Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Securing Wireless Sensor Networks in Industrial IoT Lightweight Encryption Techniques

Mohammed. I. Alghamdi

Computer Science Department, Faculty of Computing and Information, Al-Baha University, Al-Baha, 65779, Saudi Arabia

For the security of "Wireless Sensor Networks (WSNs) in "Industrial Internet of Things (IIoT)", several custom models or lightweight encryption techniques like CLEFIA or PRESENT are designed to be widely used for low power consumption as they give priority to minimal memory usage and computational overhead, while still providing resource-constrained nodes or proper data confidentially, making them ideal for industrial applications where a lot of sensors should transfer data with processing capabilities and limited power. The "Internet of Things (IoT) enables users to collect control devices, sensor data, and analyze data collected over the web. IoT devices are located in various environments and support a lot of applications. To prevent cyber threats in IoT systems, it is recommended to support the CIA triad (Confidentiality, Integrity and Authentication).
However, there are limited computational and energy resources in IoT devices. This study has proposed lightweight encryption techniques for IoT as per the review of recent studies. This study also explores communication protocols and lightweight security along with challenges in adopting a secure IoT system. Hence, this study combines lightweight security and communication protocols. These protocols will be approached from the point of view of a practitioner. They provided different applications to help readers with minor security background to understand such techniques and priority of CIA triad elements.

Keywords: CIA triad, IoT devices, IoT system, Internet of Things, Industrial Internet of Things, Wireless Sensor Networks, Lightweight Encryption Techniques

1. Introduction

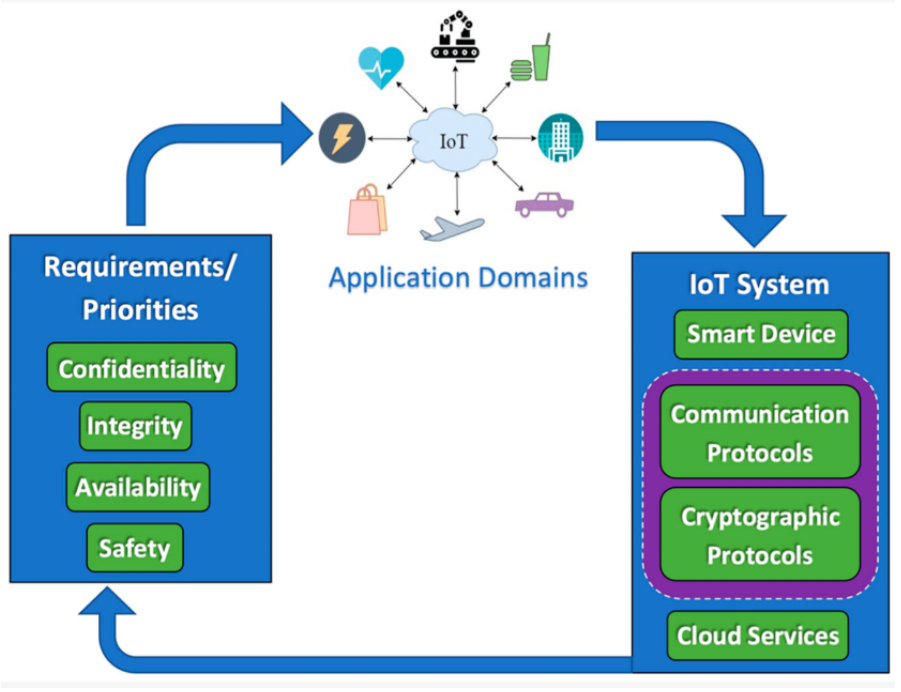
The concept of adoption of "Internet of Things (IoT)" in the industry has emerged in 2010, even though defining the term of IoT was brought in 1999 when "radio-frequency identification (RFID)" tags were used (Lueth, 2014). Among the community, the dominant belief was that IoT would be just another acronym in computer network. However, engineers with experience in "embedded systems" or "wireless sensor networks (WSNs)" could recognize their work as IoT. Later on, IoT research has gained attention on security (Ferrag et al, 2017).

Each IoT device plays a vital function as per the domain of application. In turn, each domain of application has varied security need. New startups or traditional industries promote small-

scale devices which can be used in various applications like surveillance, asset tracking, environmental monitoring, healthcare, and "industrial control systems (ICS). The rising adoption of IoT devices and rapid advancement in various industries need users to understand those technologies to deal with roadblocks related to adoption of IoT domains. On the other hand, there are several questions which should be answered – What is needed for operating with small-scale IoT devices? How to protect the device and its data from malicious actors? Which should come first in CIA triad for various applications? (Brooks, 2019).

For example, ICS systems are using IoT widely like in power transmission, production, and distribution (Chaudhary et al, 2018; Nielsen et al, 2015). They have to transfer data reliably among control centers and field devices. Since they are known to control physical processes, one can assume that data availability and integrity and control commands are more vital. Meanwhile, confidentiality is much needed in systems carrying sensitive data like healthcare. Figure 1 illustrates the concept of various security requirements of various sectors like food industries, manufacturing, transportation, smart cities, healthcare, and energy in terms of safety and CIA triad, which can determine the type of communication protocol of IoT and encryption features. It can ultimately be updated as per the recent technologies or modified security needs.

Figure 1 – Security Requirements for IoT applications in terms of CIA triad



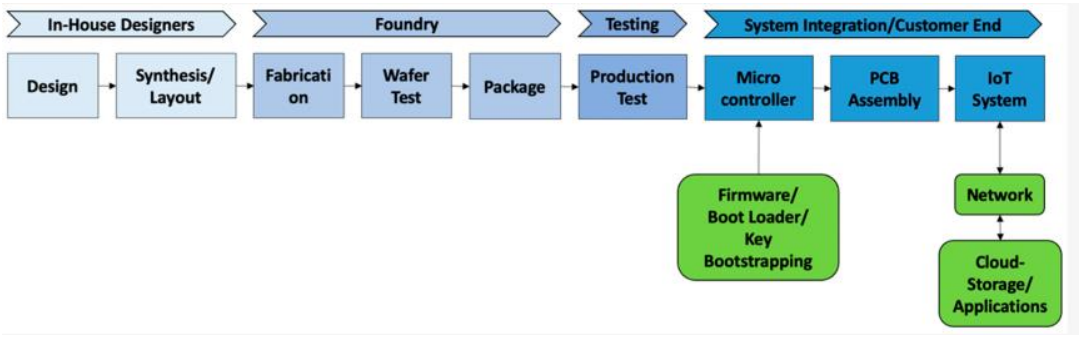
Source – Goulart et al (2022)

Every application of consumer or industrial IoT is subject to cyber threats. "False Data Injections (FDI)" in control systems can have significant impacts on real processes (Meneghello et al, 2019; Wlazlo et al, 2021). Consumer devices are prone to different cyber-attacks like surveillance cameras which can reveal sensitive data with unauthorized location

tracking and video recording (Hinshaw & Pop, 2019). The term "massive data" is widely applicable to IoT, as in the work of Nielsen et al (2015) which defines how phaser measurement units (PMUs)" and smart meters use cellular communications to send reports regularly to control center. When transferring all the data over the web, the question rises up on protecting the same.

