Open Access
2021, Vol. 18 No.2 (Suppl. June)
Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

DOI: http://dx.doi.org/10.21123/bsj.2021.18.2(Suppl.).0989

A Scoping Study on Lightweight Cryptography Reviews in IoT

Ikenna Rene Chiadighikaobi [1*] *Norliza Katuk* [2]

[1] MailZip Tech Services LTD, Nigeria.
[1,2] Universiti Utara Malaysia, Malaysia.
[*]Corresponding author: chiadighikaobiikenna@yahoo.com, k.norliza@uum.edu.my
[*]ORCID ID: https://orcid.org/0000-0002-4770-6938 , https://orcid.org/0000-0001-8805-2574

Received 28/3/2021, Accepted 14/4/2021, Published 20/6/2021

Abstract:

The efforts in designing and developing lightweight cryptography (LWC) started a decade ago. Many scholarly studies in literature report the enhancement of conventional cryptographic algorithms and the development of new algorithms. This significant number of studies resulted in the rise of many review studies on LWC in IoT. Due to the vast number of review studies on LWC in IoT, it is not known what the studies cover and how extensive the review studies are. Therefore, this article aimed to bridge the gap in the review studies by conducting a systematic scoping study. It analyzed the existing review articles on LWC in IoT to discover the extensiveness of the reviews and the topics covered. The results of the study suggested that many review studies are classified as overview-types of review focusing on generic LWC. Further, the topics of the reviews mainly focused on symmetric block cryptography, while limited reviews were found on asymmetric-key and hash in LWC. The outcomes of this study revealed that the reviews in LWC in IoT are still in their premature stage and researchers are encouraged to explore by conducting review studies in the less-attended areas. An extensive review of studies that cover these two topics is deemed necessary to establish a balance of scholarly works in LWC for IoT and encourage more empirical research in the area.

Key words: Encryption, Internet of Thing, Lightweight cryptography, Review, Sensors, Scoping study.

Introduction:

The fast development in information and communication technology has witnessed the emergence of the Internet of Things (IoT), a technology in which electronic devices and electrical appliances are interconnected and are able to transfer data (1, 2). IoT is expected to facilitate and automate information exchange to a broader context of data communication (3, 4) which consequently improves the quality of life (5-7) and business processes (8). IoT applications cover smart homes (9), smart cities (10), smart vehicles (11), healthcare (12), smart grids (13), and smart farming (14), to mention a few. They mainly use sensors and wearable devices that are capable of communicating with each other and other devices in a network. Sensors and wearable devices are resource-constraint in which they are powered up by batteries and have limited processing and storage capabilities.

In terms of data communication, sensors and devices in IoT work in a way similar to mobile and wireless communication. Therefore, they are also susceptible to security threats and attacks which require similar approaches for protection (15, 16). For example, data are required to be in an encrypted form when they are transferred in the network to protect their confidentiality and secrecy (17). It is commonly known that cryptographic systems are a suitable approach for protecting data confidentiality, secrecy and authenticity. However, conventional cryptographic systems are complex and use high computational power, making them not suitable for resource-constraint devices within the IoT environment (18). Due to the limitations in the IoT resource-constraint devices, there is a need for lightweight cryptography (LWC) to address the issue (19). Generally, cryptography is a study of data encoding and decoding using logical and mathematical principles to protect the secrecy of information (20, 21). The encoding and decoding processes are also called encryption and decryption respectively. In an IoT environment, the LCW is a crucial component that protects the data exchanged between interconnected devices from spoofing and modification attacks.

In supporting the need for LWC in IoT, the National Institute of Standards and Technology (NIST) has started developing a standard for LWC algorithms to be used within resource-constrained devices. The call for algorithms was published, and currently, the process for developing a standard for LWC is taking place. Apart from that, many scholarly studies were also conducted a decade ago by researchers in the area to design LCW algorithms suitable for an IoT environment. The significant number of scholarly works increased the review and survey studies reported in the academic databases. These review studies shared a common aim in providing a basic understanding of LWC in IoT and its state-of-the-art. Academic papers reporting on LWC in IoT are beneficial for researchers to acquire information about the domain systematically more quickly than performing research from scratch. The increase in the number of review studies also indicates that the domain is constantly being developed with many new studies emerging, and more improvements being added to the literature.

Due to the vast number of review studies on LWC in IoT being available in academic databases, it is not clear what the studies cover and how extensive the review studies are. Therefore, this study aims to bridge the gap in the review studies by conducting a scoping study to answer the two questions stated above. The outcome of this scoping study could suggest the areas of studies on LWC in IoT that have received much and also less attention. Consequently, it may encourage researchers to explore the potential of conducting review studies in the less-researched areas. Hence, the next section of this article describes the methodology for conducting the scoping study, and the results are described in the following section. Finally, the last section concludes the study.

Methodology:

The main objective of this study is to provide an in-depth coverage of available review studies on LCW within the IoT environment. A scoping study following the method proposed by Arksey and O'malley; and Pham et al. was conducted to identify the review studies related to LWC (22, 23). The method is presented in Figure 1. It comprised five stages: identifying the research questions (RQ), identifying relevant studies, selecting the relevant studies, sorting and documenting the data, and finally, summarising and reporting the results.

