Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

A Survey on Energy-Efficient and Security Algorithms using Edge Computing Architecture for IoT in Cloud based Process Industries

PunithaNicholine J[1*], Preethi D M D[2], Arul Prasanna M[3]
[1]Assistant Professor,[2,3]Associate Professor,
[1,2]Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul.
[3]Department of Electrical and Electronics Engineering, PSNA College of Engineering and Technology, Dindigul.
*infantia.1@gmail.com

ABSTRACT

Internet of Things (IoTs) embraces of controlled sensor-based devices and machineries connected with each other and collaborating over the internet. In a distributed IoT environment lot of issues such as Power Consuming, battery backup, storage, running cost and Safety in the system. In this paper, numerous cryptographic algorithms are analyzed based on the size of block & Key and number of iterations. Apart from the above analysis security structure of IoT and challenges faced with result comparisons. Finally, a safe environment system with a facility enhancement for an improved resource guarded IoT environment and open concerns are discussed.

Keywords
Energy Efficient,Lightweight Cryptography, Symmetry key, Block Cipher, IoT.

Introduction

Internet of Things (IoT) is the progressively prevalent technology that permits physical devices, automobiles, house hold appliances, etc. to connect, even share and operate with one another. [1]. In modern times, a range of cloud-based devices have entered into the market with a scope to support the process automation Industries to being supplied with energy utilizations as securely, reliably and efficiently as possible. We discuss the prospects and threats that are available in the cloud-based tools in these industrial environs. We take the standpoint that the benefits of data-driven and platform-based approaches prevail over the well-known risks even in security- safety and sensitive areas of process and chemical industries. On the other hand, the advantages of global process transparency enhance the cost savings and improved performance efficiency which are barely manageable by traditional methods. Also cloud-based approaches involved in secured data asset and patch management with energy efficiency and power quality analytics were also discussed [2]. Wireless Sensor Networks (WSN) focus on linking between the cyber and physical worlds. The security occupied importance due to the data transfer between the cyber & physical environments without any protection. The operational restrictions in the sensor nodes claim security primitives with small enactment size and low power utilization. Genuine encryption is a tool provided for these systems with increased secrecy, honesty, and validation of sensitive data. In this paper we are trying to explore the alternatives for authenticated encryption through generic compositions, to measure the expenses of these security approaches in WSN. Some primary primitives for the generic compositions such as two symmetric ciphers, two hash functions, AES, Present SHA and spongent are used for analysis. From the results obtained, it is exposed that the lightweight ciphers suggestively subsidize to reduce application area and energy consumption expenditures with extending lifetime of the sensor nodes [3]. The implementation costs in traditional encryption, through several aspects such as area, throughput, latency, and power and energy consumption. When designing LWC algorithm, we must consider the trade-off between security, cost, and energy and performance demonstrates fig 1. There are three

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

objectives for this trade-off security and cost, security and performance, which are difficult to improve at the same time. There are also several measures to provide security for devices with restricted environment when designing, low power, energy consumption, speed is acceptable. The goal of LWC is to reduce the overall[4].

