Chapter 18
Physical Unclonable Function (PUF)-Based Security in Internet of Things (IoT): Key Challenges and Solutions

Mohammed Saeed Alkatheiri, Abdur Rashid Sangi, and Satish Anamalamudi

Abstract Security protocols play a pivotal role in transmitting the sensitive application data through packet switched and circuit switched data communication. State-of-the-art research comes up with the constrained IoT design to provide the connectivity in between things without any human intervention. Hence, IoT becomes a promising solution to provide the end-to-end connectivity through constrained network resources. Physical Unclonable Function (PUF) is a digital logic design that is incorporated in Integrated Circuit (IC). It is lightweight, unclonable, and simple to implement. Security mechanisms based on PUF can be an efficient way to provide security for resource-constrained IoT networks. This chapter describes different security aspects/scenarios of IoT that can use PUF-based mechanisms.

Keywords Internet of Things (IoT) · Security Physical Unclonable Function · IoT gateway · LLN nodes

1 Introduction

Recently, Internet of Things (IoT) is evolving as one of the promising and significant areas of the 5G communications. With 5G communication, millions of devices can be interconnecting around the globe where IoT can be considered as an integral part of several applications like smart cities, intelligent transportation services, smart grids, and many others. Each application of IoT promises to deliver an enhanced

M. S. Alkatheiri
University of Jeddah, Jeddah, Saudi Arabia

A. R. Sangi (✉)
Huaiyin Institute of Technology, Jiangsu Sheng, China

S. Anamalamudi
SRM University-AP, Amaravati, Andhra Pradesh, India

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_18

quality of experience in day-to-day activities. For example, the real motivation behind the development of smart cities is to have control over the available resources which will in turn promote healthy economy and sustainable growth. To achieve the successful implementation of IoT, an interconnected network of IoT requires every device to be connected to its utility gateway (IoT gateway or LLN gateway) directly or indirectly. For that, these constrained devices are needed to be equipped with smart sensors (or actuators) to collect the application data and forward it into their network center for further processing. Different types of IoT networks that are being proposed are centralized and distributed networks. In addition, both random access-based packet switched and deterministic networks are being proposed to implement within the IoT networks. Some applications in IoT (e.g., Industrial and Medical Machine to Machine Communication) need to have end-to-end dedicated spectrum channels to support control/data streams for time-critical applications. For such applications, securing the data is most crucial to protect the end user safety. Thus, enabling security to the end-to-end communication in IoT is very significant to provide safety to the end users. The widespread use of mobile devices is systematically providing ease and further aids human tasks. For example, RFID is one of the most important technologies designed to have the capability to assist numerous human tasks. RFID can be used to identify and authenticate person, animal, or product and prevent counterfeiting and cloning of goods, drugs, and money. However, the pervasiveness of the digital and computing devices has raised the security risks and delivers new security challenges/threats. These security threats and challenges are increasingly becoming intricate and awaiting to be overcome. Because such devices have significant limitations in terms of energy, implementation, and physical tampering as well as side channel attacks. Numerous existing cryptography algorithms are powerful to prevent some security attacks, but require complex implementation, such as public key cryptography. Even though there are many lightweight encryption algorithms provided by researchers, these efforts are always based on the assumption that the secret keys stored in non-volatile memory are well protected. However, physical system attack can easily breach/crack this sensitive information. Therefore, the cryptography primitive, namely Physical Unclonable Functions (PUF), is designed to address the above issue and successfully prevent counterfeiting, cloning, and prediction. For security-sensitive applications, PUF provides a cost-effective solution, and it can address the problems of existing solutions.

