Benha Journal of Engineering Science and Technology (BJEST)

مجلة العلوم الهندسية والتكنولوجية بكلية الهندسة ببنها

2018; Vol-55-61
Journal Homepage: www.bu.edu.eg/bjest

A Review on Lightweight Cryptography in Internet of Things

Amal S. Hegazy[1,*], Abdelhalim A. Zekry [2] , Amr A. Elawamry[3], Wageda I. Elsobky[4]

[1]Electrical Department, Benha faculty of engineering, Benha, Egypt, amel.hegazy@bhit.bu.edu.eg
[2]Electronics and communication Department, Faculty of engineering Ain Shams University, Cairo, Egypt
[3]Electrical Department, Benha faculty of engineering, Benha, Egypt, amr.awamry@bhit.bu.edu.eg
[4]Basic science Department, Benha faculty of engineering, Benha, Egypt, wageda.alsobky@bhit.bu.edu.eg

Abstract : The Internet of Things (IoT) empowers billions of embedded computing devices to associate to each other. The smart things cover our everyday friendly devices, such as, ovens, fridges, and TV sets**,** as well as critical IoT applications, for example, the control framework in atomic reactors or the connected medical devices in health-care. The tremendous number of devices asociated through heterogeneous frameworks increases the risk of attacks. To overcome these security threats in the IoT, robust security arrangements must be considered. However, IoT devices are limited regarding memory, computation and energy capacities, in addition to the lack of communication reliability. In this context, we look for efficient security mechanisms to build up secure communications between obscure IoT devices, while taking into account the security requirements and the resource constraints of these devices using lightweight cryptography. In this paper, a brief discussion on IoT architecture and various IoT applications has been done. Further, the security concerns with respect to data sharing and attacks have been highlighted. Related work for lightweight strategies utilized for secure data transmission is depicted in this paper.

Keywords: IoT, lightweight cryptography, resource constrained devices

الملخص العربى:

الملخص العربى: إنترنت الأشياء يمكن العديد من أجهزة الحاسوب من الاتصال بعضها ببعض. وتغطي الأجهزة الذكية حياتنا اليومية المعتادة، مثل الثلاجات والأفران وأجهزة التلفزيون، فضلا عن تطبيقات إنترنت الأشياء الهامة، على سبيل المثال، نظام التحكم في المفاعلات النووية أو الأجهزة الطبية المتصلة في الرعاية الصحية. فالعدد الهائل من الأجهزة الموصلة عبر البنى التحتية غير المتجانسة يزيد من خطر وقوع هجمات. ولمعالجة هذه التهديدات الأمنية في إنترنت الأشياء، يجب النظر في حلول أمنية قوية. ومع ذلك، فإن أجهزة انترنت الاشياء محدودة من حيث الذاكرة والحسابات وقدرات الطاقة، بالاضافة إلى عدم موثوقية الاتصالات. وفي هذا السياق، نسعى إلى إيجاد آليات أمنية فعالة من أجل إقامة اتصالات آمنة بين أجهزة إنترنت الأشياء غير المعروفة، مع مراعاة المتطلبات الأمنية والقيود المفروضة على الموارد في هذه الأجهزة باستخدام التشفير الخفيف. في هذه المقالة ، تم إجراء مناقشة موجزة حول معمارية إنترنت الأشياء وتطبيقات إنترنت الأشياء المختلفة. علاوة على ذلك ، تم تسليط الضوء على المخاوف الأمنية فيما يتعلق بمشاركة البيانات والهجمات. ويرد في هذه المقالة وصف للأعمال ذات الصلة باستراتيجيات التشفير الخفيف المستخدمة لنقل البيانات بأمان.

1. Introduction

Internet of Things (IoT) [1] is a new-fashioned technology that is the future of following period of the internet which connects different physical objects that communicate with each other without the guide of human cooperation and utilized current internet standards protocol for sharing the data over a public network. Internet of Things is the combinations of three terms (i) Things pinpoint itself (ii) Thing commutations (iii) Thing interact that builds the Ubiquitous computing environment.