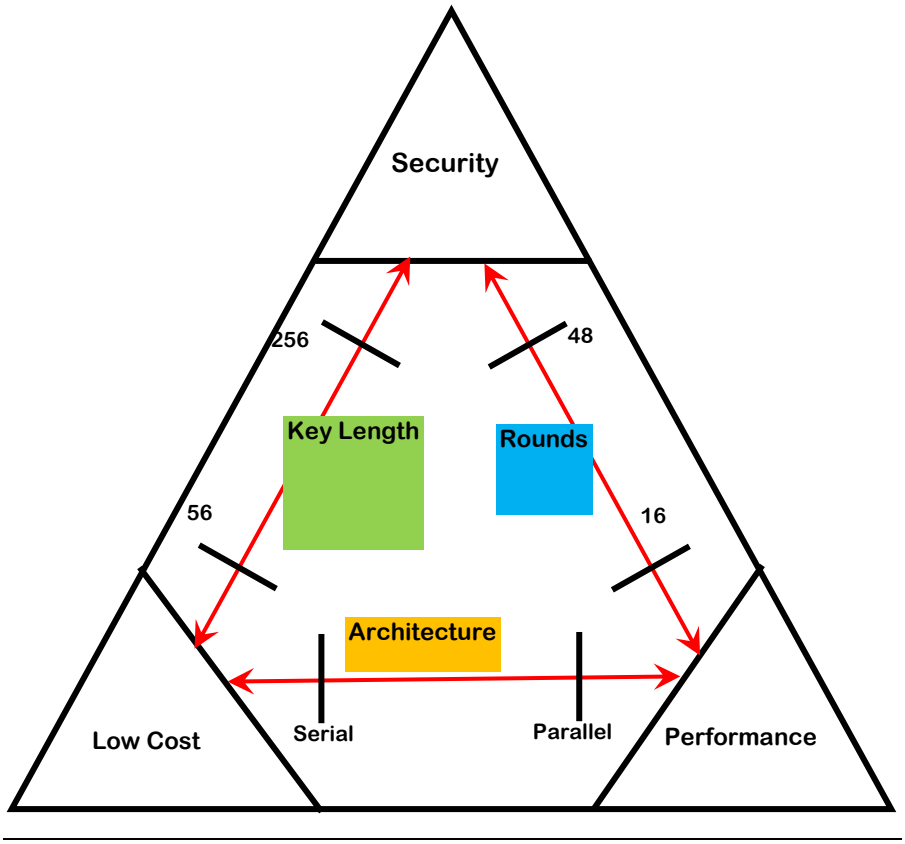

Fig.1 Trade-Off Design

Where the old cryptography techniques such as AES (encryption) and RSA/Elliptic Curve (signing), works satisfactory on systems involves real-time handling of energy and storage competences, these does not work satisfactory for a world of sensor networks and embedded systems. Thus the LWC techniques are related to shortlist the best technique among the conventional cryptography methods. This comprises limitations related to physical size, handling necessities, memory control and energy groove. This paper also summaries similar procedures which are defined as substitutions for old cryptography inside an IoT space and deliberate certain leanings in the proposal of LWC algorithms. [5]

2 REVIEW OF LIGHT WEIGHT CRYPTOGRAPHIC ALGORITHMS

Encryption can be understood by means of symmetric and asymmetric algorithms. A symmetric algorithm has two classes namely Stream ciphers and Block ciphers.For ideal IoT ciphering algorithm is independent and here stream cipher will be realized with the operation of Stream ciphers. In overall, block cipher such as AES procedures a multi-round assembly where a round function endures several iterations r. Round functions can be constructed on either Feistel Networks (FN) or Substitution-Permutation Networks (SPN) [7]

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

2.1 Overview of Light Weight Algorithms:

Lightweight cryptography is the group of cryptographic primitives, methods, and ciphers which can be practical in devices that are not able to provide most of the standing ciphers and have restricted resources (memory, power, size) for the process. The main procedures for lightweight ciphers are a balance between dependability, performance, and expense. In this work, we existent the reasonable analyze of few symmetric and asymmetric algorithms. Analysis is based on the comparison of the performance of each algorithm (encryption/decryption time, memory and power usage).

3 PERFORMANCE EVALUATIONS

3.1 Energy Consumption:

It is expected that the energy per CPU cycle is stable in order to measure the energy consumed, and it can be found using the following equation as

$$E = I * V_{cc} * \tau * N(1)\text{----------Eqn. (1)}$$

Where, I is the average load current for T Sec , V_{cc} is the voltage input for the system, τ is the Clock time period and N is the number of clock cycles. [8]

Power utilized can be found by using the technologies such as GE and CMOS techniques [10, 11]. Since Power and Energy utilization are the significant parameters thus any change in the CMOS values will effect on the gate density. Hence there is a large amount of increase in gate density for a change on CMOS with micro-meter (μm) to nano-meter (nm) Scale.

Due to this increase in the gate density the power utilization /MHz/GE decreases to a factor of 2-3. Also the Energy consumption will be found through the formula as shown in the equation.2.

$$\text{Energy/Bit} = Eb = L * P\text{----------Eqn. (2)}$$

Where Eb is the energy consumption per bit transfer and is termed in Micro-Joule (μJ). L is the Latency is the no. of clock cycles needed to make one encryption block or the time needed to convert normal data in to an encrypted data block. $P$is the Power utilized by the incurred Software/Hardware unit.

