The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

Secure Device to Device Communication for 5G Network Based on improved AES

Ardalan H. Awlla[1], Sirwan M. Aziz[2]

[1] Department of Information Technology, College of Science, University of Human Development, Sulaimaniya, Iraq
[2] Department of Computer Science, Darbandikhan Technical Institute SPU, Sulaimaniya, Iraq

Email: ardalan.hussein@uhd.edu.iq[1], sirwan.hamafaraj@spu.edu.iq[2]

Abstract:

Communication between two devices (device to device) in network systems can be defined is immediate communication between two devices without crossing the Base Station. Moreover, in a mobile network device to device communication is upcoming communication for the coming generation mobile communication network (5G), 5G is relied upon to permit high network throughput, diminishing communication delays, diminish traffic load and energy consumption. Device to device communication is a core technology of 5G. Therefore, all network types' security issues must be considered. To deal with the security issue in 5G network we propose an improved Advanced Encryption Standard (AES) with shift row and Mix Columns. The result indicates that the suggested improved AES is more significant than traditional AES.

Keywords: Security, cryptography, AES, Device to Device communication, 5G, encryption, encryption time, lightweight encryption algorithm, internet of things.

الملخص:

يمكن تعريف الاتصال بين جهازين (جهاز إلى جهاز) في أنظمة الشبكة هو الاتصال الفوري بين جهازين دون عبور المحطة الأساسية. علاوة على ذلك ، في جهاز شبكة الهاتف المحمول ، يكون الاتصال هو الاتصال القادم لشبكة الاتصالات المتنقلة (5G)من الجيل القادم لل (5G) ، يتم الاعتماد على (5G)للسماح بإنتاجية عالية للشبكة وتقليل التأخير في الاتصال ، وتقليل حمل حركة المرور واستهلاك الطاقة. الاتصال من جهاز إلى جهاز هو تقنية أساسية لـ (5G). لذلك ، يجب مراعاة مشكلات أمان جميع أنواع الشبكات. للتعامل مع مشكلة الأمان في شبكة (5G) ، نقترح معيار تشفير متقدمًا محسنًا (AES) مع صف التحول وأعمدة MixColumns. تشير النتيجة إلى أن AES المحسّن المقترح هو أكثر أهمية من AES التقليدي.

پوختە:

پەیوەندی کردن لە نێوان دوو ئامێر (ئامێر بۆ ئامێر) لە سیستەمەکانی تۆر دەتوانرێت پێناسە بکرێت بە ئەوەی کە پەیوەندییەکی دەستبەجێیە لە نێوان دوو ئامێردا بەبێ بەکارهێنانی بنکەی وێستگە. هەروەها لە تۆری مۆبایل پەیوەندی ئامێر بۆ ئامێر، دەبێتە پەیوەندی داهاتووی تۆری مۆبایلی نەوەی داهاتوو کە ئەویش تۆری (5G)، تۆری پەیوەندی 5G پشت دەبەستێت بە تۆرێك کە توانایەکی بەرزی هەبێت کە ئەویش بە دەست دێت بە، کەمکردنەوەی دواخستنی پەیوەندی، کەمکردنەوەی باری هاتوچۆی زانیاری و بەکارهێنانی وزە. پەیوەندی ئامێر بۆ ئامێر تەکنەلۆجیای سەرەکی 5G بۆیە، پێویستە هەموو جۆری کێشەکانی ئاسایشی تۆر ڕەچاو بکرێت. بۆ مامەڵەکردن لەگەڵ کێشەی ئاسایش لە تۆری 5G لەم توێژینەوەیەدا پێشنیاری خوارێزمی ستانداردی مشەفەرکردنی پێشکەوتوو (AES) کراوە بە گەشەپێدانی گۆڕینی ستوون و تێکەڵکردنی ستوون لە خوارێزمی AES. ئەنجامەکە ئاماژە بەوە دەکات کەAES ی پێشنیارکراو باشتر یان پارێزراوترە بەراورد بە AES ی نەریتی.