Usually IoT architectures are divided into three layer architecture (a) physical layer (b) commutation layer (c) application layer (fig. 1). Physical layer (also known as perceptual layer) is responsible for assembling data for each object and comprises of constrained devices and unconstrained devices, the second layer (commutation layer) duty is to transmit the data assembly by the physical layer. Commutation layer uses a transmission media, like 4G,3G,2G, wireless, wired, fiber optic, short range communications for commutating the data over the public network. The third layer is application layer which is responsible for distinguishing the form of application which will be used in IoT.

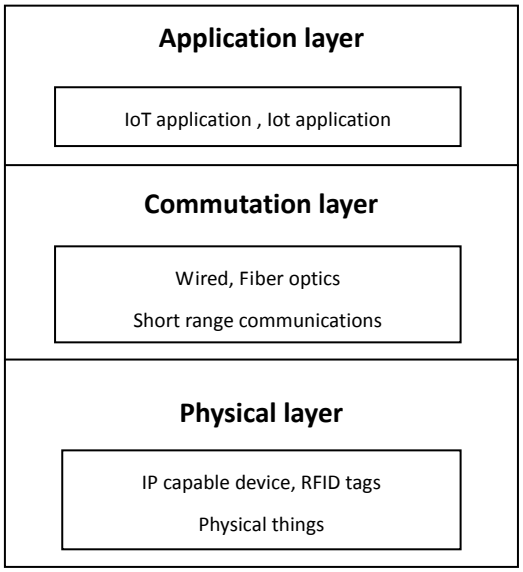

Figure 1: IoT Architecture

The IoTs are real time system which takes information through sensors impart in the network and gives facility to users to access, share and as per their prerequisite makes a move. With the improvement of wireless sensor networks, innovations have been made in IoTs. IoTs have paved their way in people everyday lives. Some applications of IoTs are mentioned below [2].

- Home automation system where electronic things at home can be controlled via cellphones and laptops thus making a system that enables a smart home. It additionally gives the facility of detecting emergencies; maintain energy consumption inside the house, *and so on*.

- Intelligent Transportation System in which traffic monitoring can be done, accidents, traffic jams and traffic rules violation can be reported to authorities.

- Natural disasters prediction and critical temperature changes reporting, by consistent observing of environment utilizing sensors. Monitoring environmental contamination like measuring level of toxic gases in air, substance of poisonous material in water, *etc*.

- Healthcare facilities like remote monitoring of patients, constant monitoring of health parameters and activities, support for independent living, monitoring prescriptions dose by the patient and many more can be provided.

- Surveillance and tracking of individuals, items and creatures, investigating spaces and deserted zones, maintenance of infrastructure and equipment, alarming systems and many more facilities have turned out to be conceivable with IoTs.

2. Types of attacks on IoT systems

Communications in IoTs happen by means of Internet, which is a publically accessible network. This makes it susceptible to different attacks which cause interference in smooth working of IoTs. Some attacks are discussed below:

- *Denial of Service Attack (DOS):* This attack stops the network services for approved users as un-approved users try to connect to that network. DOS in Physical Layer causes Jamming (the channel utilized for communication between the nodes is possessed by unauthorized party), node altering (sensitive data is extricated by physical altering of the nodes). On network layer DOS attack causes spoofing (a pointless message is sent by a malignant node which is then replayed by the attacker to produce a high traffic) [3].

- *Wormhole:* This DoS attack causes revamp of bits of data from its actual position in the network. An attacker records bits at one position in the network, channels them as needs be to another position, and then retransmits them there into the network [4].

- *Man-in-Middle:* In this attack a mediator user gets the key of one of the communicating party and begins trading data as if it is the valid the original sender. The attacker can trick the recipient into supposing they are yet getting a correct message. RFID technology faces this sort of attack the most.

- *Eavesdropping:* This attack is on the privacy as the intruder gets hold of the information being shared amongst sender and recipient. The other devices can always monitor information of the compromised device and can likewise transmit false messages to assemble personal information of that device [5].

- *Alteration:* data handled by IoT devices can be tampered or changed by attackers causing threats to the integrity necessities of IoT framework. Attackers do this to delude the communication protocol.

- *Fabrication:* Here the attacker causes unapproved addition, alteration of information into the IoT system. This causes threat to the authentication of the system as the sender has no idea that the system is endangered [6].

