Enhancing Security and Efficiency in IoT-Based Oil & Gas Pipeline Monitoring Systems with a Novel Lightweight Cryptography Framework

Maniru Malami Umar
Department of Computer Science
Usmanu Danfodiyo University,
Sokoto, Nigeria
maniru.umar@udusok.edu.ng

Sadiq Aliyu Ahmad
ICT Directorate
Federal University, Dutse
Jigawa, Nigeria
sadiqaliyu@fud.edu.ng

Abdulhakeem Abdulazeez
Department of Computer Science
Usmanu Danfodiyo University,
Sokoto, Nigeria
abdulhakeem.abdulazeez@udusok.edu.ng

Ziya'u Bello
Crusader Sterling Pensions
Sokoto, Nigeria
ziyaulhaqbello@gmail.com

Bello Alhaji Buhari
Department of Computer Science
Usmanu Danfodiyo University,
Sokoto, Nigeria
buhari.bello@udusok.edu.ng

Asma'u Shehu
Department of Computer Science
Sokoto State University
Sokoto, Nigeria
asmausidi4@gmail.com

***Abstract* — The oil and gas industry rely heavily on the seamless and secure operation of pipelines to transport valuable resources. In this context, the integration of Internet of Things (IoT) technologies offers the potential to enhance monitoring systems, providing real-time insights and data-driven decision-making. This study presents a novel framework for IoT-based oil and gas pipeline monitoring, designed to bolster security, data accuracy, and operational efficiency. The framework encompasses strategic sensor placement, a rotational cluster head selection scheme, efficient data aggregation, and robust data encryption using the ASCON-128 Cipher. By strategically positioning IoT sensors and employing advanced data aggregation techniques, redundant data transmission is minimized, significantly improving the accuracy and efficiency of data collection. Additionally, the rotational cluster head selection scheme optimizes power consumption, extending the operational lifespan of IoT devices. While this framework is currently in the conceptual phase, it holds great promise for addressing industry-specific challenges. Future work should focus on practical implementations, security protocol development, performance evaluations, scalability assessments, user authentication enhancements, and system integration.**

Keywords—Lightweight, Cryptography, IOT, Pipeline Monitoring

I. INTRODUCTION

The recent advancement in technology is now leading the world to a stage where devices and everything will be able to communicate and be connected. The type of technology that provides communication among any devive, any place, and at any time is termed as Internet of Things (IoT). It is sometimes referred to Internet of the future that will enable machine-to-machine (M2M) learning [1]. The Internet of Things (IoT) is a network of connected devices equipped with sensors, software, or other technologies to gather, store, and share data via the internet. The IoT is used to address issues related to human living such as energy management, climate change, transportation, healthcare, business logistics, building automation, oil and gas, etc.

The vision of IoT is to build a smart environment by utilizing smart things/objects/devices that have sensory and communication capabilities to autonomously generate data and transmit it via the Internet for decision-making [2]. Such decisions are used to address issues related to human living such as energy management, climate change, transportation, healthcare, business logistics, building automation, oil and gas, etc. The oil and gas industry is one of the largest, most complex, and important global industries. In the oil and gas industries, data need to be generated, gathered, communicated, stored, and processed at the upstream, midstream, and downstream sectors. Research in [3] highlighted some of the applications of IoT in the three sectors of the oil and gas industry supply chain. At the upstream, data at the reservoir can be integrated with real-time field data to plan well placement and flow rates. IoT is used at the midstream where sensors are installed in the pipeline to monitor leakage and other usual movements around the oil pipelines. At the downstream, refineries can plan their shutdown, improve safety, and minimize their downtime.

However, with the increasing use of IoT devices in various industries including the oil and gas industry, cybersecurity has become a major concern. Cybersecurity for IoT devices focuses on protecting, monitoring, and remediating threats related to IoT devices that are connected to the internet. The devices include traditional endpoints such as computers, laptops, mobile phones, tablets, and servers as well as non-traditional items such as printers, cameras, appliances, smart watches, health trackers, navigation systems, smart locks, or smart thermostats. The oil and gas industry is one of the largest industries in the world and has heavily embraced digital transformation with an acute focus on IoT. However, this industry is vulnerable to cyber-attacks due to its unique structure divided into upstream, midstream, and downstream segments. The upstream segment responsible for exploration and extraction of raw materials is often spread across vast geographical areas making cybersecurity oversight a daunting task. The midstream sector tasked with transportation and storage faces similar challenges compounded by reliance on third-party vendors.

