IoT Security for D-App in Supply Chain Management

Teodor CERVINSKI, Cristian TOMA
Bucharest University of Economic Studies, Romania
cervinskiteodor17@stud.ase.ro, cristian.toma@ie.ase.ro

The fast advance and evolution of technology in Internet of Things (IoT) is a double-edged sword, striking with new performant solutions and backfiring with a lot of unanswered questions. Due to cheap manufacturing costs and large-scale production, sensors, actuators and even microcontrollers are not designed with security on the first place. Also, the IoT market is a new one and that means that it is still unregulated and there isn't a well-defined set of standards to control and manage better these problems. The IoT ascent has impacted many industries, but probably the most changes were made to the Supply Chain Management (SCM) industry. The forementioned question of cheap devices that need to be manufactured with a minimum of costs, very fast and ready to be deployed, is digging a big security hole in this kind of ecosystems. This paper aims to discuss the challenges involved in hardening de security in embedded devices, protecting the data and the communication channels between an IoT node and an IoT gateway and finally, assuring the persistence of data and its security after is stored. All these matters are addressed with privacy and security in design. Because SCM is a multi-party ecosystem that involves many different actors each with its tasks and data handling components, it is important to assure the fact that they will not interfere, tamper, or profit in a bad manner of each other. One solution for this problem is decentralization that comes with strings attached. Finally, and on short, this paper will try to describe a security model based on decentralization in a SCM flow, addressing its threats and how they can be overcome.
Keywords*: IoT, Blockchain, Security, Cryptography, Decentralization, Supply Chain Management*
DOI: 10.24818/issn14531305/28.1.2024.06

1 Introduction

As the rest of commerce's fields, Supply Chain Management is evolving blazingly fast. Being strongly corelated and heavily tied to cross-domain fields such as engineering (industrial and systems), logistics, operations, and procurement, can be looked like a real challenge when discussing information theory's new breakthroughs. Such an ecosystem is complex by design and each core component has its problems to address. Recently, with the advance of IoT, the Supply Chain Management has seen big improvements. There are a lot of capable, performant internet connected devices, and as many software solutions that aid those system to be more efficient and productive. For example, the sensors are becoming "smart", being connected to the Internet, and providing real time telemetry data, the data is stored in cloud and the clients have mobile apps which can query the data and generate reports in real time. But for all mentioned things, there can be raised a big question: how is security addressed in such solutions?

The recent trends [1] showed that threat actors are more and more menacing, hitting with success every target they want to compromise. Talking about security incidents in fields tangent with Supply Chain Management a recent example is *Colonial Pipeline ransomware attack.*

The paper is addressing the challenging task to design a Supply Chain Management having security in its design. More than that, such a system implies work from more than 2 parties. Those parties can be data controllers and data processors meaning that data is at stake and privacy should be also a big concern.

2 Literature Review

The security concern has been addressed but only in research papers. There is a lack of standards in this field, and it's shown by how