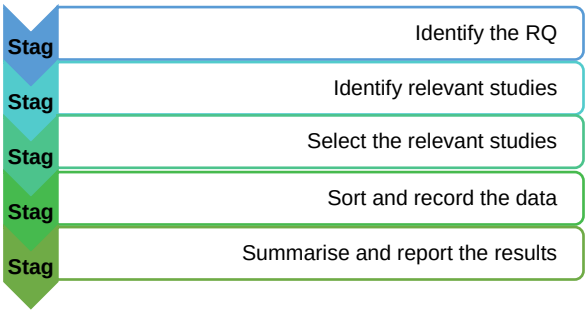

Figure 1. Method for Conducting the Scoping Study (Arksey & O'malley, 2005; Pham et al., 2014)

In Stage 1 (i.e. identify the RQ), two RQs were formulated to guide the scoping study. They aimed to investigate: "What are the topics covered by the review studies?" (RQ1) and "How extensive are the studies in covering the various aspects of LCW in IoT?" (RQ2). Based on the specified RQs, this study identified the keywords that would be used in the database search for Stage 2 of the method (i.e. identify the relevant studies). The keywords were "lightweight (cryptography OR encryption OR cipher) + IoT + (review OR survey)." An initial search from the database in the middle of February 2020 returned approximately 4080 documents. A filtering process was conducted on the search results by analyzing the abstracts of the documents. Three key elements were identified in the abstracts that were selected; (a) review articles, (b) reporting lightweight implementation of the cryptography techniques and (c) in the IoT domain. Only studies that reviewed lightweight cryptography techniques within the IoT environment were selected. At the end of the filtering process, irrelevant documents were discarded. Documents that reported empirical research in LWC within IoT were also discarded.

Finally, only forty-nine documents were selected for content analysis in the next stage of the scoping study method. In Stage 3 (i.e. select the relevant studies), a full-text document search was conducted to identify whether the review studies were relevant to LCW in IoT. Eight documents were not included in the scoping studies because (a) four documents were duplicated, (b) three documents had no full content published on the Internet, and (c) one document was not relevant as it reviewed hardware implementation. Therefore, forty-one review studies were selected for further analysis, as listed in Table 1. In Stage 4 (i.e. sort and record the data), the full-text of the contents of the documents was analyzed and reported in the next section.

Table 1. Information of the Review Studies of LCW in IoT

Study	Year	Num. referenc	Type of review	Type of IoT environment	Type of document	Country of the first author	Types of cryptography
Kushwaha et al. (24)	2014	20	Literature review	Generic IoT	Journal article	India	Symmetric block cryptography
Kong et al. (25)	2015	200	Literature review	Generic IoT	Journal article	Malaysia	Symmetric cryptography
Mohd et al. (26)	2015	138	State-of-the-art review	Generic IoT	Journal article	Jordan	Symmetric block cryptography
Manifavas et al. (27)	2016	124	Critical review	Generic IoT	Journal article	United Arab Emirates	Symmetric stream cryptography
Hosseinzadeh and Hosseinzadeh (28)	2016	59	Critical review	Generic IoT	Journal article	Iran	Symmetric cryptography
Younis and Abdulkareem, (29)	2016	78	Literature review	RFID	Journal article	Iraq	Cryptography methods
Singh, Sharma, Moon, and Park (30)	2017	87	State-of-the-art review	Generic IoT	Journal article	South Korea	Cryptographic algorithms
Bhardwaj, Kumar, and Bansal (31)	2017	30	Overview	Generic IoT	Conference article	India	Cryptographic algorithms
Buchanan et al. (32)	2017	33	Overview	Generic IoT	Journal article	United Kingdom	Cryptography methods
Okello, Liu, Siddiqui, and Zhang (33)	2017	27	Overview	Generic IoT	Conference article	China	Generic cryptography
Philip (34)	2017	28	Overview	Generic IoT	Conference article	India	Symmetric cryptography
Biryukov and Perrin (35)	2017	180	State-of-the-art review	Generic IoT	Report	Luxembourg	Symmetric cryptography
Bansal and Verma (36)	2017	18	Overview	Generic IoT	Journal article	India	Genericcryptography
Orúe, Encinas, Fernández, and Montoya (37)	2017	25	Overview	RFID	Conference article	Spain	Pseudorandom number generators
Kaur and Sidhu (38)	2017	10	Critical review	Wireless sensor network	Journal article	India	Symmetric block cryptography
Lara-Nino et al. (39)	2018	110	Systematic review	Generic IoT	Journal article	Mexico	Elliptic curve cryptography
Surendran et al. (40)	2018	28	Overview	Generic IoT	Conference article	UAE	Symmetric block cryptography
Sadkhan and Salman (41)	2018	13	Overview	Generic IoT	Conference article	Iraq	Generic cryptography
Sehrawat & Gill (42)	2018	76	Literature review	Generic IoT	Journal article	India	Symmetric block cryptography
Hussain and Abdullah (43)	2018	26	Overview	Generic IoT	Conference article	Pakistan	Generic cryptography
Pawar and	2018	10	Overview	Generic IoT	Journal	India	Generic

Pattanshetti (44)					article		cryptography
Sallam and Beheshti (45)	2018	55	Literaturere view	Generic IoT	Conference article	USA	Generic cryptography
Mustafa, Ashraf, Mirza, and Jamil (46)	2018	22	Literature review	Generic IoT	Conference article	Pakistan	Generic cryptography
Chauhan, Borikar, Aote, and Katankar (47)	2018	11	Overview	Generic IoT	Journal article	India	Generic cryptography
Carracedo et al. (48)	2018	74	Literature review	Generic IoT	Conference article	UK	Generic cryptography
Hatzivasilis et al. (49)	2018	159	Systematic review	Generic IoT	Journal article	Greece	Symmetric block Cryptography
Bokhari and Hassan (50)	2018	24	Critical review	Generic IoT	Chapter in book	India	Generic cryptography
Dinu et al. (51)	2019	62	Critical review	Generic IoT	Journal article	Luxembourg	Symmetric block cryptography
Shah and Engineer (52)	2019	22	Systematic review	Generic IoT	Chapter in book	India	Generic cryptography
Gunathilake et al. (19)	2019	19	Overview	Generic IoT	Conference article	UK	Generic cryptography
Dutta, Ghosh, and Bayoumi (53)	2019	35	Systematic review	Generic IoT	Conference article	USA	Symmetric block cryptography
Beg, Al-Kharobi, and Al-Nasser (54)	2019	13	Critical review	Generic IoT	Conference article	Saudi Arabia	Symmetric block cryptography
Shahbodin, Azni, Ali, and Mohd (55)	2019	59	Literature review	RFID	Conference article	Malaysia	Symmetric block cryptography
Rana (56)	2019	20	Critical review	Generic IoT	Journal article	Bangladesh	Symmetric block cryptography
Singh, Singh, and Singh (57)	2019	35	Critical review	Generic IoT	Journal article	India	Symmetric block cryptography
Masoodi and Javid (58)	2019	43	Critical Review	Generic IoT	Chapter in Book	India	Cryptographic algorithms
Malik et al. (59)	2019	114	Systematic review	Generic IoT	Journal article	India	Public key cryptography
Kousalya and Kumar (60)	2019	14	Overview	Generic IoT	Conference article	India	Symmetric block cryptography
Syal (61)	2019	19	Overview	Smart home	Chapter n book	India	Generic cryptography
Patil, Banerjee, and Borkar (62)	2020	8	Overview	Baby monitoring camera	Chapter in book	India	Generic cryptography
Dhanda et al. (63)	2020	108	Literature review	Generic IoT	Journal article	India	Generic cryptography

