Iraqi Journal for Computers and Informatics (IJCI)
Published by University of Information Technology and Communications (UOITC)

LT10 a Lightweight Proposed Encryption Algorithm for IOT

Alaa Q. Raheema[1]
[1] Building and Construction Engineering Department, University of Technology, Baghdad, Iraq
alaa.qassim1967@gmail.com

Abstract: ***In this paper, algorithm (LT10) which is originally consist of four kasumi elements is proposed as a lightweight encryption algorithm, the proposed algorithm take into account that the IOT devices have a limit computation abilities and the sensitivity of smart homes and IOT network information that need to be exchanged the key length is 128 bit and the block length is 128 bit.***

Keywords: TL10 algorithm, kasumi, IOT, internet of things.

1. INTRODUCTION

The Internet of Things (IoT) is the new paradigm which comprises the ordinary entities side to side with the ability of sensing for the connected devices and the communication of these devices with the use of Internet [1]. Since the internet became more and more available and the general costs reduced every day more sensors and device start connecting to it and used it ability to send data accurate , fast and easy [2]. These circumstances lead to the growth of the internet of thing (IoT), the main concept of this model is connecting almost every device to the internet with ability to take decision to make life easier for humans [3].

By adding advanced chips and sensors in the physical sense which encompass us, each transmitting with profitable information, the procedure of sharing such extensive measure of information starts by the gadgets themselves that should safely be communicating with the internet of things platforms what's more, apply examination to impart the most important information to the implementations. The IoT takes the traditional web, sensor systems and mobile system to a new level as everything will be associated and in connection with the web. An issue of worry which has to be kept in mind is guaranteeing the matters identified with authenticity, confidentiality and integrity which will develop by virtue of privacy and security [4].

2. IoT APPLICATIONS:

With the progression of time, an ever increasing number of devices get connected with the Internet, the PC, laptops, tablets, smart mobiles, and new smart televisions, computer game consoles even the fridges and aeration and cooling systems are able to convey via Internet. This pattern is expanding outwards and it is assessed that by 2020 there will be more than 50 B. items that are connected with the Internet [6]. This produces an estimation that for every individual in the world there will be nearly 6.6 items on the web (online).

The earth will be covered by a great many sensors that gather data from physical protests and will transfer that data to Internet.

It is proposed that use of IoT is still in the beginning time yet is starting to advance quickly [7], [8]. It is recommended in [10] that different ventures have a developing enthusiasm to the utilization of IoT. Different uses of internet of things in social insurance enterprises are examined in [11], [12] and the change openings in human services acquired by internet of things will be tremendous [13].

It was anticipated that the internet of things will take part in really taking shape the mining generation more secure [14] and the determining of catastrophe will be made conceivable. It is normal that the internet of things will change the car administrations and transport frameworks [15]. As more physical items will be furnished with sensors and RFID labels transport organizations will have the capacity of

tracking and screening the protest development from inception to goal [16], along these lines internet of things indicates high perspective conduct in the coordination's business too.

3. IoT SECURITY:

For the technology of internet of things adoption it is important to confidence the certainty amongst the clients about its security and protection of privacy that it won't make any genuine risk their information confidentiality, data integrity and authority. Naturally the internet of things is vulnerable against different sorts of security dangers, if fundamental safety efforts aren't taken there will be a risk of data leak or may demonstrate a harm to economy [17], [18]. This type of dangers might be taken under consideration as a real block in the internet of things [19], [20]. IoT is to a great degree prone to attack [21], [22], due to the fact that there's a reasonable possibility of physical assault on its parts as they stay without supervision for too long. Furthermore, because of the wireless connection media, the listening stealthily is to a great degree basic. In conclusion the constituents of IoT bear low competency as far as vitality with which they are worked and furthermore regarding computational capacity. The execution of traditional computationally costly security calculations will bring about the obstruction on the execution of the vitality compelled gadgets. It is anticipated that considerable measure of information is required to be produced whereas the internet of things is utilized for checking implementations and it's essential to safeguard information unification [23]. Absolutely, information trustworthiness and confirmation are the concerning issues.

