New Hybrid Lightweight Data Encryption Algorithm for Operation System Protocol in Internet of Thing Environment

[1]Intisar Abd Yousif, [2]Salam Ayad Hussein, [3]Haider K. Hoomod, [4]Qutaiba Humadi Mohammed

[1 2 3] Computer Science Dept., Education college, Mustansiriyah University, Baghdad, Iraq.
[4] College of Nursing, University of Baghdad, Baghdad/Iraq

Abstract: *Lightweight cryptography is an intriguing information security issue. Due to rising component utilization, time, power, and memory needs, lightweight cryptography is needed. In June 2013, the NSA created Speck, a suggested algorithm. This article presents an IoT device security solution for a building's rooms. This post also offers a secure way to protect hardware against robbers and building mishaps in schools, hospitals, companies, and homes. This work provides robust and fast encryption algorithms for military security. This proposal employs a lightweight technique to encrypt environmental data, whether urgent, fast, or normal. This article applies the SPECK method to sensor data from a collection of rooms in the company building using a simple encryption scheme. In this post, the Ethernet-shielding Arduino UNO3 is linked to another set of sensors to collect environmental data. One of Arduino's simple encryption methods, the PRESENT technique, encrypts sensor data from numerous corporate building rooms. PRESENT encrypts sensor data to protect it from hackers. The Raspberry Pi re-encrypts data using SPECK encryption before sending it to the PC over MQTT to publish subscriber data for further security. Secure, private, and ciphered output will be transferred to the cloud. Sensors, a Raspberry Pi, Ethernet shield Arduino devices, and a computer are needed. Python, Arduino IDE, and Raspberry OS are software needs.*

Keywords: *SPECK encryption (SPE); Internet of Things (IoT); Sensors; Arduino; Security.*

INTRODUCTION

The IoT is an information network that senses, controls, and integrates smart and non-smart objects. Thanks to new enabling technologies like cloud computing, SDN, and NFV, IoT enables many new applications. The Internet of Things (IoT) includes readers for RFID chips and tags, smartphones, actuators, and sensors. These gadgets have several features, including connection, energy budgeting, Internet access, etc. Batteries power some gadgets, which have limited energy. The gateway, base station, or sink, the controller, receives data from the devices. [1-3].

Since Internet of Things data may threaten user privacy, it must be transferred securely. IoT connects smart meters, RFID tags, sensors, and physical items to the internet. Internet-connected things can be dynamically accessible anywhere. IoT is used in healthcare, home automation, urban planning, agriculture, and business. Internet-connected items let people observe and participate in the environment dynamically from anywhere. The objects may broadcast personal or environmental information. Private sensitive data has to be safely sent through IoT [4-6].

Lightweight cryptography techniques were developed to provide sufficient security with minimal memory and computing resources. These methods are better for IoT scenarios with limited computing resources. The IoT and development utilize Arduino extensively. IoT research often uses Arduino, which may be utilized to develop an environmental protection system [7]. Lightweight cryptographic methods have three advantages over traditional ones: First, IoT applications seldom need to encrypt data. Second, attackers can't record sufficient protected IoT data for cryptanalysis. Only modest security is needed for lightweight cryptographic algorithms. Light cryptographic methods are often employed on 8-bit microcontrollers, hence efficiency is critical [7-9].

** The strategy entails making use of a suitable cryptographic algorithm in order to deliver safety features such as authentication, integrity, and confidentiality. The provision of security services makes use of a wide variety of cryptographic systems, which may be divided into two categories: symmetric and asymmetric[10]. On the other hand, the vast majority of traditional cryptosystems are not suitable for use in secure constraint contexts like the Internet of Things (IoT) since they are designed to work with restricted devices that are equipped with a finite amount of battery life, power, and memory [11].

As a direct consequence of this, the development of cryptographic algorithms that are both effective and lightweight in order to ensure the security of data transmission on limited devices becomes a challenge. Low-energy, low-computational, and low-memory requirements ought to be appropriate with lightweight encryption. Additionally, it should provide the best possible balance of performance, affordability, and safety [12].

The phrase "lightweight cryptography" denotes a growing approach that provides information security in a manner that is more effective than conventional methods. This is due to the fact that the developing method uses fewer resources than the conventional methods while still providing greater throughput and requiring less power from the battery. [13]. It is common knowledge that anybody who designs systems for lightweight cryptography must take into account concerns regarding performance, cost (Gate Equivalent GE), and security. Furthermore, the system must be able to strike an appropriate balance between these three factors. When it comes to any two of the three designs, it is often not difficult to find the most effective combination of safety and price, security and efficiency, or cost and performance, respectively. As can be seen in Figure 1, it will be difficult to concurrently accomplish all three goals at the same time. [14]

Cryptographic algorithms may be broken down into two different categories: symmetric encryption and asymmetric encryption are two types of ciphers. Block ciphers and stream ciphers are two types of symmetric encryption algorithms. Lightweight symmetric encryption algorithms are frequently employed in both of these. [11] The cipher serves as the foundation for the incredibly lightweight algorithm block known as PRESENT [15] dependent on the configuration of the SBN The Hummingbird-2 [16] method is a mix of block cipher and stream cipher that is based on the SPN structure. It is a very lightweight algorithm. The Hummingbird-2 is a lightweight encryption that is an upgrade on the Hummingbird-1 [17]. It was aimed at being as efficient as possible.