3. IoT Security Challenges

In section 2 the attacks on IoT network is discussed, so security is required to keep all connected devices secure. The IoT security is classified in 3 ways. These are:

• *Security and Data Protection:* Since IoT devices are wireless and share sensitive data on open networks they become vulnerable to pernicious attacks and data theft. It requires advance technology to guarantee system security [7]. Cryptographic algorithms are a good method to secure information in the IoT. Yet many IoT devices are not sufficiently powerful to support such robust procedures. Accordingly, to empower them on the IoT, algorithms need to be less power consuming, but should not compromise on their efficiency [8].

• *Authentication and Identity management:* It is an essential constituent of any security model. Each object in the IoT network should have the ability to distinguish other objects and authenticate them. Individual identifiers can be utilized to create personal identities of these objects. It guarantees the identity of smart objects before communicating between them. A mechanism that empowers devices to mutually authenticate before each interaction is extremely fundamental for the success of IoTs [9].

• *Privacy:* As objects are becoming traceable through IoT, threats related to privacy have expanded manifold. Securing information is important so it is not abused by any third person. In spite of this, issues related to data ownership ought to be addressed. In order to make the user feel comfortable in being part of the IoT system, measures must be taken. The ownership of the data gathered from various smart objects must be distinctly settled. The owner must be ensured that the information will not be utilized without their approval, particularly when it will be shared over the internet [10]. Privacy of data can be guaranteed through Privacy Policies. Smart devices can be supplied with these policies. Therefore, when the smart objects contact with each other, they can go through their relating privacy policies for compatibility before imparting any data [11].

4. Previous Research

A few types of existing schemes that are relevant encryption technique for IoT and utilized for protecting information transmission in IoT are discussed here.

M.A. Simplicio Jr. et al. in [12] *"Lightweight and escrow-less authenticated key agreement for the internet of things"* evaluated lightweight and escrow-free schemes, assessing their security and performance regarding processing time and power consumption in the TelosB platform. In addition to demonstrating that some very proficient schemes are actually imperfect, they showed that the blend of SMQV (strengthened-Menezes-Qu-Vanstone) with implied certificates results in a secure and lightweight AKA scheme.

A. Mathur et al. in [13] *"A secure end-to-end IoT solution"* introduced IoT system that handles the issue of security from different angles. First, confidentiality and information authentication are included utilizing the AES-GCM 256-bit cipher, which performs better than other schemes. Second, key management schemes are comprised with frequent key updates, command-based key updates and key-generation features. These schemes are upheld by ECDH, HMACand HKDF standards that ex-

ceed other schemes. Third, the PRNG from Contiki's 'C' library is dissected using the NIST's statistical test suite. This provided approaches for seeding the PRNG to enhance its randomness, accordingly, providing more knowledge into the significance of random number generators in key-management. To conclude, the system proposed in this paper furnishes a high level of security with cloud connectivity for IoT enabled devices. Moreover, a working implementation on different technologies i.e. openmote, Intel Edison, Cloud and PC was exhibited.

J. Jang et al. in [14] *"An effective handling of secure data stream in IoT"* proposed a technique to enhance the usability of encrypted data streams in the IoT environment. They implemented IoT devices that created data streams utilizing Raspberry Pi, a desktop computer, and collectors that collect data streams. The results of experiments utilizing temperature sensor information showed that the communication time for data stream transmission decreased by 56.1–75.5%. Moreover, the power consumption of IoT devices for data transmission decreased by 54.8–75.3%. To proceed compression handling by the IoT device, the maximum memory usage and CPU usage increased by 0.3% and 10.1%, separately. As a result of this research, it is expected that the transmission time to collectors, in addition to the energy consumption of IoT devices, can be reduced while securing data streams produced by IoT devices.

A. Salman et al. in [15] *"A Light-Weight Hardware/Software Co-Design for Pairing-Based Cryptography with Low Power and Energy Consumption"* introduced a quick and power efficient hardware/ software co-design implementation of pairing appropriate for resource-constrained devices. They utilized Barreto-Naehrig (BN) BN-158 and BN-254 curves, represented in 160-bit and 256-bit field sizes (respectively), to excute pairing protocols. Their solution comprised countermeasures against Simple Power Analysis (SPA) and first order Differential Power Analysis (DPA) attacks. They compared their hardware/software co-design against a pure software implementation regarding area (LUTs and slices), latency, and throughput-to-area (TP/A) ratio. Furthermore, they measured power and compute energy per- bit of the hardware components on a Spartan-3E FPGA. The results demonstrated enhancements of more than 200% regarding latency for some functions when compared to the software implementation and indicated low power and energy consumption.