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

1. Introduction

Communication between two devices (device to device) in network systems became identified as one of the most fundamental enabling technologies in 5G networks [1]; device to device communication has several benefits in mobile networks [2]. First of all, it can increase the exploration of every cell in a mobile network as a transmission platform for sending information to the device placed exterior of cell inclusion. Second, device to device communication assists with diminishing the energy utilization of the base station by conveying straightforwardly among devices. Ultimately, the performance of reutilizing the identical radiofrequency is enhanced. In device to device communication, the space among nodes is pretty lower as compared to the distance among devices and a base station. This indicates the conflict of radiofrequency lower in device to device communication strategy, and it facilitates transmitting the different data utilizing the same radiofrequency. Because of these benefits, the 5G also consist device to device communication technology. Nevertheless, in mobile network device to device communication has a few protection threats [3]. The device to device communication technique includes three strategies which are node detection; establish a connection, and transmitting data [4][5]. For this procedure, due to the lack confirmation process for approving device integrity. When nodes deliver demand for establish a connection to transfer data, any other node responds by transmitting an acknowledgment message. In addition, device to device communication doesn't utilize cryptography for secrecy and message verification to prevent from unauthorized alteration in the conversation procedure. This implies the attacker is able to handle attacks, for example, eavesdropping, imitation, listening, location spoofing, and privacy sniffing. Additionally, technology in the internet of things is connected with the 5G network to handle their service requests. However, the internet of things' applications deals with multiple sensitive data, and the internet of things devices need restricted means [6] with regard to memory, accomplishment, and energy utilization. These functions of the internet of things make the previously mentioned security challenges more critical and difficult to deal with due to the fact usual safety solutions can't be applied or processed adequately. To address the security difficulties of device to device communication in the 5G internet of things' network, 5G require a protected device to device communication network that consists of a suitable authentication technique among devices. Lightweight cryptography algorithm can be appropriate remedies for covering properties-restrained devices.

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

2. Overview of AES

The cryptography Advanced Encryption Standard (AES) algorithm, additionally recognizable by name Rijndael, it's a cryptography algorithm for the encoding of digital data built up via the National Institute of Standards and Technology (NIST) in the U.S. government in 2001 [7]. The AES operates work on a 128-bit plaintext and use the identical key for encryption and decryption process. The AES algorithm is to replace the Data Encryption Standard (DES) algorithm of cryptography due to key length, DES short key length of 56-bits makes it too insecure for applications [8] and it is being surprisingly influential with inside the development of cryptography. Cryptography design for the AES is a symmetric block cipher; the key lengths of the AES are 128, 192, and 256-bit. The key length decides what number of rounds to be performed. The 128-bit key lengths apply 10-rounds, 192-bit apply 12-rounds, and 256-bit apply 14-rounds [9]. AES arithmetic's procedures are subtraction, addition, multiplication, and division, operations depend on key length. All rounds have four transformations individually: Sub Bytes, Shift Rows, Mix Column, and Add Round Key. All transformation requires 16-byte blocks, which should be in form 4 x 4 matrices and brings matrix output with the equivalent size.

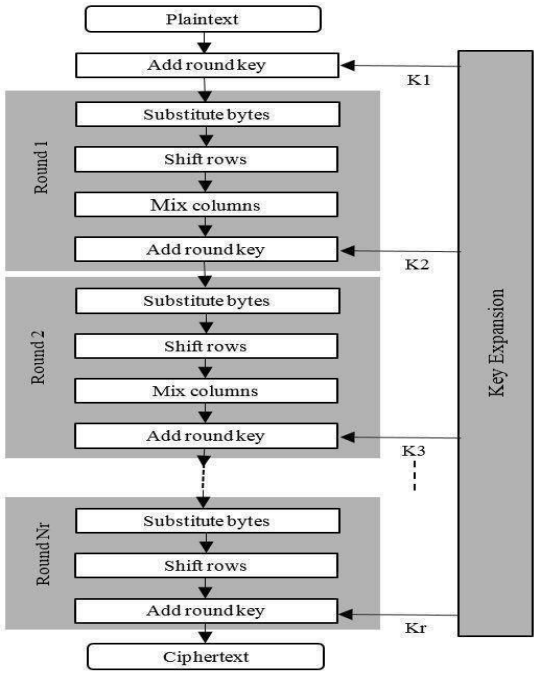

Figure I: Advanced Encryption Standard (AES) Algorithm.

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

2.1. SubBytes transformation

SubBytes transformation is the principal phase for beginning each round in AES encryption process. To execute this phase a non-linear S-box is required to replace a byte in the state to different byte based on confusion and diffusion Shannon's standards for cryptographic algorithm; this operation has significant purpose to achieve further security [9][11]. Such as if we take Hexa 40 in the AES state, it needs to exchange with Hexa FD in table 1. Which is FD generated from the crossing of row 2 and column 8. For the rest of the bytes of the state need to complete this operation.