PUF is a one way-function that is easy to evaluate by using physical system but difficult to predict as its output is perfectly random in nature. PUF is a logical circuit designed and implemented inside an integrated circuit (IC), which generates a response for a given challenge. The given challenge produces a different unpredictable response when it is applied to different chip. Moreover, PUF can generate unlimited amount of secret key for one chip and gives an ability to produce unique identifiers for each chip. Fabrication process of an IC leaves behind unique characteristic to these circuits. Due to some uncontrollable and unavoidable differences in the process at molecular scale of each chip, PUF takes the advantage of this uncontrollable randomness as its challenge, and response mapping (values

are all binary strings) depends upon these variations. Therefore, PUF provides a unique challenge-response mechanism on each chip. As an example, the security related to the authentication process of the resource-constrained Internet of Things (IoT) devices is one of the major concerns as the conventional robust cryptographic solutions that are considered being powerful against some attacks but requires prohibitive cost and requires an increased power. These robust encryptions and security mechanisms are inhibited to be equipped in these devices which are not feasible as they have strict area and limited processing power. Thus, with the above concerns, the small size and limited processing power make these devices vulnerable to the attacker to reproduce the authentication protocol for the compromised nodes in IoT. Therefore, the attractive properties of PUF, i.e., lightweight, simplistic nature for authentication mechanisms, and reduced computational cost as compared to the requirements of existing cryptographic algorithms, make it a suitable candidate. Moreover, PUF provides us some features such as low cost computation, unpredictability, and unclonability. These features make PUF a promising candidate for resource-constrained IoT devices, and it is a very effective solution to solve the issues of secure communication in IoTs. PUFs have been proposed in [1] for device identify and authentication, and authors implemented PUF in IC to be used as anti-counterfeiting. Also it has been used as secure storage of cryptographic secrets [2], key-less secure communication [3], etc. Moreover, it is worth noting as stated in [4] that the conventional attack cannot be carried out if it is replaced by an ideal PUF.

This chapter is an effort to identify security issues in IoT that can best be resolved using PUF.

2 Overview of Security Issues in IoT

Different security bootstrapping methods are discussed in [3, 5], and this section covers what are the key security issues which can arise due to a failed security bootstrapping.

Before covering all security issues, we must understand that the term security covers a vast range of concepts, and here we are dealing with two broader key aspects of security in IoT, i.e., physical security and network security. An IoT network has to be protected mainly against following security aspects: authentication, access control, confidentiality, integrity, and availability.

Authentication process is used to validate communicating nodes before they share any secure information. Even the information of routing path is also important here. In IoT, authentication must be strong and highly automated. Access control is like verifying that the communicating node is not compromised. Confidentiality refers to the protection of vital information which is shared among communicating parties over open channel, e.g., wireless medium. Integrity confirms the data is unmodified and it is exactly as been sent by one party to the other, i.e., ensuring that no modification is done while data is in transit. Availability ensures that information is available when required [6].

When examining these threats, we found that under most of the IoT scenarios, the network is ultimately connected to public network whether it is comprised of hand-held mobile devices, number of static nodes, or a combination of both. So, the prime concern would be to look toward challenges posed under network security for IoT devices.

2.1 Physical Security

As we know, IoT networks are centralized with many remote nodes. Most of these nodes are in different locations like within ad hoc and sensor networks and have very less human intervention or attention. In this type of scenario, the attackers can seize and extract security information, keys, etc., from the device scattered in large area. Attacker can re-program the node or use physical or manufacturer info for their own needs. In case if common network key is used, then attack is more severe than the separate key in use [7]. DoS and DDoS attack can also be done in order to disrupt network communication, and these are very hard to detect [8, 9].

2.2 Network Security

2.2.1 Authentication Failure

This attack occurs at network layer; it aims the network route information and secure data. This type of attack happens when any of communicating node is compromised [7]. The prevention to this attack is authentication in the best possible way so that no illegitimate node is able to join the network.

2.2.2 Man in the Middle Attack (MitM)

MitM attacks are done by capturing information being sent between communicating nodes. This can be done by analyzing traffic, by which attacker is able to learn about the network. Such types of attacks can be mitigated by encrypting all data used for routing. It is mandatory to implement Advanced Encryption Standard (AES)-128 in Counter with CBC-MAC (CCM) mode for low power and lossy networks [10]. CCM combines the counter mode for encryption and the cipher block chaining message authentication code technique for authentication. MitM can also be done by analyzing traffic flow through network to successfully map traffic flow pattern; this happens in case the routing information remains unencrypted at data link and network layer [11]. These can be mitigated by using multi-path routing which requires more power consumption and is not very suitable for resource-constrained IoT networks.

