Security Model for the Internet of Things, Through Blockchain

Yesid Díaz Gutiérrez[1], Juan Manuel Cueva Lovelle[2], Diana Carolina Candia Herrera[3] *

[1] Software Engineering, Corporación universitaria Iberoamericana, Bogotá (Colombia)
[2] Ph.D. in Computer Science, Oviedo University, Oviedo (Spain)
[3] Software Engineering, Corporación universitaria Iberoamericana, Bogotá (Colombia).

* Corresponding author: yesid.diaz@ibero.edu.co (Y. Díaz Gutiérrez), cueva@uniovi.es (J. M. Cueva Lovelle), diana.candia@ibero.edu.co (D. C. Candia Herrera)

Received 12 December 2022 | Accepted 22 November 2024 | Early Access 20 February 2025

Abstract

Due to the proliferation of computer crimes related to information vulnerability handled by people and entities and evidenced in attacks of financial, commercial, personal and even family nature; a need has been identified to implement, security strategies and protocols in each and every one of these areas, which make possible the effective protection of the integrity and privacy of data. Regarding this, there are protection schemes such as cryptography and reliable time stamping which undoubtedly have managed to partially solve this problem by attacking structural and crucial points. However, the evolution in the technology field has been currently represented in the fourth industrial revolution and its context towards 4.0 technologies and smart industries; Various technologies have been positioned in the emerging and disruptive categories, among which the Internet of Things (IoT) stands out. This technology has become the target of multiple computer attacks, due to the processes of Extraction, Transformation, Loading and Transmission of large volumes of data. Alongside its widespread connection to the Internet, it's become a strategic target for such attacks.

A possible alternative solution to this situation is blockchain, which allows information to be public and stored in different blocks, which makes it easier to guarantee the integrity of information based on the following aspects: Identification of the attacked and / or compromised information, which can be marked as invalid information; Public report of the attack; Information backup in another block to facilitate its recovery.

In this regard, it is important to highlight that these functional and technological characteristics offered by the blockchain, facilitate the management of information and its integrity. However, it is necessary and essential to previously guarantee the structure of the information generated; as some processes of Business Intelligence (BI), such as the Extraction, Transformation and Load scheme (ELT), would be of great relevance and support during the development of this procedure.

Keywords

BlockChain, Business Intelligence, Cryptography, Immutability, Internet of Things, Referencing, Safety, Smart Industries.

DOI: 10.9781/ijimai.2025.02.009

I. Introduction

The fourth industrial revolution, also known as the era of digitalization, has generated substantial changes in the processes of reception, management and transmission of information; This considers the emergence of multiple technologies framed in the concept of 4.0 Technologies. BlockChain technology, Business Intelligence, Data Analytics, Machine Learning and the Internet of Things are some examples of the new emerging and disruptive elements that have gained great relevance in these times and that, in one way or another, have conditioned and modified the treatment of data as the primary input of information.

Regarding this, it is very common to find evidence of computer attacks that seek to violate the integrity and privacy of data and therefore of information, which have been proliferating in this context of digitization for two fundamental reasons. On the one hand, due to the diversification of new technologies that generate large amounts of data and that, due to their recent appearance, had not been contemplated in existing security models; and, on the other hand, due to the importance of data and information in the current global context. Given the importance of the processes of effective management and treatment of information, derived from the dynamics of IoT solutions through their interconnectivity, it is essential to analyze two specific contexts; one from the perspective

Please cite this article as:
Y. Díaz Gutiérrez, J. M. Cueva Lovelle, D. C. Candia Herrera. Security Model for the Internet of Things, Through Blockchain, International Journal of Interactive Multimedia and Artificial Intelligence, vol. 9, no. 5, pp. 154-162, 2025, http://dx.doi.org/10.9781/ijimai.2025.02.009

of the security of IoT architectures and the other from the integrity and security of data.

In accordance with the contexts mentioned above, it is important to highlight that the pervasiveness factor of the IoT devices that are part of a solution has led to many concerns about the security on how the information is transmitted and used to communicate, specifically in five specific characteristics:

- **Confidentiality**: Protected data generates the user's confidence and peace of mind about their privacy, in regards to it there are strategies such as data encryption and two-step verification to control unauthorized access. This is mainly dedicated to applications that manage personal or financial information such as: health monitoring devices or payment control systems such as those used by banks.
- **Integrity:** Protection against hackers who through internal or external interfaces, can intercept the transmission of information and capture it in order to manipulate its uses. [1] strategies such as cyclic redundancy check (CRC), monitoring that their integrity is not altered during transmission.
- **Availability:** Authorized information, with initial validations and assurance of the veracity of the data transmitted using strategies such as redundancy security, duplicity that allow the reliability of the data, which implies that the devices are protected from denial of service (DoS) attacks.
- **Authentication:** This element ensures that data can only be accessed if authentication is mutual between devices and IoT services.
- **Efficiency:** One of the requirements that guarantees communication within IoT security protocols is to be able to certify the resource even if it is low powered and keep the resource functional [2].

According to the above characteristics, it is possible to catalog the data and its integrity as the main asset that the productive sector has in the 4.0 society, that's why it is essential to ensure its treatment through technological and methodological schemes designed for that purpose. In that order of ideas, it is essential to highlight BI (Business Intelligence) as one of the technologies that offers the most benefits in this regard, since it not only provides tools for the processing and analysis of data, but also data standardization schemes to convert them into reliable and structured information.

Regarding the above, the website, (Forti, 2019), in the article entitled "Because Business Intelligence is Data Intelligence", published in 2019, mentions that in 1958, Hans Peter Luhn defined the concept of "Business Intelligence" as "The ability to understand the interrelationships of the facts presented in such a way to guide action towards a desired goal". Similarly, in this same article, it is indicated that, based on this definition, in 1989, Howard Dresner described Business Intelligence as "The concepts and methods for improving business decision making through the use of systems based on supporting facts" [3]; **providing** a context oriented towards the use and implementation of BI with applications in IoT solutions.

