International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2018): 7.426

New Technique for Internet of Things Security based on the Hybrid Mcrypton - Blowfish and Chaotic System

Haider K. Hoomod, Ahmed A. Ali

AL-Mustansyriah University - Education College - Computer Science Department

Abstract: ***Internet of Things is a topic of much interest and, in last few yearas one of the main focuses, links various kinds of devices to the Internet and even exchanges its data. The advent of IoT which has vast amount of connected devices enables us to monitor and control of real world and changes our daily lifestyle never available before.An important need to protect the data transferred from the devices of the user (mobile devices) and devices control things over the Internet .In this paper we propose a mechanism based on an algorithm that combines two algorithms to solve the problem of security in data transmission .We used a mobile phone to control and send signals to the raspberry pi, Which in turn controls and related devices that run in smart home .***

Keywords: internet of things security, blowfish, mcrypton, chaos

1. Introduction

In today's world, basically all devices are interconnected to each other via networks. There are multiple devices are in homes, offices, cars and production plants and they run various tasks to help with daily tasks. The number of connected devices is increasing all the time because manufactures present every day new internet connected devices for helping the users of these devices in their everyday life and creating new digital experiences. The existing and new Internet based devices are related to smart house appliances, smart cities, smart energy plants, automobiles health care services, retail stores and transportation. Examples from those areas are home surveillance cameras and[1] fridges, smart city applications for helping citizens to find a vacant parking slot and for health care sector's personal trainer appliances Those devices produce different kind of information, raw data, and information are shared with other systems. The data which internet connected devices generate can be stored and then used for various purposes. For example, a fridge can tell the owner about the shortage of groceries which need to be ordered .One example could be from health care sector about the wearable sensor or monitor which tells the person's state of health. That information is then shared via network with professionals in health care.The manufacturing business uses different kinds of sensors and monitoring tools for collecting important data from manufacturing machines and their conditions; based on that data the production is adjusted to be more effective For example the mobile phone connected to the Internet can control the refrigerator or smart home when you transfer information from your mobile to the raspberry pi through the Internet; there are many weaknesses that enable the hacker to get this information and manipulation so We need a powerful way to protect the powerful information transmitted online. We propose in this paper a powerful and fast way to protect information transmitted via the Internet using a proposed algorithm based on the mCrypton and blowfish [2]

2. Blowfish

Blowfish algorithm is a symmetric block cipher which can be used as a drop-in replacement for IDEA or DES. It takes a changeable-length key, from 32 bits to 448 bits, which makes it perfect for both exportable and domestic use. Every round is made up of a key- and data dependent substitution and a key-dependent permutation. All operations are additions on 32-bit words and XOR. The only additional operations, for every round are performed in the following way [3]

- Split each block into halves

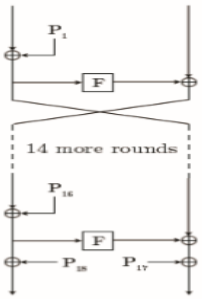


Figure 1: Blowfish Feistal Structure of 16 rounds

Right half becomes new left half -

- The right half is made when XOR is done on the left half and the result we get after applying 'f' to the right half and the key [4].
- The rounds which are prior can be obtained even if the function 'f' is not turned upside down

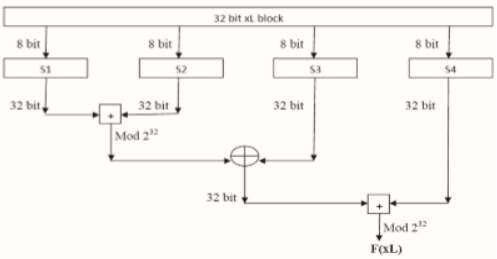


Figure 2: S-Box operation (F function) ofBlowfish algorithm

3. mCrypton

The mCrypton as a high-adapting algorithm, the mCrypton key length can be set according to different application scenarios to 64bit, 96bit or 128 bit, the proposed rounds is 12. mCrypton algorithm uses four 4x4 S-boxes as its nonlinear transform components, unlike other block encryption algorithms operating the entire byte, each byte of mCrypton is divided into two parts, or we may call these parts two nibbles.[5] In addition, the transformation of the linear layer is also based on the bit rather than the byte. The 64 bits input of the mCrypton algorithm will be divided into 8 bytes per block, then each byte is divided into two 4-bits, or two 4-bit nibbles. As a result, all 16 nibbles.