insecure things are especially in IoT. R. Mahmoud et al. [2] explained that security should be enforced at every layer to obtain a secure IoT system. The fact that there are not many standards or standardized protocols, and solutions give malicious users a large vector of attack. N. Neshenko et al. [3] did surveys regarding the attack vectors and kept a classification of common vulnerabilities met in such ecosystems. The main problem is the variety of systems involved within inner core of smart Supply Chain Management solutions. More than this, low power devices such as sensors or actuators are very targeted toward DoS and DDoS attacks. More than this the same nature of constrained devices, that makes them vulnerable to high loads from DDoS attacks, is also a problem regarding cryptography. A study from 2021 [4] did a comparison and a classification of more than 50 lightweight cryptography algorithms present in the current market and more than 57 algorithms submitted at NIST recent competitions. Judging by their names, constrained devices run in a very limited space of memory and computing power. However, improvements have been made regarding hardware constraints and today there are a lot of microcontrollers with powerful CPUs (especially ARM processors) and a very generous amount of RAM. Problems don't cease with technological advance though; they evolve at the same time with it. Hackers adapt their techniques and are starting to look for and attack specific flaws in the new hardware architecture, trying to dump memory or leak data. Even if that thing is hard to achieve, there are always communication channels that might be vulnerable and targeted by malicious users. It's very important to take these matters into consideration because there are not many ways to assure data confidentiality without pre-shared keys or a key sharing agreement. Each way of work has its advantages and disadvantages. Also, the search for a solution should be done by teams united from the device manufacturer, software developers and end-user clients at the same time for being able to deliver something that is secure, respect the privacy and could be easily used by who needs it. Mendez et al. [5] conducted a solid and detailed survey of the current state regarding security threats and issues on different levels in IoT and IIoT systems. More than that they presented their research on the current state of the art publications focused on IoT security. As many other industries the major concerns in IoT are confidentiality, integrity, and availability (CIA). According to Noor et al. [6] major impacts are encountered at the communication technologies that are used for linking the devices together. Security issues are present although at the operational layers, such as 6LoWPAN, LoRaWAN, routing and so on. Another major concern is the computational effect of cryptographic algorithms such as elliptic curves-based schemes.

In terms of the supply chain management solutions, there are the following well-known solutions:

- SAP Supply Chain Management (SCM): offers a comprehensive suite of tools for managing various aspects of the supply chain, including demand planning, inventory optimization, supplier collaboration, and logistics management. It provides real-time visibility into supply chain operations, enabling better decision-making and responsiveness to changing market demands.
- Oracle Supply Chain Management (SCM) Cloud: provides end-to-end supply chain visibility and control, with features such as demand forecasting, procurement, order management, inventory optimization, and logistics management. It leverages advanced analytics and artificial intelligence to improve forecasting accuracy and streamline operations.
- IBM Sterling Supply Chain Suite: enables a suite of supply chain solutions designed to enhance visibility, collaboration, and agility across the supply chain. It includes modules for order management, inventory optimization, transportation management, and supplier collaboration, with capabilities for real-time tracking and monitoring of shipments.

- Microsoft Dynamics 365 Supply Chain Management: provides tools for managing procurement, manufacturing, inventory, warehouse operations, and logistics. It integrates with other Microsoft products, such as Azure IoT, Power BI, and Office 365, to enable data-driven decision-making and process automation.
- JDA Software (now Blue Yonder) Supply Chain Management: JDA offers a range of supply chain solutions, including demand planning, inventory optimization, transportation management, and warehouse management. Its solutions leverage advanced algorithms and machine learning to improve forecasting accuracy, reduce costs, and enhance operational efficiency.

Features common across these solutions include:

- Demand Planning: Forecasting demand based on historical data, market trends, and customer insights to optimize inventory levels and ensure product availability.
- Inventory Management: Optimizing inventory levels, reducing carrying costs, and minimizing stockouts through better inventory visibility, demand forecasting, and replenishment planning.
- Procurement: Streamlining the procurement process, managing supplier relationships, and ensuring timely delivery of goods and services.
- Order Management: Managing customer orders, orchestrating order fulfillment processes, and ensuring on-time delivery.
- Logistics Management: Optimizing transportation routes, managing carrier relationships, and tracking shipments in real-time to improve delivery efficiency and reduce costs.
- Warehouse Management: Optimizing warehouse operations, including receiving, storing, picking, packing, and shipping goods, to improve inventory accuracy and order fulfillment speed.
- Analytics and Reporting: Providing insights into supply chain performance, identifying areas for improvement, and facilitating data-driven decision-making to enhance operational efficiency and customer satisfaction.

These supply chain management solutions aim to address the complexities and challenges of modern supply chains by providing end-to-end visibility, automation, and optimization capabilities.

In terms of integration of the Supply Chain Management solutions and Blockchain, there are used Ethereum and Hyperledger Fabric because they offer the ability to run smart contracts, but also, they have a lot of features which enables the collaboration among different entities.