However, and despite having architectures based on security protocols, such as those related previously and with schemes to standardize and refine the data as those proposed by the BI; it is necessary to really guarantee the integrity of the data through complementary and related technologies such as the blockchain, to consolidate an articulated, robust and structured security model, such as the one proposed in this document; which seeks to articulate IoT architectures, Business Intelligence and blockchain as structural components of such a model. It is appropriate to mention that the Internet of Things is a technological revolution that represents the future of computing and communications and its development needs the support of some innovative technologies [4].

"Information added to the blockchain is public and can be consulted at any time by any user of the network. Information can only be added to the blockchain if there is an agreement between most of the parties. After a certain period of time, it can be assumed that the information added to a block can no longer be modified (immutability) [5]. This statement makes it possible to identify three (3) fundamental elements, as preliminary conclusions of this first part of analysis:

- Blockchain capacity to "tag" specific blocks.
- Access to any block at any time, by any user.
- Immutability as an information protection scheme.

Based on the aforementioned and on the benefits that each of these technological pillars can offer in terms of data integrity, the development of this document has been oriented specifically in three components; firstly, a review of the state of the art regarding the architectures used in IoT solutions and their security protocols. Secondly, it has been carried out a functional analysis of the process of Extraction, Transformation and Loading of Business Intelligence as a data standardization scheme, and finally a characterization of the strengths in terms of information security that the blockchain offers. All of the above as part of the construction of a security model for the Internet of Things through blockchain.

II. Methodology

The methodological approach was structured from a (1) general framework of work, delimited by the dynamics of the Deming cycle, better known as PHVA or of continuous improvement, which begins with a study of the current situation, during which the data to be used in the formulation of the improvement plan are gathered. [6] This cycle regulates the methodological and management actions from the general context, because from the research and disciplinary context it is complemented by the scientific method and the Scrum methodology. From this perspective, the work methodology has 3 fundamental elements:

- General work framework.
- Research methodology (Scientific Method).
- Disciplinary methodology (Agil Scrum).

For better understanding, the general framework is presented graphically below. Fig. 1

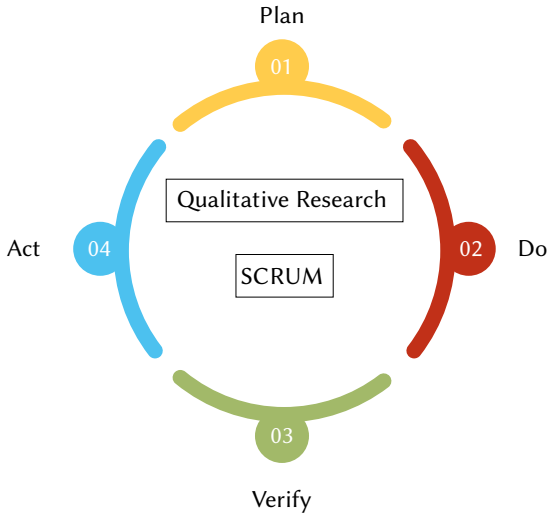

Fig. 1. General Work Framework.

Within the **planning** of the development work process, the starting point was the identification and delimitation of the current state of the object of study, addressing as a main tool, the review of the state of the art of the architectures and protocols used in IoT solutions, seeking to identify the following aspects:

- The Information generated by application processes and IoT devices that do not have a standard structure to control and protect it.
- Possible absence of controlled storage processes that restrict access and prevent its modification.
- Generation of alerts against possible attacks to the integrity of the information.

Based on the identification of these elements, research questions, along with the hypothesis are generated, in order to highlight two work approaches to address this problem; on one hand, the research approach and on the other hand, the disciplinary approach, projecting general and specific objectives. These elements allowed the identification of a general work framework and a particular and coherent methodological scheme with these two approaches, selecting the scientific method as a research methodological driver and Scrum as an agile methodology for disciplinary development.

Regarding "**Doing**", it is important to highlight that, although each of the selected methodologies (scientific method and Scrum) has its particular dynamics; from the general framework of work, a control of such actions is performed by means of the PHVA cycle. It is there where "Doing" facilitates the approach of solution schemes by means of tests developed in a controlled environment avoiding the interaction of external factors that affect the design of the final solution.

According to the above, the exercises of the methodological structure will be delimited through an IoT solution prototype structured on a standard architecture that will allow validating the impact and efficiency of the disciplinary and research processes. This prototype will yield specific results that will make fundamental aspects possible to determine and that will guide the research towards the design of an integral solution.

Once prototypes have been applied in the framework of preliminary tests or pilot tests, it is necessary to verify the results obtained during the application process, to determine if the projection of the solution satisfies the needs identified in the planning. It is also necessary to make a comparison between the results obtained and the objectives set.

This dynamic verification allows to take as input the results of "**Doing**", obtained in the methodological framework of the research and disciplinary exercise, establishing a direct relationship between these and each of the methodologies (Scientific Method and Scrum), to determine how the degree of their contributions enrich the design process of the proposed solution.

1. Materials

The context of the materials and tools used for the development of the process is delimited by 5 essential components:

- Analysis of security architectures and protocols in IoT solutions.
- Analysis of architectures for the Internet of Things through IoT functional prototyping.
- Functional analysis of Business Intelligence ETL process through pentaho prototyping.
- Identification of information security strengths evidenced by the blockchain through prototyping.
- Proposed security model for IoT through blockchain.

a) Analysis of Architectures and Security Protocols in IoT Solutions

As part of the bibliographic revision and the analysis of some models of architecture of solutions for the Internet of Things, it is possible to identify that it is composed of four essential layers

A **perception layer** in charge of gathering data by means of physical elements such as sensors. [7] which at the same time can suffer from common threats such as: tag cloning and electronic identity theft through the impersonation of the device identity, also known as spoofing.

On the other hand, there is the **network layer**, where the data coming from the perception layer is transmitted using channels such as the mobile network, internet or any other type of network; it also displays security attacks such as: code injections that cause the loss of control of the network, sybil attack that consists of staying in a network node and multiplying the identity by giving incorrect information responses and attacks related to sleep deprivation which depletes the battery charge of the nodes until it shuts them down to completeness [8].

