Lightweight Algorithms for Low Powered IoT Devices Comparative Analysis

D.M. Sheeba, R. Varalakshmi, N. Anbumani

Abstract--- ***Internet of Things is the Connections of embedded technologies that contained physical objects and is used to communicate and intellect or interact with the inner states or the external surroundings. Rather than people-people communication, IoT emphasis on machine-machine communication. This paper familiarizes the status of IoT growth. The IoT embeds some intelligence in Internet connected objects to communicate, exchange information, take decisions, invoke actions and provide amazing services. This paper addresses the existing development trends, the generic architecture of IoT, its distinguishing features and possible future applications. This paper also forecast the key challenges associated with the development of IoT. It emphasizes the use of lightweight algorithms to increase the security of content with less iteration.***

Keywords--- ***Internet of Things, ubiquitous computing, Lightweight Algorithm, IoT architecture, IoT applications, IoT security.***

I. INTRODUCTION

Internet of Things (IoT) is a network of connected devices with unique identifiers in the form of an IP address which have embedded technologies or are equipped with technologies that enable them to sense, gather data and communicate about the environment in which they reside and/or themselves. [1]. IoT provides better chances of making world a greater level of accessibility, availability, scalability, confidentiality, and interoperability [3]. But, how to protect IoT is a challenging task. System security is the foundation for the development of IoT. [2].IoT is widely applied to social life applications such as smart grid, IoT is considered as the future evaluation of the Internet that realizes machine-to-machine (M2M) learning [4].

The IoT links real life and physical activities with the virtual world, the numbers of Internet connected devices are increasing at the rapid rate. These devices include personal computers, laptops, tablets, smart phones, PDAs and other handheld embedded devices. Mobile computing devices use different sensors and input mechanisms that can sense, do compute, decides on the actions to be done and transmit processed decisions & data over the Internet. Given that the shared data contains a large amount of private information, preserving information security on the shared data is an important issue that cannot be neglected [5].IoT devices are increasing in many folds day by day, in mean time power requirement and processing capacity of device is being considered as a key factor while designing IoT devices.

Due to size constraint and power utilization data security becomes vulnerable while computing using small or low-powered IoT devices. Low-energy technologies in the Internet of Things (IoT) era are still unable to provide the reliability needed by the industrial world, particularly in terms of the wireless operation that pervasive deployments demand. Most of the industrial wireless performance has achieved good results, but it is difficult task to achieve energy-requirement of an application [6]. Enabling low-powered IoT devices with efficient algorithms to handle Data Security, Integrity and Availability is need of the hour. In this paper we bring out current algorithms used in IoT devices and its performance with respect to low-powered devices and also propose research guidelines on how it can be improved.

II. IOT ARCHITECTURE

IoT devices are commonly now available in following segments of daily use, Consumer Services, Smart house; Smart meters in energy division, Smart mobiles, and Smart wearable devices on consumer computing devices, connected cars, Motors and manufacturing metrics, Physical objects[42] are the few areas where industry utilizes power of IoT.

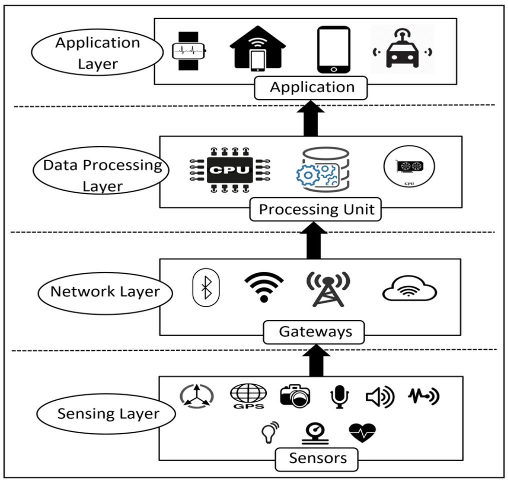

Fig. 1: IoT Architecture Layers

Layer	Protocol Used	Security Protocol	Attacks
Application	COAP	Not fixed designed by user	Depend on Protocol
Transport	UDP	DTLS	Attack on RC4, DoS Attack
Network	IPv6, RPL	IPSec	DoS Attack
Perception	IEEE 802.15.4 PHY, MAC	IEEE 802.15.4 security	DoS, Attack on authentication, integrity