Ethereum and Hyperledger Fabric are both blockchain platforms, but they have different design goals and architectures.

As similarities, there are several points where Ethereum and Hyperledger Fabric are implementing the same concepts, such as:

- Blockchain Technology: Both Ethereum and Hyperledger Fabric utilize blockchain technology, employing distributed ledgers, cryptographic techniques, and consensus mechanisms to ensure the integrity, immutability, and transparency of transactions.
- Modularity: Both platforms are designed with modularity in mind, allowing developers to customize and extend their functionalities according to specific requirements. However, Hyperledger Fabric places a stronger emphasis on modularity, providing a more flexible and modular architecture for building enterprise-grade blockchain applications.
- Smart Contract Support: Both platforms support smart contracts, enabling developers to create self-executing contracts with predefined rules and conditions, which are automatically enforced upon fulfillment of those conditions.

As main differences, there are the following:

- Use Case Focus: Ethereum is primarily designed for public blockchain applications, focusing on decentralized applications (D-Apps), smart contracts, and cryptocurrency transactions.

Hyperledger Fabric, on the other hand, is more suited for enterprise-level, permissioned blockchain networks, with a focus on providing modular and customizable solutions for businesses.

- Consensus Mechanisms: Ethereum uses a proof-of-work (PoW) consensus mechanism (though transitioning to proof-of-stake in ETH2), where miners compete to validate transactions and create new blocks. Hyperledger Fabric supports pluggable consensus mechanisms, allowing for more flexibility in choosing consensus algorithms tailored to specific use cases, such as Practical Byzantine Fault Tolerance (PBFT).
- Permission accessing: Ethereum is a permissionless blockchain, meaning anyone can join the network, participate in transaction validation, and deploy smart contracts. Hyperledger Fabric is permissioned, requiring participants to be authenticated and authorized before accessing the network, providing greater control and privacy for enterprise applications.
- Smart Contracts: While both platforms support smart contracts, Ethereum's smart contracts are typically written in Solidity, a high-level programming language, and executed on a global virtual machine. Hyperledger Fabric supports smart contracts written in various programming languages, such as Go, JavaScript, and Java, and executes them in isolated environments within each peer, providing better security and privacy for enterprise applications.

In summary, while Ethereum and Hyperledger Fabric are both blockchain platforms, they address different use cases and have distinct architectural features tailored to their target audiences, whether it's public decentralized applications or permissioned enterprise solutions.

3 IoT security in Supply Chain Management solutions

In practice, more exactly in this industry it's very hard to talk about a solution as a whole application or a whole system. Supply Chain Management is a concept that involves many parties. Starting from the producer and ending with the retail company there are a lot of actors, a lot of data and a lot of processing being done. The system is alike gearing with a lot of cogs. If one gets rusty, the rust will spread to all of them. The same goes with Supply Chain Management systems. They represent an entire software and hardware "ecosystem". In the past years this industry has witnessed a lot of improvements regarding digitalization. With the purpose of being more efficient and maximize the costs, the inner processes include a lot of technical features such as smart sensors, wireless connectivity, and embedded computers with a considerable amount of computing power.

Starting with the lowest level there are sensors and actuators. These tiny, low power devices take analog or digital data in most of the cases from the outer world. A sensor can detect and register changes in the pressure, temperature, distance, or velocity. If the sensor takes analog input from the outer environment, it is lately connected to ADC (Analog to Digital Converter). In most of the cases, when the sensors are referred as "smart", it's involved a microcontroller, more exactly a single-board microcontroller. This may offer wireless connectivity or computing power for processing the data received from the sensors. In Supply Chain Management, when the product is valuable and needs to be handled with care, the data should be encrypted. Encryption done at microcontroller level represents a challenge because there appear some important matters like secret key distribution, key generation, protocol security. The environment is a constrained one that doesn't have the capabilities of a normal computer. For sure, the technology advanced and managed to squeeze more memory and processing power in such boards but engineers still need to be cautious regarding the resource space. Talking about encryption of data received from the sensors, most of the time the keys are burned inside the board before putting it into production [7]. This may present an issue if the board gets

