How to cite this paper:

Taqiyah Khadijah Ghazali & Nur Haryani Zakaria. (2017). An enhancement of lightweight encryption for security of biometric fingerprint data for smart home environment in Zulikha, J. & N. H. Zakaria (Eds.), Proceedings of the 6th International Conference of Computing & Informatics (pp 729-734). Sintok: School of Computing.

AN ENHANCEMENT OF LIGHTWEIGHT ENCRYPTION FOR SECURITY OF BIOMETRIC FINGERPRINT DATA FOR SMART HOME ENVIRONMENT

Taqiyah Khadijah Ghazali[1] and Nur Haryani Zakaria[2]

[1]Universiti Utara Malaysia, Malaysia, taqiyah_khadijah@ahsgs.uum.edu.my
[2]Universiti Utara Malaysia, Malaysia, haryani@uum.edu.my

ABSTRACT. The capabilities of Internet of Things (IoT) of smart home technologies and networks are able to allow novel attacks. To ensure the security of smart homes, access control need to be established, for example by cryptography and authentication between the communicating objects. Biometric fingerprint is one of the most popular and reliable biometric-based authentication methods for personal identification. It is efficient and is already widely used. For smart home devices which are resource-constrained, the usage of lightweight encryption is proposed. Currently the Advanced Encryption Standards (AES-128) is one of the cryptography solutions that are available in lightweight category. However, AES does not offer authentication mode which is important for providing protection to biometric fingerprints. This study intends to highlight the necessity to enhance the existing lightweight encryption particularly the AES to protect the biometric fingerprint authentication data.

Keywords: lightweight encryption, smart home, lightweight block cipher, authenticated encryption mode, biometric fingerprint

INTRODUCTION

Security is one of the important elements in smart home. The capabilities of home technologies are able to allow novel attacks, hence there is a need to analyse and reduce traditional as well as new risks in smart home environments. Internet of Things (IoT) environments networks such as in wireless sensor network and RFID have major threats, consisting of malicious software and various hacking techniques. These are the most likely attacks in network transmission and therefore are important threats to be alleviated for example by authentication and cryptography between the communicating objects (Denning, Kohno, & Levy, 2013).

Authentication is one of the elements in access control in smart home environment, whereby it will identify and verify the residents through several security authentication mechanisms such as password, PIN number, smart card or biometric recognition like fingerprint or iris. Security authentication mechanisms have various benefits and issues. There are no perfect authentications but rather its efficiency and convenience for the residents to choose (Ishengoma, 2014).

This paper intends to review the security of smart home environment, focuses on biometric fingerprint and lightweight encryption. This paper will be organised as follows; the next section will present security of smart home, biometric fingerprint and lightweight encryption, followed by authenticated encryption and finally discussion, conclusion and future work.

SECURITY OF SMART HOME: BIOMETRIC FINGERPRINT AUTHENTICATION

Biometric fingerprint is one of the most popular and reliable biometric-based authentication methods for personal identification (Kim, Yoon, Joo, & Yi, 2014). It is highly distinctive and unique to every person, since identical twins have different fingerprints. Furthermore, it is also easily available, highly accurate and very reliable. In addition, because of its characteristics of acquisition, more sources are available whereby it can be obtained from the ten fingers. Besides, its uses in collections by law enforcements and immigrations are highly reputable. Fingerprints standards development is an important component in fingerprint recognition because of the enormous variety of algorithms and sensors offered on the market (Maltoni, Maio, Jain, & Prabhakar, 2003). Therefore biometric fingerprint is suitable for use in authentication mechanism of smart homes.

LIGHTWEIGHT ENCRYPTION

Concerning security issues of communicating devices in smart homes, a significant research effort has been carried out on cryptography designed for low-cost, low throughput, resource-constraint devices, etc. This area has been referred to as “lightweight cryptography”, and has resulted in a variety of new protocols that have been suggested for small devices, such as RFID tags and wireless sensor networks (WSNs) (Jacobsson, Boldt, & Carlsson, 2014).

The solutions based on the devices’ capabilities are classified in four groups: ultra-lightweight, low-cost, lightweight and specific domain. Lightweight and ultra-lightweight ciphers typically provide 80 to 128 bit security (Manifavas, Hatzivasilis, Fysarakis, & Rantos, 2013). Lightweight cryptography can be measured in two distinct contexts: in software and in hardware. Lightweight in software does not suggest lightweight in hardware and vice-versa (Mohd, Hayajneh, & Vasilakos, 2015).