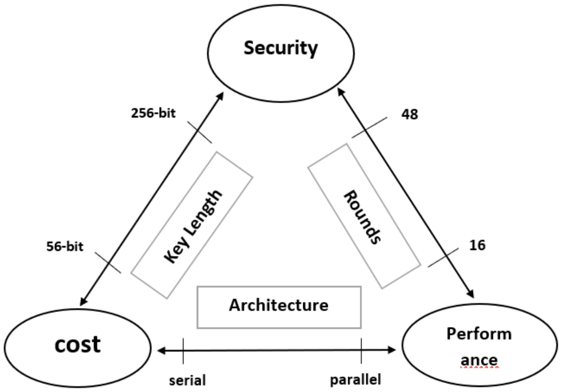


Figure 1: Design Lightweight Algorithm Factors

The HB-2 algorithm is applied in several low-cost applications, such as electronic card readers, RFID tags, and nodes with wireless connections for sensor networks. It was designed in order to meet the severe standards that had to be met regarding the quantity of power used and the speed of response. It utilizes a tiny block size of 16 bits to meet the needs of ciphering short messages in applications involving RFID, and it continues to use the hybrid structure as a form of security compensation for the small block size that it employs. This is done to satisfy the need for encrypting short messages in applications involving RFID. Despite knowing that HB-1's new mixed structure, which combined a block-cipher system and a stream encryption algorithm, was meant to give 256-bit safety, HB-2 maintains the design idea of HB-1. HB-1's new mixed structure was designed to provide 256-bit security. The size of the key was reduced to 128 bits so that it could accommodate the actual need for devices with fewer storage options. This was carried out with the goal of protecting against potential weaknesses.[12-17]

In addition, the capacity of the internal state has been raised from 80 bits to 128 bits, and in order to boost throughput, the non-linear keyed transformation that is used in HB-2 now uses just four of the S-boxes rather than all five of them[17-19]. The establishment of a chaotic system is one of the activities that is anticipated to take place in connection with the growth of a non-linear scientific system. This activity is one of the things that can take place with certain system values and characteristics. Systems that exhibit chaotic behavior. When considered through the prism of differential equations, chaotic systems are depicted as flows, and the graphical representations of differential equations can be referred to as maps[24].

Lightweight Encryption Algorithm

In the context of computer-embedded systems, platforms are limited by a number of different criteria, the most significant of which are the hardware resources available to them (including the central processing unit, both static and dynamic memory, and energy). Therefore, software developed specifically for this purpose has to take these constraints into consideration. Every design that has the intention of doing what is right will make an effort to reduce the quantity of hardware and power that is needed to operate it. Because the design calls for a security layer that is independent of the services provided by the operating system, there will be an increase in the use of device resources that is in excess of what is typically seen when software is running. Because of this, an issue about which security primitives need to be used to cut down on this cost emerges.

The subject has been analyzed in great detail over the course of several years, and researchers have concluded that lightweight block cipher layouts provide the best answer. In order to develop a lightweight implementation, several different approaches have been studied; the one that has received the most attention is one that recommends simplifying the operations, cutting down on the number of operations carried out in each round, and increasing the amount of replacement boxes. The vast majority of the strategies concentrate solely on size reduction since it is impossible to do an accurate power evaluation without first gaining an understanding of the execution environment.[20].

Review of Previous Work

The lightweight block cipher has established itself as the most important encryption structure for usage with limited resources ever offered since it was first developed. This is due to the fact that it requires very little in the way of computing power. Many different works deal with Hummingbird-2, PRESENT with Chaos system independently. As a result, a plurality of scholars from across the world suggested a range of unique lightweight ciphers.

X. Fan and G. Gong [21] are responsible for this. Hummingbird-2's protection against side channel cube assaults according to the single-bit leakage model. According to the results of their studies, it is possible to retrieve the first 48 bits of the secret key to the Hummingbird-2 by making use of a single bit of data that escapes from its internal state after the third iteration of the initial block cipher Ek1. The complexity of the proposed attack data is around 218.