3.2. Memory Consumption:

Since the memory storage size is proportional to the type of encryption algorithm the implementation methods will have some memory constraints. The memory needed will depend on steps involved in the encryption algorithm, size of Key used, Vector size and facility type. The total cost of the process depends on the memory size which is to be reduced as much as possible in order to minimize the cost involved.

3.3 Execution time:

The execution time is the important factor that is to be concentrated while developing any encryption algorithms along with the security measure development. It is the time taken by the algorithm to encrypt or decrypt a particular data.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

3.4 Security Evaluation:

We analyzed and compared some symmetric cipher algorithms security level achieve the for authentication**.**

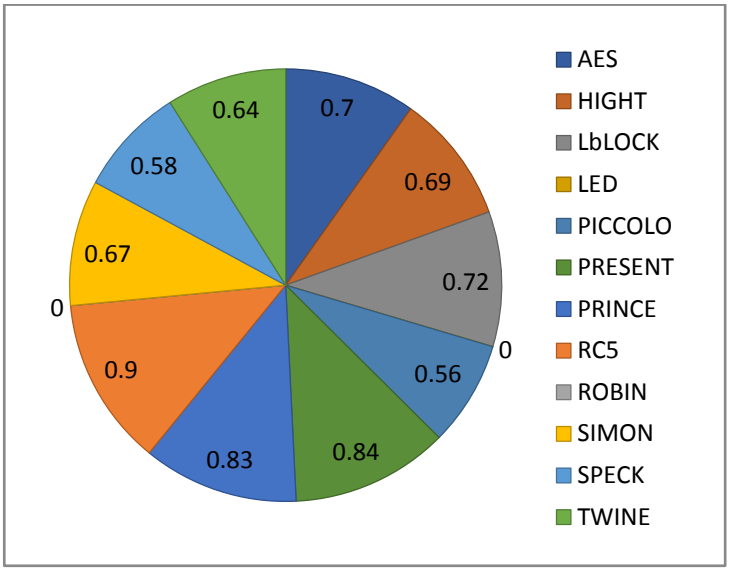

Fig.2 Security level for LWC cipher algorithms

4 EDGE COMPUTING ARCHITECTURE

Increase in the IoT devices increases the required bandwidth to some upper limits when they are used at the edge of the network which requires enormous number of data to be processed at the data Center [13]. Even though there is a considerable enhancement in the network technologies there is no guarantee in the rate of Transmission and response times by the data Center [14]. Moreover the edge devices continually utilizes the data from the cloud which forces the delivery data networks to decentralize the original data and service provisioning to the user a leveraging one.

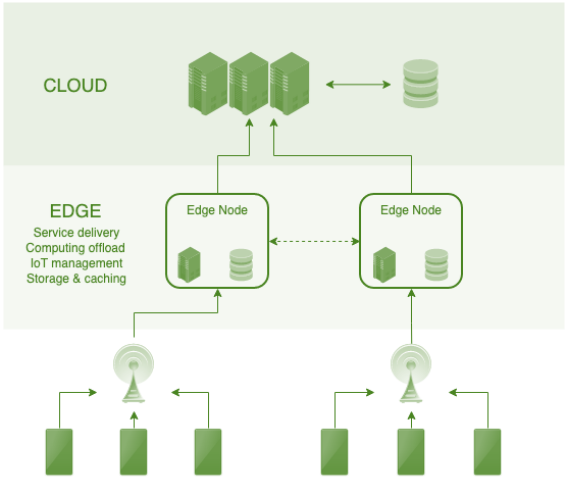

Fig 3. Edge computing Architecture

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

In analike way to move the computation to the edge of the network instead of processing it at the data Center the mobile phones, network gateways are allowed to perform tasks and to provide service instead of the cloud [15]. By moving the process to the edge of the network there is a considerable result in the response time and transfer rates for Caching of Content, Delivery, Memory size and IoT device Management etc. But in the meantime logic distribution over different networks brings together some new issues and problems.