Security increases overhead costs like extra delay in encryption model, additional messages to exchange keys, and added bytes at the end of message to offer integrity. An important question is whether it affects the safety and availability of such systems. Cryptography is widely used for providing authentication, secrecy, and integrity (Schneier, 1996). It can be achieved with protocols which defines a lot of steps which all parties should agree to abide in the process of communication. For secrecy, cryptographic protocols adopt hybrid systems which have public key encryption models and symmetric models. There is a need to address various aspects of hardware security, like creation, manufacturing, and design of embedded system with "field programmable gate array (FPGA), microcontroller, and printed circuit board (PCB)" (Figure 2). The focus is made on the consumer end of creating devices (right side of Figure 2). This is when node is prepared to be connected to the network and be the part of IoT solutions.

Figure 2 – Various stages of physical device security



Source – Goulart et al (2022)

2. Literature Review

A cryptographic encryption model with minimal output space and low memory requirements involves reduced overheads for computation without compromising on security and strength of encryption is needed for limited devices in "wireless sensor networks (WSNs)". "Internet of Things (IoT)" supports streaming and automated collection of sensitive data in different devices online. Insecurity of the internet has been amplified in communication of critical data across the nodes in IoT because of data privacy compromises and current data breaches on those networks in this day and age. Asare et al (2020) addressed the challenge of data integrity and data privacy breaches among IoT devices with proposal of an approach with thin cryptography scheme combining the MD5 and Feistel cipher when offering improved security for node data of IoT. Findings suggested improved and quick data encryption among sink node and IoT edge devices.

WSNs are used widely in different applications. Attackers might eavesdrop on chats and

manipulate digital devices. The data can also be modified by attackers which has been connected or connect unofficial devices to the network if they are deployed in real environment. For WSN security, exchange of message among nodes of communication should be encrypted and network should store a key for decryption and encryption. On the other hand, key management is very important to achieve WSN security. Obtaining such arrangement is needed in a resource-limiting environment for energy-efficient and secure data transmission. Existing models have some security issues like brute force attacks, susceptibility to plaintext attacks, computational complexity, and side-channel attacks. Apart from clustering, cryptography has been known to be efficient and practical technique to improve energy-efficient and secure data transmission. Urooj et al (2023) used asymmetric "Elliptic Curve Cryptography (ECC)" approach for key generation while decryption and encryption of data has been performed by hybrid of ECC cryptography and "Advanced Encryption Standard (AES)". They developed a novel model which combines both of these techniques apart from clustering with "LEACH protocol" to improve data security, energy efficiency, and network lifetime. The proposed model could overcome the problem of key exchange which plagues AES, more than AES and easier than ECC. It can address different security threats like side-channel attacks. The proposed model is better and compared to existing techniques related to encryption time, time complexity, and decryption time to prove its efficiency.

The IoT has anticipated future technology promising to connect a lot of devices online. WSNs are known among the most important IoT subnetworks. Sensor networks are widely used by IoT to monitor, send, and gather sensitive data in wireless networks. Since data transferred with WSNs is exposed easily to cyber-attacks, data security is a concern. The adversary of the attackers in WSNs deteriorate and halt the effective use of the network and affect network services, making them inaccessible to the users and providing false feedback to the user. As users cannot control the data transferred over wireless network or stored in middleware, it can be accessed by anyone with the internet. It risks the integrity, authenticity, and confidentiality of data as unauthorized users can easily alter, manipulate, and access the data in transit. Mahlake et al (2023) proposed hybrid model "Lightweight Security Algorithm (LSA)" which consists of "Secure IoT (SIT)" and "Security Protocol for Sensor Networks (SPINS)" encryption to improve data security of WSNs while reducing the power consumption and threshold of attacks in WSNs without affecting network performance. In addition, the proposed LSA reduces time for key generation by 102mS to ensure 99% of security. At the time of data transmission, it is possible to reduce power consumption by 411.2uJ on average and "Packet Drop Ratio (PDR)" from 90% to 99% when it is compared with Feistel techniques and SPN.

WSNs are networks of smart devices with less resources that can collect various data for different purposes. Security and energy play a vital role in such networks and aspects of MAC are important for their management. Traditional security methods are not suited for WSNs given limited resources, which subsequently need light cryptography systems to achieve high security. Tropea et al (2022) provided a security analysis and compared LMAC and BMAC protocols to determine the protocol with RSA, AES, and elliptic curve techniques and best trade-offs when receiving packets and power consumption.

As "Industrial Wireless Sensor Network (IWSN)" is deployed majorly in unattended or extreme environment, privacy security has a lot of challenges in data aggregation. Currently,

the protocols of data aggregation focuses mainly on improvement of efficiency of data aggregation and transmission and to improve data security. Performance of secure protocols of data aggregation are the trade-offs of various metrics, which consist of energy efficiency, fusion/transmission, and security in WSNs. There is a research gap in systematic analysis on performance of secure protocols for data aggregation, be in WSN or in IWSN. When considering IWSN, Fang et al (2019) review security techniques and requirements in WSN aggregation. They provided holistic insight to traditional secure protocols for data aggregation, which are split into "hop-by-hop encrypted data aggregation, end-to-end encrypted data aggregation and unencrypted secure data aggregation". In this way, they analyzed the pros and cons of current security schemes in each category with characteristics of industrial applications and realized the energy efficiency and security for IWSN. Finally, they concluded the approach and techniques in such categories and highlighted future directions for preserving privacy in IWSN.

2.1 Research Gap

Symmetric models depend on session key to decrypt the ciphertext and encrypt the plaintext. Each node has a pair of private and public key in public-key modes. Public key is used to encrypt plaintext in other nodes. Only the node with consistent private key can decrypt ciphertext. Public-key models are widely used to share the session key safely. These crypto-systems create "message integrity codes (MICs)" or digital signatures to ensure data integrity and authenticity of parties involved. However, hybrid crypto systems are problems in IoT devices due to limited memory, power and computational resources (Gurunath et al, 2018). For instance, public-key encryption is mathematically complex due to high computation cost (Miorandi et al, 2012).

In addition, cryptographic protocols need larger keys which need high computing and memory capacity to generate and store keys. For the distribution of keys, verification of digital signatures, encryption of plaintext, and decryption of ciphertext, time is needed, which leads to processing delays which can make physical processes to be controlled or monitored. Lightweight cryptographic protocols are needed to prevent malicious attacks on IoT systems while using few of the resources from the end device. This study fills the much needed research gap by investigating recent "lightweight security encryption" techniques for IoT by focusing on IoT networks from the standpoint of CIA triad. This study will be helpful to the readers to understand various IoT security techniques, including the light variants of ciphers like "Elliptic Curve Cryptography (ECC)" and "Advanced Encryption Standard (AES)" in a practical and clear way.

