 2022, doi: 10.11591/eei.v11i3.3758.

[16] D. B. Stewart, “Measuring Execution Time and Real-Time Performance,” *Embed. Syst. Conf. (ESC SF)*, no. September, pp. 1–15, 2002.

[17] G. A. A.-R. Abdulrazzaq H. A. Al-Ahdal and and N. K. Deshmukh, “Sustainable Communication Networks and Application Proceedings of ICSCN 2020,” 2021.

مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية مجلة جامعة بابل للعلوم الصرفة والتطبيقية

ISSN: 2312-8135 | Print ISSN: 1992-0652

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com

info@journalofbabylon.com | jub@itnet.uobabylon.edu.iq | www.journalofbabylon.com ISSN: 2312-8135 | Print ISSN: 1992-0652

الخلاصة

المقدمة:

نتيجة للتطور الحاصل في تكنولوجيا المعلومات و الاتصالات ظهرت العديد من المفاهيم المهمة و المرتبطة بالأنترنيت. يعتبر إنترنت الأشياء (IoT) احد اهم المفاهيم التي تطورت بسرعه كبيره والتي تنتج كميه كبيره من البيانات التي يجب تخزينها بشكل آمن. على الرغم من أن الحوسبة السحابية هي طريقة مفيدة لتخزين بيانات إنترنت الأشياء ، إلا أن الكثير من البيانات تتعرض لمخاطر أمنية ولها زمن انتقال كبير عند إرسالها من أجهزة إنترنت الأشياء إلى السحابة.

طرق العمل:

ينفذ العمل المقترح مرحلة المصادقة وتقنيات التشفير بين أجهزة إنترنت الأشياء والسحابة من أجل مواجهة التحديات الأمنية في أنظمة الحوسبة السحابية لإنترنت الأشياء. يستخدم النظام بروتوكول Elliptic Curve Diffie–Hellman (ECDH) من جانب العميل لإنشاء مفتاح سري مشترك يُستخدم لتشفير بيانات المستشعر باستخدام طريقة التشفير خفيفة الوزن (SPECK). تتم مصادقة البيانات المشفرة أيضًا باستخدام عملية التجزئة ، مما يضمن صحتها ودقتها. على جانب الخادم ، يتم تنفيذ عمليات فك التشفير باستخدام نفس خوارزميات التشفير.

الاستنتاجات:

تظهر النتائج في القراءة الأخيرة بحجم البيانات 9198 بايت أن النظام زاد من قيمة Entropy (العشوائية) إلى 7.594 وسيكون وقت التنفيذ 173 مللي ثانية ، والإنتاجية 53.16 بايت / مللي ثانية. تعتبر النتائج التي تم الحصول عليها من النظام المقترح ذات قيمة جيدة من حيث معايير تقييم الأداء مثل وقت التشفير وفك التشفير والإنتاجية والانتروبيا. مما يجعل هذه الخوارزمية أكثر كفاءة وأمانًا.

الكلمات المفتاحية: أمن البيانات ، إنترنت الأشياء ، الحوسبة السحابية ، الخوارزمية الخفيفة ، SPECK