Table 1: AES S-box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	2b	67	fe	d7	6f	f2	30	63	7c	c5	ab	76	77	7b	6b	1
01	af	a2	9c	a4	47	fa	ad	ca	82	f0	72	c0	c9	7d	59	d4
02	f1	e5	71	d8	f7	36	34	b7	fd	cc	31	15	93	26	3f	a5
03	e2	80	eb	27	5	18	7	4	c7	9a	b2	75	23	c3	96	12
04	b3	d6	29	e3	5a	1b	52	9	83	a0	2f	84	2c	1a	6e	3b
05	39	be	4a	4c	b1	20	6a	53	d1	5b	58	cf	0	ed	fc	cb
06	7f	2	50	3c	33	43	45	d0	ef	85	9f	a8	aa	fb	4d	f9
07	21	da	10	ff	38	92	bc	51	a3	f5	f3	d2	40	8f	9d	b6
08	3d	7e	64	5d	44	5f	c4	cd	0c	17	19	73	13	ec	97	a7
09	14	b8	de	5e	90	22	46	60	81	88	0b	db	4f	dc	2a	ee
0a	62	ac	91	95	24	49	c2	e0	32	5c	e4	79	3a	0a	6	d3
0b	ea	f4	65	7a	4e	8d	6c	e7	c8	a9	ae	8	37	6d	d5	56
0c	1f	74	4b	bd	b4	1c	e8	ba	78	c6	8b	8a	25	2e	a6	dd
0d	b9	57	86	c1	f6	48	61	70	3e	0e	1d	9e	b5	66	3	35
0e	e9	87	ce	55	8e	69	9b	e1	f8	94	28	df	98	11	d9	1e
0f	0f	2d	b0	54	42	bf	41	8c	a1	68	bb	16	89	0d	e6	99

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

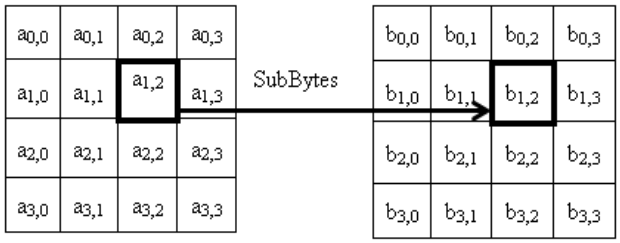

Figure 2: Substitute byte transformation

2.2. ShiftRows Transformation

The second operation stage beyond the SubByte which carries out on the state is ShiftRow. Most important concept beyond this stage is to shift bytes of the state cyclically toward left in every single row except row number zero. During this technique, bytes in the row number zero stays and never perform any transposition. But in first row a single byte is moved circular toward left. Then in the second row two bytes are moved toward left and in the final row three bytes are moved toward left, then every row of the state moves consistently toward a particular offset. As illustrated in Equation

1. $r^s,c = r^s,(c + shift(r, nb)) \% Nb$ for $0 < r < 4$ and $0 \leq c < Nb$ ……..(1)

The shift value shift (r, N_b) counts on the row number r, as illustrated in equation 2.

Shift (1, 2) = 1; shift (2, 4) = 2; shift (3, 4) = 3 …….. (2)

Regardless this operation size of the new output state is not modified, it stay because the identical authentic dimension 16-bytes array as represented in figure 3.

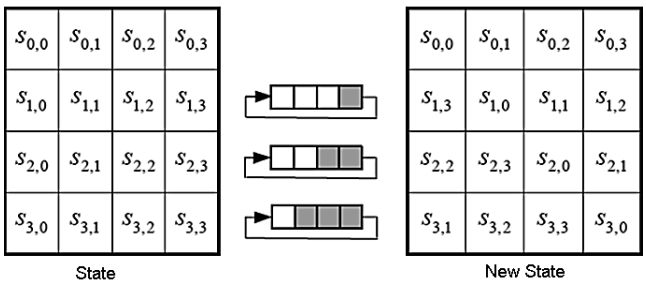

Figure 3: Shift Rows

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

2.3. MixColumns Transformation

The next operation which is performing on the state is MixColumn. In this operation columns in the state are classed as polynomial over Galois field (GF), GF(2^8) then columns is multiplied block $x^4 + 1$ with the a coefficient polynomial c(x) determined by equation 3:

$a(x) = \{03\}x^3 + \{02\}x^2 + \{01\}x + \{02\}$ ……..…..(3)

It can be composing as multiplication matrix which is b(x) = c(⊕ a(x).