J. Guan, K. Zhang, L. Ding, and J. Li are the authors of [22]. They arrived at the conclusion that the Hummingbird-2 algorithm is unable to withstand related key attacks. They presented a related-key chosen IIV attack on Hummingbird-2 that, when combined with differential methods, is capable of cracking the algorithm in real-time. They identified many vulnerabilities inside the round function WD16. related-key chosen-IIV assault A method is shown here that, when used in conjunction with a fundamental key loading mechanism, may successfully obtain the whole secret key. It is possible to recover the 128-bit starting key by employing 15 pairs of related keys, making use of 227 chosen IIV, and exhibiting a computation complexity of O. (227).

Hoomod, Haider K[23], and coworkers suggested a revolutionary 5-D that is based on the safe collection of data from the Internet of Things. As well as newly designed encryption techniques (that comprise hybrid cipher as well as two improved algorithms), fuzzy logic is employed to keep order inside a hyperchaotic system. This is done in conjunction with the usage of new encryption algorithms.

A technique for encrypting data that combines the algorithmic foundations of the PRESENT along with SPECK algorithms with a novel chaotic five-dimensional system. This technique is unique in its own right. Furthermore, for the reason of data encrypting, the adapted round-step methods of the PRESENT algorithm that had been created by SPEECK and were employed for the transit of data among IoT devices were implemented. When it comes to the management of change operations, the system that has been recommended is intended to provide users with a significant amount of flexibility while at the same time ensuring that everything is as simple as it can be. This includes accelerating encryption techniques and intruding on the information contained inside message packets (various types and types of sensory data) during the origin point, in addition to decoding and certifying the authenticity of the contents of packets not long after they have been received. This is all part of the process of speeding up the transmission of sensing data. In addition to that, this requires interfering with the information contained within message packets at their point of origin. The proposed method of encryption, in addition to the one-of-a-kind chaotic system, was subjected to a variety of analyses in order to determine its effectiveness. There should be at least 22560 different potential pairings of secret keys for there to be any chance of a brute-force attack being successful against the newly generated chaotic key space.

C. G. Thorat and V. S. Inamdar [24] are responsible for this. A brand new encryption technique that is tiny, hybrid, and lightweight has been revealed. Regarding the non-linearity, This technique combines the PERMS instruction, which is known to be the fastest bit permutation instruction, with the PRESENT S-box layer. In order to do a random n-bit permutation in a shorter amount of time than the logarithm of n requires, the PERMS instruction is utilized. On an ARM processor, the Cadens tool evaluates the performance of this innovative hybrid system, testing both its software and its hardware components. with reference to the CPU cycles.

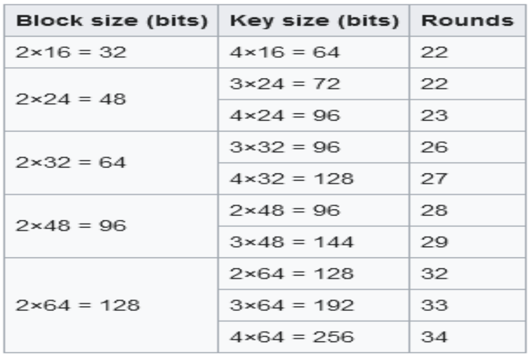
M. Hussam, G. H., and others [25] They suggested deploying a hybrid algorithm that combined a portion of the PRESENT algorithm (PA) as well as a portion of the TWINE algorithm (TA) by employing separate chaotic keys for both the purposes of encryption and decryption. This method would work in conjunction with the PRESENT algorithm (PA) and the TWINE algorithm (TA). In order to strengthen the cloud's protection and guarantee the accuracy of the data. The method of

Chaos key generation was used to create random numbers by using a novel chaotic system with separate initials and parameter values so as to produce Chaos key 5-D. These random numbers were then fed into the algorithm so that it could produce chaos key 5-D. In order to generate random numbers, this step has to be taken.
Kubba, Z. M. J., and Hoomod, H. K., et al. [26] They came up with a method that combined PRESENT and Salsa20, which are two separate encryption algorithms. This approach is called a hybrid method. In addition to this, a 2D logistic map of a chaotic system is employed to produce pseudo-random keys, which eventually contributes to an enhanced level of difficulty for the recommended encryption approach. The objective of the recommended algorithm is to accomplish the objective of giving a hybrid algorithm to raise the level of complexity of the current PRESENT method while retaining as low a degree of performance as feasible in terms of computational activities. This may be accomplished via the use of the suggested algorithm. The suggested approach was shown to function successfully while only requiring a small amount of time to be carried out, and the results of the investigation generated at random sequence keys satisfied the randomness tests carried out by the NIST suite.