The mCrypton algorithm is composed of four basic transformations: nonlinear substitution ,bit Permutation , column-to-row transposition and key addition.

Figure 3: MCrypton algorithm encryption process

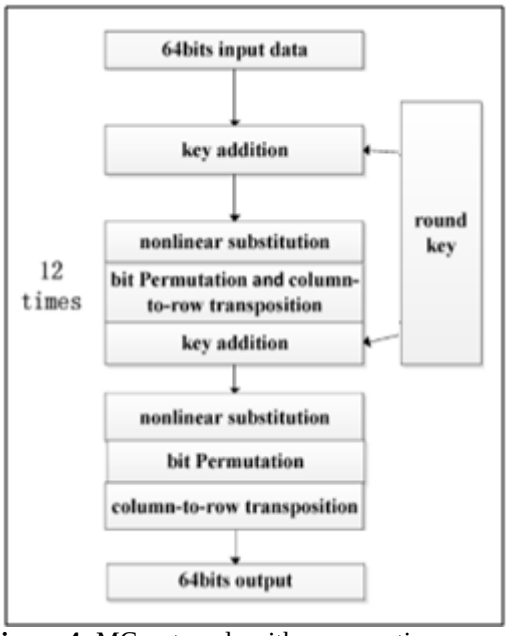


Figure 4: MCrypton algorithm encryption process

4. The Proposed Algorithm

The proposed algorithm combines two algorithms The mCrypton and blowfish .Encryption begins with a 64 bit block element of plain text that will be divided into a 64 bit cipher text. The 64 bit segment is immediately split into two equally sized segments that will be used as the base of the propose algorithm. The exclusive-or-operation (XOR) is performed between the first 32 bit block segment (L) and the first P(Generated from chaos).[6] The resulting 32 bit data is passed to the (F) function The 32 bits as input to the function algorithm will be divided into 4 bytes per block, then each byte is divided into four 2-bits, or four 2-bit nibbles. As a result, all 16 nibbles [7]

$$\begin{matrix} a_0 & a_1 & a_2 a_3 \\ a_4 & a_5 & a_6 a_7 \\ a_8 & a_9 & a_{10} a_{11} \\ a_{12} & a_{13} & a_{14} a_{15} \end{matrix} = \begin{Bmatrix} A[0] \\ A[1] \\ A[2] \\ A[3] \end{Bmatrix} = (A[0]A[1]A[2]A[3])$$

The mCrypton algorithm is composed of four basic transformations: nonlinear substitution r, bit Permutation 7[,column-to-row transposition T and key addition a . 1) Nonlinear substitution r : it is a nonlinear transformation on each nibble of the matrix A, and it is also the only one of then online ear transformation components.[8] Relationships between the four S boxes are use the chaos logistic map as Follow xn+1 = rxn(1-xn)

$x_4=S_4x_3 \;=S_3x_2=S_2x_1=S_1$

Bit permutation π each component column permutation π_i is defined for nibble columns

$$b=\pi_i(a) \Leftrightarrow b_j=\oplus_{k=0}^{3}(m_{i+j+k \bmod 4} \bullet a_k)$$

Of which, stands for multiplication mod 2, and

$$a=(a_0a_1a_2a_3)^t \quad , \quad b=(b_0b_1b_2b_3)^t$$

Where four masking nibbles m_i are given by chaos logistic map[9]
xn+1 = rxn(1-xn)
mi =xi

Then we could define π(A) as

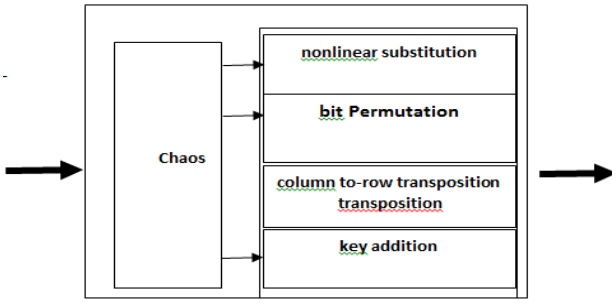
$$\pi(A)=(\pi_0(A_c[0])\pi_1(A_c[1])\pi_2(A_c[2])\pi_3(A_c[3]))$$

Column-to-row transposition T: it simply moves the nibble at the[10] i,j)-th position to the(i,j)-th position(

$$B=\tau(A) \Leftrightarrow b_{i,j}=a_{j,i}$$

Key addition a for a round key are generate the key from chaos logistic map.
K = (K [0], K [1], K [2], K [3])