From the viewpoint of the abnormal state, the internet of things includes 3 parts which are, Equipment, Middle-ware and Introduction [1]. Equipment is made up of sensors and actuators, the Middle-ware provides stockpiling and processing apparatuses and finally, the introduction provides the elucidation devices open on different steps. It is not plausible the processing of information that has been collected from a great number of sensors, which set mindful Middle-ware arrangements are suggested for enabling a sensor for choosing the most critical data to be handled [24]. Characteristically speaking, the design of the internet of things offers no suitable edge to achieve the fundamental actions connected to the process of confirming and data honesty. The gadgets in the internet of things, for instance, RFID are sketchy for accomplishing the fundamental necessities of the verification procedure incorporating continuous correspondence to the servers and exchange messages with hubs. In the secure models the data secrecy is maintained and it's guaranteed that during the process of message exchange the information holds its inventiveness and no alteration is hidden by the modal. The internet of things includes several little gadgets, for instance, RFIDs which stays unattended for broadened times, it is of a less degree of demand for the intruder to reach the data stored in memory [25]. For the sake of giving the resistance against Sybil attacks in RFID labels, received signal strength indication (RSSI) based philosophies are utilized as a part of [26], [27], [28] and [29]. A wide variety of arrangements were suggested for the remote sensor systems that considers the sensor as a part of Web interconnected using hubs [30]. Notwithstanding, in the internet of things the sensor hubs are considered to be the Web hubs that influence the confirmation to procedure quite huge. The integrity of data likewise ends up essential and needs additional considerations in terms of holding its unwavering quality.

4. PROPOSED LT10 ALGORITHM:

LT10 is a symmetrical block cipher algorithm which uses 128-bit key and plaintext. In symmetrical key calculation the cipher procedure comprises of encryption rounds four elements of the kasumi encryption algorithm is utilized which contain a few adjustments, every round is dependent on some numerical abilities to make disarray and dispersion. Increasing in number of rounds ensures better security, on the other hand, in the end brings about incrementing in the use of compelled vitality. However to more improve the vitality proficiency, each one of the encryption rounds includes scientific tasks working on 4 bits of information. For the sake of making sufficient perplexity and dissemination of data to go up against the attacks, the computation utilizes the feistel model of substitution dispersion capacities.

Proposed TL10 Algorithm:

Input: 128 bit plaintext and key

Output: 128 bit cipher text

Step0: start

Step1: The input information is adjusted by static information held in a 64-bit enroll and an (augmenting) 64-bit counter BLKCNT.

Step2: The figure key CK of KASUMI is gotten from calculation's figure key Kc

Step3: KASUMI works on 64-bit information squares and its handling is controlled by a 128-bit encryption key that infers the sub keys KL, KO and KI

Step4: Each round of KASUMI comprises of the segments FL and FO.

Step5: FL is connected on information before FO for odd rounds and the opposite procedure occurs for even adjusts

Step6: 32-bits information utilizing sub keys KL

Step7: usage FO comprises of 2 rounds where in the primary we utilize parallel calculation of two FI segments.

Step8: Part FI is characterized as a 4-round structure utilizing non-direct look-into tables S7 and S9

Step9: Along these lines we utilize each S7 and S9 part 120 times.