4.1.Privacy and security Measure

This method represents the heterogeneous surroundings of a transformation in security systems used in Cloud. In edge computing, facts are transferable among dissimilar scattered nodes together concluded the Internet, and That need different encryption utilizations self-regulating nodes of domain. Edge nodes could stand reserve secured strategies, restrictive the excellent in terms of safe keeping approaches. Apart from centralized top-down structure, a modification is needed for a dispersed dependence traditional method [13].

4.2. Scalability Measure

Dispersed structure has so many problems because of scalability. The heterogeneity of the approaches, consumes varied routine and energy boundaries, the tremendously self-driven condition and the steadiness of the connections, related to more powerful structure of cloud data centres. Security provisions may extant supplementary latency in the communication between knobs, which may decrease the speed of scaling process[11].

4.3. Reliability Measure

In order to sustain a provision active procedure the failovers in supervision is becoming so critical. If a node becomes inaccessible or miserable then the users might be able to access the data without any interruptions by becoming static. Each scheme must preserve the network topology of the whole discrete system such that the error detection and recovery will be easy. Diverse range of reliability of the linked machineries used will also affect the above feature. Further the efficiency of the produced data at the edge devices may be inaccurate under some environmental situations [14].

4.4 Speed Measure

The computation speed for any logical computational stuff improves to a remarkable level since it is carried out at the end users side. It is very effective when compared to the conventional cloud based systems. For a given request the response time for edge computing is a expressively the most conceivable choice compare to the cloud computing. Considering with the human judgment like mud pack acknowledgement which involves a computation time of 370-620ms to complete the process. Thus edge computing is more preferred to be best methods in the view of response time compared to humans which improves the certainty in distinguishing them.

4.5. Efficiency Measure

Due to the immediacy of the investigative properties to the edge users, refined diagnostic outfits and Simulated Intellect outfits can track on the verge of the system. This assignment at the edge aids to growth active effectiveness, donates much compensation to a particular scheme. Moreover, the practice of edge computing in an extreme phase between consumer strategies and the broader internet outcomes in competence reserves this will be established in the subsequent illustration: A user trick needs computationally rigorous dispensation on audio-visual records to

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

be done on exterior servers. By placing attendants on a resident edge grid in order to complete such calculations, the video files that are most needed alone will be allowed to be transferred in the limited link. Circumventing diffusion on the internet effects major bandwidth investments and consequently growths efficiency [15]. Edge request facilities diminish the measurements of documents that have to be motivated, the resultant circulation, and reserving that data must travel which affords lesser dormancy and cuts the communication costs. Computation offloading in some real-time requests which involves algorithms for face recognition shows substantial enhancements in its time of response as depicted in some earlier researches [16].

5ENERGY EFFICIENCY

The efficient usage of energy consumption becomes an essential thing in order to meet out the energy costs, Power transfer difficulties and irregular energy resources availability under changing universal weather conditions. There is a significant energy saving capabilities in all ingesting divisions that grow into deceptive when achieving discernibility on energy feeding at a high quality level with liberal resolution. For the goal to observe the growth of overall energy performance over a period of time the defining key performance indicators (KPI's). For a data processing of the order of 100 to 102 MB of data per day at a single site involves some 25 different measures of electrical quantities are monitored so as to calculate the energy consumed for the uploaded data. The result obtained is tested and compared for its efficiency and cost which is then analyzed for meaningful information so that this phenomena can be implemented for similar different sites and equipment's in parallel. This improves the efficiency both time and scope of the duties of energy managers and sites management too.