Results:

This section summarises the analysis of the selected review studies on LCW in IoT. It is divided into three subsections covering the background of the selected review studies, the topics covered by the review studies (RQ1), and the

extensiveness of the studies in covering the various aspects of LCW in IoT (RQ2).

Background of the Selected Review Studies

Forty-one documents were found reporting on review studies related to LWC in IoT. They included twenty articles published in journals, fifty articles published in conference proceedings, five chapters in a book, and one technical report. Figure 2 shows a pie chart representing the types of documents reporting the reviews of LCW in IoT.

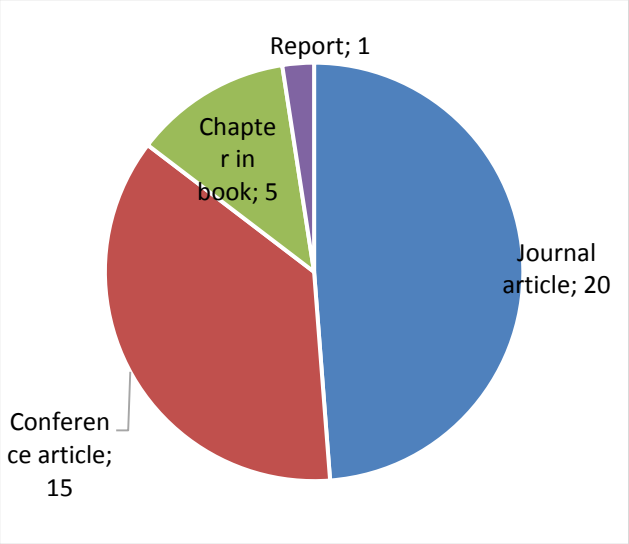

Figure 2. Types of Documentr Reportingr Reviews on LCW in IoT

One hundred and seventeen authors authored the forty-one review studies with 111 unique authors. Authors like Biryukov, Beheshti, Manifavas, Hatzivasilis, Fysarakis and Asif had their names on two documents (19, 27, 32, 35, 40, 45, 49). Further, this study analyzed the country of the first author of the selected review studies. The result of the analysis suggested that seventeen of the first authors were from India, three from the United Kingdom (UK) and two from Malaysia, the United States of America (USA), the United Arab Emirates (UAE), Luxembourg, Pakistan and Iraq, while countries like Bangladesh, China, Jordan, Greece, Spain, Iran, Saudi Arabia, Mexico, and South Korea had one first authoreach. Table 2 lists the first authors' countries.

Table 2. The Country of the First Author

Country	Frequency
India	17
UK	3
Malaysia	2
USA	2
UAE	2
Luxembourg	2
Pakistan	2
Iraq	2
Bangladesh	1
China	1
Jordan	1
Greece	1
Spain	1
Iran	1
Saudi Arabia	1
Mexico	1
South Korea	1
TOTAL	41

This study further analyzed the year in which the individual review studies were published. A review study on LCW in IoT was first published by Kushwaha, Singh, and Kumar (24). Then, two studies were published in 2015, followed by three studies in 2016. The number of review studies increased three times in 2017 as compared to the previous year. In 2018 and 2019, twelve review studies were published. Up to February 2020, two review studies have been published. It is expected that a similar number of review studies on LCW in IoT will be published in 2020. Figure 3 demonstrates a bar chart representing the number of studies published each year.

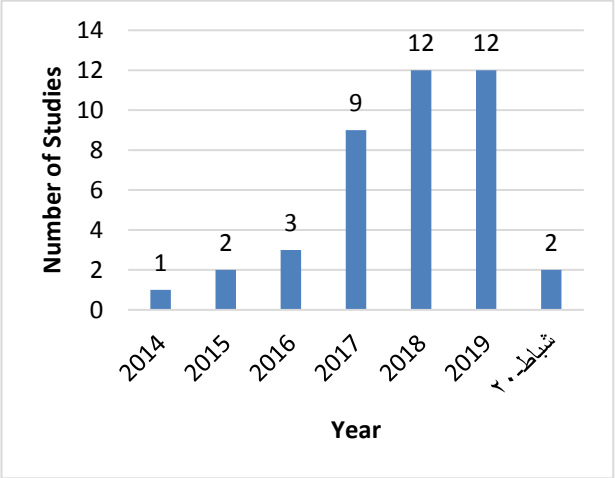

Figure 3. The Number of Documents Reporting Reviews on LCW in IoT According to Years

RQ1 - The Topics Covered bythe Review Studies

Katz and Lindell defined cryptography as a scientific study of techniques for securing digital

information, transactions and distributed computations (64). Stalling categorized modern cryptography into three categories: symmetric-key, asymmetric-key and hash function (65). The symmetric-key can be divided into block and stream cryptography. Symmetric key cryptography uses a shared secret key to encrypt and decrypt messages. The asymmetric-key is also known as public-key cryptography which uses a public key and a secret key for encryption and decryption respectively. A hash function returns the hash value of a message that can be used to check that the message is not altered. These three classifications of cryptography have been used in modern computer systems since the 1970s. Apart from these three generic classifications, cryptography is operable and is implemented through unique algorithms that efficiently run a computing environment. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) and Blowfish are examples of algorithms for symmetric block cryptography while RC4 is an example of symmetric stream cryptography. On the other hand, RSA, Diffie-Hellman, and elliptic curve cryptography are examples of asymmetric cryptography while Message Digest 4 (MD4) and Message Digest 5 (MD5) are examples of hash functions. In the context of LWC in IoT, cryptography classification remains the same while many new methods and algorithms have emerged to support the need for resource-constraint devices. The methods include bit-wise rotation, permutation, substitution and reducing the number of blocks or steps in the whole encryption and decryption processes.