Meanwhile, the downstream segment which focuses on refining and distribution often relies on legacy systems lacking effective measures to fend off modern cyber threats.

Incidents of oil thefts, pipeline vandalizations, fire, and others have been the order of the day in communities where oil pipelines are located such as Niger Delta in Nigeria. Apart from the traditional methods of monitoring pipelines i.e., deploying security personnel to monitor the pipeline, some companies deploy several technologies/systems to monitor oil pipelines [4]. Several IoT-based solutions have been proposed to address some of the challenges faced in monitoring pipelines in the oil and gas industry [5]. However, it is important to ensure that these solutions are secure from cyber threats. To secure transmitted data between IoT devices and local service servers in IoT systems such as those used in oil and gas industry supply chain management systems, a lightweight security system comprising Cryptography and Cybersecurity of IoT has been proposed.

Sensors deployed in close proximity to one another will usually report similar or the same data about the condition of the pipeline. Therefore, the sink will require a lot of processing power to receive and forward data to the control center. However, ensuring the security of data transmission in these systems, particularly with the introduction of a lightweight security system, leads to the following problems: 1. Bandwidth Efficiency: Due to the close proximity of sensors, redundant data transmission results in inefficient bandwidth utilization, and decreasing goodput. 2. Processing Overhead: The sink, responsible for data forwarding, faces increased processing demands due to duplicate data, potentially straining infrastructure capabilities. 3. Battery Drainage: The sink's battery life diminishes rapidly due to extensive data processing, requiring frequent maintenance in remote locations. 4. Cyber Threats: Transmitted data is vulnerable to cyber threats, including breaches and unauthorized access, posing risks to operational integrity and sensitive information

Therefore, the main contributions of this research work are:

1. Development of a robust Lightweight Cryptography Framework tailored to meet the stringent security requirements of IoT-based oil and gas pipeline monitoring systems. Which will ensure data confidentiality and integrity, significantly reducing vulnerabilities to cyber threats.
2. Introduce a clustering technique that will decentralize the transmission of data from sensing devices thereby increasing the goodput of the collected data.
3. Maximizing the operational lifespan of IoT sensing devices, we propose a rotational cluster head selection scheme. This scheme effectively balances power consumption among sensing devices, resulting in prolonged battery life, reduced operational disruptions, and minimized maintenance requirements.

The remaining sections of the paper is organized as follows: Section II gives an overview of related works. Section III presents the proposed framework of the system (methodology). The discussion & future research is given in section IV. Finally, the conclusion is given in Section V

II. RELATED WORK

A. Application of IoT in monitoring oil pipelines

In a study conducted by [6], a reliable IoT-based architecture for the oil and gas industry to monitor various operations in the upstream, midstream, and downstream sectors of the oil and gas industry. The architecture comprises three modules; smart object, gateway, and the control center module. The system performs predictive maintenance of the various oil and gas industry assets by analyzing the sensed data and detecting failure modes before or when the equipment fails or needs to be serviced.

[7] presented a resilient IoT-based monitoring system for crude oil pipelines for detecting and mitigating pipeline failures. The scheme has three major components: Coverage, detection, and resilience. At the coverage part, the scheme deploys several sensors by considering the crude oil propagation properties in the pipeline which is contrary to the traditional way of deploying sensors where sensors are only deployed at key junctions. The scheme further uses a combination of Pressure Point Analysis (PPA), Gradient-Based (GB), and Negative Pressure Wave Method (NPWM) as techniques for leak detection to reduce inefficiency and high rate of false alarms. The scheme improves the detection rate of leakage because of the multiple sensor deployment but wastes resources due to the fact that multiple sensors can report the same information.

[8] proposed an IoT-enabled pipeline leakage detection and real-time alert system that detects. The real-time monitoring was achieved by using a measurement of flow rate (rate of flow of liquid) technique with the aid of a flow sensor. The scheme effectively monitors leakages on pipelines in real time and necessary actions are taken by the system such as turning on the safety alarm and shutting down any pipeline system that has several leakages. However, the battery power of the sensors will be drained as they communicate directly with the IoT system.

