International Journal of Computer Science & Communication (ISSN: 0973-7391)
Special Issue, Page80-83, December 2020 ------ available at www.csjournals.com

Security Consideration in Energy Efficient Resource Constrained Device Environments

RASHMI H C [1] Dr.C D GURUPRAKASH[2]
[1]Assistant professor, Dept. of ISE, Sri Siddhartha Institute of Technology, Tumakuru
[2] Professor, Dept. of CSE, Sri Siddhartha Institute of Technology, Tumakuru

Abstract: IoT is the cutting edge technology. IoT brings a new revolution in this new era. As internet plays major role in connecting people as well as things made humans life more comfort. As the usage of IoT devices increased there is a notch need for security as for the device data is concerned. The legacy techniques will not survive to meet the security needs for the IoT devices, which works under very constrained environments. In this paper survey has been done on various techniques to give better security for IoT devices. Survey focused mainly on light weight cryptographic techniques which provide privacy for IoT data in constrained environments. And new methodologies also discussed to bring better security which may help in trusting IoT devices and their functionalities.

Keywords: IoT device, security, cryptography

I. INTRODUCTION

Internet of things plays vital role in connecting vast number of smart devices across the world. Which helps in accumulation and distribution of data. And led to evolution in the field of internet [1]. And these devices are capable of communicating themselves without human intervention and internet plays a vital role in connecting these devices. Billions of IoT devices connected each other [2]. The IoT devices involved in all areas such as smart home, smart traffic control, office automation, in agriculture and production management and so on.

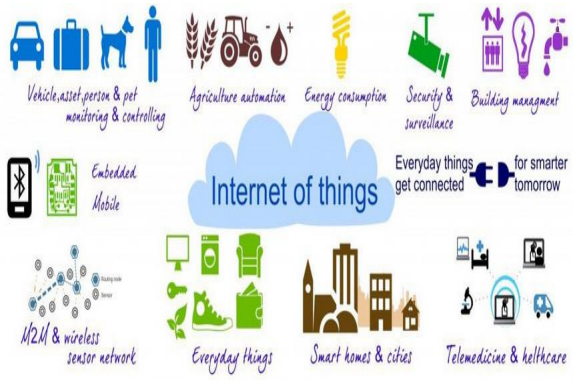

Fig 1: Areas of IoT use.

As the number of IoT devices increasing day by day, security is the main challenge because device data may prone to vulnerable attacks. Because the data generated by these devices is enormous. And the graph of connected devices through IoT increasing day by day [3].

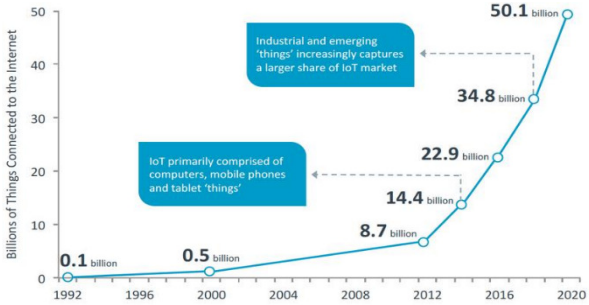

Fig 2: Increse in Connected device

The data may prone to attack and may get hamper the security also. This may results in lower to higher level of degradation of device performance and is a major drawback in the technology. To overcome these limitations there are many techniques of cryptography has been used since from ages.

But the legacy cryptography techniques are not suitable for the new era smart devices [4]. Because they works under very constrained environments, in terms of memory, processing power bandwidth and so on. So, there is a dire need of security algorithm which works under constrained environments. Day by day IoT smart devices are still able to work with very least constrained environments. To deal with this, still a better algorithm required when compared to the previously designed cryptographic algorithms. Light weight cryptography considered as an alternative solution by NIST [5] for energy constrained devices in IoT. Here we focused on various techniques which applied previously to overcome security challenges for device data. And observations made on each of these to enlighten on various problems concerned to security, and existing solutions and probability of research challenges and trends.

II. VARIOUS ATTACKS ON ENERGY CONSTRAINED DEVICES

Since many IoT devices communicate each other the delivery of device data may get expose during communication with other entities and it is a non-avoidable situation. Hence, the attackers attack in many ways. In [22], many attacks has been discussed.

International Journal of Computer Science & Communication (ISSN: 0973-7391)
Special Issue, Page80-83, December 2020 ------ available at www.csjournals.com

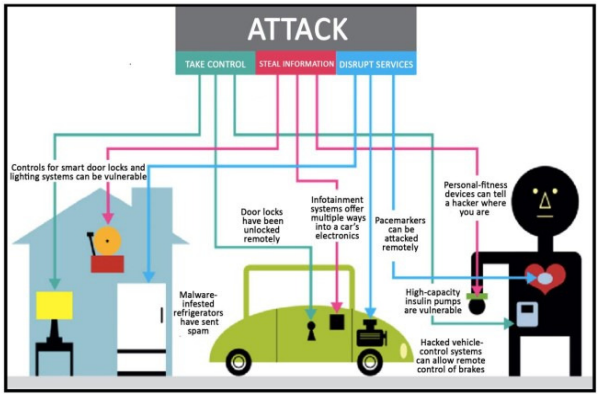

Fig 3: various Attacks on IoT devices.