compromised by, for example, side channel attacks. A solution to this problem may be a key sharing agreement and establishment of a new key per communication session between the node and the gateway. Due to the large number of manufacturers of boards and sensors there is a lack of standardization regarding this kind of operations. More than that, manufacturers are oriented to cost efficiency and profit maximization thing that will determine them to produce simple and inexpensive devices to ship them in large masses. These devices (sensors, actuators, boards) lack security, for time and resource saving from the manufacturer; the matter will fall in the hands of the entity that needs the product, to enhance it with security and made it foolproof as much as possible. This is the first level in the ecosystem. A microcontroller, more exactly a microcontroller single board in IoT is called a node. A node needs to communicate with a gateway to send its data. Microcontrollers may have Wi-Fi chipsets, Bluetooth or Infra-red to send data to the gateway. The node is responsible solely for reading and understanding the sensor and to pass data over to processing. This communication should be done on an encrypted channel. MQTT (MQ Telemetry Transport) is probably one of the most popular and the most used IoT protocols. It is somehow different from client-server architecture. The MQTT protocol has one central server which is referred as a message broker. The broker allows two types of connections from clients: publishing or subscribing. Publishers send messages to a specific topic to the broker. Subscribers are subscribing to one or more topics. A topic is an identifier used by the broker to filter messages received from publisher. The protocol is designed for constrained devices with limited resources or bandwidth. MQTT supports TLS encryption, data traveling safely between the clients and the broker. However, it is indicated to encrypt the payload.

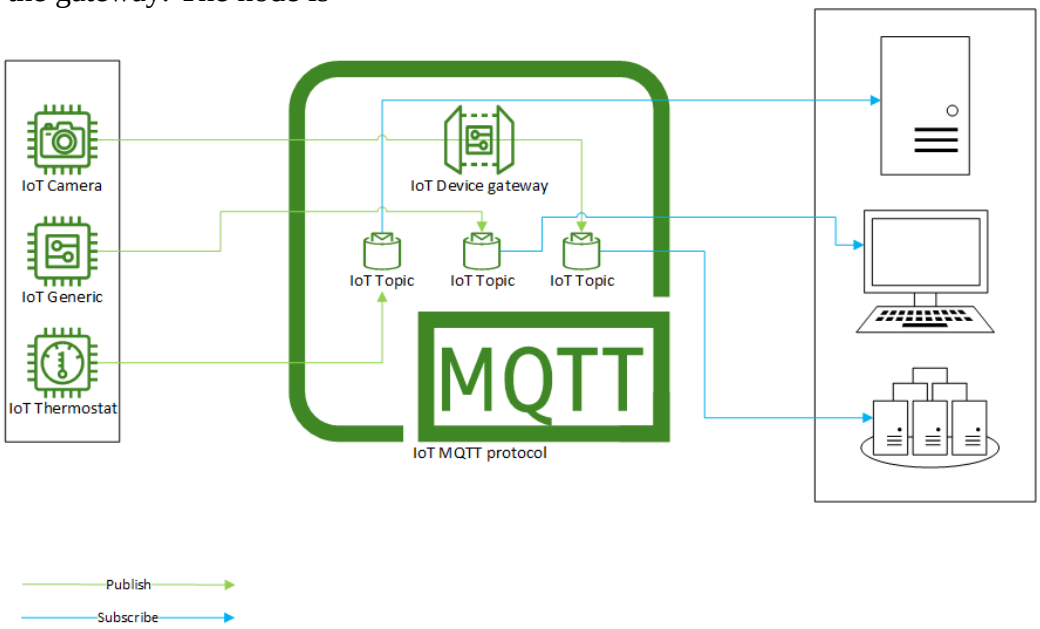

Fig. 1. Architecture of the solution

As seen in Figure 1, MQTT based architectures consists of one broker, which can be the IoT gateway, a few topics, publishers, and subscribers. Having only security assured at transport layer there can be multiple vectors of attack. Moreover, involving such many machines, compromising one can mean leverage for attacking the entire network or ecosystem. One solution is to encrypt data. If the secret key is burned onto device that most probably will be the microcontroller that will publish,

