Designing of Lightweight Security Scheme for IoT

Chandrakala Arya,
Asst. Professor, SOC (School of computing),
GEHU-Dehradun Campus

DOI: 10.48047/jcr.07.09.589

Abstract: Research and development is continuing to improve privacy for low-resource Internet of Things devices, and two examples are encrypted client-side and secure provisioning. Since conventional security methods need the use of resource-intensive cryptographic algorithms, they are often incompatible with the limited computing power of IoT devices. Therefore, developing new security schemes or adapting current ones as lightweight is a possibility for restricted IoT devices. In this paper, we introduce the Efficient Security Encryption Standard (ESS), an improved variant of the Advanced Encryption Standard (AES). Power-constrained IoT devices may use this technique to improve their security in areas like client-side encryption and secure provisioning, among others. Data produced by IoT devices should be secured on the client side before transmission to chosen cloud platforms, since cloud computing is the fundamental enabler for the mass provisioning of IoT devices. However, a significant difficulty still persists when attempting to satisfy several competing needs. Rapid computation

Keywords : Advanced Encryption Standard, Internet of Things (IoT), classical security algorithms, Lightweight algorithm

Introduction

The Internet of Things (IoT), or a network of connected things, is a technology topic that has recently transitioned from theoretical discussions to a realistic actualization, spanning multiple other technology topics including Low-power wide-area networks (WAN), handheld devices, embedded as well as prevalent communication, cloud computing, information analytics, and artificial intelligence [1]. This has made it possible to provide a myriad of new services, such as the gathering and analyzing of huge data sets from various sources. Between 20 and 50 billion IoT devices are expected to be in use by 2025, according to many studies [2, 3]. The rapid advancements that the IoT makes possible and encourages can be seen in almost every element of human life, and their economic ramifications are far-reaching. Its applications are discussed in [4], and they contribute to the rapid improvement of AI.With the advent of the Internet of Things, it will be possible for more "Things" than ever before to exchange data with one another. In the future, the IoT will have an impact on many other spheres, including but not limited to: business models [5-9], agricultural [10, 11], transportation [12-14], autonomous industrial processes [15-17], homes, infrastructure, security, trade standards, and many more. While the eventual widespread use of Internet of Things (IoT) technologies has many potential benefits, there are also many challenges that must be overcome, such as safety and privacy issues..

Security and privacy in the context of the Internet of Things (IoT) apply not only to the means by which the data generated and sent by IoT devices may be safeguarded, but also to the identities of users in the IoT ecosystem and the ethics of their use of the technology. New approaches are required to guarantee its safe and moral usage [09], yet extreme connection will bring about hitherto unimaginable levels of efficiency and economy. The writers of [10] recognize the importance of the IoT to the development of new mobile applications that enrich children's life and education. But they also note that kids are more likely to encounter inappropriate content like pornography, violence, and drugs on these applications. The Internet of Things (IoT) security problems are dissected and investigated in [12]. Node reputation, information surveillance, access control, terminal security, privacy, and the usage of diverse technology in the network are only a few examples of the kinds of challenges that might arise. Wireless network security architectures often start with the Open System Interconnection (OSI) paradigm. Presentation, Transport, Network, Datalink/MAC, and Physical layers make up the seven logical levels in this concept. Most modern security techniques, in an effort to address the security issues plaguing wireless communication, use a layered approach. However, in traditionally established networks, most devices are hardwired into place and get power from a central source, such as a wall outlet or a switch.

There was a good basis for developing robust encryption algorithms to guarantee the security of electronic communications between these devices because of their stable/continuous power supply and high (compared to ordinary IoT devices) computational capacity. The reality of secure communication based on these principles, however, has undergone a drastic upheaval with the introduction of the IoT. This is because the Internet of Things has made it possible to roll out low-power wide-area networks on a massive scale, leading to a proliferation of widely scattered, battery-operated devices with limited computational capabilities.