2.2 Research Objectives

- To discover recent "lightweight security encryption" techniques by focusing on IoT networks as per CIA triad
- To investigate various IoT security techniques like "Elliptic Curve Cryptography (ECC)" and "Advanced Encryption Standard (AES)"

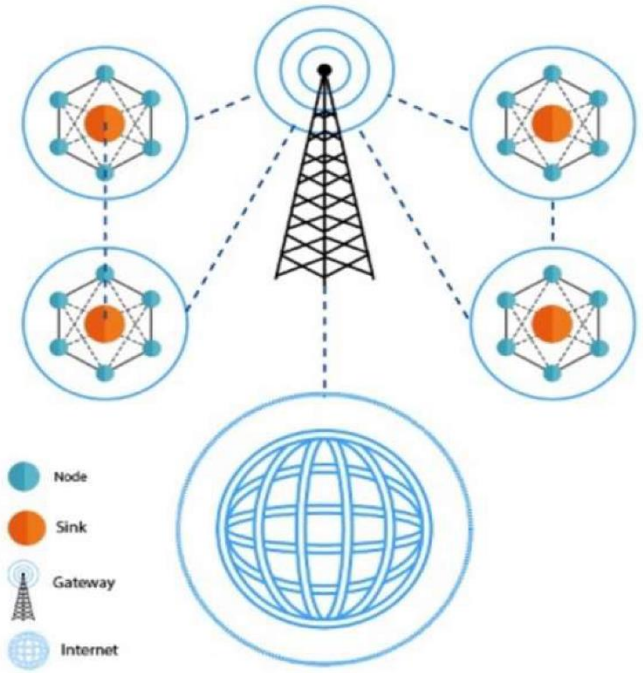
3. Research Methodology

This study focuses on a comprehensive review of earlier studies on lightweight and IoT security protocols and it is related directly to industrial IoT and lightweight encryption techniques. Research studies conducted on these categories are input to discuss the security of wireless sensor networks in industrial IoT applications.

4. Data Analysis

A WSN consists of limited range of sensors which can control and sense physical characteristics like light, sound, humidity, temperature, and others in geographical regions. WSN nodes communicate with base station and other nodes with wireless channels (Figure 3).

Figure 3 – A Diagram of Traditional WSN Architecture



Source - Hussein et al (2022)

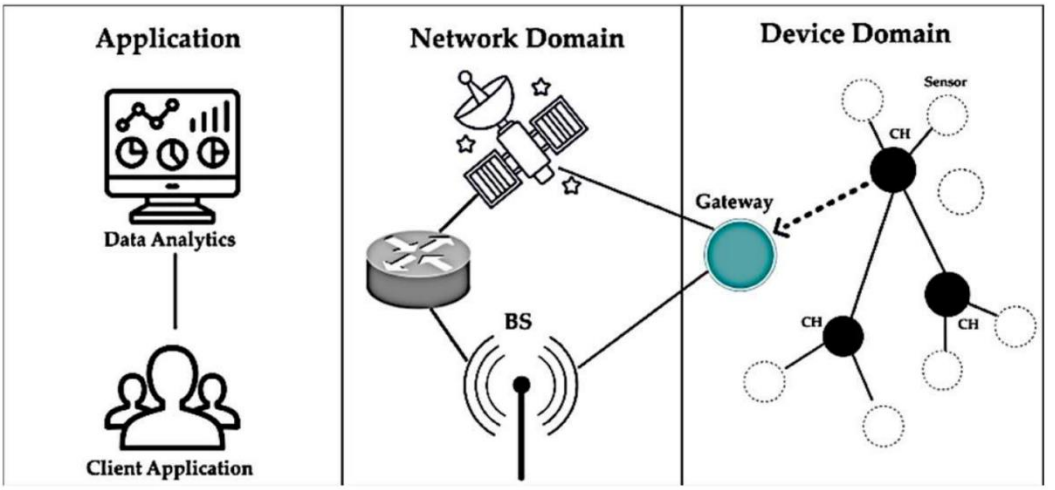
Sensor nodes have limited CPU, memory, and energy capacity. A sensor node has processing unit, power unit, multiple sensing units, antenna, transceiver, and other components like a power generator, actuator, and a position finding system. Volume of nodes of the sensor varies from “cubic nanometers to cubic decimeters” (Sohraby et al, 2007). Node location of sensors may be known/unknown, logical, or actual communication in a network between nodes and other devices to evaluate the topology. There are different topologies in a WSN as per the node tasks or network. WSN heavily depends upon the reliability and speed of delivery of data.

Routing protocols are responsible for finding out how data moves with the network. For WSNs, routing approaches must take coverage area, energy use, and other considerations. As

per network topology, routing protocols of WSNs should be classified as either location-aware, flat, or hierarchical (Devika et al, 2013).

As mentioned in Figure 4, the IoT architecture includes three domains – network or communication, a layer of services and interfaces, a device or hardware. First layer includes actuators and sensors. For example, an irrigation system consists of moisture sensors, sprinkler heads, actuators, and temperature sensors, which are linked to the network with various protocols. A microprocessor is used in end devices in this layer as per "Interplanetary File System (IPFS)" which can distribute data integrity and data storage while considering problems related to core systems, "Real Time Operating System (RTOS)", "X86 or ARM architectures," and so on (Javed et al, 2020). For the layer of application software, there are cryptographic protocols, custom applications, and third-party drivers and libraries. Communication layer or network domain presents collection and transfer of data to application domain. Various protocols can connect objects with gateways to the cloud and online applications.

Figure 4 – An illustration of IoT Architecture Layer



Source – Hussein et al (2022)

In a lot of cases, WSNs are not centrally managed and deployed in unfavorable environments and use untrustworthy modes of communication. Hence, security mitigation of WSN cannot depend on standard solutions for IT network because of interconnection and complexity of different protocols and devices, while there are different services and routing protocols available. Hence, there is an insufficient security mechanism in use. A lot of trends and techniques have been used for certain range of security levels like encryption techniques and trust management relying on lightweight approaches for cost-effective and power-efficient encryption devices. Routing protocols may also be vulnerable to serious threats and attacks like injecting malicious or false routing information in a network, causing packet losses or delays because of routing issues. There have been a lot of solutions proposed to avoid routing attacks like data correlation and encryption among various nodes (Oreku & Pazynyuk, 2016).

4.1 Lightweight Security Encryption Techniques

Even though thee are several lightweight models for encryption like PRESENT, CLEFIA, and ISO/IEC 29192, a lot of protocols for IoT communication use "Advanced Encryption Standard (AES)" to provide authentication, integrity, and confidentiality (NIST, n.d.). The "IEEE 802.15.4 data link and physical layer protocol" is the good example. It provides seven 128-bit blocks and AES-128 based security levels –

- Security level 0
- Security level 1 to 3 – It provides only authentication and integrity by generating various sizes of "message integrity code (MIC)"
- Security Level 4 – It provides security and confidentiality only
- Security levels 5 to 7 – They provide authentication, integrity, and confidentiality.