Revised Version Manuscript Received on 22 February, 2019

D.M. Sheeba, Dept of Computer Science, New Prince Shri Bhavani Arts & Science College, Chennai, India. (e-mail: me@sheeba.co.in)

R. Varalakshmi, Dept of Computer Applications, VISTAS, Chennai, India. (e-mail: rvara.scs@velsuniv.ac.in)

N. Anbumani, Networks & Cryptography, Selima Groups, Chennai, India. (e-mail: me@anbumani.co.in)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The physical objects are equipped with Radio-Frequency Identification (RFID) tags The RFID adaptor can detect data from RFID tags , applying the RFID adaptor in IoT environment, it can interoperate data/events of other applications in IoT[41].To secure the interoperability of data and physical objects several layers and protocols are defined to prevent attacks and vulnerabilities[45].

The common architecture of IoT devices / Computing devices through Internet has Application, Transport, Network, Physical Layers. Each layer is enabled with different kind of algorithm or security measure to handle data securely[44]. When we talk about power consumption at each layer, it depends on how frequently computing done on incoming data.

A. Physical Layer

Physical Layer is bottom layer of IoT responsible for sensing and providing required data for processing. On connectivity front, these are connected to Ethernet or Wifi networks and secured by non-alterable physical Universally Unique identifiers (UUID) [7].

B. Network Layer

Network Layer is responsible for communicating with network management and communication channels through multiple protocols [8] as in Fig 2.

C. Data Processing Layer

Data Processing Layer is responsible for providing services based on available data from sensing devices stored in databases [9]-[10].

In above architecture, each layer carries the data till Application Layer to present it as a usable and meaningful data. In this stream of data flow Security, Integrity, Confidentiality is essential in order to maintain a reliable IoT network [11].

III. RECENT SECURITY THREATS & COUNTER MEASURES IN IOT DEVICES

An IoT system can be attacked physically, or attacked from within its network, or from applications on the system, and lastly from attacks on encryption schemes. IoT is implemented using various existing[47] network technologies (Wireless Sensor Networks, RFIDs, Internet, etc.). Thus, there is a need for a proper categorisation of the attacks such that it encapsulates all of the different types of threats, so that better counter measurements can be developed and implemented for securing it. However, it is worth mentioning that Environmental Attacks (Earthquakes etc.) are omitted from this paper as their scope is beyond our research that focuses on intentional attacks from an adversary.

A summary of the classification [12]-[14] of the attacks is shown in Table 1 below.

An IoT system consists of three different layers each with vulnerabilities and security attacks. To address these attacks and to successfully protect the IoT system, this section presents a multi-layered security approach that should be structured to give an optimal layered protection at each layer in an IoT system[15]-[23] as shown on the next page in Table II.

Physical Attacks	**Network Attacks**	**Software Attacks**	**Encryption Attacks**
Node Tampering	Traffic Analysis Attacks	Virus and Worms	Side Chanel Attacks
RF Interference	RFID Spoofing	Spyware and Adware	Man In the Middle Attack
Node Jamming	RFID Cloning	Trojan Horse	Cryptanalysis Attacks: a) Ciphertext Only Attack b) Known Plaintext Attack c) Chosen Plaintext or Ciphertext Attack
Malicious Node Injection	RFID unauthorised Access	Malicious scripts	
Physical Damage	Sinkhole Attack		
Social Engineering	Man In the Middle Attack		
Sleep Deprivation Attack	Denial of Service	Denial of Service	
Malicious Code Injection on the Node	Routing Information Attacks		
	Sybil Attack		

The existing protocol at each layer, along with security protocol and attacks at each layer is summarized shown in Table 1.