Another layer where security problems are presented in the communication of interconnected physical devices is the middle layer, which is responsible for ensuring the service between objects, but it faces security problems in relation to DoS attacks where the services of the devices are turned off taking them out of the system as unavailable, also unauthorized access is common within this architecture since the attack prohibits IoT access.

And finally, the **application layer** provides IoT applications for the different scenarios that require them, such as health, industrial, transportation, among others [7]; here there are also logical affectations such as denial of service attacks as in the middle layer, but focused on launching the attack directly to the user to obtain privacy from their data; phishing attacks by means of identity theft through credentials obtained in social engineering strategies and another common attack is the injection of malicious code that steals information that can eventually breach the application.

Considering that there is no specific architecture model for IoT solutions, Fig. 2 proposes a general IoT architecture supported in its four (4) layers.

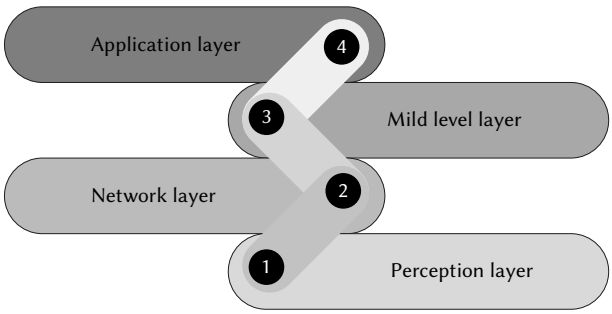

Fig. 2. General architecture IoT.

Derived from the definition of the general IoT architecture, it is possible to identify three levels of behavior of the elements that are part of each one of the layers and that are specifically oriented to manage the physical part of the solution (IoT devices) and the logical part of the solution (generated data), as follows:

Level 1 - IoT Devices: where connection elements, networks, device access control and security protocols are located.

Level 2 - IoT Platforms: Focused on managing the IoT devices that are part of the solution.

Level 3 - Cloud Data: Focused on data storage and processing and complementary tools for data analysis, visualization and integration [9].

In Fig. 3, it is possible to see the IoT architecture structured in its four (4) layers, articulated with the three (3) levels related above.

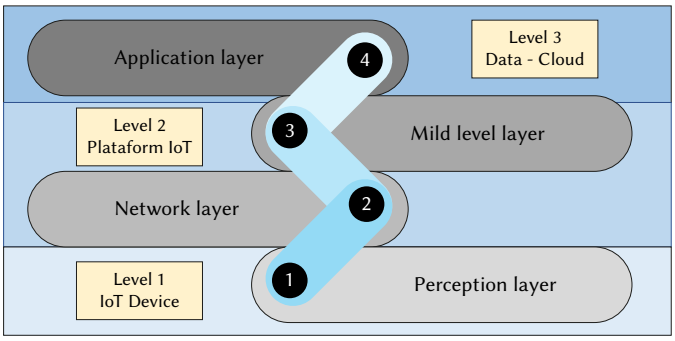

Fig. 3. Architecture Levels IoT.

b) Analysis of Architectures for the Internet of Things Through IoT Functional Prototype

Considering the defined architecture and its articulation with the three (3) levels; an IoT solution was built for a coffee crop to measure and report its temperature.

The following components were used for its construction:

Rogue Card: Arduino component, on which Xbee wireless modules are incorporated as WIFI for data transmission.

Xbee Wireless Modules: IoT devices designed to send and receive data wirelessly by using the IEEE 802.15.4 protocol. Due to their wireless connectivity characteristics, they can be interconnected through a network acting as a coordinator module. Router or end device. [10].

TMP36: Analog sensor that measures temperature and can be easily interconnected to Xbee modules [11]

Java Application: It allows receiving and transmitting data from and to IoT devices through the Xbee library for java, generating an XML file with the information received. Fig. 4 shows the working diagram of the solution.

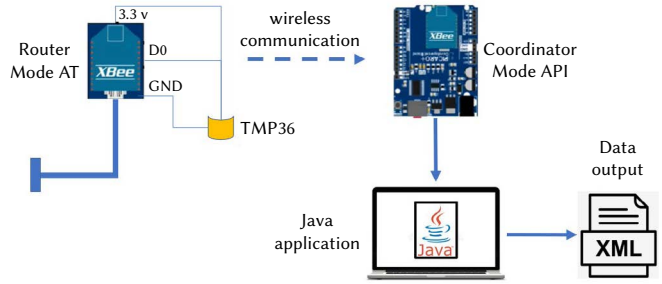

Fig. 4. Working diagram prototype IoT.

Regarding its functionality, and based on the work diagram presented in Figure 4, it is important to highlight that the IoT solution will have two Xbee Modules, where the first one was configured as coordinator in API mode, connecting to the rogue card, to receive the data through the java application, storing them in an XML file. Similarly, the second Xbee was configured as a Router in AT mode, i.e. automatic transmission, connected to pin D0 the temperature sensor TMP36. From where the data reported by the sensor will be wirelessly emitted to the API coordinator module [11].

Once the prototype was implemented and as part of the analysis of the results within the experimental process, distance tests were performed to determine the maximum range of the Xbee wireless modules in order to ensure reliable data transmission without signal loss or attenuation [12]; finding that its maximum range was 100 meters outdoors. In addition to the above, it was identified that the emitted data will have a different format according to the type of sensor implemented in the solution, which prevents a standardization of the information to be treated in a general way in future processes [13].

According to the results obtained, the following findings are consolidated:

- Generation of large volumes of data in IoT schemes.
- Multiple data formats (Structured, Semi-structured and Unstructured)-

Taking into account these findings, the need to guarantee the standardization of data to a structured format was identified, so a functional prototype was consolidated to evaluate processes for such standardization.

