Due Date: Tuesday, 5 Nov. 2024

AES-RC4 Encryption Technique to Improve File Security

Nur Atikah
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
nuratikah998@gmail.com

Mutia Rizky Ashila
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
mutiarizky147@gmail.com

De Rosal Ignatius Moses Setiadi
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
moses@dsn.dinus.ac.id

Eko Hari Rachmawanto
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
eko.hari@dsn.dinus.ac.id

Christy Atika Sari
Department of Informatics Engineering
Dian Nuswantoro University
Semarang, Indonesia
atika.sari@dsn.dinus.ac.id

Cite as: N. Atikah, M. R. Ashila, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto and C. A. Sari, "*AES-RC4 Encryption Technique to Improve File Security," 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 2019, pp. 1-5.*

***Abstract*— In communicating in public networks, data security becomes very important. There are many risks of data theft by other parties. Cryptography is one technique for securing data. In cryptography, there are two main processes, namely encryption, and decryption. Encryption is the process of encoding the original or plaintext file into an encrypted or ciphertext file. While decryption is the process of returning encrypted data or ciphertext into original or plaintext data. There are various encryption algorithms nowadays, where the more complex encryption logically encryption will be stronger and harder to solve. This study proposed a combination of the AES and RC4 algorithms to provide protection against confidential data. The combination of this method aims to make the algorithm more complex and strong. To find out how safe an algorithm is, test the avalanche effect (AE). AE measurement is done by changing the value of one bit in the key, then the two results are ciphertext compared to the difference. The greater the difference, the better the encryption results. The ideal AE is around 50% and the greater the AE value means the better the quality of data encryption. Based on the combination test of the AES-RC4 method, the best AE results are 58.2%, where this value is far better than the AES algorithm, RC4 only or RC4-AES.**

Keywords—Cryptography, Encryption, Avalanche Effect, AES, RC4

I. INTRODUCTION

At present, information and communication technology is increasingly advanced and developing. Data security is very necessary to keep data from being stolen by others, especially when sending data. Exchange of data through services in cyberspace needs to be wary of attacks. Data must be protected and safeguarded because many people are not responsible for misusing information and communication technology to conduct data tapping and or data theft[1]–[3]. Therefore to improve data security can be done by cryptographic techniques. Cryptography is the technique of securing messages by converting them into a password so that they cannot be read by outsiders[4], [5]. There are two main processes in cryptography namely encryption and decryption. The process of encoding text into ciphertext is encryption. While decryption is the process of returning the ciphertext into a plaintext so that it can be read, where both processes require a key[6], [7]. The key is also one of the most important things to get a strong encoding[7].

Cryptography has many algorithms used to secure data, namely Caesar Cipher which includes a simple algorithm, Vigenere Cipher, Rivest Cipher 4 (RC4), Data Encryption Standard (DES), Advanced Encryption Standard (AES)[1], [8]–[10]. Each algorithm has a different encryption process. In the Ritambhara study[11] it was stated that the AES algorithm is the most sophisticated and powerful encryption algorithm at the moment. The implementation of AES in data security can prevent data theft that can be done by anyone. The AES algorithm is also better than the DES algorithm[3]. AES is a symmetric key algorithm where this key is used for the encryption and decryption process. So the confidentiality of the key needs to be maintained so that it is not easily decrypted by other people[6]. The AES key length can use 128-bit, 192-bit, 256-bit keys. The longer the size of the key the ciphertext produced is also increasingly random and more difficult to decrypt other people. To encrypt a file, AES is safe because it has a rotation of 10, 12 or 14, depending on the length of the key[11]. The AES algorithm can be implemented in software or hardware. It's just that based on testing the size of the AES encryption file will be even greater[12]. Of course, it will reduce space. AES is also vulnerable to brute force attacks where the attacker tries all the keys that are possible during the encryption or decryption process[11].

