iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55513

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

A Review on Cryptography in the Field of Internet of Things

Dr. Bhumika Charnanand[1], Chetan Rathod[2]
[1]*Department of Computer Science, School of Science & Technology, Vanita Vishram Women's University, Surat*
[2]*Research Scholar, Department of Computer Science, Saurashtra University, Rajkot*

Abstract: ***In this contemporary age of technological advancements, the expanse of IoT devices has permeated every facet of our surroundings. IoT has evolved into an indispensable component across various domains. The proliferation of IoT devices has inevitably brought forth concerns regarding the security of the data they produce. With the accumulation of exabytes of data from IoT devices, a pressing need for ensuring data security, particularly as it traverses the internet, has arisen. The consistent generation of substantial data by IoT devices on a daily basis further complicates the task of safeguarding this information. Cryptography emerges as a potent solution in addressing this challenge. By leveraging cryptographic techniques, it becomes feasible to establish a robust and effective layer of security within the realm of IoT. This study is primarily dedicated to the escalating presence of IoT devices and the role of cryptography in furnishing solutions for managing the data generated by these IoT devices.***

Keywords: Cryptography, Internet of Things, Security, Lightweight Algorithm, WSN,

I. INTRODUCTION

As the technology is touching its edge of height, everywhere and everything is influence by the technology. In this growth IoT (Internet of Things) plays a vital role. IoT is collection of the physical devices which can gather data from the environment and take action according to the requirement by transferring data on the internet. As IoT devices and Internet becoming more and more accessible to the world, number of end nodes in IoT devices are increasing so dramatically that causes many problems to the data and security. When data is transfer over the internet using the IoT devices there is less security of data. But now in today's world it becomes necessary to protect and secure that data over the internet.

As moving through more and more automation in every field, use of IoT devices is also increased dramatically. As per the data of year 2020, 54% devices out of 21.7 billion devices on internet are IoT devices. This number will increase and reach more than 30 billion by the year 2025[1]. With increasing of the devices, security concern also increased. For example in the projects of smart cities, all the controls are done by the devices. In year 2015 a cyber attack was done by a group in the Ukrainian residents and 230000 people suffered from no-supply of electricity as the target was an electric gride[2]. To protect domain of IoT encryption can play a vital role.

II. HOW TO USE ENCRYPTION IN INTERNET OF THINGS

As discussed, security becomes major concern in the field of IoT. One of the solution is to protect data transfer using proper encryption methodology. By using encryption, it becomes more secure to transfer even sensitive data over the internet by the IoT devices.

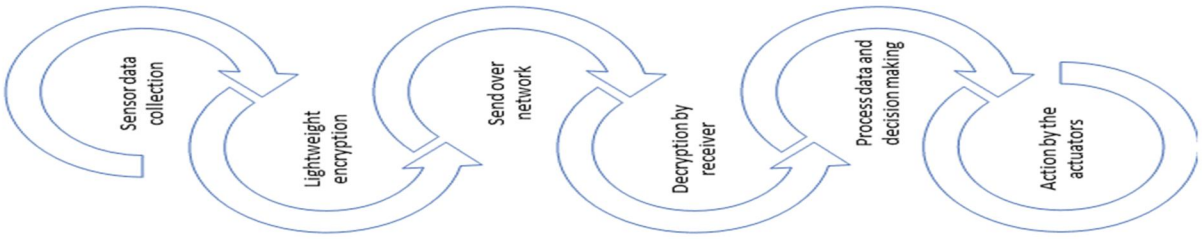


Figure 1: How to implement encryption in IoT devices.

©IJRASET: All Rights are Reserved

As show in above figure 1, data are collected by the sensors then in general data are directly transfer to the server or on the cloud over the internet. But here, encryption can help to secure those data. As data are generated by the sensors then data will encrypted by any lightweight encryption methodology and then the data will be send to the server or on cloud. As the receiver receive the data, it performs the decryption using a predefine key for each device, and do the further processing on the data and take a necessary decision. Then again this decision will transfer to the actuators (actuators are IoT device which convert electric signal into physical movement) and appropriate action will be taken.

III. CHALLENGES IN CRYPTOGRAPHY IN IOT

In the vast realm of the Internet of Things (IoT), ensuring the security of our interconnected devices is a paramount concern. One approach to safeguarding data is encryption, a technique that involves encoding information to make it unreadable to unauthorized users. However, applying encryption to IoT devices presents a unique set of challenges[3,4].

IoT devices are engineered to handle small, lightweight packets of data. These devices are optimized for efficiency and often lack the computational power required for executing complex encryption algorithms. This sets the stage for a conundrum: the traditional encryption methods that have proven effective for more powerful systems might not seamlessly translate to the realm of IoT.

Prominent encryption standards like AES, RSA, DES, Blowfish, and RC6, while highly effective in conventional contexts, struggle to adapt to the diverse and dynamic nature of IoT environments. IoT encompasses an array of devices operating in intricate networks, and these devices demand scalability, flexibility, and real-time responsiveness. Unfortunately, conventional encryption methods might not neatly align with these requirements, posing a formidable roadblock to their direct implementation within the IoT framework[5].