From this perspective of technological integration between IoT and blockchain, it is important to take into account the contributions made by Guofeng Zhang, Xiao Chen, Lei Zhang, Bin Feng, Xuchao Guo, Jingyun Liang, Yanan Zhang (2022), in their work on the integration of the agricultural Internet of Things (IoT) and blockchain in the context of precision agriculture, since not only the structural and functional compatibility of these two technologies is evident, but it is also possible to partially analyze the existing vulnerabilities in issues of information transmission from data sources, providing complementary mechanisms such as cryptography technologies [14].

c) Functional Analysis of the ETL Process of Business Intelligence Through Pentaho Prototype

Taking into account the ability of Business Intelligence through its Extraction, Transformation and Loading process (ETL), to standardize information regardless of the structure of the data source [15]; a functional prototype was designed by linking the following tools:

- **Pentaho Data Integration (PTI)**: Pentaho ETL tool, which allows extracting data from any data source, to refine, standardize and convert it into information with a standard structure [16].
- **XML:** File format that stores the data generated by the IoT solution, which will act as a flat data source.
- **MySQL**: Tool that allows working with SQL language,

Which for the particular case of this prototype will act as the destination, where any type of information that passes through the ETL process will flow there, but with a standard structure. It is important to highlight that MySQL is portable and runs on commercial operating systems supported on enterprise server hardware [17].

In regards to the functionality of this prototype, it is appropriate to mention that once the data source is identified, it undergoes a transformation and refinement process through the PTI, to standardize and store it in a MYSQL database, seeking to unify a standard information structure for any IoT solution.

In Fig. 5, it is possible to identify the functional structure of the prototype.

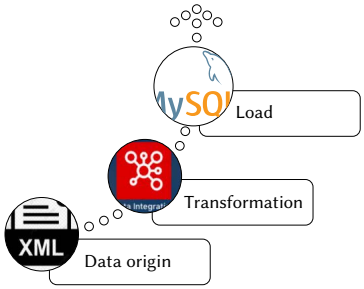

Fig. 5. Functional Structure Prototype ETL.

The functional phase of the prototype is composed of three fundamental phases:

- **Connection**: allows to directly relate the ETL tool (Pentaho), with the final structure where the information will be stored once it has been transformed and standardized (MySQL DB). This process requires to define 5 elements to establish the connection (The Host (Localhost) - The Name of the Database (school) - The port by which the connection will be established (3306) - The user name of access to the server (Root) - The type of connection (MySQL)). See Fig. 6.

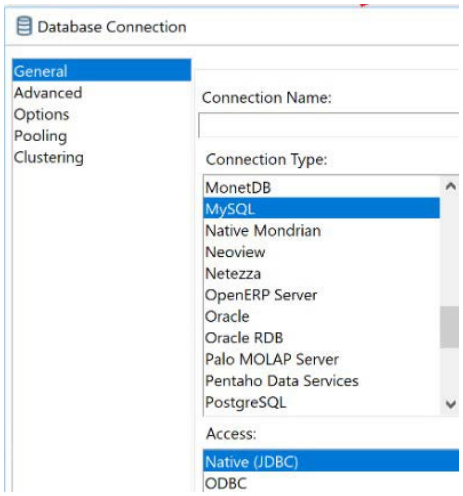

Fig. 6. Connection Testing Pentaho – MySQL.

- **Data Source**: In this step the type of data source that will be linked to the process and from where the base data for the transformation and standardization of the information will be extracted is selected. In this case, the Pentaho component called (Microsoft XML Input) is used to load the XML source file.
- **Data Output**: Once the connection and the source have been defined, it is necessary to configure the data output, which is done by means of the Pentaho component called (Table output), where the MySQL database is related to the data source, by means of the connection created in Step 1. Subsequently, a SQL statement is automatically processed to create a table that will store the final information. See Fig. 7.

It is important to highlight that the tool selected to work with MySQL is the WAMP Server, which offers, in addition to the console for the use of SQL code, a database administrator and a local Apache server [18].

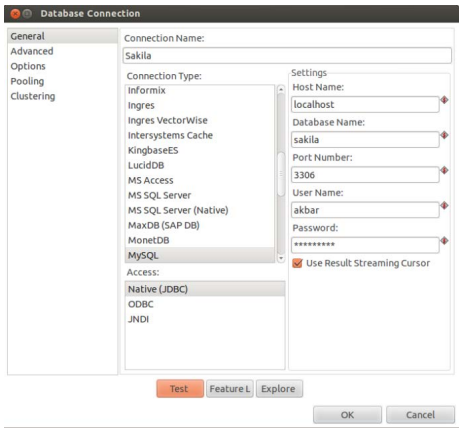

Fig. 7. Output Configuration MySQL.

Once the data source, connection and output have been configured, the transformation process is performed in Pentaho with the following activities:

- Selection of the data to be extracted and thus elimination of the NOT relevant data.
- Identification of the headers (which will become table attributes in MySQL).
- Elimination of blank spaces and those with invalid characters.
- Preview of the transformed information.

In this way a standardized structure for the information is generated regardless of the characteristics of the data source. See Fig. 8.:

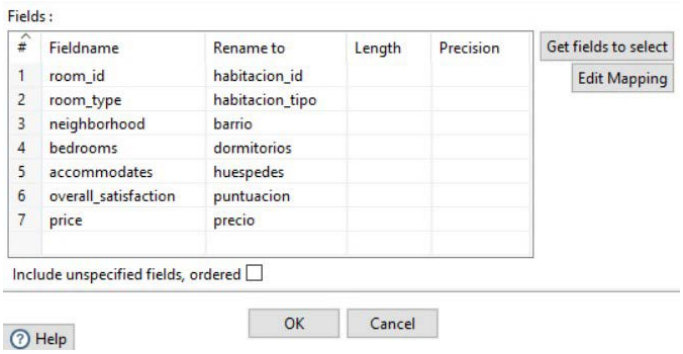

Fig. 8. Data transformation.

After ensuring that the data has been transformed, refined and standardized, the loading process is executed, which will take the data from the data source, process the defined transformation and dispose the refined information into the data output. See Fig. 9.

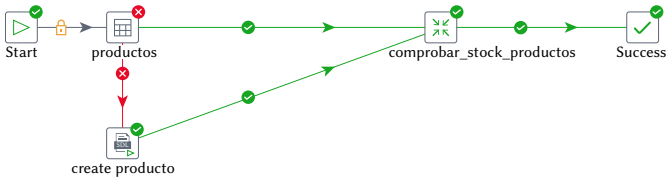

Fig. 9. Information loading to the output.