A distributed leakage detection and localization technique was proposed by [9]. The scheme was aimed at reducing the high rate of false detection alarms. It deployed several sensors in a distributed manner using a mesh connection and pre-processing of information among geographically close sensors. The scheme improves the accuracy of alarm reporting and also eliminates the single point of failure by implementing a distributed leak detection technique. However, there is an increase in the processing overhead due to the large volume of data processed by the sink. Transportation of oil and gas products from the exploration sites to refineries or any storage facility is one of the most important stages in the oil and gas industry, and in most cases, the transportation is done via pipelines. Therefore, there is a need for an efficient oil pipeline monitoring system that will effectively monitor transportation, collect accurate data, and improve the battery life of the sensing devices.

B. Cyber Security

[10] highlighted the escalating vulnerabilities of Internet of Things (IoT) devices, emphasizing the increasing frequency of attacks, both physical and through social engineering, targeting these devices. They pointed out that such attacks compromise users' devices, infiltrate data, and enable surveillance of user activities, potentially leading to malicious operations, reputation damage, or financial theft. The authors stressed that IoT devices, including laptops and computers, are highly susceptible to electronic crimes and underscored the urgent need for heightened security measures and user awareness in this interconnected IoT environment.

In their paper, [11] draw attention to a critical issue: the absence of HSTS policy implementation in the web servers of IoT devices. To provide clarity, they categorize these issues into two primary categories and explore the potential exploitation of these vulnerabilities through simulations in a local IoT environment. This research highlights the importance of addressing security concerns in IoT device web servers to enhance overall cybersecurity.

[12] have introduced an innovative IoT security framework aimed at enhancing authentication and authorization protocols to safeguard IoT systems from various attacks, including man-in-the-middle, reply, and brute-force attacks. This framework combines an improved token authentication system with a novel sender verification mechanism based on timestamps, potentially reducing the need for localized identity verification on IoT devices. Through comprehensive security analyses, the authors demonstrated the framework's superior capability in protecting IoT networks against a range of attacks when compared to existing security frameworks. Additionally, they implemented and validated the framework using Windows applications, affirming its practicality and efficiency within real network environments while assessing its impact on payload time.

[12] presented a novel approach to enhance security in IoT data transmission, enabling individual device identification and efficient key exchange using an asymmetric cryptosystem. Their research demonstrated that this hybrid cryptosystem achieved minimal time delays, making it a practical and effective solution for IoT security.

Numerous encryption algorithms have been proposed to address security concerns [13][14][15]. A fundamental approach to securing transmitted data is to employ a shared security code between the data transmitter and the receiver. By using the same security code, data can be encrypted at the sender's end and decrypted at the receiver's end.

In network communication, the exchange of data between different hosts is a common practice. However, without adequate protection measures, this data is vulnerable to eavesdropping by malicious third-party entities or attackers [16][17]. Furthermore, in the absence of encryption, sensitive information is susceptible to interception and exposure. Therefore, the implementation of data encryption is essential to safeguard data from unauthorized access.

Given the diversity of IoT devices, it is crucial to consider the computing resources and capabilities of different types of IoT devices[18]. This is especially relevant in IP-based network environments where IoT devices need to secure and exchange data [19].

Using a common security code or security key allows IoT devices with limited computing resources to provide adequate security for transmitted data. Notable cryptographic methods such as Message Digest Algorithm 5 (MD5) and Secure Hash Algorithm (SHA-2) have been proposed to enhance data security [20] Hash functions play a vital role in data encryption, enabling secured data to be decrypted by both the sender and receiver using the same encryption hash function.

III. METHODOLOGY

The security, effectiveness, and accuracy of data are crucial in the context of IoT-based oil and gas pipeline monitoring. This section offers a reliable way for extending these monitoring systems' functionalities using a lightweight cryptography framework. Our methodology addresses important issues in this field by utilizing IoT sensors, rotational cluster head selection, effective data aggregation, and encryption using the ASCON-128 cipher. User authentication additionally secures data retrieval, resulting in a comprehensive framework that raises the bar for security and dependability in oil and gas pipeline monitoring. This section describes the methodical procedures used to create and validate our framework, which helped it gain acceptance and prove useful in practical industrial applications.

