**SECURITY MECHANISMS FOR INTERNET OF THINGS (IOT)**

**Abstract**. Internet of Things (IoT) is a concept that involves various objects and methods of communication to exchange information. Today, IoT is primarily a vision that dictates that everything should be interconnected over the internet. IoT is currently and for sure will be, the foundation for future development because it brings new opportunities for novel services. All objects will be connected and communication need to happen between all, while CIA triad (at least) should not be compromised, at all. This aspect leads to major security challenges, which will be treated hereinafter.

1. **Introduction**

The Internet of Things (IoT) is not a newly introduced term to ICT industry. Back in 1982, four students at Carnegie Mellon University, Mike Kazar, David Nichols, John Zsarnay and Ivor Durham wired up a vending machine so that they could see the availability and coolness of the soda cans in each dispensing column, remotely, over ARPANET. After that, it was mentioned by Kevin Ashton in 1999, while having a presentation at Proctor & Gamble [1] trying to explain the value of the recently introduced technology of RFID in supply chain industry. Since then, the need of interconnection of all available objects over internet is increasingly demanding. Big consulting companies calculate the number of these connected objects to reach 20bn by 2020, while the market is estimated to reach 3bn USD. The IoT industry is flourishing since the number of computations that a computer can execute almost doubles biyearly, while the size and the amount of power needed is almost half for the same period. This means that smaller and more powerful devices are available for interconnection and data exchange offering a wide range of applications. The Internet of Things covers several different domains and technologies, introducing challenges regarding interoperability between different stacks, and implementation of standards on low powered and low energy devices. All these combined, bring new challenges in security and questions regarding how to ensure confidentiality, integrity and availability. As all innovative developments and IoT as well, ensure the users a superior life right now and in the years to come, but there is a great security concern. Especially today, the privacy is increasingly concerned by the public. To make IoT pervade people’s everyday life, the security of the IoT must be strengthened.

Security of IoT is crucial to the development of IoT industry. The IoT is an immature technology. The key issue that affects the development of IoT is that a mature and complete security models and standards is lacking. Compared to the traditional network, IoT integrates many different networks such as WSN, RFID systems, mobile vehicle network, 3G 4G 5G technologies, WiMAX, personal area network, VPNs and so many others. As the IoT environment becomes more and more complex and demanding, the security issues coped, are more and more complex than any other existing network systems. My motivation for conducting the research in IoT, is the lack of sustainable and flexible solutions which to address some of the main security issues. Some early security mechanisms and solutions are now being implemented, but they still need improvement and standardization. The full potential of IoT goes beyond the enterprise centric systems and moves towards a user inclusive IoT, in which IoT devices and contributed information flows provided by people, are encouraged. This will allow new user centric IoT information flows and new cohort of services of high value for the society. Security is one of the main IoT challenges nowadays. An important consideration is which protocol stack provides best security and privacy services. Security can be provided at different levels so deciding the optimal choice, is not simple process. Since IoT is a relatively new concept, it is still unknown and not explored by many companies and employees in industry. This limited knowledge, may cause them to be afraid of, or totally unaware of the potential security and privacy issues connected to their deployment of IoT. Therefore, many organizations want to know more about the potential threats, benefits, disadvantages, challenges, and solutions regarding security regarding IoT. Additionally, they need to know what competence in information security is necessary to realize cost effective security in conjunction with their deployment of IoT. This knowledge and competence should help in facilitating their transition from a non-IoT-business to an IoT business, as it will enable both employees and management to understand & address their doubts & concerns in terms of their investments and the potential security risks. In this way, managers can make a balanced risk-benefit analysis of the adoption of IoT for a specific application or family of applications.

