International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

IMPLEMENTATION OF DATA SECURITY FOR LOW POWER IOT DEVICE

Joel Sequeira, Abhijit Tamba

Masters of Engineering (E&TC department),Goa College of Engineering (India)
MS Electrical and computers, Rutgers University, Proprietor Eme automation (India)

ABSTRACT

With the rapid growth of network infrastructure, communication algorithms and sensor electronics,IoT(internet of things) has been on the forefront of perceivable technologies helpful to a wide cross section of the society. IoT applications span from industrial to automotive to smart home and now, in smart cities. While IoT has a huge social impact there is a worry about data security and privacy. This project focuses on security of Industrial IoT and its impact on latency. In Industrial IoT, the customers are worried about the vulnerability of their data and processes entering public/competitor domain. This has been a deterrent to some industries in switching over to IoT platforms and cloud services. This research will be helpful for evaluating performance of various technologies related to security and latency of the Industrial IoT networks.

Keywords—Authentication; Asymmetric;Cryptography ;Integrity; Security; Symmetric.

I. INTRODUCTION

In a world where not only computers are connected, but also any kind of devices, it is becoming more and more important to protect communications channels from being spied out or to securely authenticate the devices communicating to each other by proven techniques. Self-made algorithms as well as not securely stored crypto keys (like in software) lead to hacks which we are currently seeing on the market. Hacked cars which are controlled from outside, printers sending information to an external server, TV cameras giving access to private lives or attacked industrial plants are just some examples. Therefore, it is important to already add security on a board level.

II. MOTIVATION

2.1 Security drives growth .

IoT, cloud, wearable's, vehicle–to-vehicle communications, and mobile market growth will give rise to billions of smart nodes and platforms. That increases the number of entry points hackers can attack. So, robust security is desirable.

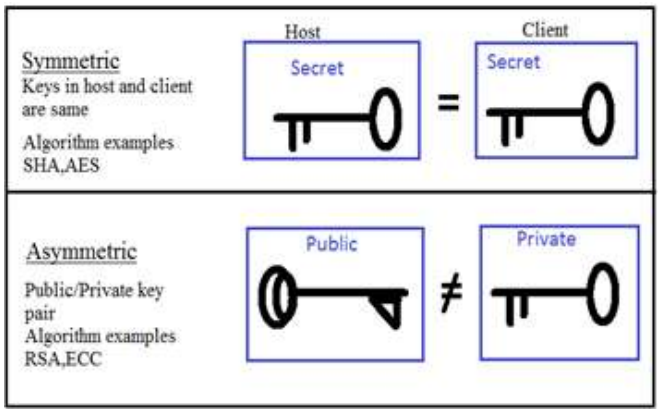
2.2 Security matters more than ever.

Even with the explosion of data breaches, security is still treated as a reflection. Security should, in fact, be the criterion of any discussion about a data system or any type. Engineers, executives, investors, and researchers alike have been screeching past the graveyard hoping that their digital welfares will not be attacked too badly. Of course that is irrational because targets are super easy to find now.

III. LITERATURE REVIEW

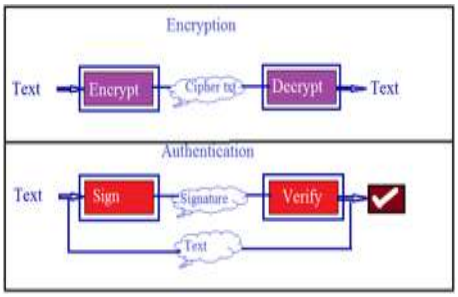
3.1 Symmetric and Asymmetric Authentication.

Authentication can be done in two methods, Symmetric and Asymmetric. The key difference between the two is associated to the use of keys. If the same secret key is used on the client and also on the host then the application is symmetric. If the keys are equal then the system is symmetric. Otherwise, if there is a mathematically linked private and public key pair being used then the application is asymmetric. If the keys are not the same on each side then it is asymmetric. Atmel has devices for both types. Asymmetric, is also called public-key infrastructure or "PKI" and it is very well suited for real world use. A person having the public key can send encrypted messages to the proprietor of the private key. When a receiver gets an asymmetric message, he or she will decrypt it with their private key. In distinction, because symmetric cryptography uses the exact same key for both encryption and decryption, only the senders and receivers with that specific private key can communicate to each other.