The RC4 algorithm is a stream cipher algorithm to encrypt data developed by Ronald Rivest[13]. There are two algorithms in the encryption process in RC4 namely the Key Scheduling Algorithm (KSA) and the Pseudo-Random Generation Algorithm (PRGA). Both of these processes produce a keystream that is used to encrypt file[14]. In the RC4 encryption process, it is more efficient and simpler than AES. The RC4 encryption file is the same size as the original file, so it doesn't reduce space. Also, it does not require a long time for the encryption process. RC4 encrypts bits per bit by operating XOR plaintext with keys. But from the plaintext XOR process with pseudorandom, RC4 is easily attacked by determining a few bytes of the original message through the XOR process between two sets of byte ciphers. In the RC4 algorithm, Bit-Flipping (BFA) attacks also occur, which makes the attacker know the plaintext of the ciphertext without knowing the key to the encryption. The attacker will change 1 bit of the ciphertext, from 0 to 1 or vice versa [15].

Avalanche effect is a change of one bit in the plaintext or key that causes a big change in the ciphertext [8], [16], [17]. The AE value is said to be good if the change in one bit in

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

Authorized licensed use limited to: UNIVERSIDAD DE LAS AMERICAS PUEBLA. Downloaded on October 20,2023 at 22:29:14 UTC from IEEE Xplore. Restrictions apply.

the plaintext or key can change at least half of the total number of bits [16], [18]. Avalanche effect is also important to know the strength of encryption from BFA attacks [8], [19]. BFA attacks change the ciphertext of the encryption process without having to be decrypted.

In research conducted by Ketan and Vijayarajan [6] proposed the RC4 and AES algorithms that were combined to develop new hybrid ciphers. In the hybrid process, only certain parts are taken so that the resulting file size does not increase and the encryption time from the test results can be faster than the standard AES. However, in this study only testing the file size, time and limited security testing. To determine the strength of encryption algorithms necessary to test the security of such an avalanche effect to determine whether good or not and how to secure the cryptographic algorithm[8]. In the study[3], [11] concluded that the AES algorithm can improve data security, both on software and hard. Whereas in [14] proposed the RC4 method combined with Shuffling and successfully improved security. Based on research [3], [11], [14] in this study a combination of AES and RC4 algorithms were proposed to improve data security which would later be measured by AE testing.

II. Related Work

Research conducted by Ketan and Vijayarajan [6] proposed hybrid RC4 and AES methods with modifications. The number of rounds at AES is reduced from 10 to 6 to increase encryption speed. Based on the results of the test, this method can indeed work faster than the AES method but is longer than the RC4 method only. This research also claims that this method has good security, but the security tests performed are incomplete and only analysis.

In the research proposed by Bhoge and Chatur [17] test the AES algorithm based on the avalanche effect. It was concluded that the ciphertext results from AES encryption were very strong. And it is difficult to decrypt to the initial plaintext. This is evidenced by testing the avalanche effect which changes 1-bit on key characters generated by encryption ciphers very different.

Giradkar and Bhattacharya [20] proposed the RC4 algorithm for encrypting video. RC4 was chosen because it is a fast and reliable stream cipher cryptographic algorithm. Tests are performed on compressed video files with H.264 / AVC. Where the video streaming process can be performed smoothly and can work well. This RC4 algorithm is quite reliable and has fast computing.

Many other studies also propose the AES and/or RC4 algorithms to be implemented in encrypting a file. This study proposed a combination of AES and RC4 to encrypt files. This research is implemented web-based using PHP script language. Because the AES algorithm encrypts a file by doing several rounds of 10, 12 and 14 depending on the key length so that when the file is encrypted using AES at the beginning it will be safer. Entering the RC4 algorithm in encrypting a file is a fast process compared to other algorithms. So the combination of AES and RC4 can create a cryptographic algorithm that is safe against attack and fast. For file types tested, the existence of .doc, .xlsx, .pdf, .pptx, and .jpg. The encryption results are measured using the avalanche effect, while the decryption results are measured using a bit error ratio (BER) to ensure that the decryption results are exactly the same as the original files.