COAP was earlier using the security of IPSec and DTLS. The predefined security mechanisms are vulnerable to aforementioned attacks. So, cryptography algorithms can be incorporated in them. Cryptography algorithms can be symmetric and asymmetric.

Symmetric algorithm uses a single private key for communication. Sender and receiver share same key for communication. Symmetric key assures confidentiality and integrity of data, but do not guarantee authentication. Advantage of symmetric is less number of keys required with less key size. Disadvantage is secure key distribution among both the parties, and it does not authenticate the sender. Traditional Symmetric algorithms AES, DES, Triple DES, Blowfish, IDEA are compared on the basis of their properties like data size, key size, number of rounds, structure and existing attacks shown in Table 2.

Asymmetric uses pair of public and private key for communication. Asymmetric assures confidentiality, integrity, and authentication. For confidentiality and integrity sender encrypts the data using public key of receiver that can be only decrypted by private key of receiver. To assure authentication, data is encrypted by private key of sender and receiver confirms it by decrypting it with public key of sender. Advantage of Asymmetric cryptography is it supports all security services, but disadvantage is the large size of key which will increase the complexity of algorithm.

The most common algorithms used are RSA by Rivest, Shamir and Adleman, Deffie Helmen key exchange (DH), Elliptic Curve Cryptography (ECC), and Hash functions.

Traditional Symmetric and Asymmetric algorithms are not apt for IoT environment due to the limited power devices, low computational resources, and less memory capacity of IoT. So, lightweight security algorithms were proposed for IoT. Lightweight solutions are light in terms of their key size, memory requirements and execution time so that fewer resources will be utilized as compared to heavy weight solutions.

IV. SYMMETRIC LIGHTWEIGHT ALGORITHMS FOR IOT

Advanced Encryption Standard (AES): AES is used as an inbuilt solution in COAP at application layer. It is a symmetric block cipher standardized by NIST. It uses substitution permutation network and works on 4*4 matrix having block length of 128 bits. Every byte gets affected by subbytes, shiftrows, MixedColumns, AddRoundKey[24]. Key size than can be used is 128, 192, 256 bits. AES is still vulnerable to man-in-middle attack[25].

High security and lightweight (HIGHT): Hight uses very basic operations like addition mod 28 or XOR to work for Feistel network. It has a block size of 64 bits, work in 32 rounds on128 bit keys[26]. Its keys are generated while encryption and decryption phase. A parallel implementation of higth was proposed in[27] that requires less power, mentioned in few lines of code, and improves speed for RFID systems. Higth is vulnerable to saturation attack.

Tiny Encryption Algorithm (TEA): TEA is used for constrained environments like sensor networks or smart things. It is written in very few lines of code. It does not use a complex program but requires simple operations of XOR, adding and shifting. It uses a block size of 64 bits and 128 bit keys and does not make use of existing tables or any predefined computations[28]. Number of variants exists for TEA like extended TEA[29], Block TEA and so on. These extensions try to resolve the problems in original TEA like equivalent keys. But still due to its simple operations TEA and its variant are susceptible to number of attacks.

PRESENT: It is based on SPN and is used as ultra lightweight algorithm for security. It works on substitution layer uses 4-bit input and output S-boxes for hardware optimization. It has key size of 80 or 128 bits and operates on 64-bit blocks[30]. PRESENT has been presented as a lightweight cryptography solution in ISO/IEC 29192-2:2012 "Lightweight Cryptography"[31]. PRESENT is vulnerable to differential attack on 26 out of the 31 rounds[32].

RC5: It was first coined by Rivest for rotations that are data independent[33]. It posses Feistel structure and can work well as lightweight algorithm as it is used in wireless sensor scenarios. RC5 is considered as w/r/b, where w refers to word size, r stands for number of working rounds, and b will tell about the number of bytes in encryption key. RC5 generally works on 32 bit size but its variants can be 16, 32, 64. It can work for 0, 1, .., 255 rounds using 0,1,..255 key bytes. Standard key size is 16 byte on 20 rounds of operation. RC5 is vulnerable to differential attack [34].