SPECK Algorithm

Speck is a lightweight block cipher that is efficiently employed in software implementations, but Simon, the sister algorithm of Speck, has been optimized for use in hardware applications. Microsoft was the creator of Speck. An Add-Rotate-Xor (ARX) cipher is the name of the encryption that Speck uses. The Speck cipher makes use of a variety of blocks, each of which includes two words. These blocks can have a length of 16, 24, 32, 48, or 64 bits, and the key can consist of 2, 3, or 4 words as shown in table 1. The round function consists of two cycles, the first of which involves adding the right word to the left, followed by XORing the key with the left expression. The second cycle involves combining the left word with the right. The number of rounds played can be decided based on a variety of different parameters [27, 29–30]. Figure 2 shows the structure of Speak algorithm.

Table 1 The Speak a variety of blocks, key size, and rounds relation



Block size (bits)	Key size (bits)	Rounds
2×16 = 32	4×16 = 64	22
2×24 = 48	3×24 = 72	22
	4×24 = 96	23
2×32 = 64	3×32 = 96	26
	4×32 = 128	27
2×48 = 96	2×48 = 96	28
	3×48 = 144	29
2×64 = 128	2×64 = 128	32
	3×64 = 192	33
	4×64 = 256	34

On every platform, the SPECK algorithm has been the most compact and quickest of all the available cryptographic algorithms. The SPECK64 and SPECK128 lightweight block encryption algorithms are the two varieties of Speck that are available. These categories were taken into consideration for restricted devices that make contributions to the Internet of Things [28,29, 32].

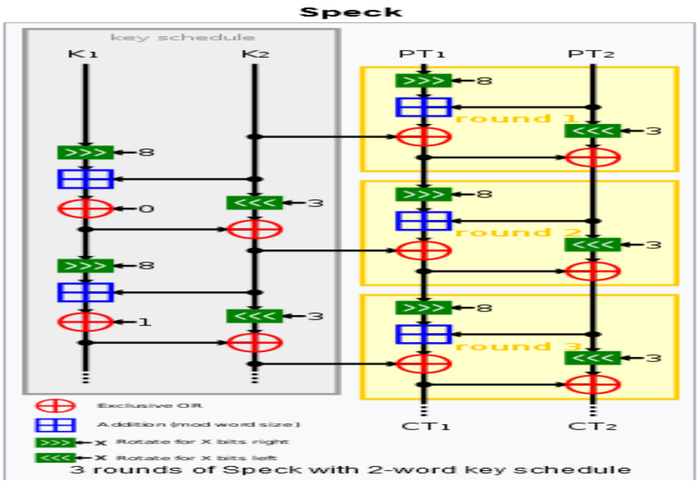


Figure.2 SPECK algorithm round key [29]

THE PROPOSED SYSTEM

We recommended using a new hybrid cipher approach that combines SPECK-128bit and Hummingbird 2 to make the MQTT protocol used in the IoT operation system and communication more secure. The block SPECK-128bit approach was utilized in large part due to the fact that it encrypts data with an exceptionally low computational burden and operates at lightning speed. A block cipher, which would mostly be dependent on the structure of the cipher that is already in place, would serve as the key structure. In the course of this task, a collection of sensors will have to be put in various places in the rooms included inside the business establishment. Each location will have its own unique assortment of sensors. These sensors are going to be utilized to read the condition of the system and gather data from the surrounding environment, which will then be used to make a decision. Every single group of those sensors is managed by a microcontroller, pretty much like an Arduino UNO. After that, a number of sensors are linked to Arduino, and the Hummingbird 2 algorithm is used to collect data that is acquired by sensors in Arduino in a number of rooms within the business establishment. This is one of the simpler encryption methods. In Raspberry Pi 4, techniques for hybrid lightweight encryption known as H2SPECK (Hummingbird2-SPECK) with block size 128bits (with 24 rounds) are utilized in order to provide protection for the sensing data prior to its transmission over the network. The result will be provided to the administrator in an encrypted, secure, and secret format in order for them to make the decision. The suggested research for this work is laid out in Figure 3.