Step10:end

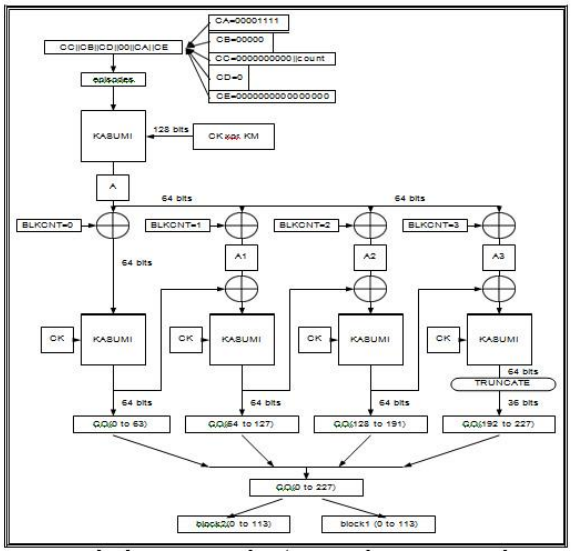

Figure (1): Proposed TL10 Diagram with four KASUMI elements

KASUMI is utilized as a part of a type of yield criticism mode and creates the yield bit stream in products of 64 bits. The input information is adjusted by static information held in a 64-bit enroll and an (augmenting) 64-bit counter BLKCNT. Clearly KASUMI part require an extensive usage territory. Consequently we utilize just a single KASUMI segment that is utilized as a different element. The figure key CK of KASUMI is gotten from calculation's figure key Kc . Right off the bits we compute enlist A with KASUMI segment and afterward we utilize successively KASUMI to infer 64-bits of yield inevitably. KASUMI is a square figure and has a Feistel structure containing eight rounds. Eight isn't an arbitrary number since with investigation it may be conceivable to discover a few assaults to 6 rounds, however not to the full 8 round KASUMI. KASUMI works on 64-bit information squares and its handling is controlled by a 128-bit encryption key that infers the sub keys KL, KO and KI. Each round of KASUMI comprises of the segments FL and FO. FL is connected on information before FO for odd rounds and the opposite procedure occurs for even adjusts. To limit the territory, our execution has just a single of every part FL and FO. For better understanding we exhibit the full procedure in the figure 2. Segment FL is a direct capacity that is basic and quick, yet the security of KASUMI isn't intended to rely upon this capacity. Its primary design is to be a minimal effort extra scrambling, making singular bits harder to track through the rounds. It applies on 32-bits information utilizing sub keys KL. Its structure is appeared in the figure 2. Segment FO is a 32-bit non-straight blending capacity. FO is an iterated "stepping stool configuration" comprising of 3 rounds of a 16-bit non-straight blending capacity FI. FO fulfills the "Torrential slide Effect" that is each yield bits relies upon each information bit. In this manner changing a solitary one info bits Changes the yield. In our usage FO comprises of 2 rounds where in the primary we utilize parallel calculation of two FI segments.

Part FI is characterized as a 4-round structure utilizing non-direct look-into tables S7 and S9. All capacities included will blend the information contribution with key material. FI part is the fundamental randomizing capacity of KASUMI with 16 bits info and 16 bits yield and fulfills the "Torrential slide Effect".

FI segment is made out of a four-round structure utilizing two non-direct substitution boxes S7 and S9. The structure is compacted in two rounds utilizing parallelism. The unequal division of FI is because of the way that objective elements of odd size are for the most part superior to those of even size from the perspective of provable security against direct and differential cryptanalysis .

S7 and S9 have been planned in a way that stays away from direct structures in FI. This reality has been affirmed by measurable testing .S-boxes (S7 and S9) are actualized in combinational rationale despite the fact that they could be executed by "look-into tables" to diminish the extent of our usage. As a result of the parallelism, just two part of each S7 and S9 is required for the calculation of A5. Along these lines we utilize each S7 and S9 part 120 times.