According to the results obtained within the experimentation process with this simulation prototype, it is evident that, through the application of business intelligence, specifically the ETL process, it is possible to solve the requirements detected in the experimentation of the IoT prototype regarding the handling of large volumes of data and its standardization.

Once it was possible to determine the type of data generated by the IoT devices and to identify a successful process to refine this data into structured information with a defined integrity that enables its processing and storage in resources such as MySQL, it is necessary to determine the functional characteristics of a blockchain application with encryption schemes.

d) Identification of Information Security Strengths Evidenced by the Blockchain Through Prototyping

Conventional blockchain technology can provide an alternative solution by decentralizing the fully distributed control plane over an architecture that relies on eventual consistency achieved through Consensus Algorithms [18]. Based on the above, it is proceeded to build a blockchain prototype with the ability to encrypt information through the SH-256 hash function. This prototype had six (6) structural elements:

- **Index**: This element facilitates the identification and counting of each of the blockchain, allowing the identification of the number of

blockchain involved in a process and the position that is currently being validated. Due to its functional characteristics, it facilitates the search for some type of data within the chain and allows the tracking of information within multiple chains.

- **Hash**: It allows identifying the information contained in each of the blocks, which in this case is encrypted with the hash function sh-256.
- **Previoushash**: It facilitates the linking of blockchain, fully identifying the previous chain, with the aim of linking it with the new chain. It is important to highlight that in blockchain it is essential to identify the previous chains when proceeding with the creation of a new chain. In addition to the above, its use determines the top of the blockchain identifying the end of it, in this way and with the articulation with the index, it is not only possible to determine how many chains have been created but which is the beginning and the end, facilitating the navigation and route for the search process.
- **Nonce (Number that can only user once)**: The number that can only be used once is a random number used in cryptographic processes as part of the security protocol in the user authentication process; its interrelation with the hash generates a control scheme that violates the information contained in each one of the blocks from possible attacks, guaranteeing the integrity of the information, especially during the transmission of data.
- **Transactions**: Records each of the transactions carried out, which in the case of the prototype and its application with the voting station, records the information of each of the votes.
- **Contracts**: Records the operations generated each time a transaction is executed in the application.

Fig. 10 allows identifying, from the coding context, the structure of a blockchain applied to the voting station.

```
{
        "Index",
        "previoushash",
        "hash",
        "nonce",
        "transactions": [
                                {
                                        "Dato1",
                                        "Dato2",
                                        "Dato3"
                                }
                        ]
}
```

Fig. 10. Blockchain Code Structure.

Similarly, in order to facilitate and guarantee communication between each of the nodes to make the articulation of the chain viable, it was necessary to use PreviousHash and the NewHash, as shown in Fig. 11.

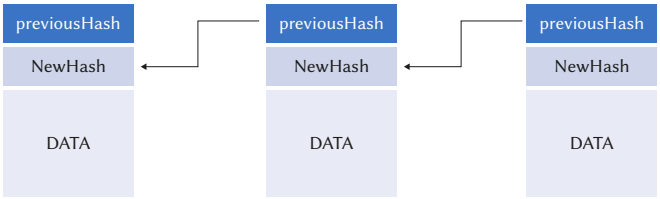

Fig. 11. Communication scheme among blocks.

For the construction of this prototype, the following tools were used:

- **JavaScript**: programming language used to create the blockchain.
- **Node.js**: Environment for the creation of the server layer on top of JavaScript language.
- **Js-sha256**: JavaScript library to encrypt data and generate the hash.
- **Body-parser**: It allows us to process the data received from the client through HTTP requests.
- **Node-fetch**: It facilitates the construction of a JavScript interface to handle requests and responses in the HTTP channel.
- **Expres**: It facilitates the creation of a Node.js based web environment.
- **Encoding**: It allows to replace instances of some characters by one (1), serving as a marker or identifier.
- **Json (JavaScript Object Notation)**: It facilitates the representation of structured data (i.e. once they have been refined by ETL), in JavaScript.

Considering that a large part of the security model is structured on the dynamics of blockchain and the security benefits offered by the sh-256 hash function; it is essential to understand a little more about the functionality of this hash, as shown in Fig. 12, the results of applying the mathematical algorithm of the 256 hash, when converting any data block into a collection of 64 characters, regardless of the original size.

Texto	Hash criptográfico 256			
Comprobando	81d2aa6e	f5e99328	881f95c3	1a27f7ae
	a51099cf	bcb5e0ed	daf4b6a4	a264eb9c
Comprobando la funcionalidad	d96ce280	9a2f5a03	fbbaef79	c6868fdd
	48557fac	2464fc2b	840706b4	a22edad6
Comprobando la funcionalidad del hash 256	32f27710	dd3449ca	f6307f9a	7e21b13f
	3392eb28	d16bdbc6	2bc1974c	1f740159

Fig. 12. Conversion to 64 characters of a Text Block - Function sh-256.

Under this scenario, it is possible to identify that, despite the size of the original text, the result of applying the 256 hash will always be a unique encryption. of totally different 64 characters. This encryption model guarantees data protection and articulation with the dynamics of the blockchain in the face of its variability in each of the blocks [19]. It also allows efficient data manipulation, once, regardless of the size of the text received, it can be handled with a standard storage size of 64 characters in each of the transactions carried out, keeping the proportions and structures previously identified.

2. Tasks and Methods

Next, the context of application of the SCRUM methodology as a disciplinary driver is developed, highlighting that its application is focused on the demands of the prototyping exercise that has been developed. The aforementioned taking into account that Scrum is an incremental and iterative agile software developmental framework for product management [20].

From this perspective, SCRUM was defined as a methodological framework under three (3) essential components:

- **Ceremonies:** They are specific meetings with a differential lenght and context among them, from which the agile reviews and follow-ups were performed against the fulfillment of the commitments agreed in the development of each of the prototypes. These meetings were held dynamically and, in some cases cyclically:
- **Sprint Planning**, from which the planning of what is called the Sprint was carried out, which is nothing more than the time frame defined for the development of the product, in this particular case each of the prototypes.