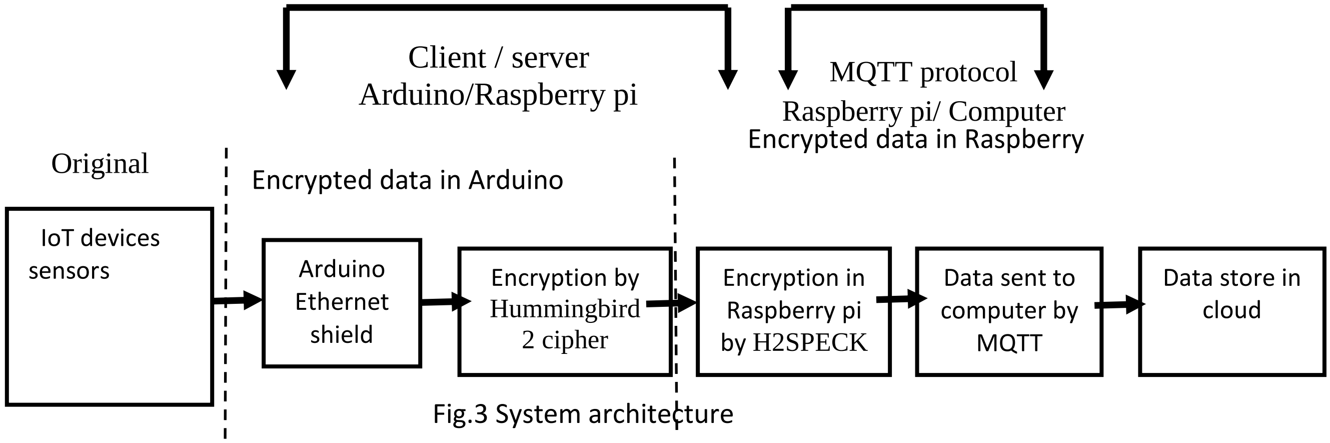
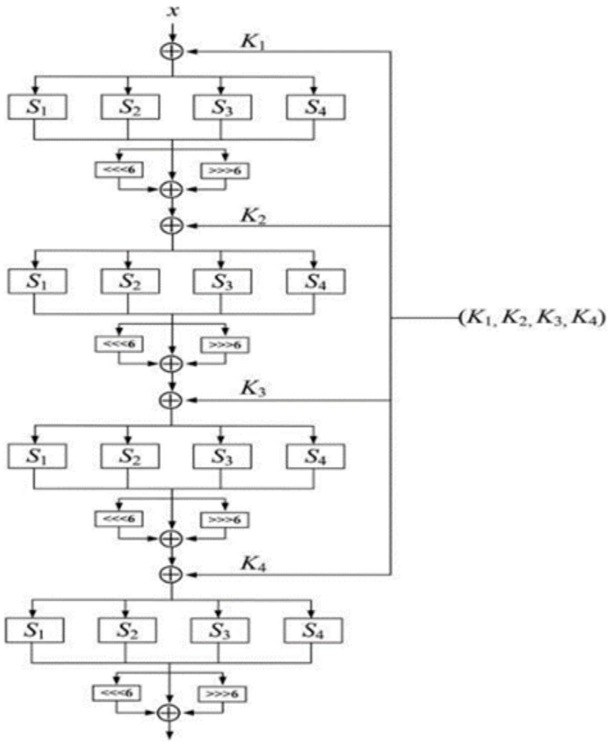
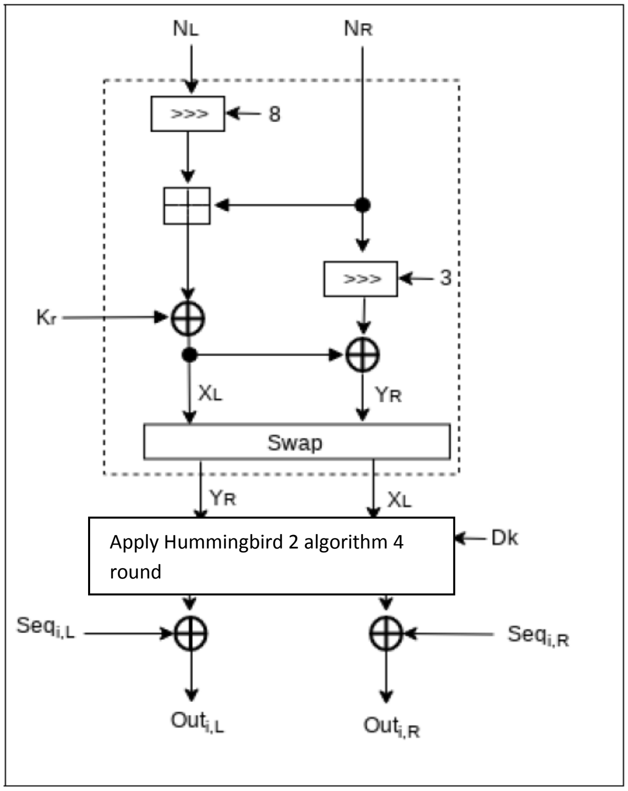

Client / server
Arduino/Raspberry pi
MQTT protocol
Raspberry pi/ Computer
Encrypted data in Raspberry
Original
Encrypted data in Arduino
IoT devices sensors
Arduino Ethernet shield
Encryption by Hummingbird 2 cipher
Encryption in Raspberry pi by H2SPECK
Data sent to computer by MQTT
Data store in cloud

Fig.3 System architecture

The original SPECK -128bit work with 34 rounds while the proposed H2SPECK work with 24 rounds to decreased the execution time and make H2SPECK still ultra lightweight algorithm. The information is collected from the environment using a variety of sensors; for instance, five sensors measuring temperature and humidity (DHT11), as well as sound, light, door, and flame sensors, are among the sensors that collect information for this study. These data are encrypted using the Hummingbird 2 encryption algorithm on a group of Arduinos that are housed within a series of rooms.