6 RESULT AND DISCUSSION

Results of Implementation of Asymmetric Algorithms shown in Table 1 and Block Cipher Algorithms shown in Table 2and Solutions for Secure IOT in Cloud shown in Table 3 and Comparison of various Machine Learning Algorithms shown in Table 4

Table1 Comparison of Asymmetric Algorithms

Security level	No. of bits	RSA			ECC		
		Key Size	Encryption time (ms)	Decryption time(ms)	Key Size	Encryption time (ms)	Decryption time(ms)
80	64	1024	1366	5337.2	160	21685	5909.9
112	64	2048	163.5	20410.8	224	9985.5	6933.3
128	64	3072	167.2	46478.2	256	15088.2	7358.4

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

Table 2 Performance evaluation of LWC algorithm (Block cipher Algorithms)

Algorithm	Block size (bit)	Key size (bit)	Rounds	Hardware Encryption		Latency	Power (µW)	Throughput at 100khz (Kpbs)	Energy (µJ/Bits)	Processing speed (ms per 16-byte message)
				Logic process (µM)	Area (GE)					
AES	128	128	10	0.13	3100	1032	2.48	56.64	493.3	2.29
KLEIN-64	64	64	12	0.18	1220	96	1.83	100	14.50	1.97/2.5
KATAN-40	48	80	254	256	2032	256	0.80	12.5	64.50	120/121
PRESENT-80	80	64	31	0.18	1030	10792	0.18	12.4	5.76	6.6/11.1
PRINT-48	64	128	48	0.18	503	238	0.75	100	96.00	28.3/21.3

Table 3 Solutions for Secure IOT in Cloud

Author Year	Methodology	Merits	Recommendations
Junxu Xia Year: 2020	A robust and secure edge storage (RoSES) method using the totally local reconstruction code (TLRC) method and a trust-oriented data access (TODA) strategy for our RoSES model is described	It can achieve data robustness, high security, and lightweight computation at end devices.	This model can proficientlyrecognize the memory, data recovery, and sharing at the edge of network, **saving about 35%** of **memory cost** and 76% corrupted latency level.
Blumenthal Year: 2019	The chances and threats that incurred with cloud-based technologies used, especially in the context of secondary assets.	The benefits of ubiquitous process transparency, among others, along with data-based levers for cost savings and performance increase which are hardly accessible by traditional means.	This paper needs to cover **cloud-based approaches** to **secure** asset and patch management, **energy efficiency** services, and power quality analytics.
Wei Zhou Year: 2019	Security and privacy of 8 Internet of Things attributes including the causes of threats and solutions are discussed.	Various new protocols introduced are likely to have potential vulnerabilities, which requireadditional efforts to resolve thecomplications.	It is necessary to examinemore to determine the **origin**of new IoT security threats, and to developaadditionalgeneral and **appliedshielding measures**.
VIKAS HASSIJA1 Year: 2019	To increase the level of security in IoT4diversecomputing tools such as block chain, fog computing, edge computing, and ML were discussed.	Achieving a high degree of trust in the IoT applications are discussed.	A comprehensiveevaluation of the security-related tasks and **origin of risk in the IoTsolicitations**is to be done. The **security issues**, severalemergent and available technologies are also discussed.
Dong Zheng Year: 2018	This paperuses attribute-based encryption for secured data transfer and the online/offline encryption methodology in the encryption phase.	To solve the privacy issues in users data sharing and in order to improve the efficiency of encryption	The **data allocation scheme**required to be secured and has to**improve data processing**capability in IoT data transfer.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 1513 - 1522
Received 16 February 2021; Accepted 08 March 2021.

Christos Year: 2018	New technologies and the use of various open source tools, such as CC Analysers and Simulators discussed.	For the requirement of enhanced transmission of high-quality data animproved and enhanced technology of IoTwith the addedassistance of the Cloud Computing technology is needed.	Thusthe researchersare recommendedto develop algorithms with**improved and more efficient media data transmission**.
Mirza Year: 2017	Twelve different types of attacks happened in IOT were discussed in detail.	Improved Solutions to handle these attacks are described.	**Disabling the features** that are **not used** may decrease the chances of security attacks.