2.2.3 Attacks on Data Integrity

Data integrity refers to unauthorized modification in a message or in stored data [12]. This attack can be mitigated by using access control for messages.

2.2.4 Spoofing

Spoofing is also known as identity theft; this means a communication node is not the one which it is pretending. This type of attack happens when an attacker gains access to a communicating node, either physically or via a network. If the attacker is able to create multiple false identities, then these are called Sybil attacks. By these attacks, the attacker can read secure data and send false routing information to disrupt normal routing process [13]. These attacks can be mitigated by applying correct authentication scheme at network layer.

2.2.5 Routing Information Replay Attacks

These attacks occur when the attacker records a message that is sent over a network and replays it multiple times to the network to disrupt operations [14, 15]. The IETF routing over low power and lossy networks (RPL) is designed to mitigate this attack. In RPL, repeated message or older messages are ignored by communicating parties [RFC6550].

2.2.6 Byzantine Routing Information Attacks

In this type of attacks, communicating node gets compromised by an attacker; that still contains a valid identity and security credentials. These attacks are very hard to detect; even authentication mechanisms could not counter such attacks.

2.2.7 Availability Attacks

Availability or selective forwarding attacks aim to routing paths and to disrupt communications among nodes. As seen in Fig. 18.1, the attacker can be able to send selected messages and creates confusion within the network. A situation where packets (msg1|msg2|msg3) are sent by Node A but the attacker node drops all the packets it receives is known as a black hole attack [16]. These types of attacks can be mitigated either by using end-to-end or hop-by-hop multipath routing protocols to send out the packets. Multipath method requires more energy; thus, it is not advised to be used in low power and lossy networks. Please refer to Table 18.1 for availability attacks in selective forwarding.

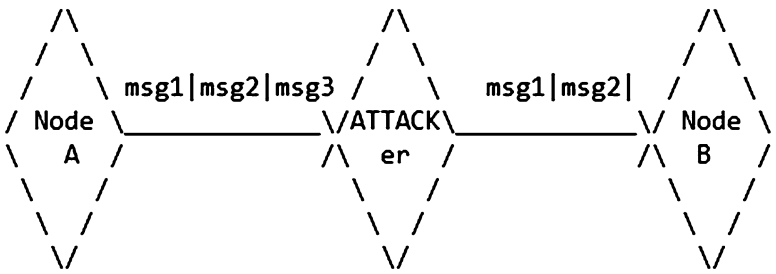

Fig. 18.1 Availability or selective forwarding

2.2.8 Wormhole Attacks

These attacks occur when two nodes with very short path among them get compromised. This attack forces nodes to recalculate network path. It is hard to detect but does not affect the data. In most of the cases, this attack is used in combination with other attacks like availability/selective forwarding to disrupt network communications [16]. Mitigating such attack is only possible with protecting the nodes to identity theft or false authentication.

2.2.9 Overload Attacks

Overload attacks are also referred to as denial-of-service (DoS) attacks, where compromised node fills the network with random traffic. These are aimed for exhausting network resources like routing and power, hence resulting in network breakdown. These attacks can be mitigated by limiting network usage to each node and also by isolating nodes which are sending excessive amount of traffic [17, 18].

3 Types of Physical Unclonable Function (PUF)

PUF is of various types and the following are two main types that can be suitable for resource-constrained IoT networks.