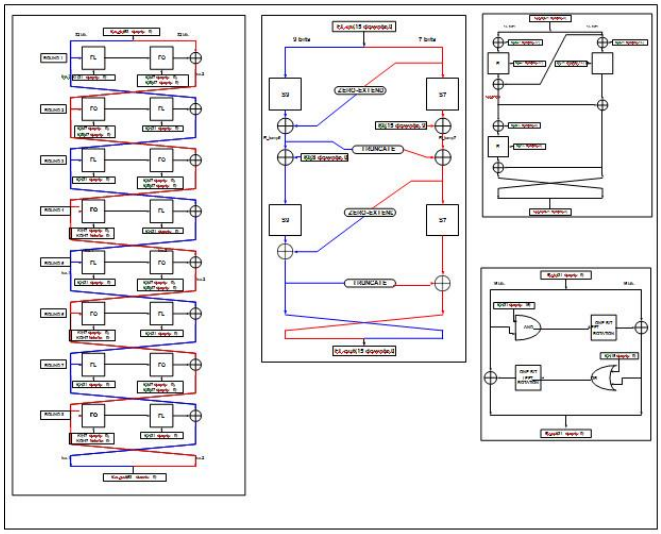

Figure (2): The Kasumi block cipher

4.1 Algorithm estimation and comparison:

The system is modeled and programmed in visual studio 2017 connecting to and IOT network via wifi and internet.

Time consumption is playing very important role in security field especially in IOT where the whole encryption and decryption process is done in real time, figure(3) shows how the time been compared with known encryption algorithms (AES,RSA).

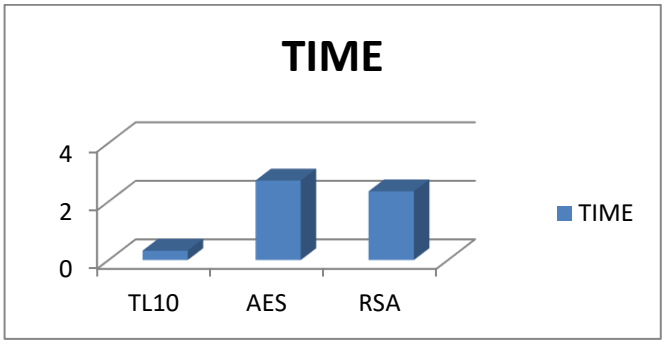

Figure (3): Time comparison with known algorithms

Table (1) illustrates the Comparison of Light weight Cryptographic Algorithms the most effected factors to the IOT encryption algorithm are mentioned in face to compare with the proposed algorithm.

The key size , block size ,rounds and cycle will provide a clear vision for compression that support our proposed algorithm as a light weight algorithm in IOT.

Table (1): compression with other cryptographic

\

Ciphers	Function	Architecture	Structure	Key size	Block size	Rounds	Cycles
PRINT	Encryption & Decryption	Serialized	SPN	80	48	48	768
SIMON	Encryption & Decryption	Round-based	LFSR	80	32	254	1872
KATAN	Encryption	Serialized	Fiestel	56	32	254	255
PICOLO	Decryption	Serialized	Fiestel	64	80	144	2309
BORON	Encryption	Round-based	LFSR	64	36	36	178
TWINE	Encryption & Decryption	Serialized	Fiestel	80	64	12	1304
KLEIN	Encryption	Round-based	LFER	64	254	255	1528
LT10	Encryption & Decryption	Serialized	Fiestel	128	128	64	335

5. CONCLUSIONS

Sooner rather than later the IoT will be a fundamental element in people's daily lives. A wide variety of vitality compelled gadgets and sensors will ceaselessly be communicating with one another, the security of which is not to be taken lightly. Therefore, a light-weight security calculation is suggested in this paper, this calculation is referred to as LT10. The usage demonstrate promising comes about making the calculation an appropriate possibility to be embraced in the applications of the internet of things. Soon enough, people will occupied with the detail process assessment and cryptanalysis of this model on different devices and programming stages for conceivable assaults.

References

[1] [1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things
[2] (iot): A vision, architectural elements, and future directions," Future Generation Computer Systems, vol. 29, no. 7, pp. 1645–1660, 2013.
[3] [2] R. Want and S. Dustdar, "Activating the internet of things [guest editors'introduction]," Computer, vol. 48, no. 9, pp. 16–20, 2015.
[4] [3] J. Romero-Mariona, R. Hallman, M. Kline, J. San Miguel, M. Major,and L. Kerr, "Security in the industrial internet of things," 2016.
[5] [4] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: areview," in Computer Science and Electronics Engineering (ICCSEE),2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651.
[6] [5] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner,"Smart locks: Lessons for securing commodity internet of things devices," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 461–472.