A. Design of Data Collection through IoT Sensors:

IoT sensors, including flow sensors and gas sensors, are strategically placed within the oil and gas pipeline environment to continuously gather data. These sensors monitor various crucial parameters, such as fluid flow rates and gas concentrations, providing real-time insights.

B. Rotational Cluster Head Selection Scheme:

We implement a rotational cluster head selection strategy in the framework development process to reduce the power consumption of IoT sensing devices. In order to reduce power consumption, increase the operational lifespan of IoT devices, and reduce the likelihood of operational disruptions and maintenance requirements, this theoretical plan reassigns cluster heads within the network on a regular basis. Saving electricity is crucial for extending the operational life of devices in a typical IoT network, such as sensors, which may have limited power sources like batteries. The strategy works by redistributing the cluster heads' responsibilities across the network on a regular basis. Devices known as cluster heads are in charge of managing and aggregating data from various sensors inside their specific clusters. This redistribution helps prevent specific devices from exhausting their power reserves quickly, thus extending their operational lifespan. Frequent cluster head reassignments are carried out in a coordinated manner, ensuring that data collection and transmission continue seamlessly without significant interruptions. by reducing power consumption and extending the operational lifespan of IoT devices, this scheme also minimizes maintenance requirements. Fewer device replacements and maintenance interventions are needed, contributing to cost savings and operational efficiency.

C. *Efficient Data Aggregation Mechanism*

Within the framework, we integrate an efficient data aggregation mechanism to streamline the data processing flow. This mechanism aggregates data from multiple sensors before transmission, significantly reducing the processing overhead on IoT devices. Notably, it enhances system efficiency while ensuring the accuracy and reliability of the collected data.

D. *Data Encryption using ASCON-128 Cipher*

In our framework development, we introduce a critical security measure known as "Data Encryption using the ASCON-128 Cipher." The integrity and security of the data gathered within the IoT-based oil and gas pipeline monitoring system are fundamentally protected by this encryption procedure. The ASCON-128 Cipher's use is primarily intended to dramatically increase data security. Maintaining data security and integrity is crucial when discussing sensitive information pertaining to oil and gas pipeline monitoring. Because of its lightweight and suitability for IoT contexts with limited resources, ASCON-128 was chosen. Despite being effective, this cryptographic method offers high levels of security. The ASCON-128 Cipher is used to encrypt data before it is sent from the sink node.

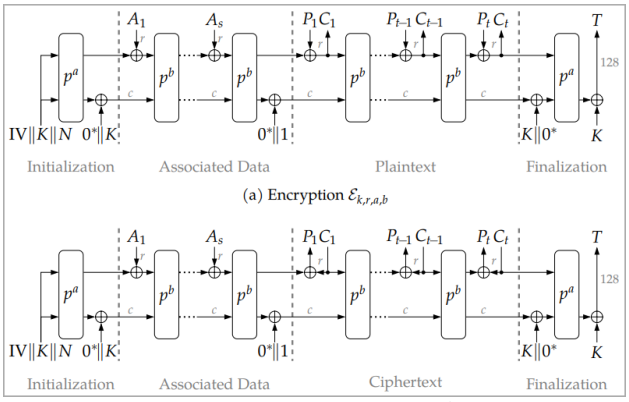

Fig 1 ASCON's encryption and decryption modes of operation (NIST)

Fig 1 above shows the ASCON encryption and decryption mode. This encryption process effectively transforms the data into an unreadable format, ensuring that sensitive information remains protected during its journey from the sensors to its destination. The ASCON-128 Cipher not only ensures confidentiality but also verifies the integrity of the data. It guarantees that the information has not been tampered with or altered during transit, thus maintaining its reliability. By incorporating this encryption process, our framework significantly enhances the overall security posture of the IoT-based oil and gas pipeline monitoring system. It shields the data from potential eavesdropping, unauthorized access, and tampering, safeguarding it against cyber threats.