then it must be pre-shared with its subscribers. A decommissioned subscriber can be targeted, leading to an ongoing information leakage. A better solution to this problem is ECDH [8]. The main problem here is resource consumption and scaling. A publisher should have a separate set of asymmetric keys for each subscriber. They can be generated each time a new client that wants to subscribe appears and disposed when that client is not present anymore. Anyway, talking about such things in constrained devices can be a sensitive matter.

In a Supply Chain Management system, as mentioned above, there are multiple parties involved. A scalable IoT solution based on MQTT and blockchain needs to manage a lot of tasks in what means authentication, authorization, and confidentiality [9]. The solution in this article is centered on a simple idea of sensitive data that needs to be transmitted to two or more parties. One or more sensors collect environmental data and process it. The sensors are scattered, and they belong to different parties. Each of them is connected to a powerful microcontroller that processes the data and publishes it, obvious, over TLS. Two or more subscribers are awaiting the same data. The principle behind is data decentralization. If some error appears in one party's systems or mechanisms, they won't be able to counterfeit the data received from the sensors. More than that, those microcontrollers are connected to the broker through TCP/IP. A simple ping probe could be done to check the status of the device and if it's down all systems will be alerted because someone or something is tampering with that device or simply it's malfunctioning. If all is working accordingly the data reaches all the subscribers. Here the best idea is to store it for future use and reporting. Keeping the decentralization trend in mind, data should be redirected through blockchain, encrypted. The problem is that the parties could be breached, data being modified or deleted. For better security and transparency, each party can encrypt the data with its private key and send it to blockchain stored in a smart contract. From here the client application cand query all the data, decrypting using the public keys from each party certificate and using for reporting, inspection, or validation. In that way the system is secure and decentralized. To assure entire control and manipulation of data, one should tamper with all parties or with the blockchain, things that are improbable and tremendous hard to achieve.