Security Challenges of the IoT

Classical cryptographic protocols and algorithms are used to secure traditional IT infrastructure, but these approaches are inefficient when used to IoT security since they were not developed with this kind of system in mind [12]. That's why, when it comes to protecting the interconnected devices that make up the IoT, we may either come up with brand-new schemes or adapt current security methods to better suit the limited resources of IoT devices. Traditional cryptographic approaches are inefficient when used to IoT security since they were not developed with these systems in mind. They proposed using hybrid lightweight models to enhance IoT security. The current algorithms may be improved by determining what parts of them are responsible for their high cost.New methods of cooperatively protecting against what would be called mixed wireless assaults will be of critical importance. In the past, communications security measures have focused on protecting particular protocol levels in isolation. Traditional layered security solutions, on the other hand, may be inefficient due to the increased processing cost and delay introduced by each tier of the protocol. Therefore, it is argued that it is necessary to handle security concerns at several layers of the IoT protocol architecture. The key exchange between the source and the destination is reported to typically be accomplished via the conventional Diffie-Hellman key agreement protocol, which calls for a trusted key management center. However, without a centralized server, managing the keys in certain types of wireless networks might be difficult. In light of this fact, while selecting a security strategy for restricted IoT devices, it is important to account for the limited power and processing capabilities of these devices. In light of these limitations and the reality that IoT devices are only one piece of a much bigger network, there is a pressing need for studies to create secure communication algorithms tailored to restricted IoT devices.

. Cloud Computing and IoT Provisioning

Cloud computing systems provide a variety of choices for storing and making use of data from IoT devices and installations, which may rapidly generate petabytes of data. More and more robust cloud infrastructure is being deployed as a result of cloud computing technologies in preparation for the massive connectivity that the Internet of Things will bring. Cloud service providers such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and The Things Networks (TTN) offer dependable cloud infrastructure to allow the broad deployment of the Internet of Things across many different use cases.

However, ensuring the safe use of the technology depends on the task of protecting the unprecedented number of devices being deployed in the IoT ecosystem. The vast majority of IoT gadgets are restricted devices, usually used for use cases including capturing/monitoring real-time circumstances and then transmitting the relevant data into secure cloud systems. The high price of encryption for IoT data and the need of ensuring secure transfer of information to the cloud make this a difficult situation to manage. In an era when the IoT requires innovative solutions for its usage, a significant security concern is the safe conveyance of data produced by these devices to a desired cloud platform. As noted in [39], delivering secure authentication to cloud systems is a challenge for cloud users. The situation is exacerbated by IoT devices' meager storage options, network speeds, and processing power. It is recommended that information be encrypted before being uploaded to a cloud service. The term for this kind of encryption is "client-side."

Literature Review

Vidya Rao et.al.,(2020) Connecting "factual-and-virtual" items located all over the world is what "makers-and-hackers" are interested in when they talk about the Internet of Things (IoT). The gadgets that make up the Internet of Things are capable of organizing and adapting themselves, and they use the public channel to exchange information. There is a risk of data and user privacy breaches in these conversations. Therefore, a hybrid authentication and data integrity approach based on elliptic curve cryptography is presented to give a lightweight crypto-solution. A client-server network built on Raspberry Pi 3 is used to conduct the experiment. The experimental results indicate that the suggested technique is faster than current ECDSA-based methods in both the signature and verification phases by a margin of 28.3–33.3% and 15.6%, respectively. Time savings of 11.73-5.45% and 7.11-5.63% have been seen while using cBLAKE2b for encryption and decryption, respectively.

Xi Luo et.al.,(2020) While IoT greatly improves people's quality of life in many ways, the absence of security practice increases the possibility of leaking of sensitive user data. Therefore, the ability to encrypt data transfer between IoT devices is essential in IoT settings like those seen in intelligent connected vehicles, smart homes, smart cities, and so on. However, the encrypted communication strategy is hindered by the restricted resources of low-cost IoT devices; even a little increase in CPU utilization of battery-powered sensors will drastically reduce the battery life. In this research, we offer a communication protocol that uses just a symmetric key-based strategy to encrypt data in transit; this approach is very lightweight while yet providing enough security. This protocol's symmetric keys are distributed using a chaotic system—the Logistic Map—to protect against key reinstallation and device theft. We use a semantic model to examine the safety features of such a protocol. In addition, the consumption of resources is measured to ensure optimal performance throughout execution.

Rohan A. Nathi et.al.,(2019) The intersection of the Internet of Things with computer science and embedded systems is generating considerable excitement. The importance of Security in the IoT cannot be overstated. Because of their limited capabilities, IoT devices pose a threat to the security of data transmission over the Internet. Security integration studies have focused heavily on IoT application layer protocols like CoAP and MQTT because of their superior suitability for low-overhead communication. The computation and handshaking technique used by TLS and DTLS, two popular protocols for ensuring network security, use a lot of bandwidth and other resources. In this research, we present a security method predicated on object (payload) security using a symmetric key approach, with CoAP serving as the transport protocol for complete message delivery.