1. **Information Security**
   1. **Historical background.** Information security processes and techniques are as old as the information each self. From the very first years of communication, the value of security mechanisms was very well comprehended. Julius Caesar was one of the first to use these practices by inventing the Caesar cipher at 50 B.C., to make his messages unreadable if they were found to unwanted hands. From the mid of the 16th century various, governments around the globe, created organizations to secure the information and communication (e.g., the UK Secret Office and Deciphering Branch in 1653). More recently, during 19th century and because of the two World Wars many authorities were created to protect the privacy of information; exchange of war related information between allies of the World War II, brought into the picture the necessity of encrypting the information to become unreadable. This brought us to the Enigma Machine [2], which was invented at the end of WWI by Arthur Scherbius but adopted by Nazis before and during the WWII to encrypt warfare related data. Enigma was successfully decrypted by Alan Turing.

At the end of the 20th century and early years of the 21st, a speedy development in telecommunications, hardware and software occurred while data encryption is happening. Things are getting smaller and smaller, more powerful, and even cheaper, bringing computing closer to everyone, appealing not only to businesses but to individuals as well. The Internet expansion and availability also helped on all these objects to be interconnected and made information publicly available.

The rapid growth of electronic business was used even for criminal acts, stimulated the need for protecting computers, networks and information.

* 1. **Information Security Definition.** Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security countermeasures of all available types (technical, organizational, human-oriented, and legal) in order to keep information in all its locations (within or outside the organization’s perimeter) and consequently, information systems, where information is created, processed, stored, transmitted and destructed, free from threats [3].

Information security is built around the three main pillars of CIA triad: Confidentiality, Integrity and Availability of IT frameworks and to the applicable information setting the targets that:

* is revealed to authorized parties (Confidentiality)
* is not subject to unapproved modification of information (Integrity) and
* information is accessed by authorized parties when requested (Availability).
  1. **The CIA Model.** The Confidentiality, Integrity, and Availability triad (CIA triad) is a model that was built to guide policies for information security within an organization. The model is also sometimes referred to as the CIA triad (Confidentiality, Integrity, and Availability). These three pillars are considered the three most crucial components for security.
     1. **Confidentiality**. Confidentiality is equal to privacy. Sensitive information is prevented from reaching the wrong people, while making sure that the right people can in fact receive it. Access must be provided to the authorized to view the data.

Some examples of practices used to ensure confidentiality is data encryption include bit not limited to, user names and passwords, two-factor authentication, biometrics, security tokens, hardware and soft tokens, etc.

* + 1. **Integrity**. Integrity means maintaining the consistency, accuracy, and reliability of data over its entire life cycle. Data must be altered only by authorized people.

Measures include file permissions and user access controls, version controlling maybe used to prevent erroneous changes or accidental deletion by authorized users, which is a problem as well, checksums and cryptographic checksums for integrity verification; backups must be available to restore the data at its original state in case of permanent loss.

* + 1. **Availability**. Availability means maintaining the service always available, offering adequate bandwidth and preventing network bottlenecks are equally important, redundancy and disaster recovery to ensure systems availability. Backup copies should be stored in a different location from the original data storage, firewalls IDS and proxy servers can be used to prevent intruders.

It is critical to comprehend that Data Protection Act prerequisites go beyond the traditional way or transmitted and stored data. he seventh data protection guideline identifies security requirements on collecting, storing and processing of personal data.

So, the security measures you put in place should seek to ensure that:

* only authorized people can access, alter, disclose or destroy personal data;
* those people only act within the scope of their authority; and
* if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

Organizations need to make sure that

* make sure you have the right physical and technical security measures to ensure data protection
* have in place all relevant processes and procedures to cope with security breaches cases
* when never new applications are being designed, security and privacy need to be taken in to account from the very beginning
* they keep track of the data sharing across the departments or/and with external parties if needed
* backup policies to be in place to ensure that data recovery will be successful
* make sure that all employees are aware of cyber threats and actively following any security plan
* have a data retention policy that allows them to destroy unneeded or “expired” data
* comply with all regulatory authorities
* at least follow and ensure the CIA triad

There are so many threads that need to be considered when coping with Information security. In Table 1, most important IoT security threats are summarized.