T. Claeys et al. in [16] *"Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment"* introduced a new authorization and authentication framework for the IoT that integrates the security model of OAuth 1.0a with the lightweight building blocks of ACE. By designing self-securing tokens the security of the framework no longer relies upon the security of the network stack. They utilized fundamental PKI functionalities to bootstrap a chain-of-trust between the devices which facilitates future token exchanges. At last, they proposed an alternative key establishment scheme for use cases where devices cannot directly communicate. They examined their proposal by implementing the critical aspects on a STM32L4 microcontroller. The results show that their framework ensures a firm level of security for IoT devices with fundamental asymmetric cryptography capacities.

M. Almulhim et al. in [17] *"Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications"* introduced a secure group-based lightweight authentication scheme for IoT based E-health applications, the suggested model will prolong mutual authentication and energy efficient, and computation for healthcare IoT based applications. Which will use elliptic curve cryptography (ECC) principles that prolong mentioned featured of proposed model.

C. G. Thorat et al. in [18] *"Implementation of New Hybrid Lightweight Block Cipher"* proposed a new compact hybrid lightweight encryption strategy. This strategy utilizes fastest bit permutation

instruction PERMS with PRESENT S-box layer for the non-linearity. An arbitrary n - bit permutation is excuted utilizing PERMS instruction in a less than the log (n) number of instructions. This new hybrid system is tested for software performance on ARM processor and for hardware performance Cadens tool is utilized. Introduced technique has resulted in a most compact implementation regarding CPU cycles. Additionally, PERMS properties brings a very good avalanche effect, and compact excution in software.

Y. Yang et al. in [19] *"Privacy-preserving fusion of IoT and big data for e-health"* proposed a privacy-preserving e-health system, which is a combination of Internet-of-things (IoT), big data and cloud storage. The system architecture and security model are defined for the suggested system. A non-interactive and authenticated key distribution procedure is designed for the medical IoT network. A batch authenticated verification algorithm is proposed to verify the source of encrypted IoT messages. Patients' EHRs are encrypted utilizing the ABE methodology to achieve access control. They also constructed a new keyword match based access policy updating mechanism to achieve fine grained policy updating control. They compared this system with other schemes and experiments to evaluate their performances. The testing results showed that this system outperformes the others and is applicable in the e-health environment.

L. Li et al. in [20] *"SFN: A new lightweight block cipher"* utilized involution related properties of the nonlinear and linear components to alter SP network structure. The modified one empowers the encryption and decryption program or circuit to work as the Feistel network structure. Furthermore, they have excuted a MixRows in SP network structure. Then they instantiate these three new ideas into the lightweight block cipher called SFN. They have performed the security assessment and the hardware and software experiments to it. The result demonstrates that compared to other lightweight block ciphers, SFN has more advantages in terms of being invulnerable to attacks. Additionally, SFN is not just compact in hardware environment but also proficient in software platforms and can be applied to constrained environments.

L. Zhou et al. in [21] *"Towards practical white-box lightweight block cipher implementations for IoTs"* investigated the possibility of lightweight block ciphers whitebox implementations for IoTs. They excuted two lightweight block ciphers, KLEIN and LBlock, as the examples for SPN and Feistel constructions. The implementation costs and the processing speeds are compared with Chow et al.'s AES whitebox implementations (which has the smallest LUT size in published designs). The comparison demonstrates that the implementation costs are strongly associated with the rounds, data path and structures of the ciphers. Despite the fact that they have examined three lightweight block ciphers with different structures, however the addition-rotation-xor (ARX) structure is also broadly utilized in lightweight block ciphers.

5. Conclusion

With the approach of smart homes, smart cities, and smart everything, the Internet of Things (IoT) has risen as a region of incredible impact, potential, and development. Nonetheless, the majority of these IoT devices are easy to hack and expose. Commonly, these IoT devices are limited in process, storage, and network capacity, and therefore they are more vulnerable to attacks than other endpoint devices such as cell phones, tablets, or PCs. In this paper we discussed about security and privacy issues and reviewed recent lightweight solutions that can be taken to solve them.