Lightweight ciphers must cope with the trade-offs between security, cost and performance. Security operations in low resource devices have a number of issues; among them are the overhead implementation, power or energy consumption, and security performance. Due to low-resource devices, the security solutions of the overhead for example memory footprint in software or gate count in hardware should be minimal. Besides, the power consumption should be less and the performance should be reasonable to support applications and end-user requirements. Furthermore, the performance of security solutions should be reasonable to support applications and end-user (Mohd et al., 2015).

Apart from that, lightweight cryptography should resist all known forms of cryptanalytic attacks such as linear and differential cryptanalysis in the context of secret-key since lightweight cryptography is not meant to be “weak” cryptography, which means a lightweight cryptographic should not be the weakest connection in the security of a system (Dinu et al., 2015).

Differences between Lightweight and Non-lightweight Cryptography

Katagi & Moriai (2008) mentioned in their work; for devices with low resource, such as battery powered, the cryptographic operation with a minimum amount of power consumption is essential. Lightweight application systems provide lesser energy for end devices. The footprint of lightweight cryptography is smaller than non-lightweights. Besides, lightweight cryptography can establish more network connections opportunities with lower resource devices. Table 1 below shows the differences between lightweight and non-lightweight cryptography.

Table 1. Differences between Lightweight and Non-Lightweight Cryptography.

Lightweight Cryptography	Non-Lightweight Cryptography
Pervasive IT – security resource constrained devices.	Existing encryption algorithms that were designed for normal computer is not appropriate for constrained devices.
Algorithm - constrained environments: • RFID tags, • sensors, • contactless smart cards, • Health-care devices, etc.	Due to the limitation of their resources. • computational capacity, • memory, and power
Efficiency and smaller footprint	Too costly to be implemented
Open possibilities of more network connections with lower resource devices	Not small
Example of lightweight encryption: Present, Klien, Prince, (AES-128).	Example of non-lightweight encryption: Twofish, Blowfish, AES-256, Serpent

Block ciphers are better than stream ciphers (Manifavas et al., 2013). Thus, in this study the authors focus more on lightweight block cipher. There are several lightweight block ciphers that are used for constrained devices, such as Present (Bogdanov et al., 2007), Advance Encryption Standard (AES) (Daemen, Rijmen, & Leuven, 1999), and Prince (Borghoff et al., 2012) to name a few.

Among these encryption techniques, AES is one of the most preferred encryptions due to its efficient performances and security reliability (Mohd et al., 2015). AES cipher has three different categories which are AES-128, AES-192 and AES-256, for which AES-128 complies with lightweight characteristic (Manifavas et al., 2013).

However, AES focuses on providing confidentiality but not authenticity. Existing encryption algorithm does not provide data authenticity (Cid, 2016) (Readers can refer to this webpage for more information). Without covering the aspect of authenticity as suggested by NIST (Stallings & Brown, 2012), AES cannot offer a complete protection to its users. Thus, this creates an opportunity for research to investigate further on improving the existing AES cipher and to improve its security.

AUTHENTICATED ENCRYPTION (AE) MODE

Security needs are varied in different cryptographic functions. In addition, the strings to be handled by such applications generally have uncertain lengths. Therefore, a block cipher has to be properly designed to process such strings and also to achieve the exact security objectives. Techniques designed for doing these are known as modes of operations of a block cipher (Chakraborty & Sarkar, 2016).

Thus, a few modes of operation on arbitrary length of message are designed. Such as, ECB (Electronic Codebook Mode), CBC (Cipher-block Chaining Mode), CFB (Cipher Feedback Mode) and OFB (Output Feedback Mode), however as some of these earliest modes, can only offer confidentiality or authenticity, but are not able to deliver both simultaneously (Chen, 2009; Krovetz & Rogaway, 2011).

Therefore, to counter this problem, GCM (Galois/Counter Mode), CCM (Counter with CBC MAC), OCB (Offset Codebook Mode) and CWC (Carter-Wegman + CTR Mode), as some of the new developed modes, can perform confidentiality and authenticity simultaneously with the appropriate underlying block ciphers, and thus are called the Authenticated Encryption (AE) mode or sometimes known as Authenticated Encryption with Associated

Data AEAD (Chen, 2009). Table 2 shows the summaries of general properties of authenticated encryption modes.

Table 2. Summaries of General Properties of Authenticated Encryption Modes.