|  |  |
| --- | --- |
| **Security issue** | **Details** |
| **Insecure Web interface** | Account Enumeration  Weak Default Credentials  Credentials Exposed in Network Traffic  Cross-site Scripting (XSS)  SQL-Injection  Session Management  Weak Account Lockout Settings |
| **Insufficient Authentication/Authorization** | Lack of Password Complexity  Poorly Protected Credentials  Lack of Two Factor Authentication  Insecure Password Recovery  Privilege Escalation  Lack of Role Based Access Control. |
| **Insecure Network** | Vulnerable Services  Buffer Overflow  Open Ports via UPnP  Exploitable UDP Services  Denial-of-Service  DoS via Network Device Fuzzing. |
| **Lack of Transport Encryption** | Unencrypted Services via the Internet  Unencrypted Services via the Local Network  Poorly Implemented SSL/TLS  Misconfigured SSL/TLS. |
| **Privacy Concerns** | More than the critical to the functionality data are collected  Collected sensitive data  Data are not anonymized  Unencrypted data collection  Unprotected personal information  Unauthorized access to personal information  No retention policies applied |
| **Insecure Cloud Interface** | Account Enumeration  No Account Lockout  Credentials Exposed in Network Traffic. |
| **Insecure Mobile Interface** | Account Enumeration  No Account Lockout  Credentials Exposed in Network Traffic |
| **Insufficient Security Configurability** | Lack of Granular Permission Model  Lack of Password Security Options  No Security Monitoring  No Security Logging |
| **Insecure Software/Firmware** | Not updated devices  Unencrypted file updates  Unencrypted connection transmissions  Ensuring the update file does not expose sensitive data  Unsigned and unverified updates |
| **Poor Physical Security** | USB Ports available on devices  Storage Media available on devices |

Table 1: IoT security threats

|  |  |
| --- | --- |
| **Requirement** | **Details** |
| **Authenticity** | Only legal users should be allowed to access the system or sensitive information. |
| **Authorization** | The privileges of device components and applications should be limited as so they are able to access only the resources, they need to do their addressed tasks. |
| **Confidentiality** | Information transmission between the nodes should be protected from intruders. |
| **Integrity** | Related information should not be tampered. |
| **Availability and**  **Continuity** | To avoid any potential operational failures and interruptions, availability, and continuity in the provision of security services should be ensured. |

Table 2: Extended CIA model

* 1. **Security elements.** For the security domains, it’s important to identify key elements for the information security (Figure 1). In the following sections, the key elements definitions are described.

Figure 1: Security elements

* + 1. **Asset**. Asset is any datum, device, or in general any module of the organization’s universe that supports information-driven processes. Assets can include hardware, software and information as well. Assets should be always protected under the CIA triad framework.
    2. **Threat**. In computer security, a threat is anything that can possibly make a damage. A danger is something that could possibly happen, or not. Dangers can prompt assaults on computer systems and that's only the tip of the iceberg.
    3. **Vulnerability**. Any Weaknesses or gap in security mechanisms that can be exploited by threats to benefit from unauthorized access to an asset is a vulnerability.
    4. **Risk**. When a treat threat is exploiting a vulnerability then a risk may be identified, the possibility for loss, damage or destruction of an asset.
    5. **Exposure**. Exposure is a state in a computing system (or set of systems) which is not a universal vulnerability, but either allows an attacker to conduct information gathering activities or to hide activities.
    6. **Countermeasures**. Countermeasure indicates any action, device, process, or technique that potentially may lead to reduce threats, vulnerabilities, or any attacks by preventing it or minimizing the damage. Corrective actions need to be taken even if it decided to simply mitigate the risk.
    7. **Security Policies**. Security Policy means the set/rules adopted by an organization to ensure that IT and network infrastructure follows the principles of data security, users are taking all appropriate measures to ensure that the CIA triad is respected when contacting any form of business activity in or out of the organization’s borders.

|  |  |
| --- | --- |
| **Layer** | **Risks** |
| **Perception** | Spoofing, signal jamming, outage, eavesdropping |
| **Network** | Wormhole, forwarding, man in the middle, floods |
| **Support** | DoS, unauthorized access, data tampering |
| **Application** | Sniffers/loggers, DDoS, social and session hijacking, injections |

Table 3: For each IoT protocol layer, different threats and risks are presented

1. **IOT**
   1. **Background.** The Internet of Things (IoT) was first used by Kevin Ashton in 1999, [1] who defines IoT as uniquely identifiable objects (things) and their virtual representations in an Internet-like structure. From a technical point of view, the IoT presents network of uncountable number of global connected objects - devices, sensors, or actuators, providing different services over the Internet. Fundamentally, IoT means a shift from reactive to proactive systems; from delayed problem management to automatic sense-and-respond capabilities.