Additionally, other standards are IEEE 802.15.4 based like LoRaWAN and Zigbee (Dragomir et al, 2016). Some of the usual short-range applications like IEEE 802.15.4, RFID, BLE, and Zigbee are IoT solutions in homes, smart buildings, and factories. Other short-range communication technologies like 5G and Wi-Fi are not low-power, but they are used widely in smart building/smart homes and industrial environments. Energy-efficient and long-range solutions are best for IoT projects in transportation, smart cities, agriculture, and utilities. Security becomes even more important with the distance factor as IoT devices are placed above the huge geographic region. These devices can save energy due to low data rate by sending small packets.

4.1.1 LoRaWAN

The "Long-Range Wide-Area Network (LoRaWAN)" secures application and network layers. The LoRaWAN sensor nodes is authenticated by the link layer protocol and data frame gets integrity. The confidentiality is given to the application layer protocol to the message end-to-end when encrypted data is transferred from the node to the server.

The proprietary protocol of LoRaWAN is devised by the "LoRa Alliance (n.d.)" which relies on a free spectrum in the "Industrial Scientific and Medical (ISM)". LoRa Alliance is split into two parts (Vejlgaard et al, 2017) –

- The "LoRa Physical Layer" standard and
- The "LoRaWAN network protocol

In the specification of LoRa physical layer, LoRaWAN uses various ISM bands as per the geographic region. LoRa relies on 8 downlink channels and 72 uplink channels in the 902-928 MHz ISM band in North America (Gunathilake et al, 2019). The "Chirp-Spread Spectrum (CSS)" has modulated the channels with various "Spreading Factors (SF)". SFs are selected as per the application as SFs provide different rates of transmission, varying from 300 bps to 50 kbps (Chaudhari & Zennaro, 2020). Higher SFs are related to lower rates of data. The benefits of spread spectrum is that various nodes can transfer in the same physical channel at the same time.

LoRaWAN nodes can start transmission with "random-access mode" at any time similar to

"unslotted ALOHA networks" (Bertsekas et al, 1992). The topology of LoRA network relays data packets in the uplink with base stations (BS) or gateways from motes to a network server at the important IP network (Wixted, 2016). The server performs functions related to security like authentication, checking the integrity of packets, and removing duplicate packets. From application server to mote for the downlink, data is usually stored in the network server from the user application to end devices. The uplink and downlink transmissions rely on the kind of LoRaWAN motes (LoRa Alliance, n.d.).

Class A devices are battery-powered which activate to send data. The device in the uplink initiate all transactions. They are used to save energy but they face longest downlink latency as they can get only downlink data after uplink transmission. Class B devices are basically battery-operated actuators which have scheduled windows. They listen to commands for performing an action. Due to receive windows, they have low latency while saving energy. Class C devices are actuators which are not limited by battery life and need fastest response time. The receive window is open all the time, except with uplink transmission.

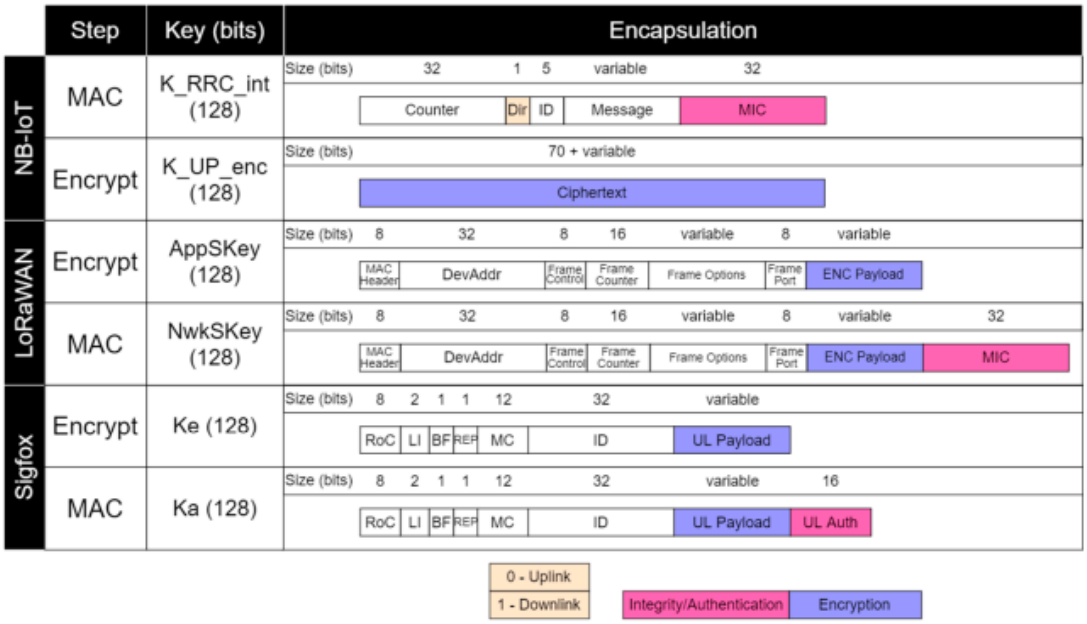
4.1.2 NB-IoT

The "Narrowband (NB) IoT" refers to the "Third Generation Partnership Project (3GPP)" and a "Cellular IoT (CIoT)" technology operating in the licensed spectrum (Shin & Jo, 2017). It has close relevance to the "Long-Term Evolution (LTE)" cellular standard but it is also catered to "low-powered devices" and improves coverage (Migabo et al, 2018; Wang et al, 2017; Mangalvedhe et al, 2016). To define the NB-IoT architecture and differentiate among NB-IoT and LTE, this section explains its architecture for both network and physical layers. In the NB-IoT network, the "User Equipment (UE)" is the IoT device, the "Evolved Packet Core (EPC)" IP network imitates the fog network in IoT system, and "enhanced NodeB (eNodeB)" is the base station (Khan et al, 2020).

Assuming AES encryption illustrates the NB-IoT secures with "MAC-then-Encrypt (MtE)". First of all, the "NB-IoT" calculates the MIC or "MAC-1". It uses AES in "Cipher-based MAC (CMAC) mode which acts as in AES-CBC mode (Eq. 1) (Pirzada, 2019). The message is divided into blocks of 128 bits and each block is used with following block in XOR operation (Song et al, 2006). The message bits, 1-bit direction (downlink/uplink), 32-bit frame counter, and 5-bit radio bearer identifier (ID) are inputs to create 32-bit MAC-I." In this step, the key used is "integrity key KRRCint created at Radio Resource Control (RRC) sub-layer."

$$\text{Cmac} = \text{AES128\_cmac}(K_{\text{RRCint}}, \text{Count} \mid \text{Dir} \mid \text{ID} \mid \text{Msg}) \quad (1)$$

Figure 5 – IoT network architecture for WAN and security protocols



Source - Goulart et al (2022)

NB-IoT is best suited for outdoor and indoor applications (Vejlgaard et al, 2017). In "Automated Metering Infrastructure (AMI) networks", smart metering is a part of IoT system where they send real-time data to electrical utility (Goulart & Sahu, 2016). Smart meters can send data to a server directly at the utility company with NB-IoT. It supports up to 128 bytes of data payloads and it can be used for reports of smart meter, which may need 300 bytes on average on each uplink input (Nielsen et al, 2015). In addition, 3GPP provides a table of various applications in a smart city, which consists of infrastructure solutions like gas, water, transportation, electricity, and waste management. Table 1 lists sensors, frequency of messages, and size of messages with NB-IoT (Fattah, 2018).