	GCM (Galois/Counter Mode)	**CCM (Counter with CBC MAC)**	**OCB (Offset Codebook Mode)**	**CWC (Carter-Wegman + CTR Mode)**	**EAX (Alternative to CCM)**
Security Function	Authenticated encryption (One-pass schemes)	Authenticated encryption (Two-pass schemes)	Authenticated encryption (One-pass schemes)	Authenticated encryption (Two-pass schemes)	Authenticated encryption (Two-pass schemes)
Associated Data	Yes	Yes	Yes	Yes	Yes
Patent-Free	Yes	Yes	Yes (for non-military used)	Yes	Yes
Initialization vector (IV) requirements	Non-repeating nonce	Non-repeating nonce	Non-repeating nonce	Non-repeating nonce	Non-repeating nonce
Parallelizability	-Encryption block level -Authentication bit level	None	Fully parallelizable	Fully parallelizable	None
Key Space	One block cipher key	One block cipher key	One block cipher key	One block cipher key	One block cipher key
Message Length Requirements	-Arbitrary message up to 2^{39}-256 bits -Arbitrary additional authenticated data up to 2^{64} bits	-Arbitrary message up to 2^{8L}bits,where L=2,...,8 -Arbitrary additional authenticated data up to 2^{64} bits	Any bit string allowed	-Arbitrary message up to 2^{39}-256 bits -Arbitrary additional authenticated data up to 2^{39}-256 bits	Any bit string allowed
Underlying Cipher Block Size Requirements	64, 128	Only 128	128, 192, 256	128, 192, 256	Any block size allowed
Reference	(McGrew & Viega, 2004)	(Bellare, Rogaway, & Wagner, 2004)	(Rogaway, 2015)	(Kohno, Viega, & Whiting, 2004)	(Bellare et al., 2004)

DISCUSSION

Fingerprint recognition consists of enrollment of the fingerprint to the scanner to extract the features and store the template in the database. Fingerprint recognition will also do the verification and identification whereby the process is to check whether the user's fingerprint and fingerprint's template stored in the database matches or otherwise. The templates stored in the database will be encrypted upon verification and identification. If the user is valid, access is granted.

Based on the review done on existing lightweight cipher, AES appears to be the highest choice for software platforms, since it is the top performer in a range of standard platforms. It provides better speed, but has a rather large code and data memory (Law, Doumen, & Hartel, 2006; Mohd et al., 2015).

Based on the Table 2, OCB mode is among the suitable AE mode to use. OCB mode was targeted to afford both message authentication and confidentiality. It is fundamentally a scheme for integrating a Message Authentication Code (MAC) into the operation of a block cipher. Thus, OCB mode prevents the requirement to use two systems: a MAC for authentication and encryption for confidentiality. The outcome is lower in computational cost compared by using separate encryption and authentication functions. Beginning January 2013, the developer has allowed a free license for any open source license certified by the Open Source Initiative (Rogaway, 2015). OCB performance overhead is minimal and it is simple and clean, and easy to implement in either hardware or software. Besides, OCB can be designed to run in very small memory: the main memory is that needed to hold the AES sub-keys. Furthermore OCB is well faster than CCM and GCM (Krovetz & Rogaway, 2011; Rogaway, 2015).

The security objectives are important elements to protect the data thus relying on the AES alone is not enough to securely hide the template data. Hence, combining AES with the authenticated encryption mode will improve data protection. The purpose behind this combination is that, AES cover the confidentiality as stated in the NIST95 (Stallings & Brown, 2012), while OCB cover the authenticity simultaneously. As a result, these two ciphers will protect the data more strongly. Readers can refer to the algorithm from this article (T. Krovetz & Rogaway, 2014)

CONCLUSION AND FUTURE WORK

In this paper, a review has been made to highlight the security in smart home environment. Lightweight cryptography is progressing in the researches that are needed for security in resource constrained devices. This need appears from essential pervasive technology applications, such as based on WSNs and RFID tags where cost and energy constraints limit the solution complexity, with the concern that existing cryptography solutions become too expensive to be carried out.

Since AES does not offer authentication mode which is important for providing protections to biometric fingerprints, this study intends to highlight the necessity to enhance the existing lightweight encryption particularly the AES to protect the biometric fingerprint authentication data. An enhancement of lightweight encryption technique for biometric fingerprint authentication can be proposed by combining the block cipher AES-128 with authenticated encryption mode which is OCB whereby this technique can aims to achieve confidentiality and authenticity.

ACKNOWLEDGMENTS

The authors wish to acknowledge the Ministry of Higher Education (Malaysia) for funding this research under the Trans Disciplinary Research Grant Scheme (TRGS), S/O code: 13164 and RIMC Universiti Utara Malaysia for supporting this research.

REFERENCES

Bellare, M., Rogaway, P., & Wagner, D. (2004). The EAX Mode of Operation B Criticism of CCM E Proof of Security of EAX, 1–44.

Bogdanov, A., Knudsen, L. ., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. ., … Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. *Cryptographic Hardware and Embedded Systems - CHES 2007*, 450–466.

Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., … Yalçin, T. (2012). PRINCE - A low-latency block cipher for pervasive computing applications. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7658 LNCS*(10), 208–225. http://doi.org/10.1007/978-3-642-34961-4

Chakraborty, D., & Sarkar, P. (2016). On modes of operations of a block cipher for authentication and authenticated encryption. *Cryptography and Communications*, *8*(4), 455–511. http://doi.org/10.1007/s12095-015-0153-6

Chen, H. (2009). *Authenticated Encryption Modes of Block Ciphers, Their Security and Implementation Properties*. Ruhr-Universität-Bochum. Retrieved from http://www.emsec.rub.de/media/crypto/attachments/files/2011/03/chen.pdf

Cid, C. (2016). Designs and Challenges in Authenticated Encryption. In *International Workshop on Cybersecurity, Kyushu University*. Retrieved from http://staff.cs.kyushu-u.ac.jp/data/event/2016/02/160107_Carlos_Cid.pdf

Daemen, J., Rijmen, V., & Leuven, K. U. (1999). AES Proposal : Rijndael. *Complexity*, 1–45. Retrieved from http://ftp.csci.csusb.edu/ykarant/courses/w2005/csci531/papers/Rijndael.pdf

Denning, T., Kohno, T., & Levy, H. M. (2013). Computer security and the modern home. *Communications of the ACM*, *56*(1), 94. http://doi.org/10.1145/2398356.2398377

Dinu, D., Corre, Y. Le, Khovratovich, D., Perrin, L., Großsch, J., & Biryukov, A. (2015). Triathlon of Lightweight Block Ciphers for the Internet of Things.

Ishengoma, F. (2014). Authentication System for Smart Homes Based on ARM7TDMI-S and IRIS-Fingerprint Recognition Technologies. *CiiT International Journal of Programmable Device Circuits and Systems*, *6*(6). Retrieved from

Jacobsson, A., Boldt, M., & Carlsson, B. (2014). On the Risk Exposure of Smart Home Automation Systems. *Future Internet of Things and Cloud (FiCloud), 2014 International Conference on*, 183–190. http://doi.org/10.1109/FiCloud.2014.37

Katagi, M., & Moriai, S. (2008). Lightweight cryptography for the Internet of Things. *Sony Corporation*, 7–10. Retrieved from http://www.iab.org/wp-content/IAB-uploads/2011/03/Kaftan.pdf

Kim, Y., Yoon, J., Joo, J.-H., & Yi, K. (2014). Robust lightweight fingerprint encryption using random block feedback. *Electronics Letters*, *50*(4), 267–268. http://doi.org/10.1049/el.2013.3775

Kohno, T., Viega, J., & Whiting, D. (2004). CWC: a high-performance conventional authenticated encryption mode. *Fast Software Encryption. 11th International Workshop, FSE 2004. Revised Papers (Lecture Notes in Comput. Sci. Vol.3017)*, 408-- 26. http://doi.org/10.1007/978-3-540-25937-4_26

Krovetz, T., & Rogaway, P. (2011). The software performance of authenticated-encryption modes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *6733 LNCS*(Fse), 306–327. http://doi.org/10.1007/978-3-642-21702-9_18

Krovetz, T., & Rogaway, P. (2014). RFC 7253 The OCB Authenticated-Encryption Algorithm, 1–19. Retrieved from https://tools.ietf.org/html/rfc7253

Law, Y. W., Doumen, J., & Hartel, P. (2006). Survey and benchmark of block ciphers for wireless sensor networks. *ACM Transactions on Sensor Networks*, *2*(1), 65–93.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2003). Handbook of Fingerprint Recognition. *Annals of Physics*, *54*(ISBN: 978-1-84882-253-5), 494.

Manifavas, C., Hatzivasilis, G., Fysarakis, K., & Rantos, K. (2013). Lightweight Cryptography for Embedded Systems - A Comparative Analysis. In *In Revised Selected Papers of the 8th International Workshop on Data Privacy Management and Autonomous Spontaneous Security* (pp. 1–18). Springer-Verlag New York, Inc.,. http://doi.org/10.1007/978-3-642-54568-9_21

McGrew, D., & Viega, J. (2004). The GCM Mode. *Submission to NIST Modes of Operation Process*, 1–43. Retrieved from http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf%5Cnhttp://siswg.net/docs/gcm_spec.pdf

Mohd, B. J., Hayajneh, T., & Vasilakos, A. V. (2015). A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. *Journal of Network and Computer Applications*, *58*(April 2016), 73–93. http://doi.org/10.1016/j.jnca.2015.09.001

Rogaway, P. (2015). OCB: Background. Retrieved from http://web.cs.ucdavis.edu/~rogaway/ocb-faq.htm

Stallings, W., & Brown, L. (2012). *Computer Security Principles and Practice*.