3.1 Arbiter PUF

Arbiter PUF is delay-based intrinsic silicon PUF which is based on number of switch blocks and an arbiter. It consists of switch block (MUXes) and an arbiter (flip-flop/latch). For "n" switch blocks, we have 2n "different delays." The circuit takes input in the form of multiple bits but gives single bit output based on the delay

Table 18.1 Overload attacks

Security issue type	Security issue description
	Based on the type of the security attack
Interception	The intruder intercepts the information through control/data signaling, but does not modify or delete; this kind of attack affects the privacy of the subscriber as well as the network operator
Reply attacks	The intruder can insert the unauthentic objects into the system that depend on the target and physical access type (e.g., spurious messages, fake service logic, or fake subscriber information)
Resource modification	The intruder creates the damage to the system by modifying the system resources
Interruption	The intruder tries to interrupt the operation by destroying the system resources (e.g., delete signaling messages and subscriber data, stop delivery, etc.)
	Based on methodologies used to cause the attack
Attacks based on data	The intruder targets the information stored in the IoT communication system and causes the damage by altering or inserting and/or deleting the data stored in the system
Attacks based on messages	The intruder targets the IoT system by adding, replacing, replaying, and dropping the control/data signaling flowing to and from the IoT network
Service logic attacks	The intruder tries to create the significant damages by simply attacking the service logic running in the various IoT network entities
	Based on the level of physical access
Class I	The intruder gains the access to the radio interface using a physical device and uses the modified mobile stations (eNodeB's) to broadcast the radio signal at higher frequency, eavesdrop, and execute "man-in-the-middle attacks"
Class II	The intruder gains the access to the physical cables connecting the IoT network switches and may cause considerable damage by disrupting the normal transmission of control/data signaling messages
Class III	The intruder will have access to some of the sensitive components of the IoT network and can cause important impairments by changing the service logic or modifying the subscriber information stored in the IoT network entity
Class IV	The intruder has the access to communication links connecting the Internet to the IoT network and can create a disruption through transmission of control/data signaling flowing between the link and adding some new control/data signaling messages into the link between the two heterogeneous networks
Class V	The intruder has an access to the Internet servers or cross network servers providing services to mobile subscribers connected to the IoT network and can cause the harmful damage by changing the service logic or modifying the subscriber data (profile, security, and services) stored in the cross network servers

(continued)

Table 18.1 (continued)

Security issue type	Security issue description
	Access of unauthorized sensitive data
Eavesdrop	The intruder intercepts the messages by continuously monitoring the operation of the communication network
Masquerading	The intruder frauds an authorized user by pretending that they are the legitimate users to obtain the confidential information from the end user or from the communication network
Analysis of the traffic flow	The intruder eavesdrops the traffic flow through length, rate, time, source, and destination of the traffic to trace out the user location
Browsing	The intruder search for data storage to trace out the sensitive information
Data leakage	The intruder obtains the sensitive information by exploiting the ways to access the legitimate user data
Inference	The intruder checks the reaction from a system by transmitting a query or control/data signal to the system
	Manipulation of sensitive data
Modification of user information	User information can be modified, inserted, replayed, or deleted by the intruder deliberately
	Unauthorized access to services
Access rights	The intruder will access the services through masquerading network entities or end user information
	Physical layer issues
Interference	The intruder intentionally creates the man-made interference onto a communication medium that causes the communication system to stop functioning due to high signal to noise ratio
Scrambling	One type of interference that is triggered based on short time intervals. With this, specific frame is targeted to disrupt a service. This kind of security attack is very complex to implement in communication network
	Medium Access Control (MAC) issues
Location tracking	The intruder monitors the presence of user equipment in a specific cell coverage or across multiple cell coverage
Bandwidth stealing	The intruder creates this kind of attack by inserting the messages during the Discontinuous Reception (DRX) period or through utilizing fake buffer status reports
Open architecture security issues	As IoT networks are IP-enabled networks with a high density of devices that are highly mobile and dynamic, an open architecture of an IP-based IoT results in increasing the number of security threats
Security issues at higher layers	The departure from proprietary operating systems for handheld devices to open and standardized operating systems and the open nature of the network architecture and protocols result in increasing number of potential security threats to the LTE wireless network, making it vulnerable to a wide range of security attacks including malwares, Trojans, and viruses