This scoping study analyzed the types of cryptography that the review studies had covered. The results of the analysis suggest that 36% of the review studies focused on generic cryptography which covered symmetric, asymmetric and hash, as well as the associated algorithms. Next, 32% of the review studies surveyed symmetric block cryptography. These two areas are the most popular areas of review studies reported in the academic database and appear every year since the LWC in IoT started. There are also review studies that generally report their findings on general symmetric cryptography, cryptographic algorithms and cryptographic methods. A review study also surveyed symmetric stream cryptography, pseudorandom number generators, elliptic curve cryptography and public-key cryptography. Table 3 lists the number of review studies for the corresponding areas of LCW in IoT.

Table 3. Number of Studies Based on the Area of Cryptography Domain

Types of cryptography	Frequency
Generic cryptography	15
Symmetric block cryptography	13
Symmetric cryptography	4
Cryptographic algorithms	3
Cryptography methods	2
Symmetric stream cryptography	1
Pseudorandom number generators	1
Elliptic curve cryptography	1
Public key cryptography	1
TOTAL	41

This scoping study further analysed the information to see how the existing review studies cover the cryptography domain areas. A hierarchical diagram of LCW in Figure 4 represents the overall coverage of the exiting review studies. Many review studies were conducted on the generic LWC in IoT as well as the symmetric block cryptography. These two are the most popular areas of the review studies on LWC in IoT. On the other hand, the diagram shows that a limited number of review studies on LCW in IoT that were conducted on symmetric stream cryptography, asymmetric-key cryptography, and hash. The asymmetric-key cryptography i is commonly used in authentication schemes to exchange secret key encryption (66 - 68). Therefore, they might use other keywords that are not included when the academic database performed the search.

Baghdad Science Journal
P-ISSN: 2078-8665
E-ISSN: 2411-7986

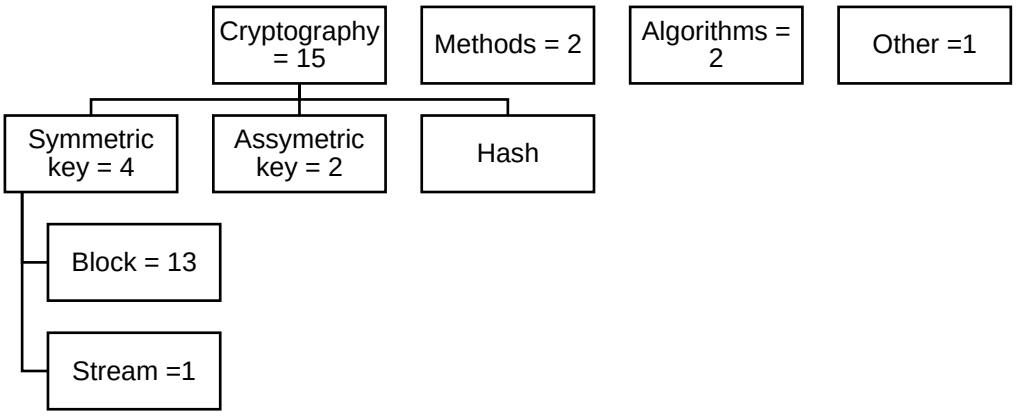

Figure 4. Number of Review Studies Based on the Cryptography Classification

The analysis conducted on the forty-one documents suggested that researchers in the area mainly focused on the generic LWC and symmetric block cryptography in their review studies. Unlike these two topics, other areas of cryptography had limited attention in terms of the review studies. This answers the RQ1 of this scoping study.

RQ2 - The Extensiveness of the Studies in Covering Various Aspects of LCW in IoT

This section describes the answer to the second RQ on: "How extensive are the studies in covering the various aspects of LCW in IoT?". In answering this RQ, this study analyzed the selected review studies on LWC in IoT and classified them into one of the fourteen types of review studies suggested by Grant and Booth (69). The fourteen types of review studies are listed in Table 4.

Table 4. Types of Review Studies (Grant & Booth, 2009)

Num.	Type of review	Description
1	Critical review	A review paper in which the authors performed extensive research in the literature and evaluated the quality of the study critically.
2	Literature review	A review paper in which the authors examined recent or current literature.
3	Mapping review/ systematic map	A review paper in which the authors classified existing literature to identify gaps in the literature.
4	Meta-analysis	A review paper in which the authors integrated and analyzed the results of quantitative studies statistically which demonstrated the combined effect of the results.
5	Mixed studies review/mixed methods review	A review paper in which the authors combined literature review with other review approaches, for example combining quantitative with qualitative research.
6	Overview	A review paper in which the authors summarised the literature by providing the characteristics of a topic.
7	Qualitative systematic review/ qualitative evidence synthesis	A review paper in which the authors compared the findings from qualitative studies and identified the themes or constructs underpinning the individual qualitative studies.
8	Rapid review	A review paper in which the authors appraised a known current issue using a systematic review.
9	Scoping review	A review paper in which the authors evaluated the potential size and scope of the available research literature to find the nature and extent of research evidence.
10	State-of-the-art review	A review paper in which the authors addressed more current matters in a topic to provide new perspectives on an issue or suggest an area for further research.
11	Systematic review	A review paper in which the authors searched, appraised, and synthesized research evidence systematically.
12	Systematic search and review	A review paper in which the authors integrated critical review with a comprehensive search process to generate a piece of comprehensive evidence.
13	Systematized review	A review paper in which the authors performed the process of doing a systematic review, however reporting the finding in a shorter and simpler version of the systematic review
14	Umbrella review	A review paper in which the authors compiled evidence from multiple reviews into one accessible and usable document.