Aishwarya Tripathi et.al.,(2018) IoT devices may now be connected to the cloud in an effortless manner thanks to the advent of cloud aided IoT. By adopting this new paradigm, even IoT devices with limited resources may take use of the cloud's scalable data storage options. However, it is difficult to meet the latency, bandwidth, scalability, and energy efficiency needs of disparate IoT devices while uploading data to the cloud. Therefore, fog computing was proposed as an interaction between the cloud and the IoT to solve these concerns. Data from Internet of Things (IoT) devices is gathered and sent to the cloud using a sophisticated, decentralized architecture known as fog computing. The security and privacy of data nevertheless remains a key problem, despite the fact that fog computing allows us to overcome some of the difficulties mentioned above. Here, using ElGamal encryption and an identity-based signature system, we present a safe lightweight data aggregation technique for cloud-assisted IoT devices. The security study demonstrates the safety of our suggested approach by ruling out the introduction of spoofed data and monitoring for data loss. The examination of performance confirms that our method is effective in comparison to other schemes currently in use.

An Improved Lightweight RFID Authentication Protocol for the IoT

One of the IoT's foundational technologies is Radio Frequency Identification (RFID), which has seen widespread development and implementation for current item automated identification. One of the most important ways to protect the privacy of your RFID data is via RFID authentication. Safe authentication procedures for RFID systems are discussed here. Here, we present a better lightweight anonymous authentication protocol for RFID systems utilizing the ECC algorithm to address the security, privacy, and efficiency issues associated with RFID technology in light of the growing security and privacy needs and the limited compute capacity of tags. Based on the results of the security study, it is clear that the suggested protocol successfully implements reciprocal authentication, secrecy, anonymity, and resistance to a wide range of attacks. The suggested protocol has been shown to be more efficient than existing RFID authentication methods, with a reduction in calculation cost of at least three times and a reduction in transmission cost of at least fifty percent. The Internet of Things benefits greatly from RFID's developed state of maturity. Information is kept electronically in the tags. The power for passive tags comes from the RFID reader's radio waves. Active tags may function at great distances from the RFID reader since they have their own power source (like a battery). RFID not only labels goods in lieu of bar codes, but also tracks their whereabouts and status in real time, providing crucial data. Retail, healthcare, facility management, supply chains, passports, etc. are just some of the useful areas where it has been implemented. One of the most important ways to protect the privacy of your RFID data is via RFID authentication. Figure 1 depicts the conventional architecture of an RFID system, which includes the RFID tag, the RFID reader, and the backend server. The system is predicated on the security of the reader's connection to the server in the background. However, there is a security risk in the link between the tag and the reader. Objects may be uniquely identified by attaching tags to them, which then retain that information. By emitting radio frequency (RF) signals, the reader may initiate interaction with the tag, allowing for data collection and transmission.