In order to provide security for the transmission of data across a network, the method known as encryption involves transforming plaintext into a form known as a cryptograph. Once again, the Raspberry Pi employs the H2SPECK cipher in order to encrypt data that has been encrypted. The lightweight protocol MQTT is implemented into the recommended solution for securely transmitting data between a Raspberry Pi and a computer via the network. The MQTT protocol is used to encrypt data before it is sent to the cloud, and the encrypted data is subsequently given to the administrator. When the sender does this, they prohibit unauthorized users from accessing and making changes to the text that was first provided over the network. Figure 4 presents an illustration of the Hummingbird 2 algorithm that is utilized in the H2SPECK method.





Algorithm 1: The Proposed H2SPECK algorithm

User Input Plaintext
The input plaintext is split into two (NL, NR)
1. Rotate (NL) to the left by 8
2. Perform addition modulo 2^n from the result of the rotated NL (from step 1) with NR
3. Rotate (NR) to the right by 3
4. Perform XOR from the result of the addition modulo 2^n, (from step ii) with the chaos key from NL.
5. Perform XOR from the result of (step 4) with the result of (step 3)
6. Swap between results of step 4 and step 5.
7. apply the Hummingbird 2 with 4 rounds on the output of step 6.
8. repeat steps 1-7 for 24 rounds.
Note that the input plaintext from the user is of arbitrary length. To achieve the desired block size, a padding technique is used by appending zeros.

Results

The newly improved encryption algorithm, that has been given the name (H2SPECK). To ensure improved protection and security we added the Hummingbird 2 with 4 rounds and H2SPECK with 24 rounds to get a suitable execution time for evaluating the performance of the hybrid encryption algorithm. NIST tests show the results of H2SPECK was guarantee its efficient and improvement of the security, randomness, and the unpredictability. the proposed algorithm passed all NIST tests as shown in table 1. keys for the Hummingbird-2 and H2SPECK algorithms are generated in this section by using chaos keys generated (using the logistic chaotic system). The comparison of the proposed H2SPECK schedule with the Hummingbird-2 timetable, which also includes evaluations of encryption techniques for files of varying sizes, is presented in table 2.

Table 1 statistical tests of NIST

NIST Tests	**Speck Algorithm**	**Hummingbird 2**	**Proposed Algorithm**
Frequency test	0.422	0.240	0.587
Block Frequency	0.512	0.632	0.754
Cumulative Sums	0.253	0.123	0.549
Runs	0.190	0.375	0.567
Longest Run	0.563	0.504	0.895
Rank	0.485	0.611	0.789
Non Overlapping	0.328	0.467	0.675
Overlapping Template	0.307	0.590	0.887
Universal test	0.154	0.523	0.650
Approximate Entropy	0.331	0.709	0.871
Random Excursions	0.108	0.332	0.543
Random Excursions Variant	0.256	0.412	0.554
Serial test	0.490	0.598	0.700
Linear Complexity	0.408	0.512	0.657

The significance value (α), whose default value is 0.01, is used in the NIST tests to determine whether or not a certain segment of the sequence is random. This determination is made based on the value. If the P-value was larger than 0.01, the series would not be deemed random. On the other hand, if the P-value was less than 0.01, the sequence would be regarded random. The suggested method and the existing encryption algorithm are both successful in passing all NIST tests; the outcomes of each test are detailed in Table 1, which can be seen below. According to the findings, the P-values of the proposed method are much higher than the P-values obtained using the Speck approach for the majority of the NIST tests. As a consequence of this, the advised tactic produces a succession that is to some extent unexpected. As a consequence of this, the strategy that is advised keeps the computing speed the same while increasing the complexity.

Table 2. Execution Time comparison in sec.

File size (byte)	H2SPECK **128 bit**	SPECK **128 bit**	Hummingbird2 64bit
128	0.021	0.0234	0.017
1 k	0.145	0.152	0.097
10 k	1.398	1.429	0.453
100 k	10.231	11.763	5.508
500 k	56.086	57.833	31.430
1M	110.007	115.487	86.112

Conclusions

A lightweight cipher was provided in this research with the primary purpose of catering to restricted devices, which may be identified by their confined power and low storage space. The Speck cipher has become one of the most well-known concepts in the area of lightweight cryptography in recent years. In this study, the lightweight cryptographic approach known as hybrid Hummingbird 2 and SPECK is introduced in order to safeguard the sensor data of Internet of Things devices during transitions across networks and name as H2SPECK. This system was developed to monitor all of the devices that are linked to the internet. In the context of Internet of Things applications, hybrid lightweight cryptographic approaches H2SPECK are more advantageous and are frequently used. Within the realm of information security, cryptography is the primary mode of communication that is utilized. It is required whenever there is interaction between many devices using the internet. On the other hand, limiting devices are unable to apply standard cryptography because to the restricted resource available at their disposal. Constraint devices make extensive use of symmetric key cryptography, which only requires the use of a single key for both ciphering and deciphering of data. On the other hand, rapid cryptographic algorithms may be utilized in order to solve constraint devices.