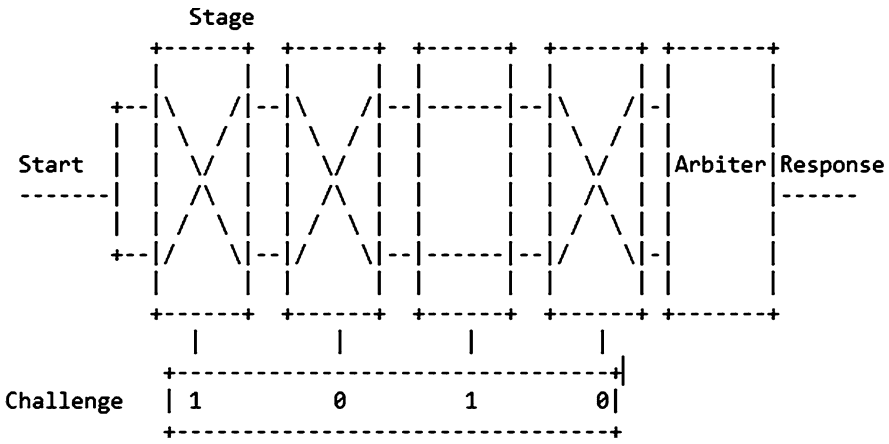

Fig. 18.2 Arbiter Physical Unclonable Function (PUF)

of two paths of equal length. The delay path is determined with respect to the input bits by controlling the MUXes. The MUXes pass through two delay signals from the left side if the input control bit is zero. Else, the top and bottom signals are switched. In this way, the circuit can create delay path for each input (Fig. 18.2).

The output is calculated based on the signal that is faster, and initially a signal is given to both paths at the same time. The signal moves through the path (facing variable delays), and an arbiter located at the end decides which signal is faster. The output is one if the signal from data input latch is faster; else output is zero. As there is more likelihood to get duplication due to precise timing, the output of PUF circuit can be obfuscated by XORing multiple outputs. There are different ways to construct k-bit response from 1-bit output in this delay-based PUF. At first, one circuit can be used k times with different inputs; a challenge is used as a seed for pseudo-random generator. Then, the PUF delay circuit is evaluated k times, using k different bit vectors from the pseudo-random number generator serving as the input X to configure the delay paths.

3.2 Ring Oscillator (RO) PUF

Ring oscillator PUF is based on ring oscillators (delay loops) and counters, rather than switch boxes and arbiter. Each ring oscillator is a particular circuit that oscillates with a particular frequency. Each oscillator oscillates with different frequency. These frequencies change with respect to environmental conditions such as temperature variation or power supply instability. Fixed sequence of oscillator pairs is selected to generate fixed bits, and oscillator frequencies are compared to generate output bit. Output bits vary from one chip to another even when compared

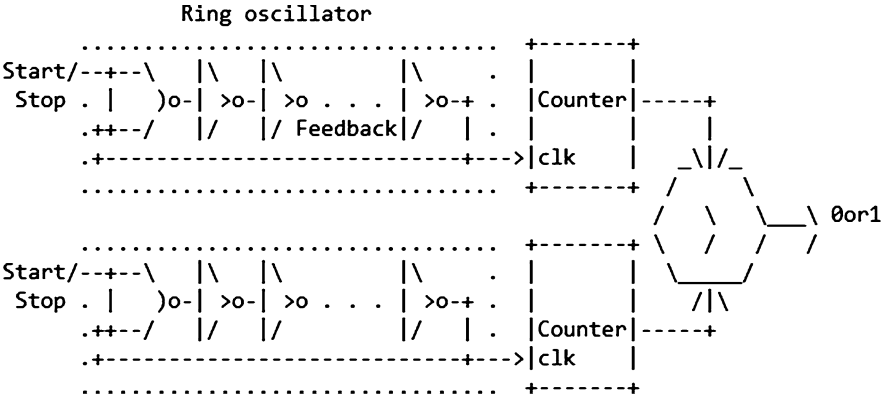

Fig. 18.3 Ring oscillator Physical Unclonable Function (PUF)

for the same sequence of oscillator pair. The output bit of oscillator is likely to be one or zero. The RO PUF has a strongly secure processor design and is more reliable than arbiter, but it is slower and consumes more power. On the other hand, we believe the arbiter PUF is more appropriate for resource-constrained platforms (refer to Fig. 18.3 above).