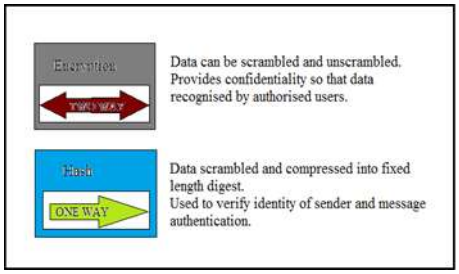
3.2 Encryption and Authentication .

Encryption and authentication are essential security purposes, but have different functions. Encryption has been used to protect messages from being read by involuntary people. Authentication is the other main pillar of cryptography. Authentication is used to see if a message is real. To make such a "realism check" a number of things have to be verified such as if it was propelled by the right sender, if messages were acknowledged in the right order, if the intended message or part of the message was erased, or if a message was changed in some way. In short, encryption is about encoding and decoding, while authentication is about verifying the identity of the sender and the integrity of the message.



3.3 Hashing vs. Encryption

A hash is a one-way operation. The hash function is its most important feature for cryptography because it is mathematically infeasible to reverse the hashing process to obtain the original message. Also, a featureof a hash function is that anychange tothe input changes the digest, so hashes are great to create digital signatures that identify and authenticate the sender and message. Hashes are also used for secure password storage, file identification, message authentication coding (MAC), and asymmetric sign verify operations. With encryption, data is scrambled and unscrambled in such a way that the input and output mapping is always one-to-one for a given key and is unintelligible to anyone other than a receiver who has the key to unscramble it. Encryption is always reversible (by definition), so encryption is used whenever there is the need to get the input data back out. However, the identity of the sender and the integrity of the message (meaning if it has been altered or not) are not guaranteed by encryption only. That is where authentication comes in.



IV. EXAMINATION OF DATA ENCRYPTION SCHEMES

Following block encryption algorithms have been considered: AES128, AES192, AES256, taking into account the different encryption modes: ECB, CBC, CFB, OFB and CTR, the one which gives best results will be considered for implementation in sensor level IoT network.

TABLE I. Performance time for encryption in CBC mode and data block sizes

Key size	Size of Data bytes		
	1024	*2048*	*4096*
AES128	0.49ms	0.79ms	1.37ms
AES192	0.55ms	0.91ms	1.58ms
AES256	0.61ms	1.01ms	1.77ms

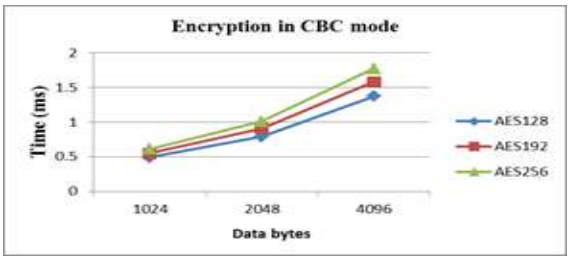


Fig. 1. Comparison of execution CBC mode encryption

TABLE II. Performance time for decryption in CBC mode and data block sizes.

Key size	Size of Data bytes		
	1024	***2048***	***4096***
AES128	0.54ms	0.85ms	1.46ms
AES192	0.59ms	0.96ms	1.66ms
AES256	0.64ms	1.06ms	1.87ms

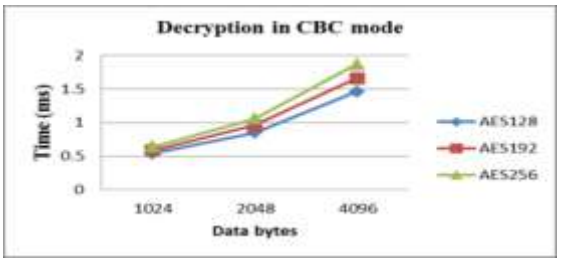


Fig. 2. Comparison of execution CBC mode decryption

TABLE III. Performance time for encryption in CFB mode and data block sizes.