Standard tests, such as those based on time and those developed by NIST, are carried out when the proposed Cipher Algorithm is being tested in order to assess its performance. Based on the findings, it appears that the H2SPECK algorithm encrypts and decrypts data in a quicker amount of time compared to other methods like the GOST and SPECK algorithm. In addition, the H2SPECK encryption technique has a less encryption duration than the SPECK algorithms, but it provides a higher level of security. The results of this study show that the strategy that was presented is successful in protecting users' data privacy and security inside cloud computing environments.

REFERENCES

[1] *Rondon, L. P., Babun, L., Aris, A., Akkaya, K., & Uluagac, A. S., "Survey on enterprise Internet-of-Things systems (E-IoT): A security perspective". Ad Hoc Networks, 12 (2022), 102-111.*

[2] *Li, S., Xu, L. D., & Zhao, S., "The internet of thing: a survey, Information systems frontiers", 17(2015), 243-259.*

[3] *Lee I. "Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management". Future Internet. 2020; 12(9):157. https://doi.org/10.3390/fi12090157*

[4] *Sruthi, M., and Rajkumar Rajasekaran. "Hybrid lightweight Signcryption scheme for IoT." Open Computer Science 11.1 (2021): 391-398.*

[5] *Tawalbeh L, Muheidat F, Tawalbeh M, Quwaider M. "IoT Privacy and Security: Challenges and Solutions". Applied Sciences. 2020; 10(12):4102. https://doi.org/10.3390/app10124102*

[6] *Gupta and K. Anil Kumar, "Security Mechanisms of Internet of Things (IoT) for Reliable Communication: A Comparative Review," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899459.*

[7] *Kurniawan, Rizki & Wahjuni, Sri & Neyman, Shelvie. (2022). Secure Communication Protocol for Arduino-based IoT Using Lightweight Cryptography. International Journal on Advanced Science, Engineering and Information Technology. 12. 453. 10.18517/ijaseit.12.2.8601.*

[8] *Ling, Z., Liu, K., Xu, Y., Gao, C., Jin, Y., Zou, C., ... & Zhao, W., "Iot security: An end-to-end view and case study". arXiv preprint arXiv, (2018),1805, https://doi.org/10.48550/arXiv.1805.05853*

[9] *Ali, I., Sabir, S., & Ullah, Z., "Internet of thing security, device authentication and access control: a review". arXiv preprint arXiv:1901.07309.,(2019). https://doi.org/10.48550/arXiv.1901.07309*

[10] *M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, "A lightweight aes algorithm implementation for secure iot environment," Iraqi J. Sci., vol. 62, no. 8, pp. 2759–2770, 2021, doi: 10.24996/ijs.2021.62.8.29.*

[11] *S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," Symmetry (Basel)., vol. 11, no. 2, 2019, doi: 10.3390/sym11020293.*

[12] *O. Jallouli, "Chaos-based security under real-time and energy Ons Jallouli To cite this version : HAL Id : tel-01633910," no. November, 2017, [Online]. Available: https://hal.archives-ouvertes.fr/tel-01633910*

[13] *S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," J. Ambient Intell. Humaniz. Comput., vol. 0, no. 0, pp. 1–18, 2017, doi: 10.1007/s12652-017-0494-4.*

[14] *S. S. M. Aldabbagh and I. F. T. Al Shaikhli, "Improving PRESENT lightweight algorithm," Proc. - 2013 Int. Conf. Adv. Comput. Sci. Appl. Technol. ACSAT 2013, no. 1, pp. 254–258, 2013, doi: 10.1109/ACSAT.2013.57.*

[15] *A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, and A. Poschmann, "PRESENT : An Ultra-Lightweight Block Cipher," pp. 450–466, 2007.*

[16] *D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, "The hummingbird-2 lightweight authenticated encryption algorithm," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7055 LNCS, pp. 19–31, 2012, doi: 10.1007/978-3-642-25286-0_2.*

[17] *D. Engels, X. Fan, G. Gong, H. Hu, and E. M. Smith, "Ultra-lightweight cryptography for low-cost RFID tags: Hummingbird algorithm and protocol," Cent. Appl. Cryptogr. Res. Tech. Reports, vol. 29, no. January 2009, 2009.*