III. Methodology

A. AES Algorithm

AES is an advanced algorithm from DES. The AES algorithm uses 3 types of cryptographic keys, 128, 192 and 256 bits. For each bit the rotation is 10, 12 and 14[6], [11], [12]. The difference in the AES key length greatly affects the number of turns. The AES encryption process is rotated according to the size of the key length. Every round is there at the type of transformation that is carried out, i.e.:

1. AddRoundKey is the process of XORing between existing ciphertexts and cipher keys.
2. SubBytes is mapping each byte of the state array using an S-Box.
3. ShiftRows is the process of shifting wrapping on the last three lines of the state array.
4. MixColumns is the process of multiplying from each element of a cipher block with a matrix. The multiplication that is done is that the dot product multiplication will then be entered into the new table cipher.

The transformation process above is repeated or in the next round with the same method. But when it arrived in the last round, the MixColumns process was not performed.

B. RC4 Algorithm

The RC4 algorithm is a symmetric encryption algorithm that is relatively simple, safe and fast. The initial process in the RC4 algorithm is to read the input key to do the key scheduling algorithm (KSA). At this stage, the process of granting the initial key value is represented in a permutation with 256 elements. Arrays that have a value of 256 this element are called S. So the result of the KSA algorithm is the initial permutation of this key scheduling stage.

The next process is the pseudo-random generation (PRGA). At this stage, each round with the keystream equal to 1 byte will be output on the PRGA algorithm based on the KSA state that was obtained above. After the keystream is generated, the XOR process will be carried out between the keystream and the existing plaintext. Before the XOR process is done the message is first to cut into bytes. The results of the XOR process are used as ciphers of RC4 encryption.

C. Proposed Encryption Scheme

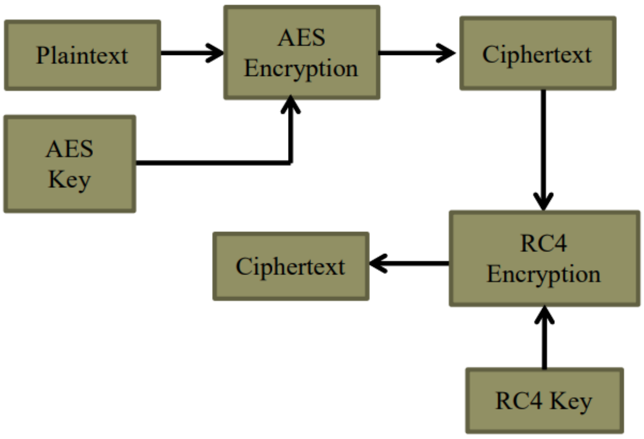

Fig. 1. Proposed Encryption method

Authorized licensed use limited to: UNIVERSIDAD DE LAS AMERICAS PUEBLA. Downloaded on October 20,2023 at 22:29:14 UTC from IEEE Xplore. Restrictions apply.

In the encryption process, several inputs are needed, i.e. plaintext, AES key, and RC4 key. In the first process, AES-256 encryption is done on the plaintext using the AES key. The results of this encryption will produce ciphertext, AES which is used as an input or plaintext RC4. RC4 encryption is performed on AES ciphertext based on the RC4 key. The results of RC4 encryption are ciphertexts that will be tested using the avalanche effect. For more details, see Fig. 1. To find out the quality of encryption, an avalanche effect is measured.

D. Proposed Extraction Scheme

In the extraction scheme, decryption is done using RC4 and AES. The process of decryption is the reverse and of the encryption process, if the encryption process is carried out by AES encryption followed by RC4, then the decryption process is carried out decryption using the RC4 algorithm first then followed by the AES algorithm. RC4 decryption is done on ciphertext based on the RC4 key. This process will produce a plaintext that is still AES encrypted. Then AES decryption is done based on the AES key to produce the actual plaintext. To see more clearly you can see Fig. 2. To ensure that the resulting plaintext is the same as the original plaintext, the test is performed using a bit error ratio (BER).