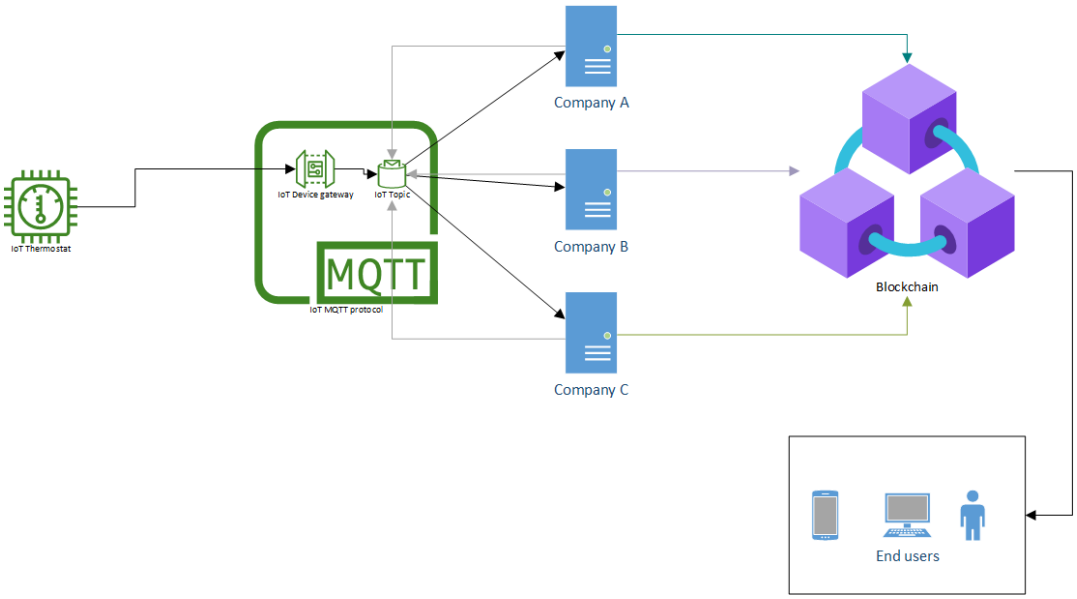

Fig. 2. IoT solution integration with the blockchain

In Figure 2 is related how such a system should look. *Company A* is in charge of manufacturing the product *X*, *Company B* assures the distribution and *Company C* is the retailer. The sensors installed in critical equipment present in each company report on the status of the product. The product needs special conditions of storage, handling, and transport. The smart sensors are publishing on different topics such as *comA/sensor1* or *comB/sensor*. All three companies are subscribers, so each know of the others. After this data is stored on the same blockchain. A client application having the certificates, queries the blockchain and decrypt the information, grouping it in tables. Timestamps are registered on subscribing and blockchain transaction. For a data set to be valid it needs to have unnoticeable timestamps differences and the same data received from all parties.

4. Solution architecture and implementation

To exemplify such a grand-scale project there can be used smaller parts and fewer actors. In simulating such an ecosystem, the weapon of choice are cost-effective friendly devices from Raspberry Pi or Arduino. Raspberry Pi launched at the beginning of 2021, its first microcontroller chip-based board. It uses the RP2040, a 32-bit dual ARM Cortex-M0+ microcontroller integrated circuit, 264 KB of RAM and 2MB flash memory. It supports Micropython and C/C++. The Pimoroni Ltd, an electronic company for hobbyists are developing diverse add-ons for Arduino, Raspberry Pi, Micro Bit and other products. Hence there is a board designed for Raspberry Pi Pico which has an ESP32 chip allowing the RP2040 board to communicate over internet. Most of the pins will be used but there will be some available for an I^2C or SPI connected device. For this project, a BMP180 temperature and pressure sensor was used, connected through I^2C with the Raspberry Pi Pico. The board will be the publisher and the clients will run on client desktop or server. The technology here is less important, Eclipse Foundation offering MQTT support for most of the languages and some technologies have proprietary support for MQTT. The hardest part is creating the MQTT publisher because there is not so much support for this board, being very new and young on the market. Speaking of the blockchain, same as the MQTT subscribers, there is plenty of languages that have libraries supporting smart contract interactions. For this PoC a simple .NET cross-platform program was created that subscribes to a topic and sends the data to a smart contract in Rinkeby Ethereum test network. A client application, most likely a mobile or web one, will query the data and will display it, live time for the end users. The MQTT broker is a locally hosted Mosquitto broker on a Raspberry Pi 4B with 2 GB RAM. The PoC uses TLS with mutual authentication. Because the tests were done on a local network the authentication is done based on the IP in the network. The publisher and the subscribers have certificates based on their IP that allows them to communicate with the broker.

Fig. 3. PoC/Demo hardware boards

Figure 3 exemplifies the hardware and the connections from the proof-of-concept system. The Raspberry Pi Pico together with the Pico Wireless Pack and the BMP180 sensors are interconnected and powered by a mobile power bank. The Raspberry Pi communicates with them just through the ESP32. The blockchain part did well keeping a fast response to the publisher speed. Around every 4.5 seconds the data is read from the sensor. Adding network delays and processing delays, around every 6 seconds a transaction to store data on the smart contract is done and this happens on every party involved with a subscriber.