Based on literature review conducted, comparison of all aforementioned symmetric lightweight algorithms is made on the basis of code length, structure, number of rounds, key size, block size and attacks shown in Table .

Symmetric Algorithm	Code length	Structure	No. of rounds	Key Size	Block Size	Possible Attacks
AES	2606	SPN	10	128	128	Man-in-middle attack
Hight	5672	GFS	32	128	64	Saturation attack
TEA	1140	Feistel	32	128	64	Related Key Attack
PRESENT	936	SPN	32	80	64	Differential attack
RC5	Not foxed	ARX	20	16	32	Differential attack

V. SYMMETRIC LIGHTWEIGHT ALGORITHMS FOR IOT

RSA: It was invented by Ron Rivest, Adi Shamir and Leonard Adleman in 1978. RSA works on generating public and private key pair by selecting two large prime numbers[35]. Find their modulus and choosing at random their encryption key and thus calculating the decryption key. Public key is published openly whereas private key is made secure[36]. A more secure RSA encryption is proposed in[37] that is used to encrypt and decrypt files for maintaining privacy of user.

Elliptic Curve Cryptography (ECC): It requires less key size as compared to RSA. Hence it has fast processing and less storage requirements. It was invented by[38]. It s built on algebraic system where it takes two points on elliptic curve. Discrete logarithm problem is used to generate key that is used to compute key. In[39] a secure hardware implementation on ECC is proposed for small areas that will lead to faster computations in real time. ECC is optimized for 6LoWPAN nodes by working on its complex multiplication operation. Rather than using microprocessors operation for multiplication, bit shifting is used in[40-45] to optimize the use for low power devices. Differential: Change in input behavior will affect the output. So this attack is able to find the key from network transformations.

VI. ATTACKS ON EXISTING ALGORITHMS

Existing security solutions in IoT are still vulnerable to following attacks:

Denial of Service (DoS): It will halt the services of network for the authorized users due to access of network connection requests from unauthorized users.

Man-in-Middle: In this an intermediary user is able to get the key of one of the sides and will start communication as if it is the valid party.

Eavesdropping: Intruder is able to listen the communication between sender and receiver. So this is attack on confidentiality.

Masquerading: An intruder possess the identity of any other authorized user. So it can tear down the resources of IoT.

Saturation: In this intruder will try to use the physical and mental ability of authorized party by its immense use.

Differential: Change in input behavior will affect the output. So this attack is able to find the key from network transformations.

VII. RESEARCH CHALLENGES IN IOT

This study reveals number of challenges allied to IoT.

Lack of human intervention may lead to physical as well as logical attacks. IoT uses wireless communication that is vulnerable to number of attacks like eavesdropping, man-in-middle, Denial of Service (DoS) and many more. Any device can connect to the network so that may cause unauthorized access to the network. IoT devices are resource constrained in terms of power and bandwidth so exercising intricate security solutions can hinder the efficient working of devices. So challenges can be things related or network related. Challenges concerning things are power limitation, heterogeneous platforms, and security and privacy[55]. Network related issues are scalability, bandwidth issues, and security and privacy.