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

The size of the state is not modified as shown in figure 4 which is matric 4x4.

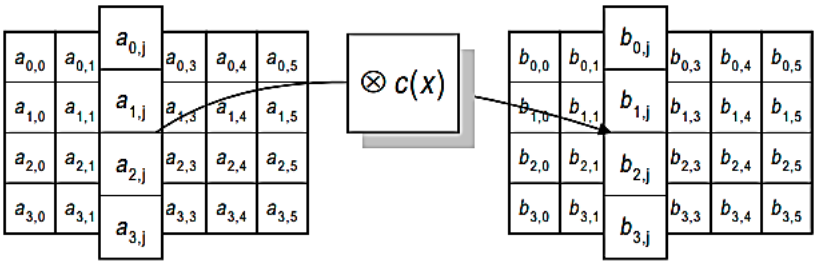

Figure 4: MixColumns transformation

2.4. AddRoundKey Transformation

AddRoundKey is the most critical phase in the AES algorithm, where every byte from the state is joined with the round key then applies bitwise Exclusive OR procedure as illustrated in formulae 4. The round key is produced from the key expansion procedure.

$[s^1_{0,c}, s^1_{1,c}, s^1_{2,c}, s^1_{3,c}] = [s_{0,c}, s_{1,c}, s_{2,c}, s_{3,c}] + [\text{round}^w * Nb + c]$ for $0 \le c \le Nb$ ……..…..(4)

The round key

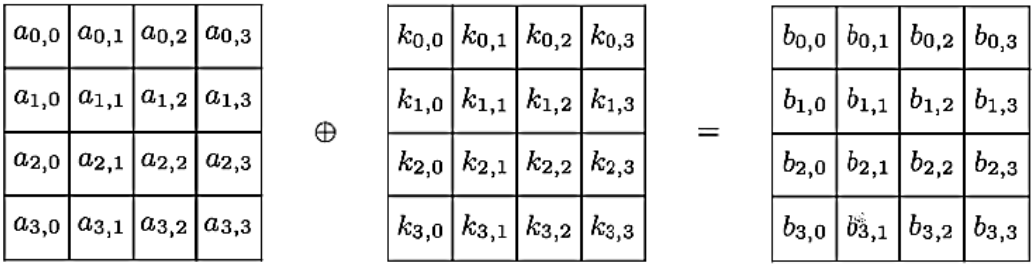

Figure 5: Add Round Key

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

3. The design approach for AES algorithm

Based on the previous clarification, Shift Row which is a circular procedure executed on the state key array which began from the second row to the fourth row of the state, the execution time for each row shift operation is O(n), such circular procedure can be quicker with the utilize of array shift row mapping that has index and value which is assigned immediately to index of the key state which need to be putting, therefore the execution time for array shift mapping which is O(n) only one time will be executed.

Table 2: Indicate circular movement for array shift row mapping.

index	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
value	0	5	10	15	4	9	14	3	8	13	2	7	12	1	6	11

For instance, if in the state index 1 moves to value 5, then the next index 2 will shift to index value 10, etc. The array shift row map can be utilized in the key state as indicated in equation 5:

Ki, j [shift row map [index] %16]……..….. (5)

Where i is an index and j is a value, these operations will decrease the circular movement procedure.

The MixColumns phase is the maximum calculation challenging phase in the AES algorithm and as a result, it wastes a maximum of the time required for required encryption and decryption process. Therefore, our second improvement is in the MixColumns technique transformation, the MixColumns phase is changed with an XOR procedure among the input state and random vector named IV. By using this XOR procedure can reduce the computing needs to 16-XOR rounds due to the input state has only 16-bytes and the XOR procedure waste one cycle for every byte to be performed.

Therefore, utilizing a minimal-cost hardware the total number of cycles could be accomplished that relies upon an 8-bit processor for execution of this plan. Regardless, this number of cycles could be enhanced if the encryption and decryption procedure is completed using hardware with better details. For instance, if the specific hardware relies upon a 32-bit processor, the complete cycle shall be decreased to just 4-cycles considering that 4-XOR procedures can be achieved using a single cycle.