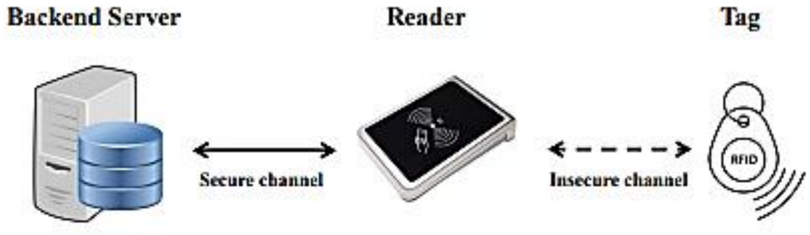


Figure 1: A typical RFID system

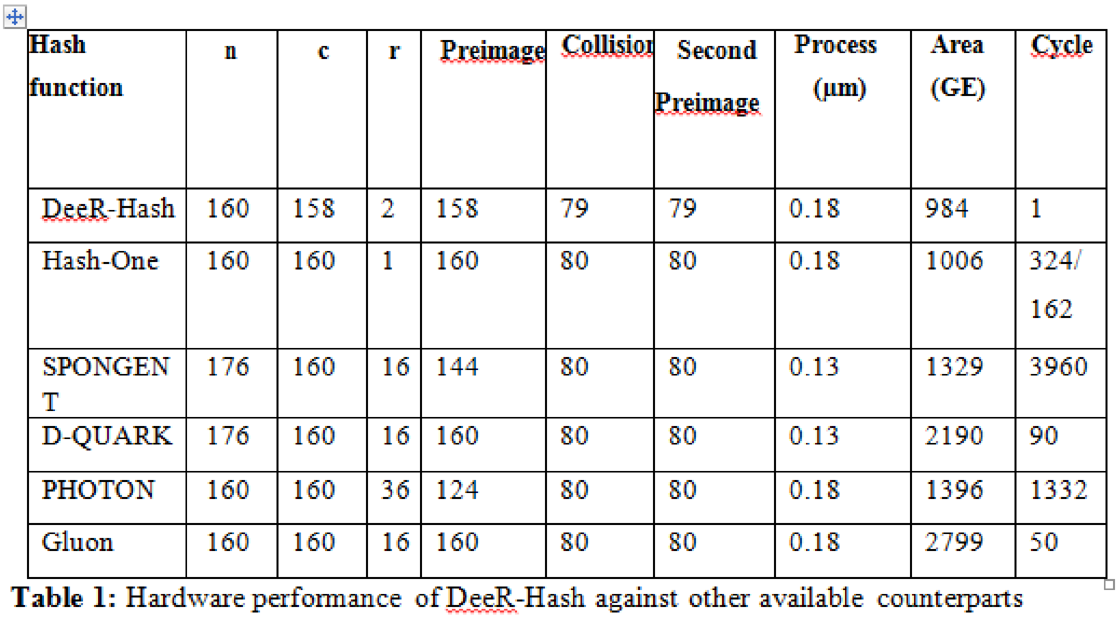
Lightweight Security System for Bank/ATM

The largest physical hazard that a bank or ATM faces today is someone breaking in without permission. Because of this, the Bank's executives have more job to do. We often hear reports of assaults on bank employees or vandalism of automated teller machines (ATMs). To avoid this, an automated system should be in place to record the information of anybody entering the Bank/ATM building who is not known to the person doing the entering. An identity verification system might be the answer Although numerous tools exist for this purpose, it might be difficult to find ones that work in a banking setting. A passbook, debit card, credit card, online account, and mobile app can all be available to a consumer in a typical situation.

Customers may be required to input a code (received through mobile device) before being granted access to the Bank/ATM. The unique identifier will be produced after their retinal image is successfully matched with their AADHAAR profile. The AADHAAR database was selected by the authors since participation is mandated. A nonce will be sent to the customer's verified cellphone number when the match is made. This code is required to unlock the bank/ATM gate. This whole procedure may be thought of as a two-way verification of the customer who is about to enter the Bank/ATM. When a customer enters a bank or uses an ATM, they will be able to see their full profile in the AADHAAR database. Instances of bank or ATM fraud will be easier to spot with this measure in place. In addition, if any of the Bank's genuine clients' cards have been stolen or cloned, the mismatch of nonce value will alert the Bank to the fact. A retinal scanner must be installed at the bank's front entrance or at the ATM. Customers may only enter the Bank/ATM using their registered mobile phone and the card they were issued. An attacker who has successfully cloned a card will be unable to get access to the ATM because he or she will lack the necessary nonce value. In addition, the technique may prevent the bank checks from being misused. Bank checks may have tiny ASIC chips inserted in them, which are activated when a scanner shines its light on the check. If the client is real, the chip will transmit a security code to their registered phone number. Only by entering the right code will the check be cancelled.

Hashing

In cryptography, hashing is a common practice employed as a protective layer over the original communication. This protection may be utilized while transmitting encryption or authentication keys. Since only the intended recipient will get the original key, this approach ensures that it cannot be stolen. Encryption will be applied to the key and hash value before transmission. The recipient will first do a full decryption of the message and then a hashing operation on the key. The key is considered legitimate if and only if the received hash value matches the calculated hash value. In this publication, the authors use a lightweight, but trustworthy and secure hashing mechanism: a sponge-based architecture. The hashing is safe against collision, pre image, and second pre image attacks because to the sponge design. A high degree of confusion is required in a cryptographic setting, and massage does this by absorbing all of the input bits in the update process. High levels of diffusion are provided by the state update process during the squeezing phase, which is also required in a cryptographic setting. The settings are optimized to maximize security while minimizing the impact on ASIC size and processing power.