VIII. RESEARCH PROBLEM

Now-a-days IoT is admitting in homes, work places, social places or in business firms that will open doors for security and privacy challenges. So, security and privacy issues are becoming major reasons of concern in operation of IoT. The amount of loss that can occur is prominent to imagine if any attack is injected in IoT. Various attacks on IoT exist like eavesdropping, spoofing, Denial of Service (DoS), replay attacks, false signals injection[51-54]. These attacks will tear down the security services of IoT like confidentiality, integrity, and authentication; moreover, it will impact the privacy of users. IoT provides inbuilt primitive security solutions at each layer, which are still vulnerable to attacks. Traditional cryptography and authentication schemes do not fit well in IoT scenario due to its constrained resources like power, real time execution. So, lightweight cryptography solutions tend to work well in IoT. Number of lightweight Symmetric and Asymmetric cryptography algorithms exists in literature like AES, HIGHT, RC5, PRESENT, RSA, ECC and many more. These existing solutions do not guarantee an optimum level of security in real time communication due to more execution time, code length, and memory requirements. Execution time includes time for key management and distribution, encryption and decryption that decides the effectiveness of the protocol[46]. Asymmetric algorithms are slow due to their large key size, whereas symmetric algorithms can provide only confidentiality and integrity but no authentication leading to attack on availability. This can affect real time information collecting and processing and will fritter away the resources of IoT. This calls for a secure algorithm for IoT that will guarantee services like confidentially, integrity and authentication in optimal time.

IX. PROPOSED IDEA

On the basis of literature survey carried out many researchers have proposed lightweight symmetric and asymmetric security algorithms for IoT. Symmetric algorithms provide confidentiality, integrity, have small key size, and are less complex but they do not offer authenticity and distribution of keys in them is a challenging task[50]. On the other hand, asymmetric algorithms provide confidentiality, integrity, and authenticity, but their key size is too large which make them more complex and not apt for constrained IoT scenario. So, there is a need of secure algorithm that will map best features of lightweight symmetric and asymmetric algorithms[56] in such a way that it will take less execution time with optimum energy requirements and will assure all security services like confidentiality, integrity and authenticity.

X. CONCLUSION

IoT faces number of challenges like power, bandwidth, scalability, heterogeneity, security and privacy. Security and privacy is the most imperative challenge to solve to maintain the trust of users in IoT[49]. Pre defined security solutions at each layer are still susceptible to attacks. So cryptography algorithms can be used to assure security. But traditional heavy weight algorithms are not apt for IoT due to their constrained environment. Hence, alternate lightweight cryptography solutions symmetric as well as asymmetric can be used.

REFERENCES

1. D. Singh, G. Tripathi, and A.J. Jara. "A survey of Internet-of-things: Future vision, architecture, challenges and services." In Internet of Things (WF-IoT), 2014 IEEE World Forum on, pp. 287-292. IEEE, 2014.
2. Johnson, L.; Adams, S.; Cummins, M. NMC Horizon Report: 2012 Higher Education Edition; Impacts of Current and Future Technologies on Higher Edudation; The New Media Consortium (NMC): Austin, TX, USA, 2012; ISBN 978-0-9846601-3-1. Available online: http://www.nmc.org/pdf/2012-horizon-report-HE.pdf (accessed on 27 July 2018)
3. JYang Lu. Li Da Xu*IEEE IoT Journal* Sep 2018. Biologically Inspired Resource Allocation for Network Slices in 5G-Enabled Internet of Things
4. Hochschule Aalen. Internet of Things. Available online: https://www.hs-aalen.de/en/courses/66/info (accessed on 27 July 2018).
5. S. Lanzisera et al., “Communicating power supplies: Bringing the internet to the ubiquitous energy gateways of electronic devices,” IEEE Internet Things J., vol. 1, no. 2, pp. 153–160, Apr. 2014.
6. Dezhgir, Hamid, And Haniyeh Hooshmand.*"Security On The Internet Of Things."* (2017).
7. Holler, J.; Tsiatsis, V.; Mulligan, C.; Karnouskos, S.; Boyle, D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, 1st ed.; Academic Press Ltd.: London, UK, 10 April 2014.