Furthermore, energy efficiency is a paramount consideration for IoT devices, which often rely on compact batteries or other limited power sources. Traditional encryption methods typically consume significant amounts of energy, primarily due to their computational complexity. For instance, the AES algorithm, which is widely recognized for its security prowess, demands a substantial memory footprint—approximately 2.9 kilobytes of flash memory and 1.2 kilobytes of RAM. While such requirements are feasible for larger systems, they are significantly burdensome for resource-constrained IoT devices[6,7].

Research indicates that many Wireless Sensor Network (WSN) sensor motes, which play a vital role in IoT networks, possess exceedingly restricted resources. These motes frequently operate with meager memory allocations, often as little as 2 kilobytes of Random Access Memory (RAM) and 1 kilobyte of Electrically Erasable Programmable Read-Only Memory (EEPROM). Consequently, deploying traditional encryption methods, which demand substantial computational resources, becomes an infeasible endeavor for these devices.

This necessitates the exploration and adoption of lightweight cryptography (LWC) algorithms tailored to the unique demands of IoT ecosystems. Lightweight cryptography is engineered to strike a delicate balance between security and resource efficiency. These algorithms are purpose-built for deployment on devices with limited computational capacities, ensuring that encryption can be implemented without overwhelming the device's capabilities.

In essence, the challenge lies in devising encryption methods that cater to the distinctive traits of IoT: lightweight, resource-constrained, scalable, and energy-efficient. The realm of IoT security calls for innovative cryptographic approaches that empower these devices to communicate securely while preserving their operational efficiency. The ongoing pursuit of such solutions underscores the dynamic nature of IoT's security landscape and the ongoing evolution of encryption methodologies.

IV. SECURING THE IOT SYSTEM

There are number of algorithms developed for securing the IoT devices. There are two broad categories of cryptography algorithms, symmetric and asymmetric. The symmetric lighted algorithms are of symmetric type of algorithms which are further divided into lightweighted block ciphers (LWBC), lightweighted stream cipher(LWSC). Elliptic curve cryptography (ECC) fall under asymmetric type of algorithm.

A. Lightweighted Block Cipher

Block cipher is a symmetric type of lightweighted algorithm which use block that can compute simultaneously. It uses into two different networks : SPN (Substitution-Permutation Network) and FN(Feistel Network). The FN is designed in such a manner that it can perform encryption and decryption using same code which ensure that less memory is required to perform the encryption and decryption of the valuable data[8]. Whereas SPN is designed in such a manner that use less execution for faster work but it result into venerability to the attack[9].

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

B. Lightweighted Stream Cipher

It is another kind of symmetric lightweighted algorithm. It perform encryption bit by bit rather then in blocks. It use LFSRs (Liner Feedback Shift Registers) and NLFSRs (Non-Liner Feedback Sheet Registers)[10]. Stream cipher requires fewer computations and are more quicker compare to the block cipher. Some famous stream ciphers are RC4, Salsa20, Trivium and Chacha. This are widely used in WSN (Wireless Sensor Network) and cell phones[10][11].

C. Lightweight elliptic curve cipher

It is asymmetric type of algorithm which ensures the authenticity and confidentiality of the data[12]. Asymmetric has large key size which make it more secure but for computing the large key it needs more memory and computation power so that it is less popular in the field of IoT. But the ECC can be use in the IoT network security. ECC use smaller key size compare to other asymmetric algorithms though it provide same level of security. So that ECC is now becoming more popular in the IoT devices to provide security.

