Performance Evaluation of AES Symmetric Key Encryption Modes in an Ambient Assisted Living System

Velislava Grishina Spasova and Ivo Tzvetanov Iliev

Abstract – **This paper presents state of the art review of cryptographic practices as well as a performance evaluation of symmetric key encryption algorithms on an Allwinner A13 based ARM embedded system - part of a fall detection Ambient Assisted Living solution. The evaluated algorithms are 5 modes of the AES (Advanced Encryption Standard) symmetric encryption algorithm.**

Keywords – **Symmetric Key Encryption, Embedded System, Ambient Assisted Living**

I. INTRODUCTION

Ambient Assisted Living is a multidisciplinary area whose focus is in building solutions that ensure higher quality of life and independence of the elderly and people with disabilities. One of the major requirements to these systems which they share with the somewhat broader area of the Internet of Things (IoT) is to ensure very high privacy, security and data integrity [1-3].

Encryption and authentication are two of the major mechanisms for better application security. In terms of encryption, there are two fundamentally different groups of generic encryption algorithms – symmetric encryption algorithms and asymmetric encryption algorithms [4].

Characteristic of symmetric encryption is that both communicating parties share a common secrete key. This key is used for both encryption and decryption, thus specific measures for secure key distribution have to be taken. The most widely used symmetric encryption algorithm currently is AES (Advanced Encryption Standard) which is a block cipher with a 128, 192 or 256 bit key (128 bit keys are most widely used). AES is considered both cryptographically secure and relatively fast. It can be used in a variety of modes in order to extend the basic block cipher into a stream cipher which can be used to encrypt arbitrary length of data, such as multimedia data. The AES modes whose performance evaluation is presented in this paper are: CBC (Cipher Block Chaining), CTR (Counter), OFB (Output Feedback), CFB (Cipher Feedback) and GCM (Galois Counter Mode) [5].

V.Spasova is with the Department of Electronics and Electronics Technologies, Faculty of Electronic Engineering and Technologies, Technical University - Sofia, 8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria, e-mail: vgs@tu-plovdiv.bg

I. Iliev is with the Department of Electronics and Electronics Technologies, Faculty of Electronic Engineering and Technologies, Technical University - Sofia, 8 Kliment Ohridski blvd., 1000 Sofia, Bulgaria, e-mail: izi@tu-sofia.bg

The other group of encryption algorithms is asymmetric algorithms. Characteristic of them is that a couple of public key - private key is used. The public key is publicly available to everyone while the private key is kept secrete by the party which generated the key couple, and is used only for decryption. The most widely used asymmetric algorithm is RSA (named after the names of its inventors – Rivest, Shamir and Adleman). In contrast to AES, RSA cannot be extended to encrypt large data such as multimedia – the maximum amount of data that can be encrypted by it ranges in the order of 100-400 bytes depending on the length of the key (1024 – 4096 bits) [5].

As both RSA and AES have their benefits and drawbacks, they are often combined into a hybrid scheme. In it RSA is used for private key exchange between the communicating parties (as a more secure alternative to the classic Diffie-Hellman key exchange algorithm) and once the communicating partied have agreed on a shared secret key, AES is used for the actual data encryption.

In recent years much research effort is focused towards encryption algorithms that are specifically tailored to images and a lot of chaos-based schemes have been proposed [6-8]. Unfortunately, due to the high complexity of the security domain and the corresponding cryptographic attacks, it is not enough for an algorithm to be mathematically and cryptographically secure – most of these new algorithms have been broken by side channel attacks [9, 10]. Thus, it is recommended to either use only established and well tested algorithms and implementations, or to at least integrate them into new schemes [5].

Finally, it should be noted that only encryption is not enough for safe data transmission. Authentication is also needed in order to ensure the authenticity and data integrity of the communicating parties. Some block cipher modes combine encryption with authentication (such as GCM mode) but the majority of encryption algorithms do not encompass authentication. For the purposes of this study the encryption algorithms were paired with the most widely deployed mechanism for authentication – HMAC (Hash-based Message Authentication Codes) [5].

The remainder of this paper is divided as follows – Section II presents a brief overview of the AAL platform that was used for the performance evaluation, as well as the architectural overview of the cryptographic module. Section III presents the results of the experimental evaluation of data encryption with the following modes: CBC, CTR, OFB, CFB and GCM. Finally, Section IV concludes the paper.

II. SYSTEM OVERVIEW

The system that was used as an experimentation platform is an AAL gateway. The architecture of the system is presented at Figure 1.