Key size	Size of Data bytes		
	1024	***2048***	***4096***
AES128	0.50ms	0.80ms	1.36ms
AES192	0.55ms	0.91ms	1.57ms
AES256	0.60ms	1.01ms	1.79ms

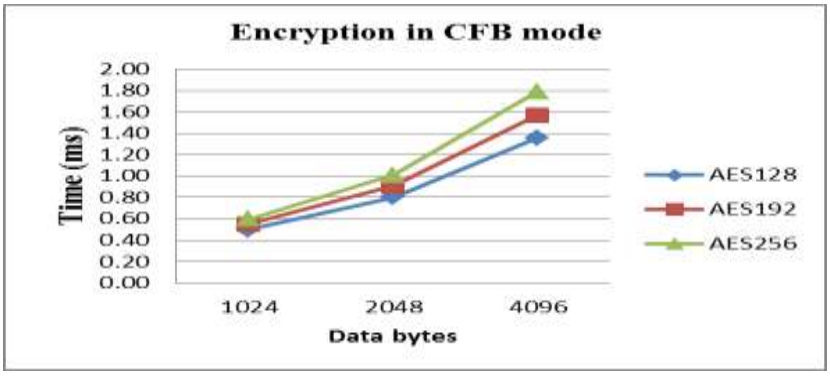


Fig. 2. Comparison of execution CFB mode encryption

TABLE IV. PERFORMANCE TIME FOR DECRYPTION IN CFB MODE AND DATA BLOCK SIZES.

Key size	Size of Data bytes		
	1024	*2048*	*4096*
AES128	0.52ms	0.84ms	1.44ms
AES192	0.58ms	0.95ms	1.66ms
AES256	0.63ms	1.06ms	1.86

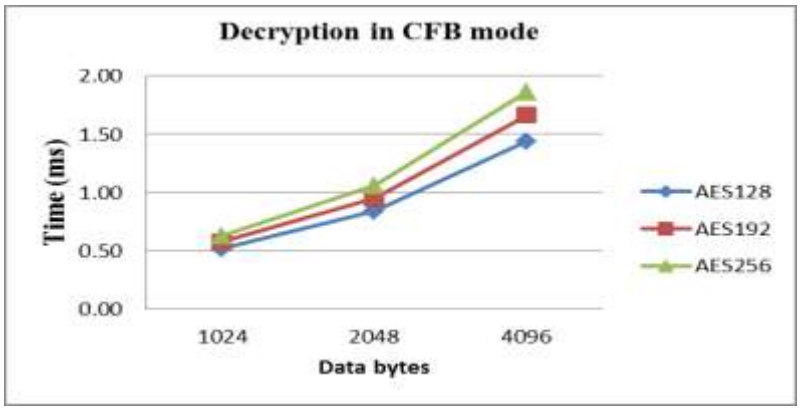


Fig. 4. Comparison of execution CFB mode decryption.

V. PROPOSED METHODOLOGY

As shown below is block diagram of implementation for communication between two Microcontrollers. The Microcontroller will contain AES software (symmetric) and Atmel chip will contain private Keys and digital signatures. Atmel ATECC508c provides this security at microcontroller level. ESP 8266 chip to be used as MCU .The communication between ATECC508c and ESP 8266 is by I2C serial. ATECC508c chip provides cost effective, and work with any Microcontroller.

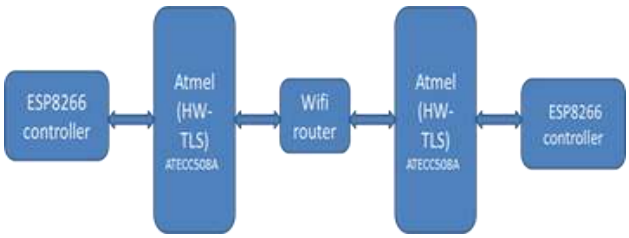


Fig. 5. Block diagram for implementation

VI. CONCLUSION

As we can see from Table I, Table II, Table III, Table IV the execution times of AES 128 and AES192 much faster than execution speed of AES 256 in the modes of operation CBC, CFB but this also concludes that AES 256 provides higher security as compared to AES 128 and AES 192.

For power comparison the AES scheme has to uploaded in the node MCU with keys and signatures stored in ATECC508c chip for analysis purpose, this will be done in future scope.

REFERENCES

[1] Suparna Biswas and Subhajit Adhikari " Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network" International Journal of Computer Applications (0975 – 8887) Volume 131 – No.17, December201

[2] Zhe Liu, Kim-Kwang Raymond Choo, Johann Grossschadl, "Securing Edge Devices in the Post-Quantum Internet of Things Using Lattice-Based Cryptography", *Communications Magazine IEEE*, vol. 56, pp. 158-162, 2018, ISSN 0163-6804.