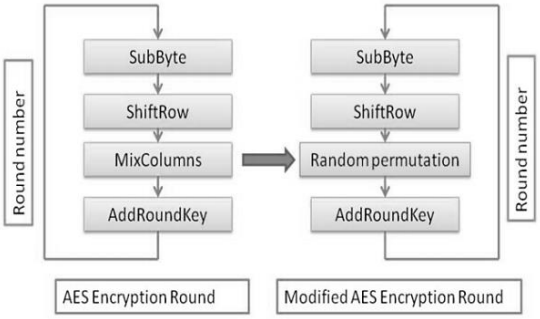

Figure 6: Modified AES

DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

The new design for replacement MixColumn with the XOR operation is shown in figure 7.

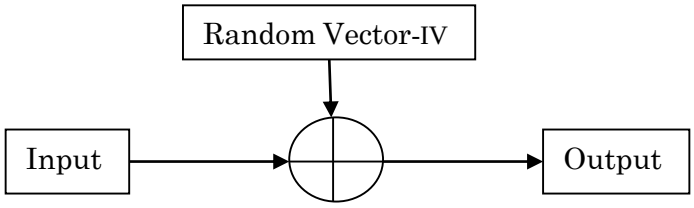

Figure 7: The XOR operation that replaces the MixColumns

This modification has two strategies for the second inputs of the XOR procedure. First, for the complete encryption and decryption procedure, it has a single IV vector. Second, for every cycle in the encryption and decryption procedure, also it has only a single IV vector.
The first strategy will speed up the encryption process at the beginning of the encryption process when the second approach will add the security complication for the adjusted design.

First approach Pseudocode:

```
  FIRST_ APPROACH (INPUT_STATE [16])
  Set OUTPUT_STATE [16] = {0}
  SetIV [16] = {0}
  For i= 1 to 16
    OUTPUT_STATE [i] = INPUT_STATE [i] ^ IV[i]
  Return OUTPUT_STATE [i]
End
```

Second approach Pseudocode:

```
 SECOND_APPROACH (INPUT_STATE [16],   ROUND_NUMBER)
// Get the number of rounds
 Set OUTPUT_STATE [16] = {0}
 SetIV [number_of_rounds, 16] = {0}
 For i= 1 to 16
  OUTPUT_STATE [i] = INPUT_STATE [i] ^ IV [ROUND_NUMBER, i]
 Return OUTPUT_STATE [i]
End
```


DOI: http://dx.doi.org/10.25098/5.1.4

The Scientific Journal of Cihan University – Sulaimaniya **PP: 57-67**
Volume (5), Issue (1), June 2021
ISSN 2520-7377 (Online), ISSN 2520-5102 (Print)

4. Result and Discussion

The proposed AES algorithm with modified shift row and MixColumn operations is evaluated on five bytes' types of data. Notice that the outcomes were processed at Windows 10 device that has core i9 on a 2.8-GHz processor.

Table 2, shows the comparison between Rijndael's AES algorithm with a modified AES algorithm, the table consists of two sections, the encryption section, and the decryption section.

Table 3: Result of AES and improved AES

AES			Improved AES	
Byte of Data	Encryption time	Decryption time	Encryption time	Decryption time
1024	3.020	4.085	1.454	2.685
2048	5.780	7.125	2.780	5.078
3072	9.050	12.687	5.950	8.116
4096	13.243	15.753	8.365	13.0852
5120	16.78	19.332	10.0211	17.008

The table 3 indicates encryption and decryption time for the modified AES algorithm which is less than the existing AES algorithm.

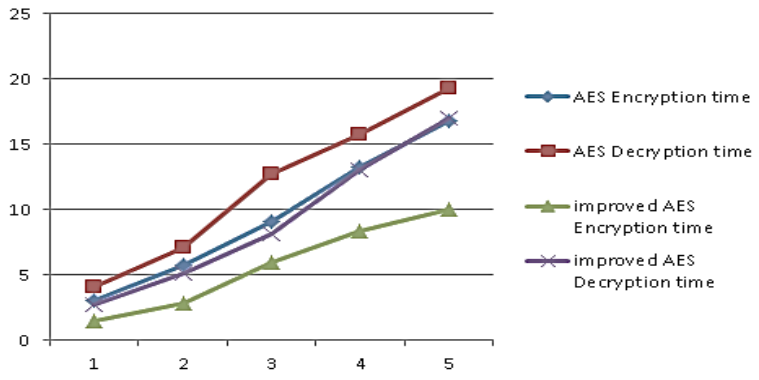

Figure 8: Encryption and Decryption time comparison between AES and Improved AES.