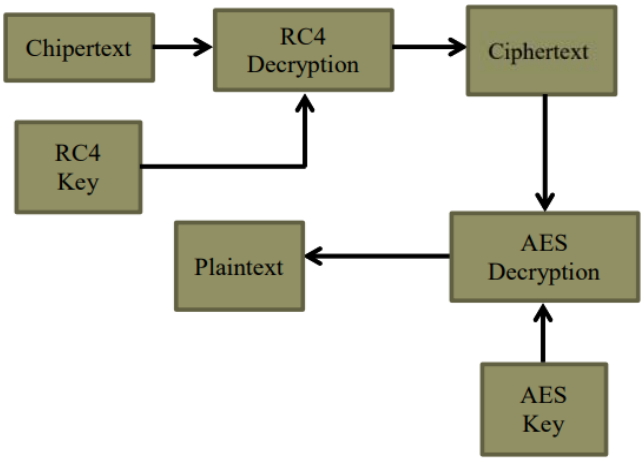

Fig. 2. Proposed Decryption method

E. Measurement

In this research, several measurements were taken to determine the quality of the proposed encryption method. The results of encryption will be measured using the avalanche effect. It has been discussed in the previous section that an avalanche effect is a tool for ciphertext quality by comparing two ciphertexts that have small differences in the plaintext or the key. Generally, the difference is only 1-bit. The binary form of the first cipher will be compared to the second cipher, the more different bits, the better the ciphertext will be. To find out more clearly how to measure the avalanche effect can see the formula (1).

$$AE(cipher1, cipher2) = \frac{diffBits}{totalBits} \times 100\% \qquad (1)$$

Where $diffBits$ is the difference in bits between $cipher1$ and $cipher2$, while $totalBits$ is the total bits of the file. In addition to the avalanche effect, the file size before and after encryption is also measured. Measurements are made in bytes. This measurement is done to prove whether true AES encryption has side effects on the results of encryption. Where in some studies it is said that the results of AES encryption are larger than the original file [7], [11]. File size measurement is also done in the decryption process to find out whether the file size will return to its original size. In the decryption process, a bit error ratio (BER) is also measured to determine whether the decryption process is running perfectly. BER can be calculated by the formula (2).

$$BER(ori, dec) = \frac{different\ bits\ of\ ori\ and\ dec}{total\ bits\ of\ original\ file} \qquad (2)$$

Where ori is original file/plaintext and dec is decryption file, total bits of original and decryption file must be the same.

IV. IMPLEMENTATION, RESULTS, AND COMPARISON

At this stage, the proposed method is implemented in a web-based application using the PHP script. Encryption can be done on all types of files, but in this research a trial was performed on files with extensions .doc, .xlsx, .pdf, .pptx, and .jpg. Each file has a different size, these files are presented in Table 1.

TABLE I. DATASET FILE PROPERTIES

File Name	Extension	Size (in bytes)
File1	.doc	430.592
File2	.xlsx	13.140
File3	.pptx	122.469
File4	.jpg	64.170
File5	.pdf	348.524

Then the encryption process is carried out in accordance with the proposed method. The results of the encryption are then tested for effect effects and post-encryption measurement. The results of the measurement of post-encryption files are presented in Table 2.

TABLE II. FILE SIZE BEFORE AND AFTER ENCRYPTION

File Name	Size (in bytes)	
	Before encryption	*After Encryption*
File1	430.592	574.136
File2	13.140	17.530
File3	122.469	163.304
File4	64.170	85.580
File5	348.524	464.712

Based on Table 2, it can be concluded that the size of the encrypted file proved to increase. The increase in file size is caused by the addition of the header file during the AES encryption process. Whereas in the testing process the avalanche effect was carried out three times wherein the first experiment the AES key and RC4 were modified at the beginning, the second experiment a key modification in the middle and third experiments were modified on the end. The key used and the explanation is presented in Table 3.

The results of the avalanche effect test based on Table 3 are presented in three tables, each in Table 4 presents the results of the avalanche effect on the original key and Modified Key 1, Table 5 presents the results of the avalanche

Authorized licensed use limited to: UNIVERSIDAD DE LAS AMERICAS PUEBLA. Downloaded on October 20,2023 at 22:29:14 UTC from IEEE Xplore. Restrictions apply.

effect on the original key and Modified Key 2, and Table 6 presents the avalanche effect results on original key and Modified Key 3.