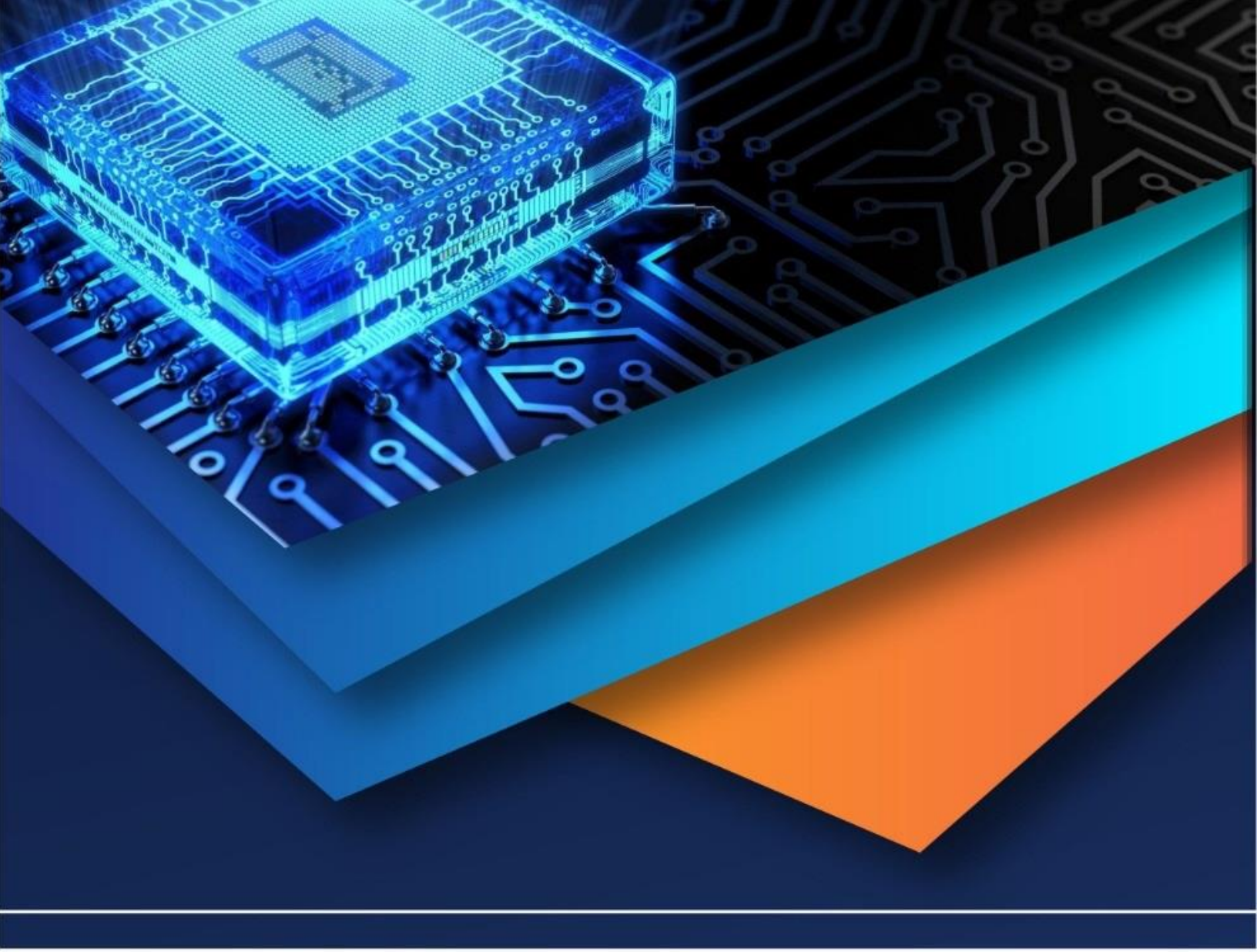
V. CONCLUSION

In the realm of IoT, the incorporation of cryptography encounters certain obstacles. While a selection of algorithms does offer commendable security for IoT systems, challenges persist. A notable requirement emerges for innovative algorithms that boast heightened speed, minimal memory usage, and the ability to safeguard the incessantly generated data stemming from IoT devices. In certain instances, IoT device boards must undergo enhancements to attain a capacity for executing the extended computations essential for cryptographic operations.

REFERENCES

[1] Web content available at : https://www.crowdstrike.com/cybersecurity-101/internet-of-things-iot-security/
[2] Cui L., Xie G., Qu Y., Gao L., Yang Y., Security and privacy in smart cities: Challenges and opportunities, IEEE Access, 6 (2018), pp. 46134-46145.
[3] Jiang X., Lora M., Chattopadhyay S. An experimental analysis of security vulnerabilities in industrial IoT devices ACM Trans. Internet Technol. (2020)
[4] Ahmed S.F., Islam M.R., Nath T.D., Ferdosi B.J., Hasan A.S.M.T. G-TBSA: A generalized lightweight security algorithm for IoT 2019 4th International Conference on Electrical Information and Communication Technology (EICT), IEEE (2020)
[5] Gunathilake N.A., Buchanan W.J., Asif R., Next generation lightweight cryptography for smart IoT devices: Implementation, challenges and applications, IEEE 5th World Forum on Internet of Things (WF-IoT), IEEE (2019)
[6] Sfar A.R., Natalizio E., Challal Y., Chtourou Z. A roadmap for security challenges in the Internet of Things Digit. Commun. Netw., 4 (2) (2018), pp. 118-137
[7] Hamzaab R., Yancd Z., Muhammade K., Bellavistaf P., Titouna F., A privacy-preserving cryptosystem for IoT E-healthcare, Inform. Sci., 527 (2020), pp. 493-510
[8] Kousalya R., Kumar G.A.S., A survey of light-weight cryptographic algorithm for information security and hardware efficiency in resource constrained devices, International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), IEEE (2019)
[9] Sumit Singh Dhanda B.S., Jindal Poonam, Lightweight cryptography: A solution to secure IoT, Wirel. Pers. Commun. (2020)
[10] Shantha M.J.R., Arockiam L., SAT_Jo: An enhanced lightweight block cipher for the internet of things, 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE (2019)
[11] R S.M.J., L A., Malarchelvi S.K., Security analysis of SAT_Jo lightweight block cipher for data security in healthcare IoT, ICCBDC 2019: Proceedings of the 2019 3rd International Conference on Cloud and Big Data Computing (2019), pp. 111-116
[12] Al-Turjmana F.M., Al-Fagihac A.E., Alsalihb W.M., Hassanein H.S., A delay-tolerant framework for integrated RSNs in IoT, Comput. Commun., 36 (9) (2013), pp. 998-1010

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)