In classifying the review studies, this study used the Search, Appraisal, Synthesis, and Analysis (SALSA) framework (69). The results of the classification revealed that fifteen studies were classified as overview studies, nine studies were literature reviews and critical reviews, five studies were systematic reviews and three studies were state-of-the-art review. The bar chart in Figure 5 shows the classification of the review studies.

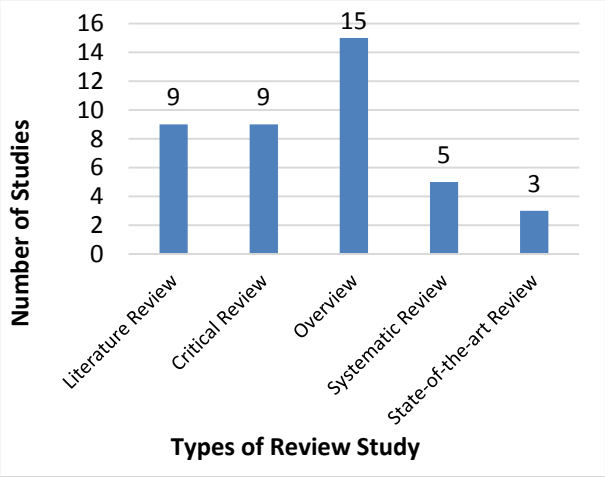

Figure 5. Number of Documents Reporting Reviews on LCW in IoT According to Types of Review Study

This study also calculated the number of references for each of the review study. A total of 2236 references were cited and referred to in the forty-one studies. However, this study did not count the unique number of references from this number. Further, this study listed eight review studies with the number of references exceeding a hundred as listed in Table 5. This scoping study believes that these review studies can be used as a starting point for researchers to understand LWC in IoT as they have a higher coverage of references and the types of review that they reported in the respective studies varied covering literature reviews (2 studies), state-of-the-art reviews (2 studies), systematic reviews (3 studies) and critical review (1 study). This study also collected the number of citations received by each paper in the Google Scholar (as of Mid-February 2020). All papers received substantial citations except for the study by Dhanda, Singh, and Jindal (2020), as the paper was newly published when this scoping study was conducted.

Table 5. List of Review Studies with More than One Hundred References

Study	Year	Num. of references	Num. of citations (*)	Type of review	Types of Ccryptography
Kong, Ang, and Seng (25)	2015	200	49	Literature review	Symmetric cryptography
Biryukov and Perrin (35)	2017	180	58	State-of-the-art review	Symmetric cryptography
Hatzivasilis et al. (49)	2018	159	42	Systematic review	Symmetric block cryptography
Mohd, Hayajneh, and Vasilakos (26)	2015	138	88	State-of-the-art review	Symmetric block cryptography
Manifavas et al. (49)	2016	124	37	Critical review	Symmetric stream Cryptography
Malik, Dutta, and Granjal (59)	2019	114	6	Systematic review	Publickey cryptography
Lara-Nino, Diaz-Perez, and Morales-Sandoval (39)	2018	110	8	Systematic review	Elliptic curve cryptography
Dhanda et al. (63)	2020	108	0	Literature review	Generic cryptography

* Google Scholar citations (as of Feb. 2020)

This scoping study also looked into the extensiveness of the review studies of LCW in IoT based on the types of review studies and the number of documents or references included in the reviews. Classification of the review studies using the SALSA framework demonstrated that 36% of the review studies provided overviews of the various aspects of LCW in IoT. About 20% provided a more comprehensive coverage of the reviews in which they provided literature reviews. The critical review also contributed 20% of the review studies. The rest covered the systematic review and the state-of-the-art review. The number of references or documents included in the selected review studies, covered various numbers, as low as eight to the highest of two hundred. The types of review studies had a relationship with the number of documents or articles listed in the reference section of the respective study. For example, the review study by Kong, Ang, and Seng (25) had 200 references for the literature review while Patil, Banerjee, and Borkar (62) had only eight references for their overview study. Hence, the outcome of this analysis answers RQ2.

The result of the scoping study suggests that many review studies focused on the areas of generic cryptography and symmetric block cryptography. Nevertheless, limited review studies were found on symmetric stream cryptography, asymmetric-key cryptography and hash for achieving LWC in IoT. Further, more than a quarter of the selected review studies reported on the overview of the cryptographic concept, which is beneficial in obtaining a basic understanding of the area. Literature review and critical review also contributed to the LCW literature, with approximately forty percent of the total number of review studies. However, the results of this scoping study reveal that a limited number of systematic reviews and the state-of-the-art reviews were conducted in the area of LCW in IoT. State-of-the-art reviews are a beneficial source of reference that can provide other researchers with information on recent fundamental advances related to LCW in IoT. It can be a starting point for further improvements that can lead to advancement in the area.

Conclusion:

The cryptography domain is considered monumental which can be applied in various domains including the emerging IoT environment. However, conventional cryptography is not working efficiently in IoT to lead to active developments in LCW. The increase in the number of review studies also indicates that the domain is constantly developing with many new studies emerging, and more improvements being added to the literature. The review studies on LCW in IoT are good sources of knowledge, especially to those who are new to the domain and to researchers who intend to obtain a general understanding of this domain. However, a significant number of review studies lead to essential questions, such as the topics that are covered by the studies and their level of extensiveness. Hence, a scoping study was conducted to seek answers to these questions. This scoping study revealed that more review studies are needed in the domain to cover specific areas of cryptography, especially on asymmetric-key cryptography and hash. Further, this study also believes that review studies should be conducted to cover specific instances of IoT technology rather than the generic ones. A few review studies covered the suitable cryptography approach for RFID, wireless sensor networks and smart homes. A similar review on other IoT technology instances could help understand the practicability of cryptography in particular instances. Review studies could also be conducted to analyze LWC for specific purposes in IoT such as authentication schemes.

Acknowledgements:

The authors thank the Ministry of Education Malaysia for funding this study under the Fundamental Research Grant Scheme (Ref: FRGS/1/2018/ICT03/UUM/02/1, UUM S/O Code: 14208), and the Research and Innovation Management Centre, Universiti Utara Malaysia for the administration of this study.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in Universiti Utara Malaysia.