4 PUF Applicability

By reviewing survey on secure bootstrapping for IoT [10], viz., Managed, P2P or Ad-hoc, Opportunistic or Leap-of-Faith, Hybrid, and all security issues in IoT including both physical security issues and network security issues, we came to conclusion that the lack of physical security leads to other attacks, and if an attacker has the physical access, then it is much easier to crack down attack on network layer; hence, tampering with data and causing nuisance are eminent. To understand these facts in simpler words and going all at once, the opinion is divided in two parts: first going with security bootstrapping methods and then security in IoT. Finally, a discussion would provide some easier and real-time PUF usage example.

5 In Bootstrapping

When it comes to context of Managed security bootstrapping methods, the centralized server-based authentication is used to verify different nodes before communicating. A PUF can be used instead of putting long algorithms and programs to verify nodes with server. The basic idea of verifying nodes with server using PUF rather than pre-shared key will result in lesser demand of power, and authentication could

be performed without executing more heavy algorithms, whereas in P2P or Ad-hoc methods where the node authentication is performed by using key exchanging program, a PUF-based mechanism to verify node-to-node authenticity would result in easier and safe authentication with less power consumption. In Opportunistic or Leap-of-Faith methods, the verification of node is done with an assumption that the network is not compromised. Even with above assumption, using PUF mechanism for authentication, which inherently is strong to break (the authentication schema), is more simple and cost-effective.

6 Securing Other IoT Aspects

In the case of security issues in IoT, again there are two parts, i.e., physical issues and network-related issues. Using PUF in IoT devices can remove all physical security issues as we had discussed earlier that output of PUF is random in nature and depends on physical factors and even if the attacker gains physical access to device or node, it is impossible to reverse engineer PUF, which proves its trustworthiness toward physical security of IoT. As regards network security issues, first, we must understand that most of the attacks are possible due to false authentication which is the beginning, and afterward other attacks are possible. To help mitigate network attacks, PUF-based mechanism is suitable.

Authentication failure can be mitigated by using PUF, as it will provide perfect authentication to legitimate devices only and false authentication is not possible while using PUF mechanism. If PUF-based authentication is in place, then there is no need to think about confidentiality attacks because there will always be the legitimate nodes communicating with one another. All other network attacks (except MitM and data integrity) are ultimately initiated with compromised nodes which can be done either by using physical attack or by using fake authentication to get inside a given network, and these all can be removed using single solution, a solution based on PUF. For MitM and data integrity over network, currently used methods, i.e., CBC-MAC, are better in terms of security as the data is encrypted using lighter encryption schemas and thus are good for resource-constrained devices.

7 More Examples

Nearly most of the security service providers offer hardware-based security solutions for software license authentication. This hardware contains PUF due to its low cost, unclonability, and security. Another example is related to the Government of India where PUF-based RFID tags are implemented for authentication system used in Fast-Tag automatic toll collection service. A renowned US based company, VERAYO, develops PUF-based IoT devices and serves well-reputed customers including US Department of Defense agencies. Moreover, a Dutch company,

"Intrinsic ID," also works in the field of developing PUF-based IoT devices and has reputed contracts including government and defense departments.

8 Conclusions

This chapter highlighted the applications of PUF in IoT and provided an insight of this fabulous technology that is believed to be suitable to use in any resource constrained environment, especially IoT. The inherent unique properties of an Integrated Circuit (every device holds at least one) can further affirm the suitability of PUF based security mechanisms in resource constrained network including IoT.

This lucrative and easy to implement technology could bring a revolution in adoptability in securing the IoT ecosystems. Further study in this regard is needed to more specifically devise novel security mechanisms based on PUF for IoT ecosystems.