9. Evans, D. The Internet of Things: How the Next Evolution of the Internet Is Changing Everything; White Paper 2011; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA,2011.Available online: http://www.cisco.com /web /about/ac79 /docs/innov/IoT_IBSG_0411 FINAL.pdf (accessed on 27 July 2018).
10. Borja Martinez ;MàriusMontón ; IgnasiVilajosana ; Joan Daniel PradesIEEE Sensors Journal (Volume: 15 , Issue: 10 , Oct. 2015)
11. Teich, P. Segmenting the Internet of Things (IoT); White Paper 2014; Moor Insights & Strategy: Austin, TX, USA, 2014. Available online: http://www.moorinsightsstrategy.com/wp-content/uploads/2014/05/Segmentingthe-Internet-of-Things-IoT-by-Moor-Insights-and-Strategy.pdf (accessed on 27 July 2018).
12. Scully, P. The Top 10 IoT Segments in 2018—Based on 1,600 Real IoT Projects. IoT Analytics: Market Insights for the Internet of Things, February 2018. Available online: https://iot-analytics.com/top-10-iot-segments2018-real-iot-projects/# (accessed on 27 July 2018).
13. Weissberger, A. TiECon 2014 Summary-Part 1: Qualcomm Keynote & IoT Track Overview. IEEE ComSoc, May 2014. Available online: https://community.comsoc.org/blogs/alanweissberger/tiecon-2014-summarypart-1-qualcomm-keynote-iot-track-overview (accessed on 27 July 2018).
14. Evans, D. The Internet of Everything: How More Relevant and Valuable Connections Will Change the World; White Paper 2012; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2012. Available online: https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf (accessed on 27 July 2018).
15. Darwish, D. (2015) "Improved Layered Architecture for Internet of Things." International Journal of Computing Academic Research (IJCAR), 4(4):214-223.
16. Evans, D. How the Internet of Everything Will Change the World. Cisco Blog, November 2012. Available online: http://blogs.cisco.com/news/how-the-internet-of-everything-will-change-the-worldforthe-better-infographic/ (accessed on 27 July 2018).
17. Bradley, J.; Barbier, J.; Handler, D. Embracing the Internet of Everything to Capture Your Share of $14.4 Trillion: More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience; White Paper 2013; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2013. Available online: http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf (accessed on 27 July 2018).
18. Mahoney, J.; LeHong, H. Innovation Insight: The 'Internet of Everything' Innovation Will Transform Business; Research Report 2012; Gartner, Inc.: Stamford, CT, USA, 2012. Available online: https://www.gartner.com/ doc/1886915/innovation-insight-internet-everything-innovation (accessed on 27 July 2018).
19. EOT Coin. IoT Needs EOT. Available online: https://eotcoin.org/ (accessed on 27 July 2018).
20. Bradley, J.; Reberger, C.; Dixit, A.; Gupta, V.; Macaulay, J. Internet of Everything (IoE): Top 10 Insights from Cisco's IoE Value at Stake Analysis for the Public Sector; Economic Analysis 2013; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2013. Available online: http://www.cisco. com/web/about/ac79/docs/IoE/IoE-VAS_Public-Sector_Top-10-Insights.pdf (accessed on 27 July 2018).