Table 1 – Applications of NB-IoT in smart cities as per 3GPP

Applications	Frequency	Message Size
Renting bikes	4 per hour	50 bytes
Gas meter	4 per hour	100 bytes
Waste management	1 per hour	50 bytes
Parking	1 per hour	100 bytes
Electricity meter	1 every 4 hours	300 bytes
Water meter	1 per day	200 bytes
Pollution tracking	1 per hour	1000 bytes

Source – Fattah (2018)

4.1.3 C-UNB/Sigfox

The "Cooperative-Ultra Narrow Band (C-UNB)" is a cellular IoT standard defined by 3GPP in the "TR45.820 technical report" (3GPP TR, 2015). A French company Sigfox developed a similar technology "triple diversity UNB (3D-UNB)" uses ISM spectrum. It uses 902 MHz band in the US. In Figure 5, both Sigfox and C-UNB are LPWA networks providing low data rates, wide connectivity, and ad-hoc access protocols for serving a lot of IoT devices. C-UNB relies on macro-channels at the physical layer, including 200 kHz GSM channels or LTE channel sidebands like NB-IoT. This way, 200kHz macro-channel is divided into micro-channels or narrow-band channels by the C-UNB uplink channels (Goulart et al, 2022).

In each micro-channel, the bandwidth is merely a few hundred per Hertz. It is one of the slowest transfer of data in LPWA and it is known as "ultra-narrowband" for this reason. Since uplink bit rate is 300 bps and modulation is "Differential Binary Phase Shift Keying (D-BPSK)", the needed bandwidth is 600 Hz for each micro-channel, i.e., 2x the bit rate. The micro-channels are also used by the C-UNB downlink, i.e., 600 bps. This way, Sigfox link has 600Hz of bandwidth in micro-channels in both uplink and downlink. The uplink relies on D-BPSK modulation and downlink uses "Gaussian Frequency Shift Keying (GFSK)". In the downlink and uplink, the total bandwidth required is 192 kHz for each macro-channel, providing 320 micro-channels in downlink and uplink (Goulart et al, 2022).

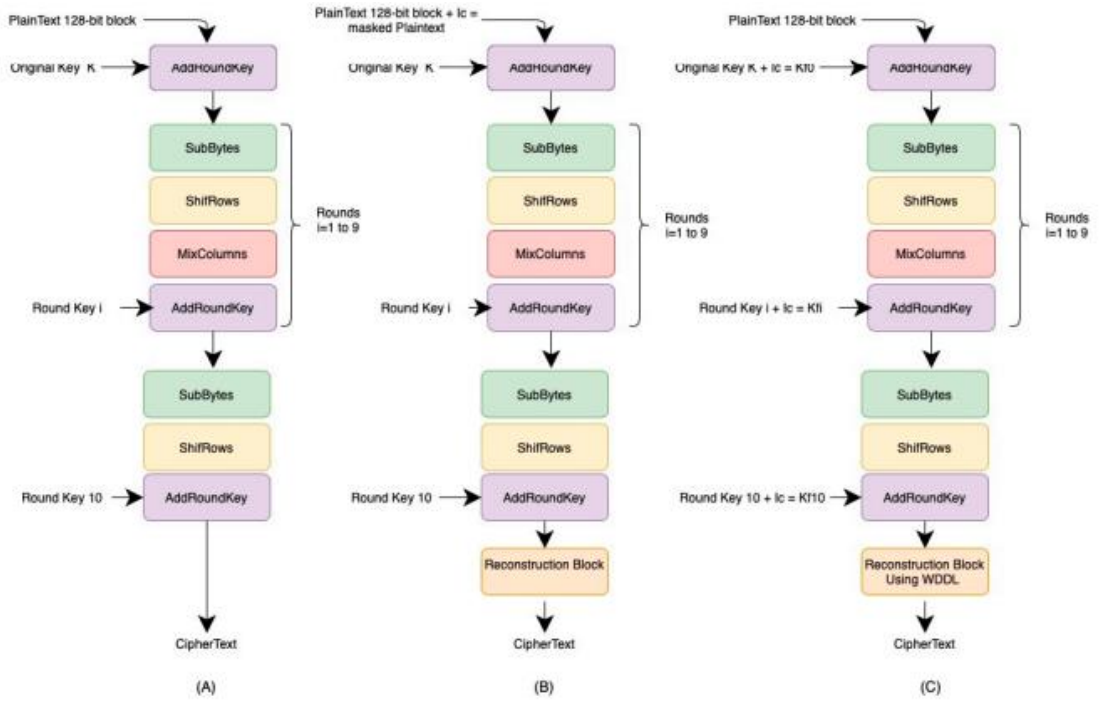
4.2 IoT Security Techniques

4.2.1 Lightweight AES

Lightweight versions of AES are being developed for IoT systems. The AES model is a symmetric cipher. The inverse of these operations and similar secret key can be performed to achieve decryption. It is possible to perform AES transformations in software or hardware. When implemented in hardware, it uses "field programmable array (FPGA)" ICs. James and Kumar (2016) presented an example of implementation of lightweight AES in FPGA which is mainly aimed to reduce latency of transformations of AES by reducing clock cycles of AES transformations.

The transformations of AES include permutation transformations and substitution. Each round of encryption includes four transformations of AES (Figure 6). A unique key is used in each round. These are obtained with key expansion on the basis of first cipher key (NIST, n.d.). Before the start of first round, the "AddRoundKey" transformation is conducted among 16-byte block (4x4 byte matrix) and cipher key. All 4 transformations are conducted in a sequence of "SubBytes, ShiftRows, MixColumns, and AddRoundKey." There are four transformations in each round, except the last round, which includes only 3 transformations.