[18] *H. Najm, H. K. Hoomod, and R. Hassan, "A New WoT Cryptography Algorithm Based on GOST and Novel 5d Chaotic System," Int. J. Interact. Mob. Technol., vol. 15, no. 2, pp. 184–199, 2021, doi: 10.3991/ijim.v15i02.19961.*

[19] *F. Thabit, A. P. S. Alhomdy, A. H. A. Al-Ahdal, and P. D. S. Jagtap, "A new lightweight cryptographic algorithm for enhancing data security in cloud computing," Glob. Transitions Proc., vol. 2, no. 1, pp. 91–99, 2021, doi: 10.1016/j.gltp.2021.01.013.*

[20] *Lara-Niño, C. Andrés, M. S. Miguel, and D. P. Arturo, "An evaluation of AES and present ciphers for lightweight cryptography on smartphones," 2016 Int. Conf. Electron. Commun. Comput. CONIELECOMP 2016, pp. 87–93, 2016, doi: 10.1109/CONIELECOMP.2016.7438557.*

[21] X. Fan and G. Gong, “On the security of Hummingbird-2 against side channel cube attacks,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7242 LNCS, pp. 18–29, 2012, doi: 10.1007/978-3-642-34159-5_2.

[22] K. Zhang, L. Ding, J. Li, and J. Guan, “Real time related key attack on hummingbird-2,” KSII Trans. Internet Inf. Syst., vol. 6, no. 8, pp. 1946–1963, 2012, doi: 10.3837/tiis.2012.08.004.

[23] H. K. Hoomod, J. R. Naif, and I. S. Ahmed, “A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system,” Period. Eng. Nat. Sci., vol. 8, no. 4, pp. 2333–2345, 2020, doi: 10.21533/pen.v8i4.1738.

[24] C. G. Thorat and V. S. Inamdar, “Implementation of new hybrid lightweight cryptosystem,” Appl. Comput. Informatics, no. May, 2020, doi: 10.1016/j.aci.2018.05.001.

[25] M. Hussam, G. H. Abdul-majeed, and H. K. Hooomod, “New Lightweight Hybrid Encryption Algorithm for Cloud Computing (LMGHA-128bit) by using new 5-D hyperchaos system,” Turkish J. Comput. Math. Educ., vol. 12, no. 10, pp. 2531–2540, 2021.

[26] Z. M. J. Kubba and H. K. Hoomod, “A Hybrid Modified Lightweight Algorithm Combined of Two Cryptography Algorithms PRESENT and Salsa20 Using Chaotic System,” 1st Int. Sci. Conf. Comput. Appl. Sci. CAS 2019, pp. 199–203, 2019, doi: 10.1109/CAS47993.2019.9075488.

[27] S. B. Sadkhan and Z. Salam, "Security and Privacy in Internet of Things- Status, Challenges," 2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA), 2021, pp. 308-312, doi: 10.1109/IICETA51758.2021.9717785.

[28] Sadek, Rowayda A. "Hybrid energy aware clustered protocol for IoT heterogeneous network." Future Computing and Informatics Journal 3.2 (2018): 166-177.

[29] Sleem, Lama & Couturier, Raphaël. (2021). Speck-R: An ultra light-weight cryptographic scheme for Internet of Things. Multimedia Tools and Applications. 10.1007/s11042-020-09625-8. Sruthi, M., and Rajkumar Rajasekaran. "Hybrid lightweight Signcryption scheme for IoT." Open Computer Science 11.1 (2021): 391-398.

[30] Abdullah, Shapina, et al. "IOT Security: Data Encryption for Arduino-based IOT Devices." Journal of Positive School Psychology 6.3 (2022): 8508-8516.

[31] Xu, Miao, et al. "Lightweight secure communication protocols for in-vehicle sensor networks." Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles. 2013.

[32] Usman, M., et al., SIT: a lightweight encryption algorithm for secure internet of things. arXiv preprint arXiv:1704.08688, 2017.

[33] Bogdanov, A., et al. PRESENT: An ultra-lightweight block cipher. in International Workshop on Cryptographic Hardware and Embedded Systems. 2007. Springer.

[34] Z. Shi, B. Zhang, and D. Feng, “Practical-time related-key attack on Hummingbird-2,” IET Inf. Secur., vol. 9, no. 6, pp. 321–327, 2015, doi: 10.1049/iet-ifs.2014.0424.

[35] D. Engels, M. J. O. Saarinen, P. Schweitzer, and E. M. Smith, “The hummingbird-2 lightweight authenticated encryption algorithm,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7055 LNCS, no. December, pp. 19–31, 2012, doi: 10.1007/978-3-642-25286-0_2.

[36] S. A. Mehdi and F. H. Abbood, “5D Hyper-Chaotic System Via Improved,” no. October 2020, 2018.