Table 4 Comparison of Various Machine Learning Algorithms

Machine Learning Algorithm	Technique	Security Attacks	Pros and Cons
Supervised Learning	**SVM**	Phishing	Data is more protected. Linkagefault and storingproblematicresolved with the use of IOT.
	CLASSIFICATION	Intrusion detection	A robust solution can provide better functionality and performance benefits.
	NAIVE BAYES	Malware	Data detainedpowerfully. Time and Storage issues are modified using security algorithms.
Unsupervised Learning	**ANN**	Denial of Service (DoS)	Make sure high data confidentiality; Cloud capacitysecurityEnthusiastic and particularclient-serversubmissions or good functionality
	SVD	Data breaches	CC established trust model is more tangible. IoT based Retreat solutions needed for operative solution.
	DEEP LEARNING	Weakening Perimeters, , web defacement	NewProtected and data transfer was fast but additional security required in IOT when execution time error was found
	K-MEAN	Intrusion detection	High level of accuracy and consistency is accomplished. Susceptibility is more. It is resolved with the use of IOT.

CONCLUSION

In recently, Internet of things is fast and achievement superior to several other technologies. Each system measuresvarious routine based iterations on the key length, rounds/cycles and Memory space/area and energy consumption. The LCW algorithms used in IoT devices for the enhanced performance of the device other than keeping the protection as precedence. We expected that this survey is to be useful by way of a valued resource for security enhancement for upcoming IoT Implementation. In this paper analyzed all machine learning techniques advantages and disadvantages and effects of security attacks and energy consumption is measured in between cloud and IoT environment. In upcoming, we design to examine new techniques for different platforms and investigate performance based on two or more machine

learning techniques should be combined with help of Lightweight cryptography systems and analyzed the algorithms' suitability for designers take better decisions when selecting an efficient algorithm by optimization techniques. We present the summarized view of feasible battery life, and also prepare a test to evaluate the energy consumption with help of Artificial Intelligence Technology. Energy conservation is important in Industry 4.0.that is big challenge not solved yet and all optimization of cryptography algorithms for control machineries in industries which provide best performance of the system. We have successfully analyzed suitable edge computing architecture for secure sharing and transferring IoT data through Cloud environment.

REFERENCES

[1] Zhou, A. Peng, Y. Zhang, "The Effect of Iot New Features on Security and Privacy: New Threats, Existing Solutions, And Challenges Yet to Be Solved, IEEE Internet Of Things Journal, DOI10.1109/JIOT.2018.2847733.

[2] R. Blumenthal, F. Cadelcu and C. Blug, "Secure, Reliable and Efficient Energy Supply in Production Processes using Cloud-Based Technologies," 2019 Petroleum and Chemical Industry Conference Europe (PCIC EUROPE), Paris, France, 2019, pp. 1-7, doi: 10.23919/PCICEurope46863.2019.9011633.

[3] Carlos Andres Lara-Nino, Arturo Diaz-Perez,and Miguel Morales-Sandoval, Energy and Area Costs of Lightweight Cryptographic Algorithms for Authenticated Encryption in WSN, Security and Communication Networks Volume 2018, Article ID 5087065, 14 pages.

[4] William J. Buchanan, Shancang Li &RameezAsif (2017) Lightweight cryptography methods, Journal of Cyber Security Technology, 1:3-4, 187-201, DOI: 10.1080/23742917.2017.1384917

[5] Nilupulee A. Gunathilake, William J.Buchanan and RameezAsif,Next Generation lightweight Cryptography for Smart IoT Devices: Implementation, Challenges and Applications 2019 IEEE 5th World Forum on Internet of Things(WF-IoT), Limerick, Ireland,pp.707-710, doi:10.1109/WF- IoT.2019.8767250.

[6] Noura, H., Chehab, A., Sleem, L. et al. One round cipher algorithm for multimedia IoT devices. Multimedia Tools Appl 77, 18383–18413 (2018). https://doi.org/10.1007/s11042-018- 5660-y

[7] MojtabaAlizadeh, MazleenaSalleh, MazdakZamani, JafarShayan, SasanKaramizadeh, Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID, Sohel, Rana, Saddam Hossain, Hasan Imam Shoun , Dr. MohammodAbulKashem, An Effective Lightweight Cryptographic Algorithm to Secure Resource-Constrained Devices, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 9, No. 11, 2018

[8] Badel, S., Dağtekin, N., Nakahara, J. J., Ouafi, K., Reffé, N., Sepehrdad, P., &Vaudenay, S. (2010). ARMADILLO: A multi-purpose cryptographic primitive dedicated to hardware. In: Proceeding of International Workshop on Cryptographic Hardware and Embedded Systems (pp. 398–412). Berlin: Springer.