- **Daily**, as a mechanism used for the daily follow-up that allowed verifying the fulfillment or not of the established commitments and the adoption of immediate corrective actions.
- **Artifacts:** These are the resources or tools used during the development of the project, in which the requirements, progress and final results of each of the products (Prototypes) were clearly documented. The artifacts used were:
- **Product Backlog**, where the requirements, tasks and activities necessary for the successful development of the prototype was delimited.
- **Sprint Backlog**, as a mechanism to divide the product into small deliverables (Task Fulfillment), in order to ensure that their fulfillment generates an advance in the process until the sum of all deliverables determines the total fulfillment of the product.
- **Increment,** related to each of the deliverables generated from the Sprint Backlog.
- **Roles**: These are the actors that participated in each of the phases of the development of each prototype and that receive their name according to the roles defined by the Scrum methodology. These roles were:
  - **Product Owner**: Role played by the doctoral student, from which the Product Backlog and the acceptance criteria of these products were elaborated, socializing these requirements to the SCRUM team.
  - **Scrum Master**: Role that was also played by the doctoral student, from which the work performed by the Scrum team was accompanied and followed up.
  - **Scrum Team**: Formed by the members of the Tools research seedbed of the "Corporación Unificada Nacional de Educación Superior CUN", in charge of creating the deliverables, according to the defined requirements and under the developed dynamics of accompaniment.

In order to have a clearer and more precise vision of the dynamics of the disciplinary methodology, the workflow and interactions in the context of the development of each of the prototypes are illustrated below. See Fig. 13.

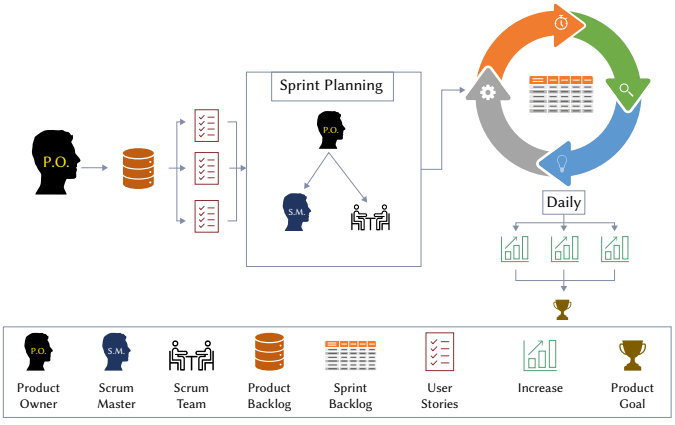

Fig. 13. SCRUM Cycle for Prototyping.

A. Results

In order to present the results obtained, which have progressively become inputs for subsequent results, due to the prototyping development chain, the results derived from each of the prototypes are listed below.

In the first instance and derived from the analysis and results obtained in the execution and testing of the connection capacity of prototype 1, it was possible to determine the connectivity capacity in the context of the test vs. distance relationship. See Fig. 14.

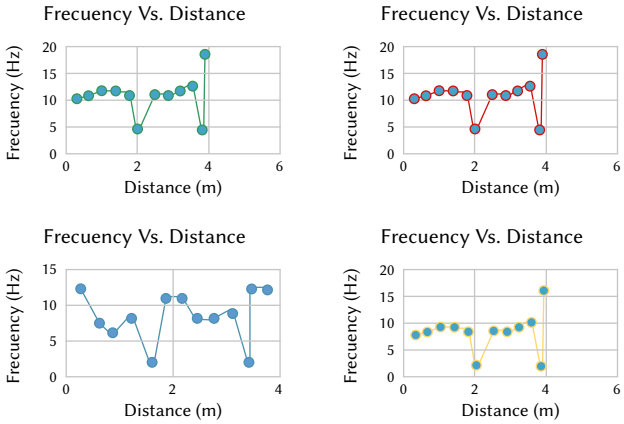

Fig. 14. Frequency VS Distance Results.

Regarding the previous illustration, it can be observed that there are differences in frequency versus distance, identifying that these frequencies do not seem to be constant. Likewise, it can be observed that in all the graphs there are important peaks in which the frequency decreases notoriously. This allows us to determine 3 fundamental findings regarding the impact of these tests.

- Stable connectivity between the IoT device and the sensors.
- Generation of large volumes of data.
- Need to standardize the data generated by the IoT device.

As long as the results obtained by the functional analysis of prototype 2 against the ETL process, the following results are presented as a table. See Table I.

TABLE I. ETL Prototype Execution Results

Moment	Element	Amount	Percentage
Extraction	Records Extracted	325	100%
	Generated Characters	23400	100%
Transformation	Valid Records	293	90,10%
	Deleted Characters	1452	6,20%
	Records Canceled for Integrity	32	9,84%
Load	Loaded Log	293	90,10%
	Generated Tables	2	100%
	Structured Attributes	26	100%

In the case of data extraction from the source generated by the IoT solution, the total number of records extracted is validated, in the case of transformation the number of valid records is validated, in regards to those extracted, number of deleted characters, records cancelled for completeness and in the case of loading in the data output, the number of records loaded, the number of tables generated and the number of structured attributes, identifying that the data output generated by the ETL process allows to standardize the format to Structured data dumped to a MySQL data warehouse in an unique format.

B. Discussion

According to the results obtained throughout this work, it is important to determine the importance of each of them in relation to the realization of the security model for the Internet of Things through blockchain. In that order of ideas, it is essential to initially identify the difficulties that were present at the beginning of the work:

- Delimitation of the physical architecture of an IoT solution.
- Types of data generated by IoT solutions.
- Mechanisms for storing large volumes of data generated by IoT solutions, to be processed later.
- Security mechanisms for data protection.

Under these initial definitions, it is possible to analyze the importance of the results obtained progressively through the prototypes developed and how they meet the previously identified needs.

IoT architecture: Regarding this architecture, the results obtained by the application of the prototypes allowed to determine a consolidated structure regarding the sensors and the connectivity they provide, regardless of the technology used. These IoT solutions show a stable and lasting connectivity with few interruptions that guarantees the permanent generation of large volumes of data.