DOI: http://dx.doi.org/10.25098/5.1.4

5. Conclusion

In the near feature 5G network will be a fundamental element of our daily lives. Many sensors and energy-constrained devices will constantly be communicating with each other the security of which must not be agreed. Encryption is a form of cryptography, which is used to secure valuable data from criminal access or modification. AES is belonging to a popular algorithms applied for encryption. But AES algorithm encounters consuming useless time to accomplish the complicated requirement required for the encryption procedure mainly for the real-time application. A few improvements had completed on the AES algorithm to decrease the wasting time or to improve the complication of the algorithm. In this paper, to use AES in real-time applications a new improvement is practiced to the AES algorithm to adjust it. The improvements can grow the efficiency of the encryption and decryption techniques at the same time the difficulty of the encryption is highest possible.

References

[1] R. Sedidi and A. Kumar, "Key exchange protocols for secure Device-to-Device (D2D) communication in 5G," 2016 Wireless Days (WD), Toulouse, 2016, pp. 1-6, doi: 10.1109/WD.2016.7461477.

[2] J. Yue, C. Ma, H. Yu and W. Zhou, "Secrecy-Based Access Control for Device-to-Device Communication Underlaying Cellular Networks," in IEEE Communications Letters, vol. 17, no. 11, pp. 2068-2071, November 2013, doi: 10.1109/LCOMM.2013.092813.131367.

[3] Y. Sun, J. Cao, M. Ma, H. Li, B. Niu and F. Li, "Privacy-Preserving Device Discovery and Authentication Scheme for D2D Communication in 3GPP 5G HetNet," 2019 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, USA, 2019, pp. 425-431, doi: 10.1109/ICCNC.2019.8685499.

[4] Y. Keshtkarjahromi, H. Seferoglu, R. Ansari and A. Khokhar, "Device-to-Device Networking Meets Cellular via Network Coding," in IEEE/ACM Transactions on Networking, vol. 26, no. 1, pp. 370-383, Feb. 2018, doi: 10.1109/TNET.2017.2787961.

[5] X. Xiao, M. Ahmed, X. Chen, Y. Zhao, Y. Li and Z. Han, "Accelerating Content Delivery via Efficient Resource Allocation for Network Coding Aided D2D Communications," in IEEE Access, vol. 7, pp. 115783-115796, 2019, doi: 10.1109/ACCESS.2019.2930728.

[6] S. Borkar and H. Pande, "Application of 5G next generation network to Internet of Things," 2016 International Conference on Internet of Things and Applications (IOTA), Pune, 2016, pp. 443-447, doi: 10.1109/IOTA.2016.7562769.

[7] FIPS PUB 197, "Advanced Encryption Standard (AES)," National Institute of Standards and Technology, U.S. Department of Commerce, November 2001.

[8] C. Sanchez-Avila and R. Sanchez-Reillol, "The Rijndael block cipher (AES proposal): a comparison with DES," Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology (Cat. No.01CH37186), London, England, UK, 2001, pp. 229-234, doi: 10.1109/CCST.2001.962837.

[9] Ziaur Rahaman, Anjela Diana corraya, Mousumi Akter Sumi and Ali Newaz Bahar, "A Novel Structure of Advance Encryption Standard with 3-Dimensional Dynamic S-box and Key

DOI: http://dx.doi.org/10.25098/5.1.4

Generation Matrix" International Journal of Advanced Computer Science and Applications(ijacsa), 8(2), 2017. http://dx.doi.org/10.14569/IJACSA.2017.080241

[10] Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap, "AES Algorithm Using 512 Bit Key Implementation for Secure Communication," International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 3, March 2014.

[11] Siddiqui N, Yousaf F, Murtaza F, Ehatisham-ul-Haq M, Ashraf MU, Alghamdi AM, et al. (2020) A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. PLoS ONE 15(11): e0241890. https://doi.org/10.1371/journal.pone.0241890.

DOI: http://dx.doi.org/10.25098/5.1.4