5. Conclusions

Building a secure scalable IoT system for a Supply Chain Management environment is a true big challenge. There are many security aspects that need to be taken in consideration, many parties that need to be satisfied and adaptable to the requirements and many constraints from the currently available technology. All the parties must conclude to use a trusted provider which can unify and satisfy the needs of the chain. The question remains if some things should not be so digitalized and to keep the old way of working, especially when there are large masses of people with different perspectives. The blockchain can be a solution for privacy and decentralization but at the very moment is expensive and slow to work with. More than this it adds security implications to ones that already exist. The present PoC and idea might be something to start of or something to build on in the long road of efficiency and digitalization in economic systems in our times.

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[2] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015.

[3] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," *IEEE*

Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2702-2733, 2019.

[4] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," *IEEE Access*, vol. 9, pp. 28177-28193, 2021.

[5] D. M. Mendez, I. Papapanagiotou and B. Yang, "Internet of things: Survey on security," *Information Security Journal: A Global Perspective*, pp. 1-17, 2018.

[6] M. b. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol. 148, pp. 283-294, 2019.

[7] E. R. Naru, H. Saini and M. Sharma, "A recent review on lightweight cryptography in IoT," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, 2017.

[8] L. . Li, "Study on security architecture in the Internet of Things," , 2012. [Online]. Available: https://ieeexplore.ieee.org/document/6273274. [Accessed 29 3 2022].

[9] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[10] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for IoT security," *Internet of Things*, Vols. 1-2, pp. 1-13, 2018.

[11] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?," *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41-49, 2018.

[12] H. Damghani and L. Damghani, "Cryptography review in IoT," in *4th Conference on Technology In Electrical and Computer Engineering (ETECH2019)*, Tehran, 2019.

[13] N. Tewari, N. Deepak, M. Joshi and J. S. bhatt, "Comparative Study of IoT Development Boards in 2021: Choosing right Hardware for IoT Projects," in *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*, London, 2021.

[14] H. P. A, M. Senthilmurugan, P. R. K and R. Chinnaiyan, "IoT and Machine Learning based Peer to Peer Platform for Crop Growth and Disease Monitoring System using Blockchain," in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, 2021.

[15] J. Backman, J. Väre, K. Främling, M. Madhikermi and O. Nykänen, "IoT-based interoperability framework for asset and fleet management," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Berlin, 2016.

[16] M. Falco, I. Núñez and F. Tanzi, "Improving the Fleet Monitoring Management, through a Software Platform with IoT," in *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTaIS)*, Bali, 2019.

[17] P. Legg, T. Higgs, P. Spruhan, J. White and I. Johnson, ""“Hacking an IoT Home”: New opportunities for cyber security education combining remote learning with cyber-physical systems," in *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, 2021.

[18] S. Sathwara, N. Dutta and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, 2018.

[19] O. Westerlund and R. Asif, "Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things," in *2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)*, Muscat, 2019.

[20] T. B. S. S. Uday Kumar, "Comparative Analysis of Cryptography Library in IoT,"

Cornell University, Ithaca, New York, 2015.

[21] M. N. Khan, A. Rao and S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4132-4156, 2020.

Teodor CERVINSKI has a bachelor's degree in Economic Informatics and a MSc. degree in Cyber Security from the Department of Economic Informatics and Cybernetics at Bucharest University of Economic Studies, Romania. His research interests are Computer Network, Computational Cryptography, Application Security, and Quantum Computing.

Cristian TOMA has graduated from the Faculty of Cybernetics, Statistics and Economic Informatics, Economic Informatics bachelor, within University of Economic Studies Bucharest in 2003. He has graduated from the BRIE master program in 2005, with practical stage in Germany and graduated from the PhD stage in 2008. He is cofounder of the IT&C | Cyber Security Master Program and cofounder of the SECITC – The International Conference on Security for Information Technology and Communications. His work focuses on the Software architectures, IoT - Internet of Things application development, Crypto Blockchain, e-Embedded/Mobile applications development/computing, Cloud/Distributed and Parallel computing/HPC - High Performance Computing, Secure Elements/Smart cards programming, e-payment Solutions, Computer anti-viruses and viruses, Quantum Computing, and computational cryptography - Cyber Security.