Hash function	n	c	r	Preimage	Collision	Second Preimage	Process (µm)	Area (GE)	Cycle
DeeR-Hash	160	158	2	158	79	79	0.18	984	1
Hash-One	160	160	1	160	80	80	0.18	1006	324/ 162
SPONGENT	176	160	16	144	80	80	0.13	1329	3960
D-QUARK	176	160	16	160	80	80	0.13	2190	90
PHOTON	160	160	36	124	80	80	0.18	1396	1332
Gluon	160	160	16	160	80	80	0.18	2799	50

Table 1: Hardware performance of DeeR-Hash against other available counterparts

Result & Discussion

Here, we'll provide a performance study of the suggested security technique based on a 64-bits implementation. Due to the proposed framework's focus on 16-bit blocks, a simultaneous four-round key update mechanism is required for a 64-bit implementation. It takes a total of 18 GE on ASIC to smoothly execute the update functionalities of a single NLFSR. Since updating the NLFSR cannot occur in parallel, the 18 GE will expend all resources necessary to complete the procedure. A total of 80 GE is needed for a 16-bit NLFSR implementation. As a result, four serial NLFSR implementations will need 320 GE.

Input message and key, both 64 bits long, will be XORed together in parallel. It will call for 64 parallel XOR operations. Four 2-input NAND gates may, in theory, form the basis of a single XOR gate. Therefore, a total of 256 GE is needed to carry out this procedure. The total amount of GE needed for the proper functioning of this encryption/decryption module is 594, as calculated by adding the individual needs for 18 GE, 320 GE, and 256 GE. When compared to other lightweight encryption methods, this one again fares the best. Please be aware that the GE needs are not maximized. Applying optimization to digital circuits may further lower the needed GE count.

Sl. No.	Algorithm	Block Size	Key Size	Area Requirement
1	DeeR-Crypt	64	64	594
2	DESXL	64	184	2,168

3	PRESENT-80	64	80	1,000
4	KATAN	64	80	1,054
5	KTANTAN	64	80	688
6	GOST-PS	64	256	651
7	GOST-FB	64	256	800
8	Piccolo-80	64	80	683
9	Piccolo-128	64	128	818

Table 2. Comparison of lightweight encryption techniques

Security Analysis

Any system of exchanged information must place a premium on safety. There is no exemption for the lightweight cryptography environments. The authors go to considerable lengths to ensure the safety of their suggested low-weight and low-energy security solution. The suggested scheme's first module, called DeeR-Gen, handles all of the necessary security precautions right away. The mechanism will arbitrarily choose one of the four inputs. The likelihood of making the correct choice is one-quarter. Once again, DeeR-Gen's NLFSRs will choose an update function from a pool of 8. Because of this, picking 0.0039 will be the best option. As a result, no opponent is likely to ever get the proper nonce value.

DeeR-Hash's update mechanism is sufficiently secure that no malicious actor can recover the hash's seed. In the first stage, we'll choose at random one of eight options, with a 0.1250 chance of getting it right. After then, it's crucial to choose four people at random out of forty openings. The authors used an algorithm to choose one slot from among eight that were each separated into five categories. As a result, the likelihood of making the right choice will drop to 0.0002. The second array will undergo the exact identical process. This means the likelihood will be 0.0002 once again. There will be a 0.00000001 chance of picking correctly over time. Due to the low value, the authors are confident in the security of their suggested hashing method.

No third party can learn who is interacting with whom thanks to the secure nature of the mutual authentication protocol. The updates are also calculated independently at each end, and only XORed values are sent. Only the designated recipient will be able to access the necessary details. Each party generates its own unique key for use in the encryption module. Therefore, the encryption keys cannot be obtained by an opponent. Another layer of protection provided by the suggested method is that the update function is varied at each cycle. The authors can confidently declare that the suggested security system is both efficient and safe for usage in a cryptographic setting since it meets all of the criteria listed above.