Figure 6 – (A) 10-round schedule of AES transformation for 128-bit keys; (B) Traditional AES implementation; (C) Masked AES implementation



Source – Yu & Köse (2017)

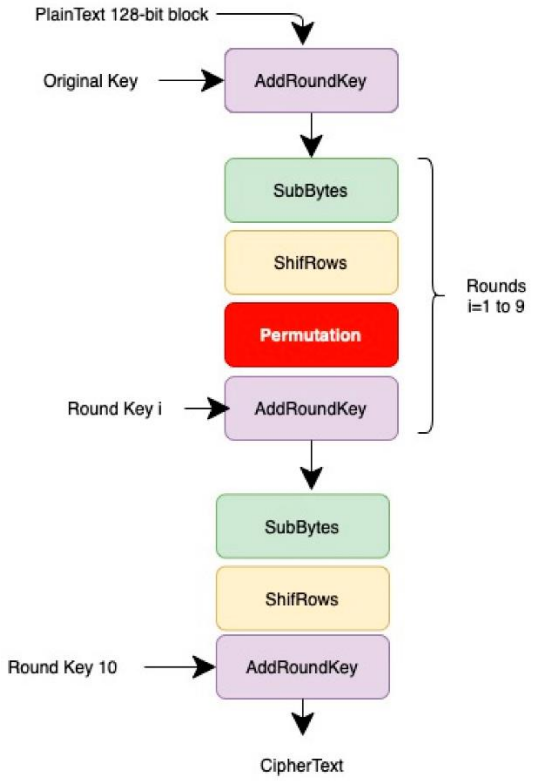
The SubBytes transformation is programmed by James and Kumar (2016) to be performed parallelly. Since SubBytes operates individually on each byte by 4x4 state matrix with S-Box substitution table, they proposed to add various bytes parallelly in the matrix. In addition, S-Box can either be generated on the basis of equations or in the device's memory as explained in the "Federal Processing Standard (FIPS) 197 AES" standard. In the work of James and Kumar (2016), the S-Box is used as a look-up table and is pre-calculated to substitute various bytes.

Another parallel operation proposed is "MixColumns transformations", performing linear transformations on each state matrix column. In the state matrix in the MixColumns transformation, each column is a vector multiplied by a fixed 4x4 matrix, making new column in state matrix. They explained multiplications of each column in parallel. James and Kumar (2016) proposed another design option and calculated the round key at every round, rather than calculating the complete schedule before storing all keys and encryption in memory. It is mainly used to save storage. These techniques address light primitives of improvements of hardware at FPGA level for devices with low resources, save memory, and reduce delays. It is possible to consider the parallel operations of MixColumns and SubBytes transformations to be known as a type of primitive of system performance, as crypto-array operations.

Acla & Gerardo (2019) proposed another "lightweight AES (LAES)" to remove "MixColumns transformation" and replaced the same with 128-bit permutation table. Fixed table is used by

this permutation operation to rearrange the columns in a state matrix. MixColumns is a non-linear change on the state matrix columns and they argued that permutation operation is another operation, although less complex to implement in hardware. When it comes to use 128-bit key, nine rounds, after AddRoundKey, consist of "SubBytes, ShiftRows, Permutation, and AddRoundKey transformations" (Figure 7).

Figure 7 – A LAES replacing MixColumns with Permutation



Source – Acla & Gerardo (2019)

In the AES round schedule, the variation improves overall performance in throughput, i.e., number of bits processed each time. It is possible to calculate performance efficiency by dividing the throughout by the FPGA circuit area.

4.2.2 Authenticated Lightweight Encryption (ALE)

It is the new "AES-128" operation mode which can be compared with high-performance encryption scheme of authentication known as "Offset Codebook (OCB)" mode which is also used with "AES block cipher" (Bogdanov et al, 2014). According to ALE designers, ALE needs less memory and smaller circuit as compared to OCB. ALE supports both authentication/integrity and encryption by generating "message authentication code (MAC)" while encrypting the data. In "single-pass" scheme, authentication and encryption is performed in similar AES rounds. Meanwhile, strategies like "Encrypt-then-MAC (EtM)" need two AES operations. First of all, plaintext data go through all the rounds of AES and encrypted data

have to pass through all AES rounds to create MAC.

In addition, design of ALE depends upon nonce (a random number which is used only once) and related data, along with the message, split into 128-bit blocks and similar-sized master key. Associated data should not be encrypted but should have calculated MAC. ALE is known to be the "single-pass authenticated encryption" with "associated data (AEAD)" model. The ALE's design is novel as compared to earlier AES lightweight schemes defined in the section. Along with optimizing hardware architecture with top performing S-Box and using MixColumns, ALE reduces number of AES rounds in a lot of operations. It reduces encryption from 10 to 4 rounds, including 4-round key schedule.

ALE is known as a hybrid scheme (Agrawal et al, 2019). The hybrid nature of ALE comes from blending stream cipher and block cipher operations as it relies on LEX streaming cipher feature (Biryukov, 2007), where a "block cipher outputs (leaks)" bits with encryption. While encrypting the data associated with four AES rounds, the ALE leaks 16 bytes (128 bits) of data. With the plaintext block or first message, the XORed create the ciphertext. This is the stage of initialization to generate data state and key state. Data state can be considered as input for creating the related data, along with 4 AES rounds. AES can be used with less rounds with simplified explanation.

When ALE is adopted in "application-specific integrated circuit (ASIC)" or chip, when it comes to circuit size, ALE is compared to ASC-1, i.e., a stream cipher (Jakimoski & Khajuria, 2012). ALE is almost half the size of implementing ASC-1, but it is roughly 4.5x faster than ASC-1. The model needs just "2500 gate equivalents (GEs)" of area which is a lot smaller than that of lightweight "AES-CCM and AES-OCB". When using parallel software with "AES new instructions (AES-NI)" by Intel, ALE performs better than "AES-GCM, AES-CCM, and ASC-1". It is well-regarded as all-round AEAD model due to its high performance and hardware efficiency.

4.2.3 Elliptic Curve Cryptography (ECC)

Whitfield Diffie and Martin Hellman (DH) introduced the concept of "public-key cryptography" to solve the problem of key management (Diffie & Hellman, 2022). Each party has a pair of keys in their concept – one is public key and another is private key. These keys are associated with one another mathematically. DH is aimed for 2-party communication. However, it doesn't suit well in situations where group members change constantly. Group communications are made with participation of two members which are supported by extension of DH, i.e., "Group Diffie–Hellman key exchange (GDH)" (Steiner et al, 1996).

A lot of approaches have been proposed to improve DH protocol for key exchange. Two different extensions of DH are proposed by Steiner et al (1996). The findings suggest best performance in the process of rekeying and they used single message. Schnyder et al (2016) proposed the drawback of works by Steiner et al (2000). They approved the communication control of last two specific parties for just the key exchange duration with active attack. Some changes are made to the previous protocol by Ateniese et al (2000) and "double DH key exchange" is used. The issue is processing a lot of rounds and sending a lot of messages in all the protocols during the communication while setting agreement of initial key. Public key cryptography is used on the basis of elliptic curves and can solve problems associated with

key management in WSNs.

Using ECC represents "lightweight asymmetric-key algorithms" to provide "128-bit cryptographic security" with 256-bit key, i.e. a lot smaller than 3072-bit key of "public-key encryption model RSA" which is used most widely (Seok et al, 2019). ECC is applied to different cryptographic models, including the "elliptic curve digital signature algorithm (ECDSA)" and "Elliptic Curve Diffie–Hellman (ECDH)". Hussein et al (2022) tested encryption method proposed with various parameters like hop counts, power consumption, packet header size, and transferred messages. They presented experimental findings in this part. Table 2 represents performance of rekeying operation efficiently on a traditional embedder processor" running full OS rather than optimized and customized image. The header specifies number of nodes in the cluster. After using 8 devices, those scenarios with asterisk which need higher number of computational threads were used. Threads were distributed evenly among devices.