Acknowledgment The authors hereby express their gratitude to the inventions of PUF and look forward to see its large scale adoption in securing IoT networks. Also, many thanks to the editor(s) of this book for providing a platform to introduce new security related concepts.

References

1. Garcia-Morchon, O., Kumar, S., Keoh, S., Hummen, R., & Struik, R. (2013, September). *Security considerations in the IP-based internet of things*. Draft-garcia-core-security-06 (work in progress).
2. Tsao, T., Alexander, R., Dohler, M., Daza, V., Lozano, A., & Richardson, M. (2014, October). *A security threat analysis for routing protocol for low-power and lossy networks (RPL)*. Draft-ietf-roll-security-threats-11 (work in progress).
3. Sarikaya, B., Sethi, M., & Garcia-Carillo, D. (2018, September). *Secure IoT bootstrapping: A survey*. Draft-sarikaya-t2trg-sbootstrapping-05 (work in progress).
4. Ruhrmair, U., Solter, J., Sehnke, F., Xu, X., Mahmoud, A., et al. (2013). PUF modelling attacks on simulated and silicon data. *IEEE Transactions on Information Forensics and Security, 8*(11), 1876–1891.
5. Gupta, B., Agrawal, D. P., & Yamaguchi, S. (2016). *Handbook of research on modern cryptographic solutions for computer and cyber security*. Pennsylvania: IGI Global.
6. Edward Suh, G., & Devadas, S. (2007). Physical Unclonable Functions for device authentication and secret key generation. In *Proceedings of the 44th annual design automation conference* (pp. 644–654). ACM.
7. Meng-Day Y., M'Raihi, D., Sowell, R., & Devadas, S. (2011, October). Lightweight and secure PUF key storage using limits of machine learning. In *Cryptographic Hardware and Embedded Systems, CHES 2011—13th International Workshop, Nara, Japan* (pp. 358–373).

8. Gupta, B., Agrawal, D. P., & Wang, H. (2018). *Computer and cyber security: Principles, algorithm, applications, and perspectives* (p. 666). Boca Raton, FL: CRC Press, Taylor & Francis.
9. Shamim Hossain, M., Muhammad, G., Abdul, W., Song, B., & Gupta, B. B. (2018). Cloud-assisted secure video transmission and sharing framework for smart cities. *Future Generation Computer Systems, 83*, 596–606.
10. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., & Alexander, R. (2012, March). *RPL: IPv6 routing protocol for low-power and lossy networks*. RFC 6550. https://doi.org/10.17487/RFC6550. Retrieved from https://www.rfc-editor.org/info/rfc6550
11. Bradner, S. (1997, March). *Key words for use in RFCs to indicate requirement levels*. BCP 14, RFC 2119. https://doi.org/10.17487/RFC2119. Retrieved from https://www.rfc-editor.org/info/rfc2119
12. Gupta, B. B., & Quamara, M. An overview of internet of things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience*, e4946.
13. Ruhrmair, U. (2012). SIMPL systems as a key less cryptographic and security primitive. *Lecture Notes in Computer Science, 6805*, 329–354.
14. Labrado, C., & Thapliyal, H. (2018). Design of a piezoelectric based physically unclonable function for IoT security. *IEEE Internet of Things Journal, 6*(2) 2770–2777.
15. O'Neill, M. (2016). Insecurity by design: Today's IoT device security problem. *Engineering, 2*(1), 48–49.
16. Kim, S. W. (2014). Physical integrity check in wireless relay networks. In: *2014 IEEE Conference on Communications and Network Security, San Francisco, CA* (pp. 514–515).
17. Kasmi, O., Baina, A., & Bellafkih, M. (2016) Multi level integrity management in critical infrastructure. In *2016 11th International Conference on Intelligent Systems: Theories and Applications (SITA), Mohammedia, Morocco* (pp. 1–6).
18. Zhang, X., Yang, X., Lin, J., Xu, G., & Yu, W. (2017, January). On data integrity attacks against real-time pricing in energy-based cyber-physical systems. *IEEE Transactions on Parallel and Distributed Systems, 28*(1), 170–187.