E. *Secure Data Transmission to Cloud or Storage*

Encrypted data is securely transmitted to designated cloud storage or storage facilities. The data transmission process guarantees the privacy and integrity of the data, preventing unauthorized access and tampering.

F. *User Authentication for Data Retrieval:*

To access the stored data, end-users are required to undergo a robust authentication process. This authentication step ensures that only authorized individuals or systems can retrieve and utilize the monitored data..

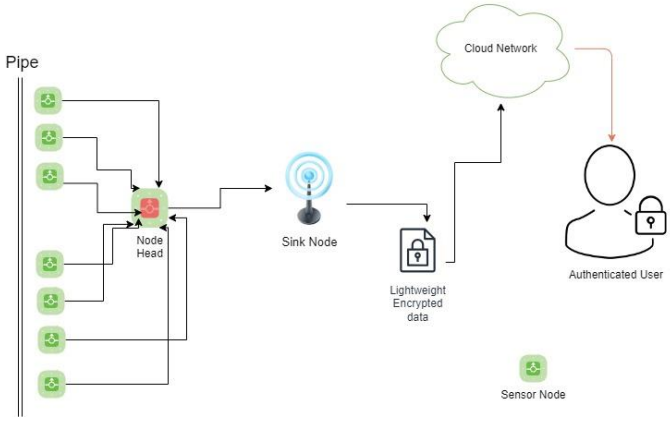

Fig 2 Framework of the Enhanced IoT-Based Oil & Gas Pipeline Monitoring.

The Fig 2. Show the framework for enhanced IoT-based oil and gas pipeline monitoring systems that integrates various components to optimize data collection, processing, and security. By employing rotational cluster head selection, efficient data aggregation, and the lightweight ASCON-128 cipher, the framework aims to enhance operational efficiency, data integrity, and security in oil and gas pipeline monitoring. User authentication further adds an extra layer of protection, ensuring that only authorized parties can access and utilize the valuable data. This comprehensive methodology enhances the capabilities and reliability of IoT-based monitoring systems in the oil and gas industry.

IV. DISCUSSION AND RECOMMENDATIONS FOR FUTURE WORK

The framework we have outlined presents a conceptual blueprint for enhancing security, data accuracy, and efficiency in IoT-based oil and gas pipeline monitoring systems. Each component of the framework serves a specific purpose and contributes to the overall improvement of the monitoring process. The strategic design of sensor placement and parameter selection are crucial for ensuring that the right data is collected. However, it's important to note that the actual implementation of sensor deployment in the pipeline environment would require careful consideration of practical factors such as sensor types, communication protocols, and environmental challenges. The rotational cluster head selection scheme holds the potential to optimize power consumption and extend the operational lifespan of IoT devices. This is particularly significant for remote and inaccessible pipeline locations. However, real-world implementation would necessitate a detailed study of the network topology, device capabilities, and coordination mechanisms. The encryption of data using the ASCON-128 Cipher is essential for ensuring the confidentiality and integrity of information during transmission. To implement this security measure, it's critical to develop secure key management processes, and encryption libraries, and ensure compatibility with IoT devices' computing resources.

V. CONCLUSION

This study introduces a comprehensive framework for enhancing the security, data accuracy, and efficiency of IoT-based oil and gas pipeline monitoring systems. The framework combines strategically planned data collection through IoT sensors, an innovative rotational cluster head selection scheme, efficient data aggregation, and robust data encryption using the ASCON-128 Cipher. The proposed IoT-based oil pipeline monitoring system promises effective monitoring by minimizing data redundancy and increasing data accuracy through clustering and data aggregation techniques. Furthermore, these techniques reduce the power consumption of sensing devices, enhancing the efficiency of the monitoring system. While this framework is currently in its conceptual stage, its potential impact on the oil and gas industry is significant. Future work should focus on practical implementations, security protocol development, performance evaluations, scalability assessments, user authentication enhancements, and system integration.

REFERENCES

[1] K. Chopra, K. Gupta and A. Lambora, "Future Internet: The Internet of Things-A Literature Review," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), Faridabad, India, 2019, pp. 135-139, doi: 10.1109/COMITCon.2019.8862269.

[2] M. Chernyshev, Z. Baig, O. Bello and S. Zeadally, "Internet of Things (IoT): Research, Simulators, and Testbeds," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1637-1647, June 2018, doi: 10.1109/JIOT.2017.2786639.