Data Origins: Considering that the architecture of an IoT solution is not defined by a specific standard but depends on the needs on which it has been designed, the generation of data does not preserve a standard format, since data of different types (structured, semi-structured and unstructured) are obtained. This diversity of formats requires a standardization process that allows ease and accuracy in its storage and processing.

Data Standardization: This process represents an obvious need in the context of data generated by IoT solutions, not only for their processing and storage, but also to ensure their security. In that order of ideas, the results obtained from the execution of the ETL prototype, managed to determine that the process of Extraction, Transformation and Loading of Business Intelligence allows formatting all the data generated to a single structured format that derives in the ease of creation of data warehouses.

Security derived from blockchain: Starting from the premise of having the data in a structured format, stored in a specific warehouse, in this case MySQL, it was possible to determine security aspects derived from the blockchain validation prototype, delimiting 3 fundamental benefits centered on the standard size of the blocks, encryption of the information and variability in the extension of the chains, making it impossible to relate one block to another.

It is important to highlight that there is a transition between the output or data output generated by the IoT solution and the blockchain that will be generated; this transaction will be the result of a transaction between the IoT solution and the blockchain that will be generated.

As a result of the above discussions, structured on the results obtained, it was possible to consolidate a final product represented in Fig. 15 as a security model for the Internet of Things through blockchain.

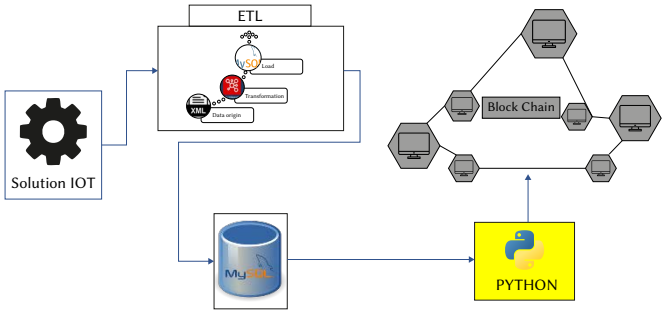

Fig. 15. Security model for IoT with BlockChains.

These blockchain, in addition to providing robust security in accordance with those discussed previously; allows largely guarantees the coherence of the information, specifically in the face of network failures, increasing its availability as part of the integrity, as evidenced by Alberto Arias Maestro, Oscar Sanjuan-Martinez, Ankur M. Teredesai, Vicente García- Díaz (2023), in his work "Blockchain-based cloud management architecture for maximum availability".

From this perspective, this technology will complement the ETL processes of business intelligence regarding information integrity, largely solving the identified problems [21].

Based on the previous model, it is necessary and fundamental to demonstrate the articulation that exists between the **prototypes**, **the results** and the **proposed model**, as part of the validation of the methodological and disciplinary exercise. In this order of ideas, it is necessary to identify the contributions of each of the prototypes and their results as a fundamental input to the definition of the model.

In the case of the **IoT prototype**, it allowed validating the architecture of a typical solution and the characteristics of the information transmission process between the AT mode router (Xbee), the API Mode coordinator (Xbee) and the Java application; especially in terms of data formats (Unstructured, semi-structured and structured).

By having multiple data formats, it became necessary and structural to standardize them to a single format that would allow identifying and characterizing their essence, which is why the **extraction, transformation and load prototype**, developed in Pentaho Data Integration, offered conceptual, procedural and technological elements that allowed us to identify a data refinement scheme, converting it into valid and reliable information, which solves the problem of required homogeneity.

Within that same sequence conceived through the previous two prototypes and once the functional and structural characteristics of the blockchain were validated, the security model was designed supported by a fully characterized IoT interconnectivity, in a standardization supported by the ETL process. of business intelligence and in a security, context based on immutability, decentralization, cryptography, consensus, transparency, resistance to censorship, auditing, traceability and smart contracts that the **application of blockchain** will offer.

C. Conclusions

As a result of the process carried out during the development of this work, the conclusions derived from the whole exercise from the research and disciplinary point of view are presented below.

- In a typical IoT environment, as is the particular case of smart cultivation where the prototype was implemented; The stability and reciprocity in the connectivity between devices represented in the results of frequency versus distance, allow us to identify constancy, regardless of the distance. From this perspective, latency, that is, the time it took for the router in AT mode to send data to the API, does not affect the functionality of the solution in terms of the transmission phase.
- The volume of data generated during the functional evaluation phase of the IoT prototype, represented in 325 records and 23,400 characters, allows us to validate, on the one hand, that a solution with this basic technological architecture can generate large volumes of data, and on the other hand. Part generates multiple formats, which in both cases require an effective process of refinement and standardization of the information.
- Based on the results of the extraction, transformation and loading process developed by the Pentaho Data Integration ETL prototype, specifically focused on the 293 valid records, that is, 90.10% of the extracted records, the 1452 characters removed, that is, the 6,

20% of the total characters generated and the 32 records canceled for integrity that represent 9.84% of the extracted records; They clearly allow us to identify that the information reported by the IoT solution, despite being structured in different formats; denotes a high percentage of integrity and relevance, contextualizing it as valid data to be standardized through the ETL.

- As a result of the data standardization process through the business intelligence ETL developed in the Pentaho Data integration prototype, a MySQL database was consolidated with 293 valid records, represented in 2 tables and 26 specific attributes; The above shows the functional articulation from the data generated by the IoT solution, the standardization of data into information and the dumping as output in a MySQl database as the only data format available for subsequent processes.
- Based on the security properties, related to immutability, decentralization, cryptography, consensus, transparency, censorship resistance, auditing, traceability and smart contracts that blockchain offer and that have been widely used. validated in solutions designed for other contexts; It is possible to affirm that the future development in the Python programming language, of the MySQL to blockchain converter as part of the proposed model; will ensure the assignment and inheritance to the model of the security properties listed above.
- Supported by the results of the architectural, structural and functional process analyzed in the development of this investigative exercise, represented in the articulation of technologies such as the Internet of Things, business intelligence with its ETL process, standardized data outputs in a database of MySQL data and the development of the converter to a blockchain; have allowed us to consolidate a functional, structured and robust security model for IoT that allows us to guarantee the integrity of the information in the transmission phase.