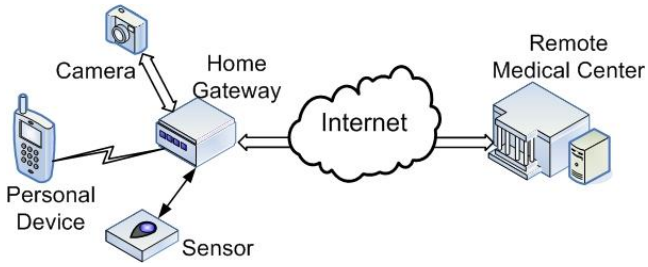


Fig. 1. AAL system architecture.

The gateway serves as the control unit of a home-sized distributed system which contains a variety of sensors such as accelerometer, camera, etc. It is also responsible for communication over the Internet with a remote medical center. As the transmitted information is predominantly personal (e.g. vital parameters, pictures of the user, information about his/her physical condition) all data should be encrypted and authenticated before transmission. The device used as a gateway is A13-OlinuXino-WiF based on the A13 microcontroller with ARM Cortex A8 core. It has a variety of communication interfaces such as WiFi and Ethernet, 512 MB RAM and 4 GB flash memory. The board runs Debian Linux

The cryptographic module that we have set up as well as the communication protocol between the gateway and a remote server are presented at Figure 2.

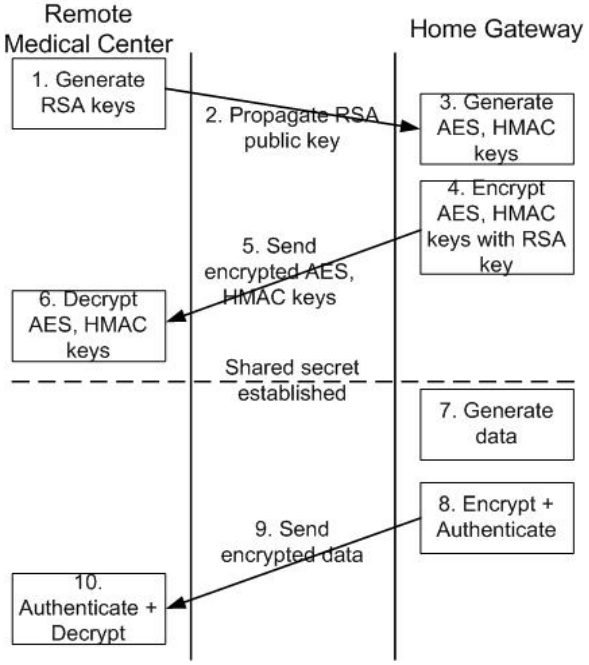


Fig. 2. Cryptographic module.

Before any encryption can take place, the two parties (in our case the gateway and the remote server) have to establish a common secret key. RSA is used for the key exchange. First, the remote server generates a 2048 bit private key - public key pair and sends the public key to the gateway. Then, the gateway generates a 128 bit AES secret key as well as a 256 or 512 bit HMAC secret key, encrypts them with the server's public key and sends them back to the server. Than, the server decrypts the message and extracts the two secret keys and the shared secret between the server and the gateway is established.

Once the server and the gateway have shared the authentication and encryption keys, the actual data transmission can take place. The gateway deploys an 'encrypt-then-authenticate' policy, according to which it first encrypts the data to a ciphertext and then authenticates the ciphertext, thus granting protection against active attacks. Consequently at the server side, the server first authenticates the received message and if it is valid, it proceeds to decryption.

III. EXPERIMENTS AND RESULTS

For the experiment a test image has been re-sized into 5 with different resolutions – 120x160 pixels (19.2 Kpx), 240x320 px (76.8 Kpx), 480x640 px (307.2 Kpx), 720x960 px (691.2 Kpx) ND 960x1280 px (1228.8 Kpx), where Kpx stands for kilo pixels. It is highly unlikely that images with higher resolutions will be transmitted through the system so this dataset is exhaustive of the use cases.

For the experiment every image resolution has been encrypted with every one of the 5 AES-128 modes: CBC, CFB, OFB, CTR and GCM, and for the modes without authentication has been authenticated with HMAC with underlying hash function SHA-256 or SHA-512 (thus with 256 or 512 bit key). All the tests are run 100 times each and the results have been averaged. The tests are implemented in Python with the *cryptography* module [11]. The results from this runtime-based performance evaluation are presented at Figure 3.