References:

1. Rahman AFA, Daud M, Mohamad MZ. Securing sensor to cloud ecosystem using internet of things (iot) security framework. In the Proceedings of the International Conference on Internet of things and Cloud Computing. 2016. https://doi.org/10.1145/2896387.2906198
2. Ratasuk R, Vejlgaard B, Mangalvedhe N, Ghosh A. NB-IoT system for M2M communication. In the 2016 IEEE wireless communications and networking conference. 2016. https://doi.org/10.1109/WCNC.2016.7564708
3. Agrawal N. Internet of things – Iot a new envisage in the domain of automation. Indian Journal of Computer Science and Engineering. 2019;10(1),1-7. https://doi.org/10.21817/indjcse/2019/v10i1/191001004
4. Caron X, Bosua R, Maynard SB, Ahmad A. The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. Computer Law & Security Review. 2016;32(1),4-15. https://doi.org/10.1016/j.clsr.2015.12.001
5. Attié E, Meyer-Waarden L. The acceptance process of the Internet of Things: how to improve the acceptance of the IoT technology. In Smart Marketing with the Internet of Things. IGI Global. 2019;21-45. https://doi.org/10.4018/978-1-5225-5763-0.ch002
6. Elemam E, Bahaa-Eldin MA, Shaker HN, Sobh AM. A Secure MQTT Protocol, Telemedicine IoT Case Study. In 2019 14th International Conference on Computer Engineering and Systems. 2019; 99-105. https://doi: 10.1109/ICCES48960.2019.9068129.
7. Harum N, Abidin ZZ, Shah WM, Hassan A. Implementation of smart monitoring system with fall dectector for elderly using IoT technology.

International Journal of Computing. 2018;17(4), 243-249. https://doi.org/10.47839/ijc.17.4.1146
8. Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 2015;4,58. https://doi.org/10.1016/j.bushor.2015.03.008.
9. Steane TNE, Radcliffe P. IOT status communication for home automation. International Journal of Computing. 2019;18(3),240-248. https://doi.org/ 10.1109/ccaa. 2016.7813916
10. Arasteh H, et al. Iot-based smart cities: A survey. In IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC). 2016;1-6. https://doi:10.1109/EEEIC.2016.7555867.
11. Großwindhager B, Rupp A, Tappler M, Tranninger M, Weiser S, Aichernig B, Römer KU. Dependable Internet of Things for Networked Cars. International Journal of Computing. 2017;16(4),226-237.
12. Baker SB, Xiang W, Atkinson I. Internet of things for smart healthcare: Technologies, challenges, and opportunities. IEEE Access. 2017;5,26521-26544. https://doi.org/10.1109/ACCESS.2017.2775180
13. Dalipi F, Yayilgan SY. Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges. In 2016 4th International Conference on Future Internet of Things and Cloud Workshops. 2016; 63-68. IEEE. https://doi: 10.1109/W-FiCloud.2016.28.
14. Jayaraman P, Yavari A, Georgakopoulos D, Morshed A, Zaslavsky A. Internet of Things Platform for Smart Farming: Experiences and Lessons Learnt. Sensors. 2016. https://doi.org/10.3390/s16111884.
15. Feroz Khan AB, Anandharaj G. AHKM: An improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in IoT. Egyptian Informatics Journal, In Press. 2020. https://doi.org/10.1016/j.eij.2020.05.004
16. Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: Current status challenges and prospective measures. In 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST). 2015;336-341. https://doi.org/10.1109/ICITST.2015.7412116.
17. Bull P, Austin R, Popov E, Sharma M, Watson R. Flow based security for IoT devices using an SDN gateway. In the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). 2016.https://doi.org/10.1109/FiCloud.2016.30
18. Tsai KL, Huang YL, Leu FY, You I, Huang YL, Tsai CH. AES-128 based secure low power communication for LoRaWAN IoT environments. IEEE Access. 2018;6,45325-45334. https://doi.org/10.1109/ACCESS.2018.2852563
19. Gunathilake NA, Buchanan WJ, Asif R. Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications. Paper presented at the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). 2019. https://doi.org/10.1109/WF-IoT.2019.8767250.
20. Mohamed NN, Mohd-Yussoff Y, Saleh MA, Hashim H. Hybrid cryptographic approach for internet of things applications: A literature review. Journal of Information and Communication Technology. 2020;19(3),279-319. https://doi.org/10.32890/jict2020.19.3.1
21. Mohan J, Rajesh R. Secure visual cryptography scheme with meaningful shares. Indian Journal of Computer Science and Engineering. 2020;11(2),146-160. https://doi.org/10.21817/indjcse /2020/v11i2/201102001
22. Arksey H, O'Malley L. Scoping studies: towards a methodological framework. International journal of social research methodology. 2005;8(1),19-32. https://doi.org/10.1080/1364557032000119616
23. Pham MT, Rajić A, Greig JD, Sargeant JM, Papadopoulos A, McEwen, SA. A scoping review of scoping reviews: advancing the approach and enhancing the consistency. Research synthesis methods. 2014;5(4),371-385. https://doi.org/10.1002/jrsm.1123
24. Kushwaha PK, Singh M, Kumar P. A survey on lightweight block ciphers. International Journal of Computer Applications. 2014;96(17). https://doi.org/10.5120/16883-6923
25. Kong HJ, Ang L, Seng PK. A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments. Journal of Network and Computer Applications. 2015;49,15-50. https://doi.org/10.1016/j.jnca.2014.09.006.
26. Mohd BJ, Hayajneh T, Vasilakos AV. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications. 2015;58,73-93. https://doi.org/10.1016/j.jnca.2015.09.001
27. Manifavas C, Hatzivasilis G, Fysarakis K, Papaefstathiou Y. A survey of lightweight stream ciphers for embedded systems. Security And Communication Networks. 2015;9,1226-1246. https://doi.org/.1002/sec.1399.
28. Hosseinzadeh J, Hosseinzadeh M. A comprehensive survey on evaluation of lightweight symmetric ciphers: hardware and software implementation. Advances in Computer Science: an International Journal. 2016;5(4),31-41.
29. Younis M, Abdulkareem M. A Survey oF RFID Authentication Protocols. Information Security. 2016;6, 1-12. https://doi.org/10.1109/ICCIT.2008.314
30. Singh S, Sharma PK, Moon S. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. J Ambient Intell Human Comput. (2017). https://doi.org/10.1007/s12652-017-0494-4
31. Bhardwaj I, Kumar A, Bansal M. A review on lightweight cryptography algorithms for data security and authentication in IoTs. In 4th International Conference on Signal Processing Computing and Control (ISPCC). 2017;504-509. https://doi.org/10.1109/ISPCC.2017.8269731.
32. Buchanan WJ, Li, S, Asif R. Lightweight cryptography methods. Journal of Cyber Security