TABLE III. ORIGINAL KEY AND MODIFIED KEY FOR AVALANCHE EFFECT TESTING

Key Type	AES Key	RC4 Key
Original Key	universitas	jayaabadi
Modified Key 1	**v**niversitas	**k**ayaabadi
Modified Key 2	unive**s**sitas	jaya**b**badi
Modified Key 3	universita**t**	jayaabad**j**

TABLE IV. AVALANCHE EFFECT OF ORIGINAL KEY AND MODIFIED KEY 1

File Name	AES Only	RC4 Only	RC4-AES	Proposed
File1	40,81%	49,99%	40,78%	58,17%
File2	40,90%	50,00%	40,73%	57,72%
File3	40,73%	49,99%	40,72%	58,14%
File4	40,87%	49,99%	40,85%	58,12%
File5	40,80%	49,99%	40,83%	58,16%
Average	40,82%	49,99%	40,78%	**58,06%**

TABLE V. AVALANCHE EFFECT OF ORIGINAL KEY AND MODIFIED KEY 2

File Name	AES Only	RC4 Only	RC4-AES	Proposed
File1	40,80%	49,99%	40,83%	58,21%
File2	40,89%	50,00%	40,70%	58,35%
File3	40,80%	49,99%	40,82%	58,13%
File4	40,77%	49,99%	40,79%	58,12%
File5	40,83%	49,99%	40,84%	58,20%
Average	40,82%	49,99%	40,80%	**58,20%**

TABLE VI. AVALANCHE EFFECT OF ORIGINAL KEY AND MODIFIED KEY 3

File Name	AES Only	RC4 Only	RC4-AES	Proposed
File1	40,78%	49,99%	40,78%	58,87%
File2	40,91%	50,00%	40,67%	53,97%
File3	40,76%	49,99%	40,80%	53,78%
File4	40,90%	49,99%	40,75%	53,84%
File5	40,77%	49,99%	40,79%	53,81%
Average	40,82%	49,99%	40,76%	**54,85%**

Based on tables 4, 5 and 6 it can be seen that the proposed method has better performance. This is evidenced by the value of the avalanche effect on the three tests resulting in a superior value and all of them more than 50%. This is because AES encryption at the beginning will make variations and the length of the cipher will increase, then RC4 encryption strengthens the AES cipher with its encryption. This method proved to be better than if the RC4-AES encryption process.

Then the decryption process is carried out, to find out that this process is running well, it is necessary to do testing and measurement using BER. The decryption of files must be perfect so that the file is not corrupted. Table 7 shows the results of the measurement of BER in the decryption file and the original file.

TABLE VII. BER MEASUREMENT OF DECRYPTION FILE AND ORIGINAL FILE

File Name	Extension	BER
File1	.doc	0
File2	.xlsx	0
File3	.pptx	0
File4	.jpg	0
File5	.pdf	0

Based on Table 7 it appears that the decryption process is running perfectly, this is evidenced by all BER values being 0, meaning that there are no different or missing bits. The last measurement is the file size (in bytes) after decryption which is presented in Table 8.

TABLE VIII. FILE SIZE BEFORE AND AFTER ENCRYPTION

File Name	Size (in bytes)		
	Original Size	***After Encryption***	***After Decryption***
File1	430.592	574.136	430.592
File2	13.140	17.530	13.140
File3	122.469	163.304	122.469
File4	64.170	85.580	64.170
File5	348.524	464.712	348.524

Based on Table 8, it can be concluded that the size of the decrypted file is the same as the size of the original file. That means the decryption process is proven to work well.

V. CONCLUSION

This study combines AES and RC4 cryptographic algorithms to get better security. Based on testing, the combination of AES and RC4 works well. In the file size, the results of AES and RC4 encryption are relatively small. In the avalanche test, the effect of AES and RC4 managed to get a high score of 58.41% compared to other algorithms. That means the change in the bit value on the modified key works well. And that means the combination of the AES and RC4 algorithms can improve the security of file encryption.

REFERENCES

[1] D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, A. Susanto, and M. Doheir, “A Comparative Study of Image Cryptographic Method,” in *2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 2018, pp. 336–341.