[9] Hatzivallis, G., Fysarakis, K., Papaefstathiou, I., &Manifavas, C. (2018). A review of lightweight block ciphers. Journal of Cryptographic Engineering, 8, 141–184.

[10] Zheng Gong, SvetlaNikova and Yee Wei Law, KLEIN: A New Family of Lightweight Block Ciphers, June 2011 DOI: 10.1007/978-3-642-25286-0_1 · Source: DBLP

[11] Ivkovic, Jovan (2016-07-11). "[Serbian] The Methods and Procedures for Accelerating Operations and Queries in Large Database Systems and Data Warehouse (Big Data Systems)". Hgpu.org.

[12] Jump up to:a b c Shi, Weisong; Cao, Jie; Zhang, Quan; Li, Youhuizi; Xu, Lanyu (October 2016). "Edge Computing: Vision and Challenges". IEEE Internet of Things Journal. 3 (5): 637646. doi:10.1109/JIOT.2016.2579198. S2CID 4237186.

[13] Merenda, Massimo; Porcaro, Carlo; Iero, Demetrio (29 April 2020). "Edge Machine Learning for AI-Enabled IoT Devices: A Review". Sensors. 20 (9): 2533. doi:10.3390/s20092533. PMC 7273223. PMID 32365645.

[14] Garcia Lopez, Pedro; Montresor, Alberto; Epema, Dick; Datta, Anwitaman; Higashino, Teruo; Iamnitchi, Adriana; Barcellos, Marinho; Felber, Pascal; Riviere, Etienne (30 September 2015). "Edge-centric Computing". ACM SIGCOMM Computer Communication Review. 45 (5): 37–42. doi:10.1145/2831347.2831354.

[15] Jump up to:a b Satyanarayanan, Mahadev (January 2017). "The Emergence of Edge Computing". Computer. 50 (1): 30–39. doi:10.1109/MC.2017.9. ISSN 1558-0814.

[16] R. Blumenthal, F. Cadelcu and C. Blug, "Secure, Reliable and Efficient Energy Supply in Production Processes using Cloud-Based Technologies," 2019 Petroleum and Chemical Industry Conference Europe (PCIC EUROPE), Paris, France, 2019, pp. 1-7, doi: 10.23919/PCICEurope46863.2019.9011633.

[17] J. Xia, G. Cheng, S. Gu and D. Guo, "Secure and Trust-Oriented Edge Storage for Internet of Things," in IEEE Internet of Things Journal, Vol. 7, no. 5, pp. 4049-4060, May 2020, doi: 10.1109/JIOT.2019.2962070.

[18] R. Blumenthal, F. Cadelcu and C. Blug, "Secure, Reliable and Efficient Energy Supply in Production Processes using Cloud-Based Technologies," 2019 IEEE Petroleum and Chemical Industry, Europe (PCIC EUROPE), Paris, France, 2019, pp. 1-7, doi: 10.23919/PCICEurope46863.2019.9011633.

[19] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," in IEEE Access, Vol. 7, pp. 82721-82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[20] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved," in IEEE Internet of Things Journal, Vol. 6, no. 2, pp. 1606-1616, April 2019, doi: 10.1109/JIOT.2018.2847733.

[21] D. Zheng, A. Wu, Y. Zhang and Q. Zhao, "Efficient and Privacy-Preserving Medical Data Sharing in Internet of Things With Limited Computing Power," in IEEE Access, vol. 6, pp. 28019-28027, 2018, doi: 10.1109/ACCESS.2018.2840504.

[22] J. Xia, G. Cheng, S. Gu and D. Guo, "Secure and Trust-Oriented Edge Storage for Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4049-4060, May 2020, doi: 10.1109/JIOT.2019.2962070.

[23] Umer Ahmed Butt , Muhammad Mehmood , Syed Bilal Hussain Shah , Rashid Amin ,M. WaqasShaukat , Syed MohsanRaza , Doug Young Suh ,and Md. JalilPiran ,"A Review of Machine Learning Algorithms for CloudComputing Security",electronice, MDPI,August 2020.