21. Miraz, M.H.; Khan, S.; Bhuiyan, M.; Excell, P. Mobile Academy: A Ubiquitous Mobile Learning (mLearning) Platform. In Proceedings of the International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance (IC5E 2014), London, UK, 30–31 July 2014; pp. 89–95.
22. G. Peretti, V. Lakkundi, M. Zorzi, "BlinkToSCoAP: An End-to-End Security Framework for the Internet of Things." (2015).
23. X. F. Wang, "Research on Security Issues of the Internet of Things." In Advanced Materials Research, vol. 989, pp. 4261-4264. 2014.
24. Z. Xu, Y. Yin, and J. Wang, "A density-based energy-efficient clustering algorithm for wireless sensor networks." International Journal of Future Generation Communication and Networking 6, no. 1 (2013): 75-86.
25. Khan, S.; Shayokh, M.A.; Miraz, M.H.; Bhuiyan, M. A Framework for Android Based Shopping Mall Applications. In Proceedings of the International Conference on eBusiness, eCommerce, eManagement, eLearning and eGovernance, London, UK, 30–31 July 2014; pp. 27–32..
26. Bradley, J.; Loucks, J.; Macaulay, J.; Noronha, A. Internet of Everything (IoE) Value Index: How Much Value Are Private-Sector Firms Capturing from IoE in 2013? White Paper 2013; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2013. Available online: https://www.cisco.com/c/dam/en_ us/about/business-insights/docs/ioe-value-index-whitepaper.pdf (accessed on 27 July 2018).
27. Soomro, S.; Miraz, M.H.; Prasanth, A.; Abdulla, M. Artificial Intelligence Enabled IoT: Traffic Congestion Reduction in Smart Cities. In Proceedings of the IET 2018 Smart Cities Symposium (SCS '18), Zallaq, Bahrain, 22–23 April 2018; pp. 81–86.
28. Alansari, Z.; Anuar, N.B.; Kamsin, A.; Soomro, S.; Belgaum, M.R.; Miraz, M.H.; Alshaer, J. Challenges of Internet of Things and Big Data Integration. In Proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London, UK, 23–24 August 2018.
29. Derbez P, Fouque PA. Exhausting demirci-seluk meet-in-the-middle attacks against reduced-round AES. International Workshop on Fast Software Encryption; 2014. p. 541–60.
30. Mitchell, S.; Villa, N.; Stewart-Weeks, M.; Lange, A. The Internet of Everything for Cities: Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities; White Paper 2013; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2013. Available online: http://www.cisco.com/ web/strategy/docs/gov/everything-for-cities.pdf (accessed on 27 July 2018)
31. Lee J, Lim D. Parallel architecture for high-speed block cipher, HIGHT. International Journal of Security and its Applications. 2014; 8(2):59–66.
32. Chaudhry, J.; Qidwai, U.; Miraz, M.H.; Ibrahim, A.; Valli, C. Data Security among ISO/IEEE 11073 Compliant Personal Healthcare Devices through Statistical Fingerprinting. In Proceedings of the 9th IEEE-GCC Conference and Exhibition 2017, Manama, Bahrain, 9–11 May 2017; pp. 319–324.