1. Having control on data: The attacker may take over the control on data and this may categorized into passive and active attacks. Passive attack involves just knowing the information and active attack involves altering the data. Many kinds of active attacks are as follows:

- Eavesdropping: here the communication patterns observed and may hamper the data.
- Impersonating: here the secrete data of the user get extracted.
- DoS: these attacks caused by sending repeated requests and it may confuse the user.

2. Information stealing: here the attacker alters the data and it may get misused by attacker.
mparison with respect to memory requirement is discussed.

III. TECHNIQUES FOR SECURITY IN RESOURCE CONSTRAINED DEVICES

A. *Optimization*

Here we focus on techniques for minimizing space and power utility of algorithms in cryptography. Multiplexer and control unit plays major role in choosing byte to process it. Space can be minimized by minimizing the number of flip flops or the registers used. Control unit can also manage memory by replacing the multiplexers by shifters.

B. *Design Libraries*

Another technique is to make use of design libraries, which includes multipliers, adders, memory compilers which eases to work under constrained environments.

For algorithm level optimization, S-box features can be altered.

IV. ALGORITHMS AND HASH FUNCTIONS

C. *AES algorithm*

In [6] proposed Advanced encryption standard (MAES) which is a light weight version of the AES algorithm. A new 1D S-Box has been introduced and square matrix in the affine transformation phase has been formulated which is suitable in energy constrained environments since it consumes less energy

- Spoofing attack: here the attacker may fakes the sender of data and it may get exposed for non-intended use.
- Sybil attack: here the attacker may present at different locations at the same time.
- Message replay: the attacker alters the message and send to the IoT devices. It may confuse the user.
- Man in the middle attack: the attacker eavesdrops the channel of communication and may replace the request for authentication.

Hence the IoT device and its data may undergo different types of attacks during its communication after sensing data, providing security is the main aspect, otherwise it may hamper the security and performance of the device. Many legacy techniques have been proposed to overcome these attacks. But their processing requirements are more. It may not suitable for the energy constrained environments. Therefore the following section of the paper focuses on different techniques to deal with security aspects of energy constrained devices. First the optimization techniques has been discussed, then various traditional algorithms has been discussed and their inefficiency in handling the IoT device security also noticed. Next, block cipher and stream cipher techniques along with hash function has been discussed. Then, it is followed by various hardware and software implementation factors to be considered in the aspect of security is discussed. And finally hash algorithm co

during packet transformations. Still the algorithm faces challenges in security needs and complexity in space.

D. *Block cipher*

Many existing block ciphers handles the performance issues of light weight block ciphers, and these are RC-5 [7], AES-128 [8], TEA [9] and XTEA [10]. And further to improve their performance block cipher has been simplified and complexity reduced. DESL [11], SPEC [12] and SIMON.

E. *Expected features in block cipher*

According to [13] the block cipher should possess the following features to provide the better security in IoT devices.

- Plain text should have reduced block size. Such as instead of having 256 bits 64 bits can be used as an alternate.
- Battery life of IoT device is a main constraint hence the key length of block cipher should be reduced as much as possible as in [14] and [15].
- The number of rounds involved in S box should be reduced as it consumes less resources as described in [16].
- Mini key generation algorithm in block cipher should consider complex keys rather than easier keys, which should fit well with resource constraints of the device.

F. *Stream cipher considerations*

As stream cipher deal with the data which is of streaming type it is best option to use it in energy constrained applications. Work in [17] describes the stream ciphers

suitable as stated by European Network of Excellence for Cryptology.

G. *Applying hash function*

Hash function involves complex computations as it makes the cipher text stronger as it should not breakable easily. Naturally, this utilizes much energy during the coding process. To deal with this hash function should designed such that to be suitable for energy constrained devices [19].

V. FACTORS RELATED TO SOFTWARE AND HARDWARE IMPLEMENTATIONS

H. *Hardware*

Less Gate equivalents play a major role in hardware implementations. Less processing capability processors, with minimum space and energy consumptions are the factors which is unreachable out of traditional cryptographic algorithms. [20]. Latency delay may happen if execution time is more [21]. Design libraries are the main considerations to provide these features.

I. *Software*

Symmetric and Asymmetric ciphers [21] can be clubbed to get better software implementation as they may concentrate on reduced block ciphers and key sizes and number of rounds during the implementation of code on resource constrained devices [20].