Conclusion

Commonplace in the commercial sector, these security precautions were used in this job. The cost of computing power required to power such systems is substantial. Internet of Things devices have limited computing power, memory, and storage. Therefore, conventional safeguards are ineffective against the IoT. As a countermeasure, we propose relaxing the standards now in place for safety. Here, we'll go through three methods that we cut down on waste. The first is the persistent labeling of sensor output as normal or abnormal in order to discover anomalies. Using machine learning methods, we compile historical data to establish a boundary inside which most incoming numbers fall. This means that identifying abnormalities in real time does not require collecting massive amounts of sensor data. The second method employs concurrent and distributed computing to search for outliers using the Random Forest method. The third component is making cryptographic procedures less computationally intensive so that they may be employed in IoT environments without compromising security. We provide experimental results from each field to prove that our method works and can be used there.

References

1. V. Rao and P. K. V., "Lightweight Authentication and Data Encryption Scheme for IoT Applications," *2020 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Udupi, India, 2020, pp. 12-17, doi: 10.1109/DISCOVER50404.2020.9278048.
2. X. Luo *et al*., "A Lightweight Privacy-Preserving Communication Protocol for Heterogeneous IoT Environment," in *IEEE Access*, vol. 8, pp. 67192-67204, 2020, doi: 10.1109/ACCESS.2020.2978525.
3. R. A. Nathi and D. S. Sutar, "Embedded Payload Security Scheme using CoAP for IoT Device," *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*, Vellore, India, 2019, pp. 1-6, doi: 10.1109/ViTECoN.2019.8899549.
4. A. Tripathi and S. K. Pasupuleti, "A Secure Lightweight Data Aggregation scheme for Cloud assisted IoT," *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*, Solan, India, 2018, pp. 187-192, doi: 10.1109/PDGC.2018.8745850.
5. M. Shariat and M. Safkhani, "How the control over smart meters is lost in the Yan et al. lightweight AKA scheme for smart grids," *2017 9th International Conference on Information and Knowledge Technology (IKT)*, Tehran, Iran, 2017, pp. 82-84, doi: 10.1109/IKT.2017.8258622.
6. F. Djebbar and N. Abu-Ali, "Lightweight Noise Resilient Steganography Scheme for Internet of Things," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, 2017, pp. 1-6, doi: 10.1109/GLOCOM.2017.8255039.
7. M. Hossain and R. Hasan, "Boot-IoT: A Privacy-Aware Authentication Scheme for Secure Bootstrapping of IoT Nodes," *2017 IEEE International Congress on Internet of Things (ICIOT)*, Honolulu, HI, USA, 2017, pp. 1-8, doi: 10.1109/IEEE.ICIOT.2017.10.
8. M. T. Arafin, M. Gao and G. Qu, "VOLtA: Voltage over-scaling based lightweight authentication for IoT applications," *2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, Chiba, Japan, 2017, pp. 336-341, doi: 10.1109/ASPDAC.2017.7858345.
9. V. Odelu, A. K. Das, M. Khurram Khan, K. -K. R. Choo and M. Jo, "Expressive CP-ABE Scheme for Mobile Devices in IoT Satisfying Constant-Size Keys and Ciphertexts," in *IEEE Access*, vol. 5, pp. 3273-3283, 2017, doi: 10.1109/ACCESS.2017.2669940.

10. N. Li, D. Liu and S. Nepal, "Lightweight Mutual Authentication for IoT and Its Applications," in *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359-370, 1 Oct.-Dec. 2017, doi: 10.1109/TSUSC.2017.2716953.
11. T. Idriss, H. Idriss and M. Bayoumi, "A PUF-based paradigm for IoT security," *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, USA, 2016, pp. 700-705, doi: 10.1109/WF-IoT.2016.7845456.
12. M. Kumar, S. Kumar, R. Budhiraja, M. K. Das and S. Singh, "Lightweight Data Security Model for IoT Applications: A Dynamic Key Approach," *2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Chengdu, China, 2016, pp. 424-428, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.100.
13. T. K. Goyal and V. Sahula, "Lightweight security algorithm for low power IoT devices," *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, Jaipur, India, 2016, pp. 1725-1729, doi: 10.1109/ICACCI.2016.7732296.
14. S. Jebri, M. Abid and A. Bouallegue, "An efficient scheme for anonymous communication in IoT," *2015 11th International Conference on Information Assurance and Security (IAS)*, Marrakech, Morocco, 2015, pp. 7-12, doi: 10.1109/ISIAS.2015.7492763.
15. A. Mukherjee, "Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints," in *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747-1761, Oct. 2015, doi: 10.1109/JPROC.2015.2466548.