33. Barbier, J.; Bhatia, P.K.; Kapoor, D. Internet of Everything in ASEAN: Driving Value and Opportunity in Oil and Gas, Utilities, and Transportation; White Paper 2014; Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc.: San Jose, CA, USA, 2014. Available online: http://www.cisco.com/web/about/ac79/docs/IoE/IoE-in-ASEAN.pdf (accessed on 27 July 2018).
34. Evans, D. Ask the Futurist: "How Will the Internet of Everything Impact Teachers' Roles in the Connected Classroom?", 12 September 2013. Available online: http://blogs.cisco.com/ioe/connected-classroom/ (accessed on 27 July 2018)
35. Ali, N.A.; Abu-Elkheir, M. Internet of Nano-Things Healthcare Applications: Requirements, Opportunities, and Challenges. Proceedings of 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob' 2015), Abu Dhabi, UAE, 19–21 October 2015.
36. Nyberg K. Links between Truncated Differential and Multidimensional Linear Properties of Block Ciphers and Underlying Attack Complexities. 2015. p. 165-85.
37. Akyildiz, I.F.; Pierobon, M.; Balasubramaniam, S.; Koucheryavy, Y. The Internet of Bio-Nano Things. IEEE Commun. Mag. 2015, 53, 32–40. [CrossRef]
38. Kalyani, V.L.; Sharma, D. IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication. J. Manag. Eng. Inf. Technol. 2015, 2, 17–23.
39. Loughran, J. Graphene radios could unlock 'Internet of Nano-Things'. Engineering and Techbology (E&T), November 2016. Available online: https://eandt.theiet.org/content/articles /2016/11/graphene-radioscould-unlock-internet-of-nano-things/ (accessed on 27 July 2018).
40. Sheikh Ferdoush, Xinrong Li "Wireless Sensor Network System Design using Raspberry Pi and Arduino for Environmental Monitoring Applications", Elsevier The 9th International Conference on Future Networks and Communications (FNC-2014)
41. Gartner. Research Methodologies: Gartner Hype Cycle. Available online: http://www.gartner.com/ technology /research/ methodologies/hype-cycle.jsp (accessed on 27 July 2018).
42. Gil Press. It's Official: The Internet of Things Takes over Big Data as The Most Hyped Technology. Forbes, August 2014. Available online: http://www.forbes.com/sites/gilpress/2014/08/18/its-official-theinternet-of-things-takes-over-big-data-as-the-most-hyped-technology/ (accessed on 27 July 2018)
43. 2. Gartner. Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor. Available online: http://www.gartner.com/newsroom/id/3114217 (accessed on 27 July 2018).
44. Lee, S.W.; Prenzel, O.; Bien, Z. Applying Human Learning Principles to User-Centered IoT Systems. Computer 2015, 46, 46–52
45. Hodges, S.; Taylor, S.; Villar, N.; Scott, J.; Bial, D.; Fischer, P.T. Prototyping Connected Devices for the Internet of Things. Computer 2013, 46, 26–34. [CrossRef]
46. Ferati, M.; Kurti, A.; Vogel, B.; Raufi, B. Augmenting Requirements Gathering for People with Special Needs Using IoT: A Position Paper. In Proceedings of the 9th International Workshop on Cooperative and Human Aspects of Software Engineering (CHASE '16), Austin, TX, USA, 14–16 May 2016; pp. 48–51.
47. Kim I, Back M, Yim H, Lee K. RFID adaptor for detecting and handling data events in Internet of Things. Indian Journal of Science and Technology. 2015; 8(5):140-8.
48. Bojanova I, Hurlburt G, Voas J. Imagineering an Internet of Anything. Computer (Long Beach Calif). 2014; 47(6):72–7.
49. Cooper, J.; James, A. Challenges for Database Management in the Internet of Things. IETE Tech. Rev. 2014, 26, 320–329. [CrossRef]
50. Dell EMC. The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things; EMC Digital Universe with Research & Analysis by IDC April 2014; Dell EMC: Hopkinton, MA, USA, 2014. Available online: https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm (accessed on 27 July 2018).
51. Marvin, R. The 5 Worst Hacks and Breaches of 2016 and What They Mean for 2017. PC Magazine, January 2017. Available online: https://www.pcmag.com/article/350793/the-5-worst-hacks-and-breachesof-2016-and-what-they-mean-fo (accessed on 27 July 2018).
52. Rahman, A.; Ali, M. Analysis and Evaluation of Wireless Networks by Implementation of Test Security Keys. In Proceedings of the International Conference on Emerging Technologies in Computing 2018 (iCETiC '18), London, UK, 23–24 August 2018
53. IEC. Internet of Things: Wireless Sensor Networks; White Paper 2014; International Electrotechnical Commission (IEC): Geneva, Switzerland, 2014. Available online: http://www.iec.ch/whitepaper/pdf/iecWP-internetofthings-LR-en.pdf (accessed on 27 July 2018).
54. A. M. Ortiz et al., "The cluster between Internet of Things and social networks: Review and research challenges," IEEE Internet Things J., vol. 1, no. 3, pp. 206–215, Jun. 2014.
55. Wollschlaeger, M.; Sauter, T.; Jasperneite, J. The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0. IEEE Ind. Electr. Mag. 2017, 11, 17–27. [CrossRef]
56. Miraz, M.H.; Ali, M.; Excell, P.; Picking, R. A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In Proceedings of the Fifth International IEEE Conference on Internet Technologies and Applications (ITA 15), Wrexham, UK, 8–11 September 2015; pp. 219–224
57. Kortuem, G.; Bandara, A.; Smith, N.; Richards, M.; Petre, M. Educating the Internet-of-Things Generation. Computer 2013, 46, 53–61. [CrossRef]