Table 2 – Calculation of rekeying operation performance in milliseconds

Total threads (nodes)	Time consumed (in ms)
8	0.000548
16	0.0011
32	0.001478
64	0.004942
128	0.013898
256	0.19402
512	0.051176
1024	0.14292

Source - Hussein et al (2022)

5. Conclusion and Future Works

IoT and WSNs have gained a lot of attention over the years for being capable to serve a lot of applications. Along with regular tasks, security and privacy are significant challenges of wireless networks because of limitations of sensor devices. This study has proposed key management approach to distribute, generate, and rekey processes with ECC for security in tough WSN scenarios. Findings suggest reliable and secure connections with limited time consumption and fewer overheads.

5.1 Lessons learned

This study is helpful for researchers to understand challenges related to hardware security for IoT systems. It explains the support of IoT communication with CIA triad by adopting either traditional asymmetric or symmetric encryption models. Here are some of the lessons learned with this study:

- Adopt encryption-only functions – For the link between the gateway and the device and for the smart device, it eases the computation when it supports only encryption. It is

practical in a lot of IoT systems and data is sent by the device in the uplink. Although device should get encrypted data, a base station or server can use the operation of decryption, as in "over-the-air-authentication in LoRa" when "Joint Accept" message is sent by the Join Server using "AES-128 ECB" decryption.

- Link layer security evaluated on the basis of public or private network – In a lot of cases, the link between gateway and smart devices is a safe haven at the edge network as it is in a private network or in a protected site. Security is very important in the public domain or in commercial network which connects gateway to application server. Though it is applied to some energy utility and manufacturing networks, although all IoT systems haven't protected wireless sensors. A lot of IoT applications like Zigbee and Sigfox support various security levels. For example, encryption mode or clear mode is supported by Sigfox, while Zigbee has various security levels.

- Hybrid lightweight ciphers are best for IoT – In existing communication technologies for IoT, like Sigfox, LoRa, and NB-IoT, AES-128 has been dominant in CTR mode. A lot of studies have been conducted on lightweight AES versions as hardware platforms either to cut down implementation of gate area, adopt smaller keys, or take limited rounds to reduce complexity. There is a lack of evidence to large-scale implementation of lightweight encryption models. Stream ciphers are well suited for resource-limiting devices as they encrypt every bit rather than blocks. It is possible to adopt series operations in hardware with limited resources as compared to parallel operations, even though operations of series are slower than others.

5.2 Limitations and Future Scope

Irrespective of best and great results obtained from the proposed approach, the model considers only 2D topology for placing the sensors, while it may not ne applied properly in areas where sensors are placed on rough surface. Homogenous setting is another limitation where all sensors have similar properties, while there are cases related to heterogeneity where different types of sensors are used to track various physical events. Future studies may consider experimental test of the solution proposed in this study in a more complex WSN environment to analyze heftiness of approach against some attacks while planning a 3D implementation.

References

1. Lueth, K.L. (2014). Why the Internet of Things is called Internet of Things: Definition, history, disambiguation. Retrieved from https://iot-analytics.com/internet-of-things-definition/
2. Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017). Authentication protocols for internet of things: a comprehensive survey. Security and Communication Networks, 2017(1), 6562953.
3. Brooks, R. (2019). The CIA Triangle and Its Real-World Application. Available online: https://blog.netwrix.com/2019/03/26/the-ciatriad-and-its-real-world-application
4. Chaudhary, R., Aujla, G. S., Garg, S., Kumar, N., & Rodrigues, J. J. (2018). SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment. IEEE Transactions on Industrial Informatics, 14(6), 2629-2640.
5. Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet of Things

Journal, 6(5), 8182-8201.
6. Wlazlo, P., Sahu, A., Mao, Z., Huang, H., Goulart, A., Davis, K., & Zonouz, S. (2021). Man-in-the-middle attacks and defence in a power system cyber-physical testbed. IET Cyber-Physical Systems: Theory & Applications, 6(3), 164-177.
7. Nielsen, J. J., Madueño, G. C., Pratas, N. K., Sørensen, R. B., Stefanovic, C., & Popovski, P. (2015). What can wireless cellular technologies do about the upcoming smart metering traffic?. IEEE Communications Magazine, 53(9), 41-47.
8. Hinshaw, D. & Pop, V. (2019). The Hapless Shakedown Crew That Hacked Trump's Inauguration. Wall Street Journal. Available online: https://www.wsj.com/articles/the-hapless-shake-down-crew-that-hacked-trumps-inauguration-11572014333
9. Schneier, B. (1996). Applied Cryptography—Protocols, Algorithms, and Source Code in C. John Wiley & Sons: Hoboken, NJ, USA.
10. Asare, B. T., Quist-Aphetsi, K., & Nana, L. (2020, December). A hybrid lightweight cryptographic scheme for securing node data based on the feistel cipher and MD5 hash algorithm in a local IoT network. In 2019 International Conference on Mechatronics, Remote Sensing, Information Systems and Industrial Information Technologies (ICMRSISIIT) (Vol. 1, pp. 1-5). IEEE.
11. Urooj, S., Lata, S., Ahmad, S., Mehfuz, S., & Kalathil, S. (2023). Cryptographic data security for reliable wireless sensor network. Alexandria Engineering Journal, 72, 37-50.
12. Mahlake, N., Mathonsi, T. E., Du Plessis, D., & Muchenje, T. (2023). A Lightweight Encryption Algorithm to Enhance Wireless Sensor Network Security on the Internet of Things. J. Commun., 18(1), 47-57.
13. Tropea, M., Spina, M. G., De Rango, F., & Gentile, A. F. (2022). Security in wireless sensor networks: A cryptography performance analysis at mac layer. Future Internet, 14(5), 145.
14. Fang, W., Zhang, W., Zhao, Q., Ji, X., Chen, W., & Assefa, B. (2019). Comprehensive Analysis of Secure Data Aggregation Scheme for Industrial Wireless Sensor Network. Computers, Materials & Continua, 61(2).
15. Gurunath, R., Agarwal, M., Nandi, A., & Samanta, D. (2018, August). An overview: security issue in IoT network. In 2018 2nd international conference on I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC) I-SMAC (IoT in social, Mobile, analytics and cloud)(I-SMAC), 2018 2nd international conference on (pp. 104-107). IEEE.
16. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.
17. Sohraby, K., Minoli, D., & Znati, T. (2007). Wireless sensor networks: technology, protocols, and applications. John Wiley & Sons, Hoboken, NJ, USA, pp. 15–18. ISBN 978-0-471-74300-2.
18. Devika, R., Santhi, B., & Sivasubramanian, T. (2013). Survey on routing protocol in wireless sensor network. International Journal of Engineering and Technology, 5(1), 350-356.
19. Javed, M. U., Rehman, M., Javaid, N., Aldegheishem, A., Alrajeh, N., & Tahir, M. (2020). Blockchain-based secure data storage for distributed vehicular networks. Applied Sciences, 10(6), 2011.
20. Oreku, G. S., & Pazynyuk, T. (2016). Security in wireless sensor networks. Cham, Switzerland: Springer International Publishing.
21. Hussein, S. M., López Ramos, J. A., & Ashir, A. M. (2022). A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks. Electronics, 11(17), 2721.
22. NIST (n.d.). Advanced Encryption Standard (AES) (FIPS PUB 197). Available online: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.
23. Dragomir, D., Gheorghe, L., Costea, S., & Radovici, A. (2016, September). A survey on secure