J. *Comparision of different hash algorithms*

Various traditional cryptographic algorithms have been analyzed in [21]. The work focused on comparison of symmetric, asymmetric and hashing techniques fig. 1

Algorithm	Output size (bits)	Block Size	Max message size (bits)	Word size(bits)
MD5	128	512	264 - 1	32
SHA-0	160	512	264 - 1	32
SHA-1	160	512	264 - 1	32
SHA-2	224,256	512	264 - 1	32
SHA-3	384,512, 224,256	512	2128 - 1	6

Fig 4: Comparision of Secured Hash Algorithms

VI. CONCLUSION

IoT plays major role in our life. As there is a drastic increase in number of IoT devices involved in many automation process there is a big challenge to manage security also. Since there is lot of communication involves in these devices the device may undergo various types of security attacks. In this regard this paper focus on analyzing various techniques available traditionally to safeguard the devices generated data. At the same time it has been noticed that the traditional techniques are not suitable for the energy constrained devices to provide better security. Hence there is a dire need of better security techniques to be get followed in both hardware and software level implementations. For example, for multiplication operations bits shifting is preferable rather than microprocessor operations. And instead of focusing on only symmetric techniques both the symmetric and asymmetric techniques can be used at the same time to provide better security, also hash functions can be designed in still more efficiently to provide better security.

REFERENCES

[1] C. Maxim, et al, “Internet of Things (IoT): Research, Simulators, and Testbeds”. IEEE Internet of Things Journal , 2018, vol. 5, no 3, pp. 1637-1647.

[2] L. In, and K. Lee, “The internet of things: investments, Applications and challenges for enterprises”. Business Horizons, vol. 58, no. 4, 2015, pp. 431-440.

[3] M. Radovan and B. Golub, "Trends in IoT security," 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, 2017, pp. 1302-1308, doi: 10.23919/MIPRO.2017.7973624.

[4] B. Padmavathi, et al, “performance analysis of AES, RSA and DES algoirithm with LSB substution”. IJSR, India, 2013.

[5] M. Kerry, et al, Repoert on lightweight cryeptography. NISITIR, pp 1-28, 2017.

[6] A. R. Chowdhury, J. Mahmud, A. R. M. Kamal and M. A. Hamid, "MAES: Modified advanced encryption standard for resource constraint environments," 2018 IEEE Sensors Applications Symposium (SAS), Seoul, 2018, pp. 1-6, doi: 10.1109/SAS.2018.8336747.

[7] R. L. Ronald, “The RC5 encryption algorithm”. International Workshop on FSE, 1994, Springer, Berlin, pp. 86-96.

[8] I. Kengo, et al, “Analysis on equivalent in current source of AES128 circuits for HD power in model verification”. International Symposium on EMC’14, Tokyo, IEEE, 2014, pp. 302-305.

[9] W. J. David, et al, “TEA, an encryption algorithm”. International Workshop on FSE, Springer, Berlin, pp. 363–366, 1994.

[10] Y. Jack, et al, “Xtea encryption-based novel RFIDsecurity protocol”. 24th CCECE, 2011, IEEE, pp. 58-62.

[11] L. Gregor, et al, “New lightweight DES variants”. International Workshop on FSE, Springer, Berlin, pp 196-210, 2007.

[12] B. Ray, et al, “The SPECK and SIMON lightweight block ciphers”. 52nd ACM/EDAC/IEEE, IEEE, 2015, Design Automation Conference (DAC), pp 1-6.

[13] “Lightweight block ciphers”. Université du Luxembourg. https://www.cryptolux.org/index.php/Lightweight_Block_Ciphers. Accessed 22 July 2019.

[14] B. Andrey, et al, “PRESENT: an ultralightweight block cipher”. International CHES Workshop, Springer, pp. 450-466, 2007.

[15] H. Jaber, et al, “A comprehensive survey on evaluation lightweight symmetric ciphers: software and hardware implementation”.Advances in Computer Science: International Journal, 2016, vol. 5, no 4, pp. 31-41.

[16] M. Bassam J, et al, “A survey lightweight block ciphers for low resources devices: a comparative study & open

issues". Journal of Network and Computer Applications, 2015, vol. 58, p. 73-93.

[17] D.Dumitru Daniel, "Secure and Efficient Implimentations of thee Lightweieght Symmitric Cryptogreaphic Primiteves". University of Luxembourg, 2017, pp. 278.

[18] S.Saurabh, et al, "Advanced lightweight and encryption algorithms in IoT devices: challenge, survey and solutions". Journal of Ambient Intelligence & Humanized Computing, 2017, pp. 1-18.

[19] J. Yogi, U, et al, "Modeling Simulation and Performance Analysis of Lightweight Cryptography for IOT-Security," 2018 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE), Jaipur, India, 2018, pp. 1-5, doi: 10.1109/ICRAIE.2018.8710387.

[20] S. Thapliyal, et al, "An Innovative Model for the Enhancement of IoT Device Using Lightweight Cryptography," 2019 Amity International Conference on Artificial Intelligence (AICAI), Dubai, United Arab Emirates, 2019, pp. 887-892, doi: 10.1109/ AICAI .2019.8701377.

[21] M. E. Haque, et al, "Performance Analysis of Cryptographic Algorithms for Selecting Better Utilization on Resource Constraint Devices," 2018 21st International Conference of Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 2018, pp. 1-6, doi: 10.1109/ICCITECHN.2018.8631957.

[22] Z. Mohammad et, al.,"Security Weaknesses and Attacks on the Internet of Things Applications," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 431-436, doi: 10.1109/JEEIT.2019.8717411.