References

[1] Ashton, Kevin. "That 'internet of things' thing." *RFiD Journal* 22, no. 7 (2009): pp. 97-114

[2] R. Khan et al., "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges," in *10th International Conference on Frontiers of Information Technology,* Dec. 2012, pp. 257-260.

[3] P. Shah et al., "Applications and Challenges Faced by Internet of Things - A Survey," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering Future Intelligent Vehicular Technologies,* Springer, 2017, pp.182-188.

[4] Y.C. Hu, A. Perrig and D. Johnson, "Wormhole attacks in wireless networks," in *IEEE Journal on Selected Areas in Communications*, 2006, vol. 24(2), pp. 370-380.

[5] Q. Xaio, T. Gibbons and H. Lebru, "RFID Technology, Security Vulnerabilities, and Countermeasures," in *Supply Chain the Way to Flat Organization,* Intech, 2009, pp. 357-382.

[6] M. Nawir et al., "Internet of Things (IoT): Taxonomy of security attacks," in *3rd International Conference on Electronic Design,* Phuket, 2016, pp. 321- 326.

[7] A. Whitmore et al., "The Internet of Things—A survey of topics and trends," in *Information Systems Frontiers*, Springer, April 2015, vol. 12(2), pp. 261-274.

[8] D. Bandyopadhyay and J. Sen, "Internet of Things: applications and challenges in technology and standardization," in *Wireless Personal Communications*, Springer, 2011, vol. 58(1), pp. 49–69.

[9] P. Mahalle et al., "Identity Management Framework towards Internet of Things (IoT): Roadmap and Key Challenges," in *Recent trends in network security and applications, communications in computer and information science*, Springer, 2010, vol. 89, pp. 430–439.

[10] R. Roman et al., "Securing the Internet of Things," in IEEE Computers, 2011, vol. 44(9), pp. 51–58.

[11] T. Borgohain et al., "Survey of Security and Privacy Issues of Internet of Things," in *International Journal of Advanced Network Applications,* 2015, vol. 6(4), pp. 2372-2378.

[12] Marcos A. Simplicio Jr., Marcos V.M. Silva, Renan C.A. Alves ∗, Tiago K.C. Shibata " Lightweight and escrow-less authenticated key agreement for the internet of things" Computer Communications Volume 98, 15 January 2017, pp. 43-51.

[13] solutionAvijit Mathur, Thomas Newea, Walid Elgenaidi, Muzaffar Raoa, Gerard Dooly,Daniel Toal "A secure end-to-end IoT solution" Sensors and Actuators A: Physical Volume 263, 15 August 2017, pp. 291-299.

[14] Jaejin Jang, Im.Y Jung, Jong Hyuk Park "An effective handling of secure data stream in IoT" Applied Soft Computing Volume 68, July 2018, pp. 811-820.

[15] Ahmad Salman, William Diehl, Jens-Peter Kaps "A Light-Weight Hardware/Software Co-Design for Pairing-Based Cryptography with Low Power and Energy Consumption" 11-13 December 2017 International Conference on Field Programmable Technology (ICFPT), IEEE.

[16] Timothy Claeys, Franck Rousseau, Bernard Tourancheau. "Securing Complex IoT Platforms with Token Based Access Control and Authenticated Key Establishment". International Workshop on Secure Internet of Things (SIOT), September 2017, Oslo, Norway. 2017.

[17] Maria Almulhim, Noor Zaman "Proposing Secure and Lightweight Authentication Scheme for IoT Based E-Health Applications**"** International Conference on Advanced Communications Technology(ICACT) February 11 ~ 14, 2018.

[18] Thorat, C.G., Inamdar, V.S., "Implementation of New Hybrid Lightweight Block Cipher", Applied Computing and Informatics (2018).

[19] Yang Yang, Xianghan Zheng, Wenzhong Guo, Ximeng Liu, Victor Chang "Privacy-preserving fusion of IoT and big data for e-health" Future Generation Computer Systems 86 (2018) pp. 1437–1455.

[20] Lang Li, Botao Liu, Yimeng Zhou, Yi Zou, "SFN: A new lightweight block cipher" Microprocessors and Microsystems 60 (2018) pp. 138–150.

[21] Lu Zhou, Chunhua Su, Yamin Wen, Weijie Li, Zheng Gong "Towards practical white-box lightweight block cipher implementations for IoTs" Future Generation Computer Systems 86 (2018) pp. 507–514.