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 years 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, m crypton, 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](image)

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) of Blowfish algorithm](image)
3. mCrypton

The mCrypton as a high-adapting algorithm, the mCrypton key length can be set according to different application scenarios to 64-bit, 96-bit 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 + Permutation, column-to-row transposition and key addition.

![Figure 3: MCrypton algorithm encryption process](image1)

**Figure 3:** 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]

\[
\begin{align*}
A_0 & = A, & A_1 & = A \\
A_2 & = A \\
A_3 & = A \\
A_4 & = A  \\
A_5 & = A \\
A_6 & = A \\
A_7 & = A \\
A_8 & = A \\
A_9 & = A \\
A_{10} & = A \\
A_{11} & = A \\
A_{12} & = A \\
A_{13} & = A \\
A_{14} & = A \\
A_{15} & = A \\
\end{align*}
\]

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

\[x_{n+1} = rxn(1-xn)\]

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

\[b = π_i(a) \Leftrightarrow b_j = +\sum_{k=0}^{n-1} (m_{n-j}) \cdot a_k \]

Of which, stands for multiplication mod 2, and

\[a = (a_0, a_1, a_2, a_3)^T, \quad b = (b_0, b_1, b_2, b_3)^T\]

Where four masking nibbles \(m_i\) are given by chaotic logistic map[9]

\[x_{n+1} = rxn(1-xn)\]

\[m_i = xi\]

Then we could define \(π(A)\) as

\[π(A) = (π_0(A_0), π_0(A_1), π_0(A_2), π_0(A_3))\]

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

\[B = T(A) \Leftrightarrow b_{i,j} = a_{j,i}\]

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

![Figure 4: MCrypton algorithm encryption process](image2)

**Figure 4:** MCrypton algorithm encryption process

**Volume 8 Issue 8, August 2019**

[www.ijsr.net](http://www.ijsr.net)

Licensed Under Creative Commons Attribution CC BY

Paper ID: ART202063

10.2175/ART202063

651
5. Result

<table>
<thead>
<tr>
<th>Data length in Bytes</th>
<th>mcrypton Time encryption</th>
<th>mcrypton Time decryption</th>
<th>Blowfish Time encryption</th>
<th>Blowfish Time decryption</th>
<th>Proposed algorithm Time encryption</th>
<th>Proposed algorithm Time decryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>20.404</td>
<td>12.999</td>
<td>15.447</td>
<td>12.990</td>
<td>13.999</td>
<td>17.009</td>
</tr>
<tr>
<td>50</td>
<td>31.900</td>
<td>35.901</td>
<td>31.705</td>
<td>32.809</td>
<td>35.885</td>
<td>19.908</td>
</tr>
<tr>
<td>64</td>
<td>40.368</td>
<td>41.368</td>
<td>38.368</td>
<td>40.567</td>
<td>22.247</td>
<td>21.911</td>
</tr>
<tr>
<td>79</td>
<td>33.789</td>
<td>23.789</td>
<td>43.454</td>
<td>41.099</td>
<td>30.989</td>
<td>30.111</td>
</tr>
<tr>
<td>110</td>
<td>50.780</td>
<td>50.110</td>
<td>48.250</td>
<td>50.205</td>
<td>49.999</td>
<td>49.888</td>
</tr>
<tr>
<td>Total</td>
<td>177.241</td>
<td>164.16</td>
<td>177.224</td>
<td>175.67</td>
<td>152.008</td>
<td>138.82</td>
</tr>
<tr>
<td>average</td>
<td>35.448</td>
<td><strong>32.833</strong></td>
<td>35.444</td>
<td><strong>35.134</strong></td>
<td>30.401</td>
<td>27.675</td>
</tr>
</tbody>
</table>

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 algorithm m crypton is (12.999 ms 20.404 ms) and algorithm blowfish is (12.990 ms 15.447 ms) while proposed algorithm is (17.009 ms 13.009 ms)

References