The Figure 4 illustrates the function for suggested algorithm



The Figure 4 function for proposed algorithm

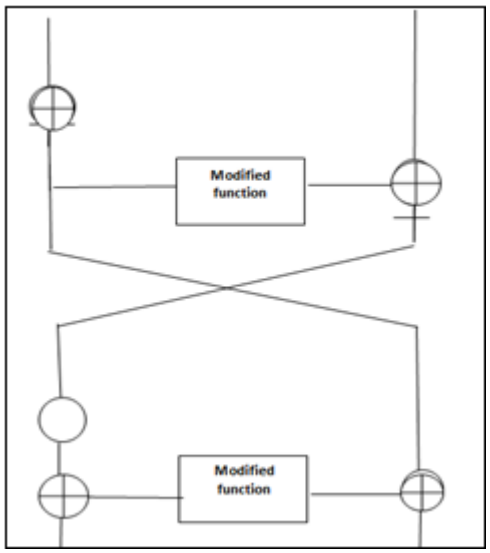


Figure 5: The proposed algorithm

5. Result

	mcrypton		Blowfish		Proposed algorithm	
Data length in Bytes	Time encryption	Time decryption	Time encryption	Time decryption	Time encryption	Time decryption
22	20.404	12.999	15.447	12.990	13.999	17.009
50	31.90	35.901	31.705	32.809	35.885	19.908
64	40.368	41.368	38.368	40.567	22.247	21.911
79	33.789	23.789	43.454	41.099	30.989	30.111
110	50.780	50.110	48.250	50.205	48.999	49.888
Total	177.241	164.16	177.224	175.67	152.008	138.82
average	35.448	**32.833**	35.444	35.134	30.401	27.675

6. Conclusion

We notice from the results that we have obtained that the proposed system is faster, better and more secure. And when we combine the two algorithms better than using a single one, and when using the chaos system, gave the system better power and performance and Through the results we observe encryption and decryption in the algorithmmcrypton is (12.999 ms 20.404 ms) and algorithm blowfish is (12.990 ms15.447 ms) while proposed algorithm is(17.009 ms 13.009)

References

[1] Mahdi, JananAteya. "Design and implementation of proposed br encryption algorithm." *IRAQI JOURNAL OF COMPUTERS, COMMUNICATION AND CONTROL & SYSTEMS ENGINEERING* 9, no. 1 (2009): 34-50.

[2] Tripathi, Ritu, and Sanjay Agrawal."Comparative study of symmetric and asymmetric cryptography techniques." *International Journal of Advance Foundation and Research in Computer (IJAFRC)* 1, no. 6 (2014): 68-76.

[3] Pavithra, S., and E. Ramadevi."Study and performance analysis of cryptography algorithms." International Journal of Advanced Research in Computer Engineering & Technology 1, no. 5 (2012): 82-86

[4] Poonia, Vaibhav, and Narendra Singh Yadav."Analysis of modified Blowfish Algorithm in different cases with various parameters."In 2015 International Conference on Advanced Computing and Communication Systems, pp. 1-5. IEEE, 2015..

[5] Singh, SimarPreet, and Raman Maini."Comparison of data encryption algorithms." International Journal of Computer Science and Communication 2, no. 1 (2011): 125-127

[6] Lim, ChaeHoon, and TymurKorkishko. "mCrypton–a lightweight block cipher for security of low-cost RFID tags and sensors." In International Workshop on Information Security Applications, pp. 243-258. Springer, Berlin, Heidelberg, 2005

[7] Park, Jong Hyuk. "Security analysis of mCrypton proper to low-cost ubiquitous computing devices and applications." International Journal of Communication Systems 22, no. 8 (2009): 959-969.

[8] Daftardar-Gejji, Varsha, and SachinBhalekar."Chaos in fractional ordered Liu system." Computers & mathematics with applications 59, no. 3 (2010): 1117-1127

[9] Wu, Xiaogang, Hanping Hu, and Baoliang Zhang."Parameter estimation only from the symbolic sequences generated by chaos system." Chaos, Solitons& Fractals 22, no. 2 (2004): 359-366

[10] Han, Zhang, Wang XiuFeng, Li Zhao Hui, Liu Da Hai, and Lin You Chou. "A new image encryption algorithm based on chaos system." In IEEE International Conference on Robotics, Intelligent Systems and Signal Processing, 2003.Proceedings. 2003, vol. 2, pp. 7