[7] [6] D. Airehrour, J. Gutierrez, and S. K. Ray, "Secure routing for internet of things: A survey," Journal of Network and Computer Applications, vol. 66, pp. 198–213, 2016.
[8] [7] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012.
[9] [8] L. Da Xu, "Enterprise systems: state-of-the-art and future trends," IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 630–640, 2011.
[10] [9] P. Zhao, T. Peffer, R. Narayanamurthy, G. Fierro, P. Raftery, S. Kaam,
[11] and J. Kim, "Getting into the zone: how the internet of things can improve energy efficiency and demand response in a commercial building," 2016.
[12] [10] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of internet of things," Information Technology and Management, vol. 13, no. 4, pp. 205–216, 2012.
[13] [11] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 529–534.
[14] [12] S. Misra, M. Maheswaran, and S. Hashmi, "Security challenges and
[15] approaches in internet of things," 2016.
[16] [13] M. C. Domingo, "An overview of the internet of things for people with
[17] disabilities," Journal of Network and Computer Applications, vol. 35, no. 2, pp. 584–596, 2012.
[18] [14] W. Qiuping, Z. Shunbing, and D. Chunquan, "Study on key technologies of internet of things perceiving mine," Procedia Engineering, vol. 26, pp. 2326–2333, 2011.
[19] [15] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent
[20] transportation system based on the internet of things," in Internet of Things. Springer, 2012, pp. 572–580.
[21] [16] B. Karakostas, "A dns architecture for the internet of things: A case study in transport logistics," Procedia Computer Science, vol. 19, pp. 594–601, 2013.
[22] [17] H. J. Ban, J. Choi, and N. Kang, "Fine-grained support of security services for resource constrained internet of things," International Journal of Distributed Sensor Networks, vol. 2016, 2016.
[23] [18] S. Khan, M. Ebrahim, and K. A. Khan, "Performance evaluation of secure force symmetric key algorithm," 2015.
[24] [19] P. L. L. P. Pan Wang, Professor Sohail Chaudhry, S. Li, T. Tryfonas, and H. Li, "The internet of things: a security point of view," Internet Research, vol. 26, no. 2, pp. 337–359, 2016.
[25] [20] M. Ebrahim, S. Khan, and U. Khalid, "Security risk analysis in peer 2 peer system; an approach towards surmounting security challenges," arXiv preprint arXiv:1404.5123, 2014.
[26] [21] M. A. Simplicio Jr, M. V. Silva, R. C. Alves, and T. K. Shibata, "Lightweight and escrow-less authenticated key agreement for the internet of things," Computer Communications, 2016.
[27] [22] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[28] [23] F. Xie and H. Chen, "An efficient and robust data integrity verification algorithm based on context sensitive," way, vol. 10, no. 4, 2016.
[29] [24] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," International Journal of Sustainable Development & World Ecology, vol. 20, no. 3, pp. 216–222, 2013.
[30] [25] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, and T. Phillips, "Guidelines for securing radio frequency identification (rfid) systems," NIST Special publication, vol. 80, pp. 1–154, 2007.
[31] [26] J. Wang, G. Yang, Y. Sun, and S. Chen, "Sybil attack detection based on
[32] rssi for wireless sensor network," in 2007 International Conference on Wireless Communications, Networking and Mobile Computing. IEEE, 2007, pp. 2684–2687.
[33] [27] S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the sybil attack cooperatively in wireless sensor networks," in Computational Intelligence and Security, 2008. CIS'08. International Conference on, vol. 1. IEEE, 2008, pp. 442–446.
[34] [28] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2418–2434, 2010.
[35] [29] S. Chen, G. Yang, and S. Chen, "A security routing mechanism against sybil attack for wireless sensor networks," in Communications and Mobile Computing (CMC), 2010 International Conference on, vol. 1. IEEE, 2010, pp. 142–146.
[36] [30] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security. ACM, 2002, pp. 41–47.