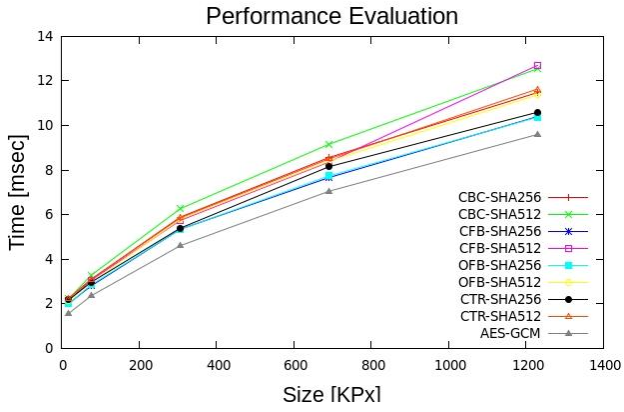
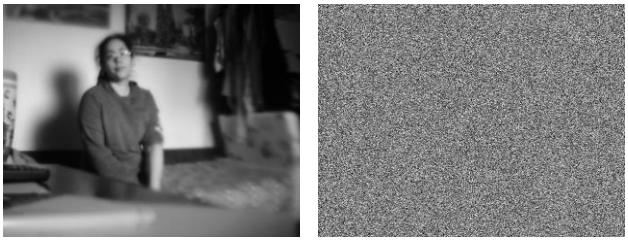


Fig. 3. Performance Evaluation of AES-128 encryption modes.

As it can be seen from the figure, all the modes have similar performance which is in the milliseconds range even for the largest image resolutions. Out of these GCM mode performs the best and has the added benefit of

automatic authentication. On the other hand this mode uses one key for both encryption and authentication which could be a drawback if the security of the system is somehow compromised. In reality any scheme – GCM or a combination of one of the other modes plus authentication, provides enough security with low additional processing cost. An example of un-encrypted image and its corresponding encrypted image with the GCM mode are presented at Figure 4.a and Figure 4.b.



a b

Fig. 4. Un-encrypted image and its corresponding encryption in AES-GCM mode.

IV. Conclusion

In this paper we have presented an overview of the requirements to privacy and security from the perspective of Ambient Assisted Living as well as a snapshot of the established state of the art cryptographic practices. An implementation of a secure data transmission system on a fall detection AAL platform has been illustrated. An evaluation of the runtimes of five of the most common modes of the AES cryptographic standard has been presented. Through this experiment we have proved that we don't have to sacrifice real-time responses for better security and that it is feasible to develop a secure system on an embedded platform with limited resources.

Future work will be concentrated on extending this system with algorithms which are more focused on image encryption as opposed to the currently deployed generic AES schemes.

V. Acknowledgement

This work has been funded by grant № 142ПД0047-03.

References

[1] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu. *Security of the Internet of Things: perspectives and challenges*, Wireless Networks, November 2014, Vol. 20, Issue 8, pp. 2481-2501.

[2] R. Roman, J. Zhou, J. Lopez. *On the features and challenges of security and privacy in distributed internet of things*, Computer Networks, July 2013, Vol. 57, Issue 10, pp. 2266-2279.

[3] H. Suo, J. Wan, C. Zou, J. Liu. *Security in the Internet of Things: A Review*, Proceedings of the 2012 International Conference on Computer Science and Electronic Engineering, Vol. 3, pp. 648-651, 2012.

[4] W. Stallings. *Cryptography and Network Security Principles and Practices, Sixth Edition*, Pearson, 2013 (in English)

[5] N. Ferguson, B. Schneier, T. Kohno. *Cryptography Engineering: Design Principles and Practical Applications*, Wiley, 2010 (in English)

[6] G. Chen, Y. Mao, C.K. Chui. *A symmetric image encryption scheme based on 3D chaotic cat maps*, Chaos, Solitons & Franctals, July 2004, Vol. 21, Issue 3, pp. 749-761.

[7] N.K. Pareek, V. Patidar, K.K. Sud. *Image encryption using chaotic logistic map*, Image and Vision Computing, September 2006, Vol. 24, Issue 9, pp. 926-934.

[8] Z. Zhu, W. Zhang, K. Wong, H. Yu. *A chaos-based symmetric image encryption scheme using a bit-level permutation*, Information Sciences, March 2011, Vol. 181, Issue 6, pp. 1171-1186.

[9] C. Li, S. Li, K.T. Lo. *Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps*, Communications in Nonlinear Science and Numerical Simulation, February 2011, pp. 837-843.

[10] C.Li, Y.Liu, T. Xie, M. Z. K. Chen. *Breaking a novel image encryption scheme based on improved hyperchaotic sequences*, Nonlinear Dynamics, August 2013, Vol. 73, Issue 3, pp. 2083-2089.

[11] https://cryptography.io/