Technology. 2017;1(3-4),187-201. https://doi.org/10.1080/23742917.2017.1384917
33. Okello WJ, Liu Q, Siddiqui FA, & Zhang C. A survey of the current state of lightweight cryptography for the Internet of things. In the 2017 International Conference on Computer, Information and Telecommunication Systems (CITS). 2017. https://doi.org/10.1109/CITS.2017. 8035317
34. Philip MA. A survey on lightweight ciphers for IoT devices. In 2017 International Conference on Technological Advancements in Power and Energy (TAP Energy). 2017;1-4. https://doi.org/10.1109/TAPENERGY.2017.8397271
35. Biryukov A, Perrin LP. State of the art in lightweight symmetric cryptography. IACR Cryptology ePrint Archive. 2017. https://eprint.iacr.org/2017/511.pdf
36. Bansal S, Verma N. Dynamic Cipher for Enhanced Cryptography and Communication for Internet of Things: A Review. International Journal of Engineering Research & Technology (IJERT). 2017;5(11),1-4. https:// doi: 10.1007/978-3-319-69155-8_6
37. Orúe AB, Encinas LH, Fernández V, Montoya F. A review of cryptographically secure PRNGs in constrained devices for the IoT. In the International Joint Conference SOCO'17-CISIS'17-ICEUTE'17 León, Spain. 2017. https://doi. org/10.4018/978-1-5225-5742-5.ch003
38. Kaur J, Sidhu BK. A Survey on Lightweight Block Ciphers for Wireless Sensor Network. International Journal of Advanced Research in Computer Science. 2017;8(5). https://doi.or g/10.26483/ijarcs.v8i5.3907
39. Lara-Nino CA, Diaz-Perez A, Morales-Sandoval M. Elliptic curve lightweight cryptography: A survey. IEEE Access, 20186, 72514-72550. https://doi.org/10.1109/ACCESS.2018.2881444
40. Surendran S, Nassef A, Beheshti BD. A survey of cryptographic algorithms for IoT devices. In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). 2018;1-8. https://doi.org/10.1109/LISAT.2018.8378034
41. Sadkhan SB, Salman AO. A survey on lightweight-cryptography status and future challenges. In the 2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA). 2018. https://doi.org/10.1109/ICASEA.2018.8370965
42. Sehrawat D, Gill NS. Lightweight block ciphers for IoT based applications: A review. International Journal of Applied Engineering Research. 2018;13(5),2258-2270. https://doi.org /10.1049/pbse009e_ch7
43. Hussain R, Abdullah I. Review of different encryption and decryption techniques used for security and privacy of IoT in different applications. In the 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE). 2018. https://doi.org/ 10.1109/SEGE.2018.8499430
44. Pawar SV, Pattanshetti T. Lightweight-cryptography: a survey. International Research Journal of Engineering and Technology (IRJET). 2018;5(05). https://www.irjet.net/archives/V5/i5/IRJET-V5I5752.pdf
45. Sallam S, Beheshti BD. A survey on lightweight cryptographic algorithms. In the TENCON 2018-2018 IEEE Region 10 Conference. 2018. https://doi.org/10.1109/ TENCON.2018.8650352
46. Mustafa G, Ashraf R, Mirza MA, Jamil A. A review of data security and cryptographic techniques in IoT based devices. In the Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. 2018. https://doi.org/10.1145 /3231053.3231100
47. Chauhan B, Borikar S, Aote S, Katankar V. A Survey on Image Cryptography Using Lightweight Encryption Algorithm. International Journal of Scientific Research in Science, Engineering and Technology. 2018;4(4),344-347. http://ijsrset.com/paper/3976.pdf
48. Carracedo J, Milliken M, Chouhan P, Scotney B, Lin Z, Sajjad A, Shackleton M. Cryptography for Security in IoT. In 2018 Fifth International Conference on Internet of Things: Systems, management and Security. IEEE. 2018;23-30. https://doi.org /10.1109/IoTSMS.2018.8554634
49. Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I., & Manifavas, C. (). A review of lightweight block ciphers. Journal of Cryptographic Engineering. 2018;8(2),141-184. https://doi.or g/10.1007/s13389-017-0160-y
50. Bokhari M, Hassan S. A comparative study on lightweight cryptography. In Cyber Security. Springer, Singapore. 2018;69-79. https://doi.org/10.1109/ICCES48766.2020.9137984
51. Dinu D, Le Corre Y, Khovratovich D, Perrin L, Großschädl J, Biryukov A. Triathlon of lightweight block ciphers for the internet of things. Journal of Cryptographic Engineering. 2019;9(3),283-302. https://doi.org/10.1007/s13389-018-0193-x
52. Shah A, Engineer M. A survey of lightweight cryptographic algorithms for iot-based applications. Smart Innovations in Communication and Computational Sciences. Springer. 2019;283-293. https://doi.org/10.1007/978-981-13-2414-7_27
53. Dutta IK, Ghosh B, Bayoumi M. Lightweight Cryptography for Internet of Insecure Things: A Survey. In the 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC). 2019. https://doi.org/10.1109/CCWC.2019.8666557
54. Beg A, Al-Kharobi T, Al-Nasser A. Performance Evaluation and Review of Lightweight Cryptography in an Internet-of-Things Environment. In 2nd International Conference on Computer Applications & Information Security (ICCAIS). 2019;1-6, https://doi: 10.1109/CAIS.2019.8769509.
55. Shahbodin F, Azni HA, Tasnuva A, Mohd KCNKC. Lightweight cryptography techniques for MHealth cybersecurity. In Proc. 2019 Asia Pacific Information Technology Conference. 2019;44-50. https://doi.org/10.1145/3314527.3314536
56. Rana S. A Survey Paper of Lightweight Block Ciphers Based on Their Different Design Architectures and Performance Metrics. International