References

[1] Y. Zhang, "Technology Framework of the Internet of Things and Its Application," in *Electrical and Control Engineering (ICECE)*, [s.f.].

[2] A. Botta, W. d. Alessio, "Integración de computación en la nube e Internet de las cosas: una encuesta," *Elsevier*, vol. 56, Napoli, Italia, 2016.

[3] F. Sánchez-Torres, I. González, and C. C. Dobrescu, "Machine Learning in Business Intelligence 4.0: Cost Control in a Destination Hotel," 2022.

[4] J. M. C. Lovelle, J. I. R. Molano, and C. E. M. Marin, "Introducción al Internet de las Cosas," *Redes de Ingeniería*, vol. 6, 2015.

[5] C. D. Retamal, J. B. Roig, and J. Tapia, "La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas," *Economía industrial*, vol. 405, pp. 33–40, 2017.

[6] F. Colorado, "El ciclo PHVA de Deming y el proceso administrativo de Fayol," *Academia*, 2009. [Online]. Available: http://www.academia.edu.

[7] D. M. Llorián and J. M. C. Lovelle, "Socialización de Objetos Inteligentes aplicando Ingeniería Dirigida por Modelos en el marco de Internet de las Cosas," Doctoral dissertation, Universidad de Oviedo, 2020.

[8] J. R. Douceur, "The Sybil Attack," in *Peer-to-Peer Systems: First International Workshop, IPTPS 2002 Cambridge*, MA, USA, March 7–8, 2002 *Revised Papers 1*, Springer Berlin Heidelberg, pp. 251–260, 2002.

[9] N. Ekedebe and W. Y., "Securing transportation cyber-physical systems," in *Securing Cyber-Physical Systems*, CRC Press, Boca Ratón, 2015.

[10] R. Faludi, *Building Wireless Sensor Networks: With ZigBee, XBee, Arduino, and Processing*. O'Reilly Media, Inc., 2010.

[11] M. Álvarez, J. J. Jiménez, M. González-Guerrero, C. Hernando, and H. Guerrero, "Total Ionizing Dose radiation test on the temperature sensor TMP36 from Analog Devices," in *2012 IEEE Radiation Effects Data Workshop*, July 2012, pp. 1–7.

[12] A. González, Y. Díaz, and W. Flórez, "Design and prototyping of an electronic cane for an indoor guie system for the blind," *Ingeniería* (0121-750X), vol. 25, no. 3, 2020.

[13] G. Zhang, X. Chen, L. Zhang, B. Feng, X. Guo, J. Liang, and Y. Zhang, "STAIBT: Secure and reliable agricultural IoT Blockchain Terminal empowered by Blockchain and CP-ABE," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 7, no. 5, pp. 66-75, 2022.

[14] W. Ruíz-Martínez, Y. Díaz-Gutiérrez, R. Ferro-Escobar, and L. Pallares, "Application of the Internet of Things through a Network of Wireless Sensors in a Coffee Crop for Monitoring and Control its Environmental Variables," *TecnoLógicas*, vol. 22, no. 46, pp. 101–116, 2019.

[15] A. B. Martínez, E. A. G. Lista, and L. C. G. Flórez, "Técnicas de modelado de procesos de ETL: una revisión de alternativas y su aplicación en un proyecto de desarrollo de una solución de BI," *Scientia et technica*, vol. 18, no. 1, pp. 185–191, 2013.

[16] M. Casters, R. Bouman, and J. Van Dongen, *Pentaho Kettle Solutions: Building Open Source ETL Solutions with Pentaho Data Integration*. John Wiley & Sons, 2010.

[17] H. E. Williams and D. Lane, *Web Database Applications with PHP and MySQL: Building Effective Database-Driven Web Sites*. O'Reilly Media, Inc., 2004.

[18] D. Ipswich, *Setting up a WAMP Server on Your Windows Desktop*. Technology Now at Smashwords, 2011.

[19] A. Arias Maestro, Ó. Sanjuán Martínez, A. M. Teredesai, and V. García-Díaz, "Blockchain Based Cloud Management Architecture for Maximum Availability," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 7, no. 5, pp. 66-75, 2022.

[20] Y. D. Gutiérrez and J. M. C. Lovelle, "Análisis de la función Hash Criptográfica en cadenas de bloques y su impacto en la seguridad de transacciones de datos," *Redes de Ingeniería*, vol. 9, no. 2, pp. 82–87, 2018.

[21] L. B. Carneiro, A. C. C. Silva, and L. H. Alencar, "Scrum agile project management methodology application for workflow management: a case study," in *2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, Dec. 2018, pp. 938–942.

Yesid Díaz Gutiérrez

Research Professor of the Software Engineering program of the Ibero-American University Corporation in Bogotá Colombia, Systems Engineer with an emphasis on software at the University Antonio Nariño, specialist in pedagogy at the Universidad la Gran Colombia in Bogotá, Colombia, Master in Strategic Management of Information Technologies and PhD student in Computer Science at the University of Oviedo.

Juan Manuel Cueva Lovelle

Professor at the University of Languages and Computer Systems at the University of Oviedo (Spain). Mining Engineer (1983). Doctor from the Polytechnic University of Madrid (1990). He was Director of the University School of Technical Engineering in Informatics of Oviedo (University of Oviedo) from July-1996 to July-2004. He was Director of the Department of Informatics at the University of Oviedo from 2008 to 2016. He was coordinator of the Master in Web Engineering at the University of Oviedo from 2005 to 2016. His research areas are blockchain, Internet of Things (IoT) Industry 4.0, Smart Mining, Drone Applications, Language Processors, Human-Computer Interaction, Model Driven Engineering and Web Engineering. He has directed more than 25 Research projects, more than 100 contracts with companies and 35 doctoral theses. He is the author of more than 200 books, articles and communications to congresses.

Diana Carolina Candia Herrera

Research Professor of the System Engineering program of the Ibero-American University Corporation in Bogotá Colombia, Systems Engineer of the Pilot University Corporation of Colombia, specialist in telecommunications of the Pilot University Corporation of Colombia and Master of Education of the Ibero-American University Corporation.