[3] S. Sicari et al., "Security Privacy and Trust in Internet of Things: The Road Ahead", *Computer Networks*, vol. 76, pp. 146-64, 2015.

[4] J. Granjal, E. Monteiro, J. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", *IEEE Commun. Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, 2015.

[5] Soumya Ranjan Moharana, Vijay Kumar Jha, Anurag Satpathy, Sourav Kanti Addya, Ashok Kumar Turuk, Banshidhar Majhi, "Secure key-distribution in IoT cloud networks", *Sensing Signal Processing and Security (ICSSS) 2017 Third International Conference on*, pp. 197-202, 2017.

[6] Syed Farid Syed Adnan, Mohd Anuar Mat Isa, Habibah Hashim, "Analysis of asymmetric encryption scheme AAβ Performance on ArmMicrocontroller", *Computer Applications & Industrial Electronics (ISCAIE)2017\IEEE-Symposium-on*,pp.146-151,2017.

[7] Haya Hasan, Tasneem Salah, Dina Shehada, M. Jamal Zemerly, Chan Yeob Yeun, Mahmoud Al-Qutayri, Yousof Al-Hammadi, "Secure lightweight ECC-based protocol for multi-agent IoT systems", *Wireless and Mobile Computing Networking and Communications (WiMob)*, pp. 1-8, 2017.

[8] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, Sophie Gire, J.M. Eghan, Nii Narku Quaynor, "Feature Based Encryption Technique for Securing Forensic Biometric Image Data Using AES and Visual Cryptography", *Artificial Intelligence Modelling and Simulation (AIMS) 2014 2nd International Conference on*, pp. 199-204, 2014.

[9] Quist-Aphetsi Kester, Laurent Nana, Anca Christine Pascu, "A Novel Cryptographic Encryption Technique for Securing Digital Images in the Cloud Using AES and RGB Pixel Displacement", *Modelling Symposium (EMS) 2013 European*, pp. 293-298, 2013.

[10] Lomné, Thomas Roche, Adrian Thillard, "On the Need of Randomness in Fault Attack Countermeasures - Application to AES", *Fault Diagnosis and Tolerance in Cryptography (FDTC) 2012 Workshop on*, pp. 85-94, 2012.

[11] Yoon Jib Kim, Ki-Uk Kyung, "Secured radio communication based on fusion of cryptography algorithms", *Consumer Electronics (ICCE) 2015 IEEE International Conference on*, pp. 388-389, 2015.

[12] Chong Hee Kim, "Improved Differential Fault Analysis on AES Key Schedule", *Information Forensics and Security IEEE Transactions on*, vol. 7, pp. 41-50, 2012, ISSN 1556-6013.

[13] Marcelo Dornbusch Lopes, Leonardo R. P. Rauta, Benjamin W. Mezger, Michelle S. Wangham, "Providing a cloud-based smart meter solution to control and monitor electrical quantities of industrial machines", *Wireless and Mobile Computing Networking and Communications (WiMob)*, pp. 1-8, 2017.

[14] Guillaume Gaillard, Dominique Barthel, Fabrice Theoleyre, Fabrice Valois, "Service Level Agreements for Wireless Sensor Networks: A WSN operator's point of view", *Network Operations and Management Symposium (NOMS) 2014 IEEE*, pp. 1-8, 2014.

[15] Inès Hosni, Fabrice Théoleyre, Noureddine Hamdi, "Localized scheduling for end-to-end delay constrained Low Power Lossy networks with 6TiSCH", *Computers and Communication (ISCC) 2016 IEEE Symposium on*, pp. 507-512, 2016

[16] A comprehensive evaluation of cryptographic algorithms in cloud computing,Inventive Computation Technologies (ICICT), International Conference ,DOI : 10.1109/INVENTIVE.2016.7823268

[17] Gautam Siwach, Amir Esmailpour, "LTE Security potential vulnerability and algorithm enhancements", *Electrical and Computer Engineering (CCECE) 2014 IEEE 27th Canadian Conference on*, pp. 1-7, 2014, ISSN 0840-7789.

[18] Shadi Traboulsi ,Mohamad Sbeiti ,David Szczesny "High-performance and energy-efficient sliced AES multi-block encryption for LTE mobile devices", Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference ,DOI: 10.1109/ICCSN.2011.6014927.