Journal of Computer Engineering and Information Technology. 2019;11(6),119-129.
57. Singh A, Singh S, Singh G. Lightweight Ciphers for Internet of things: A Survey. International Journal of Innovative Technology and Exploring Engineering. 2019;8(7),1973-1981. https://1library.net/document/eqo075kq-lightweight-ciphers-for-internet-of-things-a-survey.html
58. Masoodi IS, Javid, B. A Review of Cryptographic Algorithms for the Internet of Things. In Cryptographic Security Solutions for the Internet of Things. IGI Global. 2019;67-93. DOI: 10.4018/978-1-5225-5742-5.ch003
59. Malik M, Dutta M, Granjal J. A survey of Key bootstrapping protocols based on Public Key Cryptography in the Internet of Things. IEEE Access. 2019;7,27443-27464. https://doi.org/10.1109/ACCESS.2019.2900957.
60. Kousalya R, Kumar G. A Survey of Light-Weight Cryptographic Algorithm for Information Security and Hardware Efficiency In Resource Constrained Devices. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN). 2019;1-5. https://doi:10.1109/ViTECoN.2019.8899376
61. Syal R. A Comparative Analysis of Lightweight Cryptographic Protocols for Smart Home. Emerging Research in Computing, Information, Communication and Applications. Springer. 2019;663-660. https://doi.org/10.1007/978-981-13-5953-8_54
62. Patil A, Banerjee S, Borkar G. A Survey on Securing Smart Gadgets Using Lightweight Cryptography. In the Proceedings of International Conference on Wireless Communication. 2002. https://doi.org/10.1007/978-981-15-1002-1_51
63. Dhanda SS, Singh B, Jindal P. Lightweight Cryptography: A Solution to Secure IoT. Wireless Pers Commun. 2002;112,1947–1980. https://doi.org/10.1007/s11277-020-07134-3
64. Katz J, Lindell Y. Introduction to modern cryptography: Chapman and Hall/CRC. 2014. https://doi.org/10.3390/s16111884.
65. Stallings W. Network and internetwork security: principles and practice (Vol. 1): Prentice Hall Englewood Cliffs, NJ. 1995. https://dl.acm.org/doi/book/10.5555/193189
66. Ahmad JI, Din R, Ahmad M. Analysis Review on Public Key Cryptography Algorithms. International Journal of Electrical and Computer Engineering (IJECE). 2018;12(2),447-454. http://doi.org/10.11591/ijeecs.v12.i2.pp447-454
67. Ghazali TK, Zakaria NH. Security performance evaluation of biometric lightweight encryption for fingerprint template protection. International Journal of Advanced Computer Research. 2019;9,43. https://doi.org/10.19101/IJACR.PID49
68. Venugopal P, Viji K. Applying Empirical Thresholding Algorithm For A Keystroke Dynamics Based Authentication System. Journal Of Information And Communication Technology. 2019;18(4),383-413. doi:10.32890/jict2019.18.4.1
69. Grant MJ, Booth A. A typology of reviews: an analysis of 14 review types and associated methodologies. Health Information & Libraries Journal. 2009;26(2),91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

دراسة نطاق حول مراجعات التشفير خفيفة الوزن في إنترنت الأشياء

إيكينا رينيه تشياديغيكوبي [1] **نورليزا كاتوك [2]**

[1] MailZip Tech Services LTD، نايجيريا
[2] جامعة أوتارا ماليزيا ، ماليزيا

الخلاصة:

بدأت الجهود في تصميم وتطوير التشفير الخفيف (LWC) قبل عقد من الزمن. تشير العديد من الدراسات العلمية في الأدب إلى تحسين خوارزميات التشفير التقليدية وتطوير خوارزميات جديدة. أدى هذا العدد الكبير من الدراسات إلى ظهور العديد من دراسات المراجعة حول LWC في إنترنت الأشياء. نظرًا للعدد الكبير من دراسات المراجعة حول LWC في إنترنت الأشياء ، فمن غير المعروف ما تغطيه الدراسات ومدى شمول دراسات المراجعة. لذلك ، هدفت هذه المقالة إلى سد الفجوة في دراسات المراجعة من خلال إجراء دراسة نطاق منهجية. تم تحليل مقالات المراجعة الحالية حول LWC في إنترنت الأشياء لاكتشاف مدى اتساع المراجعات والمواضيع التي تمت تغطيتها. اقترحت نتائج الدراسة أن العديد من دراسات المراجعة تم تصنيفها على أنها نظرة عامة على أنواع المراجعة التي تركز على LWC العام. علاوة على ذلك ، ركزت موضوعات المراجعات بشكل أساسي على تشفير الكتلة المتماثلة ، بينما تم العثور على مراجعات محدودة على المفتاح غير المتماثل والتجزئة في .LWC كشفت نتائج هذه الدراسة أن المراجعات في LWC في إنترنت الأشياء لا تزال في مرحلتها المبكرة ويتم تشجيع الباحثين على الاستكشاف من خلال إجراء دراسات المراجعة في المناطق الأقل حضورًا. يُعتبر إجراء مراجعة شاملة للدراسات التي تغطي هذين الموضوعين ضروريًا لإنشاء توازن بين الأعمال العلمية في LWC من أجل إنترنت الأشياء وتشجيع المزيد من البحث التجريبي في المنطقة.

الكلمات المفتاحية: التشفير، إنترنت الأشياء، التشفير الخفيف، المراجعة، الحساسات، دراسة النطاق