[3] S. Shoja and A. Jalali, "A study of the Internet of Things in the oil and gas industry," 2017 IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), Tehran, Iran, 2017, pp. 0230-0236, doi: 10.1109/KBEI.2017.8324979.

[4] A. S. Allahloh and S. Mohammad, "Development of The Intelligent Oil Field With Management and Control using IIoT (Industrial Internet of Things)," 2018 2nd IEEE International Conference on Power Electronics, Intelligent Control and Energy Systems (ICPEICES), Delhi, India, 2018, pp. 815-820, doi: 10.1109/ICPEICES.2018.8897439.

[5] P. Flichy and C. Baudoin, "The Industrial IoT in Oil & Gas: Use Cases," presented at the SPE Annual Technical Conference and Exhibition, Dallas, Texas, USA, September 2018.

[6] W. Gharibi, M. Aalsalem, W. Z. Khan, N. Armi and W. Ghribi, "Monitoring gas and oil fields with reliable wireless sensing and Internet of Things," 2017 International Conference on Radar, Antenna, Microwave, Electronics, and Telecommunications (ICRAMET), Jakarta, Indonesia, 2017, pp. 188-191, doi: 10.1109/ICRAMET.2017.8253173.

[7] S. Ahmed, F. Le Mouël and N. Stouls, "Resilient IoT-based Monitoring System for Crude Oil Pipelines," 2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Paris, France, 2020, pp. 1-7, doi: 10.1109/IOTSMS52051.2020.9340197.

[8] K. Lalitha, V. Balakumar, S. Yogesh, K. M. Sriram, and V. Mithilesh, "IoT Enabled Pipeline Leakage Detection and Real-Time Alert System in the Oil and Gas Industry," International Journal of Recent Technology and Engineering (IJRTE), vol. 8, no. 5, January 2020.

[9] S. Ahmed, F. Le Mouël, N. Stouls, and G. Lipeme Kouyi, "HyDiLLEch: A WSN-Based Distributed Leak Detection and Localization in Crude Oil Pipelines," in Proceedings of the Advanced Information Networking and Applications, 2021, pp. 54. DOI: 10.1007/978-3-030-75100-5_54.

[10] M. M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview," Mesopotamian Journal of Cyber Security, 2023.

[11] Srivastava, A.; Shah, P. Identification of the Issues in IoT Devices with HSTS Not Enforced and Their Exploitation. In Proceedings of the 2021 International Conference on Security and Information Technologies with AI, Internet Computing and Big-Data Applications, Taichung City, Taiwan, 18–20 November 2021; Springer: Cham, Switzerland, 2023; pp. 325–334

[12] M.-S. Jian and J. M.-T. Wu, "Hybrid Internet of Things (IoT) Data Transmission Security Corresponding to Device Verification," Journal of Ambient Intelligence and Humanized Computing, 2021. doi: 10.1007/s12652-021-03122-y.

[13] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges," 2018

[14] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, and Y. Elovici, "Security Testbed for Internet-of-Things Devices," IEEE Transactions on Reliability, vol. 68, no. 1, pp. 23–44, 2019.

[15] M. G. Samaila, J. B. Sequeiros, T. Simões, M. M. Freire, and P. R. Inácio, "IoT-HarPSecA: A Framework and Roadmap for Secure Design and Development of Devices and Applications in the IoT Space," IEEE Access, vol. 8, pp. 16462–16494, 2020.

[16] H. Tschofenig and E. Baccelli, "Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security," IEEE Security & Privacy, vol. 17, no. 5, pp. 47–57, 2019.

[17] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A Survey on Security and Privacy Issues in Edge Computing-Assisted Internet of Things," IEEE Internet of Things Journal, 2020. doi: 10.1109/JIOT.2020.3015432.

[18] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8182–8201, 2019.

[19] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," IEEE Internet of Things Journal, vol. 7, no. 10, pp. 10250–10276, 2020.

[20] H. Mack and T. Schroer, "Security Midlife Crisis: Building Security in a New World," IEEE Security & Privacy, vol. 18, no. 4, pp. 72–74, 2020.