[2] D. R. I. M. Setiadi, “Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation,” *Intl J. Electron. Telecommun.*, vol. 65, no. 2, pp. 295–300, 2019.

[3] M. Mohurle and V. V. Panchbhai, “Review on realization of AES encryption and decryption with power and area optimization,” in *2016 IEEE 1st International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES)*, 2016, pp. 1–3.

[4] A. Setyono, D. R. I. M. Setiadi, and Muljono, “Dual encryption techniques for secure image transmission,” *J. Telecommun. Electron.*

Authorized licensed use limited to: UNIVERSIDAD DE LAS AMERICAS PUEBLA. Downloaded on October 20,2023 at 22:29:14 UTC from IEEE Xplore. Restrictions apply.

Comput. Eng., 2018.

[5] C. Irawan, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. Doheir, “Hybrid Encryption using Confused and Stream Cipher to Improved Medical Images Security,” *J. Phys. Conf. Ser.*, vol. 1201, no. 1, p. 012022, May 2019.

[6] P. K. Ketan and V. Vijayarajan, “An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption,” *Int. J. Comput. Appl.*, vol. 54, no. 12, pp. 29–36, Sep. 2012.

[7] A. Vassilev and R. Staples, “Entropy as a Service: Unlocking Cryptography’s Full Potential,” *Computer (Long. Beach. Calif).*, vol. 49, no. 9, pp. 98–102, Sep. 2016.

[8] C. P. Dewangan, S. Agrawal, A. K. Mandal, and A. Tiwari, “Study of avalanche effect in AES using binary codes,” in *2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 2012, pp. 183–187.

[9] S. K. Mandal and A. R. Deepti, “A Cryptosystem Based On Vigenere Cipher By Using Mulitlevel Encryption Scheme,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 7, no. 4, pp. 2096–2099, 2016.

[10] B. B. Mohammed, “Automatic Key Generation of Caesar Cipher,” *Int. J. Eng. Trends Technol.*, vol. 6, no. 6, 2013.

[11] Ritambhara, A. Gupta, and M. Jaiswal, “An enhanced AES algorithm using cascading method on 400 bits key size used in enhancing the safety of next generation internet of things (IoT),” in *2017 International Conference on Computing, Communication and Automation (ICCCA)*, 2017, pp. 422–427.

[12] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, “A performance analysis StegoCrypt algorithm based on LSB-AES 128 bit in various image size,” in *International Seminar on Application for Technology of Information and Communication*, 2017.

[13] S. Chugh and Kamal, “Securing data transmission over wireless LAN (802.11) by redesigning RC4 Algorithm,” in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1436–1441.

[14] M. H. Abood, “An efficient image cryptography using hash-LSB steganography with RC4 and pixel shuffling encryption algorithms,” in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017, pp. 86–90.

[15] P. J. Sonawane and U. S. Bhadade, “Synthesis and Simulation of FPGA Based Hardware Design of RC4 Stream Cipher,” in *2015 International Conference on Computational Intelligence and Communication Networks (CICN)*, 2015, pp. 1177–1182.

[16] S. Shen, X. Han, and X. Zhou, “Research of avalanche effect of the 3GPP integrity algorithm f9,” in *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, 2017, pp. 1–4.

[17] J. P. Bhoge and P. N. Chatur, “Avalanche Effect of AES Algorithm,” *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 3101–3103, 2014.

[18] K. D. Muthavhine and M. Sumbwanyambe, “An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect,” in *2018 International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 114–119.

[19] Jung-Woon Lee, DongYeop Hwang, JiHong Park, and Ki-Hyung Kim, “Risk analysis and countermeasure for bit-flipping attack in LoRaWAN,” in *2017 International Conference on Information Networking (ICOIN)*, 2017, pp. 549–551.

[20] S. S. Giradkar and A. Bhattacharya, “Securing compressed video streams using RC4 encryption scheme,” in *2015 Global Conference on Communication Technologies (GCCT)*, 2015, pp. 640–644.

Authorized licensed use limited to: UNIVERSIDAD DE LAS AMERICAS PUEBLA. Downloaded on October 20,2023 at 22:29:14 UTC from IEEE Xplore. Restrictions apply.