communication protocols for IoT systems. In 2016 international workshop on Secure Internet of Things (SIoT) (pp. 47-62). IEEE.
24. Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovács, I. Z., Mogensen, P., & Sorensen, M. (2017, June). Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In 2017 IEEE 85th vehicular technology conference (VTC Spring) (pp. 1-5). IEEE.
25. Gunathilake, N. A., Buchanan, W. J., & Asif, R. (2019, April). Next generation lightweight cryptography for smart IoT devices:: implementation, challenges and applications. In 2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (pp. 707-710). IEEE.
26. Chaudhari, B. S., & Zennaro, M. (Eds.). (2020). LPWAN technologies for IoT and M2M applications. Academic Press.
27. Bertsekas, D., Gallager, R., & Humblet, P. (1992). Data networks Prentice-Hall International. Inc,–544 p.
28. Wixted, A. J., Kinnaird, P., Larijani, H., Tait, A., Ahmadinia, A., & Strachan, N. (2016, October). Evaluation of LoRa and LoRaWAN for wireless sensor networks. In 2016 IEEE SENSORS (pp. 1-3). IEEE.
29. LoRa Alliance (n.d.). What Is LoRaWAN. Available online: https://lora-alliance.org/resource-hub/what-lorawanr
30. Shin, E., & Jo, G. (2017, October). Structure of nb-iot nodeb system. In 2017 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 1269-1271). IEEE.
31. Migabo, E., Djouani, K., & Kurien, A. (2018, October). A modelling approach for the narrowband IoT (NB-IoT) physical (PHY) layer performance. In IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society (pp. 5207-5214). IEEE.
32. Wang, Y. P. E., Lin, X., Adhikary, A., Grovlen, A., Sui, Y., Blankenship, Y., ... & Razaghi, H. S. (2017). A primer on 3GPP narrowband Internet of Things. IEEE communications magazine, 55(3), 117-123.
33. Mangalvedhe, N., Ratasuk, R., & Ghosh, A. (2016, September). NB-IoT deployment study for low power wide area cellular IoT. In 2016 ieee 27th annual international symposium on personal, indoor, and mobile radio communications (pimrc) (pp. 1-6). IEEE.
34. Khan, M. N., Rao, A., & Camtepe, S. (2020). Lightweight cryptographic protocols for IoT-constrained devices: A survey. IEEE Internet of Things Journal, 8(6), 4132-4156.
35. Pirzada, S. J. H., Murtaza, A., Hasan, M. N., Xu, T., & Jianwei, L. (2019, August). The implementation of AES-CMAC authenticated encryption algorithm on FPGA. In 2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET) (pp. 193-197). IEEE.
36. Song, J. H., Poovendran, R., Lee, J., & Iwata, T. (2006). Rfc 4493: The aes-cmac algorithm.
37. Vejlgaard, B., Lauridsen, M., Nguyen, H., Kovács, I. Z., Mogensen, P., & Sorensen, M. (2017, June). Coverage and capacity analysis of sigfox, lora, gprs, and nb-iot. In 2017 IEEE 85th vehicular technology conference (VTC Spring) (pp. 1-5). IEEE.
38. Goulart, A. E., & Sahu, A. (2016). Cellular IoT for mobile autonomous reporting in the smart grid. International Journal of Interdisciplinary Telecommunications and Networking (IJITN), 8(3), 50-65.
39. 3GPP TR (2015). 45.820 Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT). V13, 1.
40. Fattah, H. (2018). 5G LTE Narrowband Internet of Things (NB-IoT). CRC Press.
41. Goulart, A., Chennamaneni, A., Torre, D., Hur, B., & Al-Aboosi, F. Y. (2022). On wide-area IoT networks, lightweight security and their applications—a practical review. Electronics, 11(11), 1762.
42. Yu, W., & Köse, S. (2017). A lightweight masked AES implementation for securing IoT against CPA attacks. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(11), 2934-2944.

43. James, M., & Kumar, D. S. (2016). An implementation of modified lightweight advanced encryption standard in FPGA. Procedia Technology, 25, 582-589.
44. Acla, H. B., & Gerardo, B. D. (2019). Performance evaluation of lightweight advanced encryption standard hardware implementation. Int. J. Recent Technol. Eng. IJRTE, 8(2), 1810-1815.
45. Bogdanov, A., Mendel, F., Regazzoni, F., Rijmen, V., & Tischhauser, E. (2014). ALE: AES-based lightweight authenticated encryption. In Fast Software Encryption: 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers 20 (pp. 447-466). Springer Berlin Heidelberg.
46. Agrawal, M., Zhou, J., & Chang, D. (2019). A survey on lightweight authenticated encryption and challenges for securing industrial IoT. Security and privacy trends in the industrial internet of things, 71-94.
47. Jakimoski, G., & Khajuria, S. (2012). ASC-1: An authenticated encryption stream cipher. In Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers 18 (pp. 356-372). Springer Berlin Heidelberg.
48. Biryukov, A. (2007). The design of a stream cipher LEX. In Selected Areas in Cryptography: 13th International Workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 Revised Selected Papers 13 (pp. 67-75). Springer Berlin Heidelberg.
49. Diffie, W., & Hellman, M. E. (2022). New directions in cryptography. In Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman (pp. 365-390).
50. Steiner, M., Tsudik, G., & Waidner, M. (1996, January). Diffie-Hellman key distribution extended to group communication. In Proceedings of the 3rd ACM Conference on Computer and Communications Security (pp. 31-37).
51. Schnyder, R., López-Ramos, J. A., Rosenthal, J., & Schipani, D. (2016). An active attack on a multiparty key exchange protocol. Journal of Algebra Combinatorics Discrete Structures and Applications, 3(1), 31-36.
52. Steiner, M., Tsudik, G., & Waidner, M. (2000). Key agreement in dynamic peer groups. IEEE Transactions on Parallel and Distributed Systems, 11(8), 769-780.
53. Ateniese, G., Steiner, M., & Tsudik, G. (2000). New multiparty authentication services and key agreement protocols. IEEE journal on selected areas in communications, 18(4), 628-639.
54. Seok, B., Sicato, J. C. S., Erzhena, T., Xuan, C., Pan, Y., & Park, J. H. (2019). Secure D2D communication for 5G IoT network based on lightweight cryptography. Applied Sciences, 10(1), 217.