IEEE
المؤتمر الوطني الخامس لكليات الحاسب الآلي بالجامعات السعودية
The Fifth National Conference of Saudi Computers Colleges 2022
NCCC 5
21-22 December 2022

Cryptographic Algorithms to Secure IoT Devices: A Survey

Amgad A. Muthanna, Fatimah M. Alburaiki, Sumayah A. Alwadei and Mohammed S. Alshehri
439406227,439304330, 441305663,msalshehry@nu.edu.sa
جامعة نجران
NAJRAN UNIVERSITY

Abstract

IoT devices are often unsecured, leaving them open to attack by unauthorized persons .These individuals can intercept data or manipulate the devices for their own malicious purposes.
our paper reviews the security threats that face the Internet of Things. It does this by reviewing several related surveys on the security of IoT. In doing this, the paper will discuss the Cryptographic Schemes in IoT. It will also focus the various light weigh Cryptography algorithms and the design differences for normal block ciphers.

Introduction

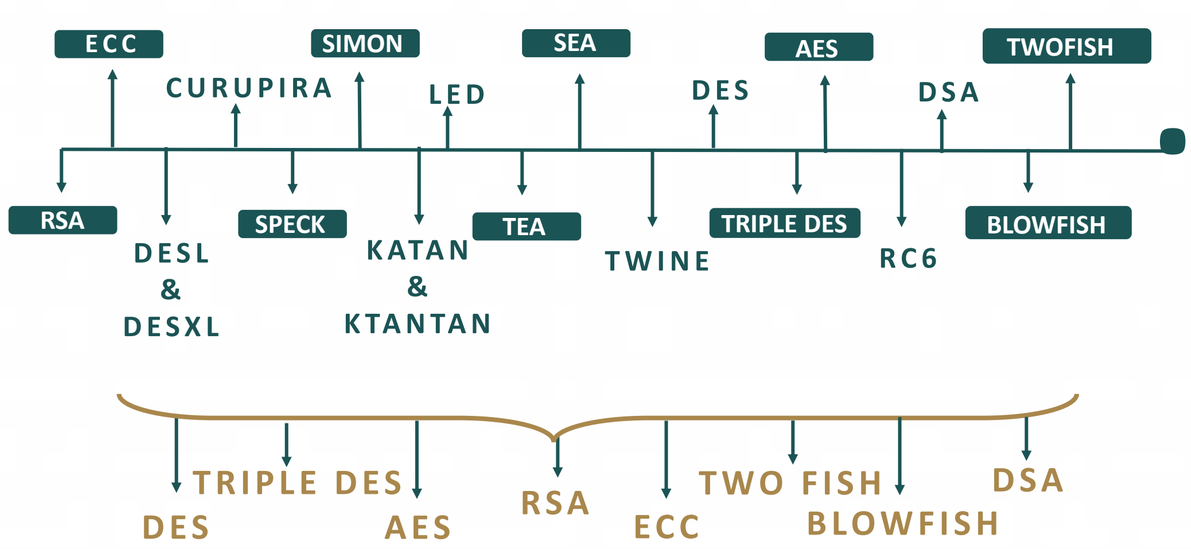
IoT systems create new capabilities and services and allow more outstanding capabilities and increase their flexibility through their reliance on public networks In the near future, there will not be any place for marketing devices that are not connected to the Internet, but these public networks are not sufficiently secure, allowing attackers to access internal systems from the outside world. We can say that our system is safe if we investigate:

CIA Security features in IoT

It is essential that we prioritize the encryption algorithms used to protect our privacy and data from potential threats. The task of testing an ideal algorithm is certainly not an easy thing and requires great focus.

Methodologies

First, we searched into 20 encryption algorithms on IoT, and then after several comparisons and conclusions, we filtered the best 8 among them, to make a more accurate comparison between them specifically . We have filtered this 8 algorithms according to : Size of key , Speed and finally determine of it is Symmetric or Asymmetric.



Based on the research we conducted, we found that: An algorithm alone cannot be fully effective for the Internet of Things because of the variety of devices and their security and performance needs. However, we can achieve a more satisfactory result by pairing the algorithm with another concept that boosts its security and performance. For example, the cryptosystem proposed in a survey by Mona, May, and Samir, ”Secure framework for IoT technology based on RSA and DNA cryptography,” which suggests a cryptosystem based on the RSA algorithm and DNA cryptography concepts with a novel approach of mixing DNA strands from encoding medical images and reports to improve security through IoT networks .

Conclusion

In this micro survey, we focused specifically on the security issues related to the Internet of Things (IoT). We also surveyed the most important cryptographic algorithms that have been used in the IoT. And based on the research we conducted, we found that: An algorithm alone cannot be fully effective for the Internet of Things because of the variety of devices and their security and performance needs. However, we can achieve a more satisfactory result by pairing the algorithm with another concept that boosts its security and performance. In future work, we plan to simulate those algorithms to deeply study them.