The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 (06/2012) [4] as “a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies”.

Diagram

Description automatically generated

Figure 2: Technical overview of the IoT [4]

IoT consists of two key elements: "internet" and "things" [5]. Communication allows things to coordinate their actions and reach decisions together it allows them to hear, see, think, compute, and act. The technology gives things making authoritative decisions that benefit various applications using intelligence and consensus. From the standpoint of passive observers, they transform objects or sensors into active members of a computing system, communicating, working collaboratively, and making critical decisions. As a result, they present challenges that require specialized communication standards [6].

The most vital part of achieving IoT is communication, is communication. No matter how smart or capable the devices are, if they cannot transmit and communicate then they cannot be a part of the IoT ecosystem. How this communication is performed is less important, since the actual physical and link layer communication within IoT can be realized in many ways.

Physical devices can communicate through communication network:

* Through a gateway, for example CCTV cameras that monitor a place
* Without a gateway
* Directly, for example two devices that are close to each other via Bluetooth or ZigBee protocols – smart home devices.

A physical thing can be mapped into the information world via one or more virtual things, while virtual things do not necessarily need to be associated with any physical thing. For example, a physical thing might execute multiple applications and thereby have multiple identities in the virtual world.

* 1. **Fundamental characteristics**. The fundamental characteristics of the IoT are the following:
     1. **Interconnectivity**: Anything can be interconnected with the global information and communication infrastructure.
     2. **Things-related services**: The IoT can provide thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. To provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.
     3. **Heterogeneity**: The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.
     4. **Dynamic changes**: The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.
     5. **Scalability**: The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet. The ratio of communication triggered by devices as compared to communication triggered by humans will noticeably shift towards device-triggered communication. Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling.
  2. **IoT Roadmap.** It is widely accepted that RFIDs were the ancestors of IoT. Originally used in supply chain industry for tracking purposes, very fast moved to the Vertical market such as security, surveillance, transportation, food safety and others enabled by the network evolution as elaborated in Figure 3. These days is mainly used for monitoring and controlling of remote or distant objects [7].



Figure 3: IoT Roadmap [7]

According to the Gartner analysis [8] 8.4 billion IoT devices are expected to be connected by the end of 2017, showing an increase of 31% from 2016, while this number is expected to reach 20.5 billion IoT connected devices by 2020. The total market is expected to reach 3 trillion USD.

|  |  |
| --- | --- |
| **Attacks** | **Risks** |
| **Spoofing** | Authenticity, integrity, and confidentiality |
| **Signal/Radio Jamming** | Availability and integrity |
| **Device-tampering/Node capturing** | Availability, integrity, authenticity, and confidentiality |
| **Path-based DoS Attack** | Availability and authenticity |
| **Node Outage** | Availability and authenticity |
| **Eavesdropping** | Confidentiality |

Table 4: IoT attacks

1. **Security in IoT**
   1. **Introduction.** Any IoT implementation requires substantial number of technologies to be able to support the offered services in terms of software, hardware, and network as well. There are many challenges need to be analyzed when we are talking about security of an IoT environment.

* The biggest challenge in IoT world is the objects themselves, either physical or virtual. By nature, IoT is based on the development of objects as much as possible and the more objects we have the more potential problems may have. Tens of years back we had only to protect our PC to access the internet, now we need to care about PCs, Smartphones, smart devices, car, wearables, anything practically that is connected over the net.
* The more devices we have the more difficult is to administer them. Firmware updates for devices or OS updates are crucial to maintain the security at a high level. Even the users may be difficult if they have some tens of devices to maintain them updated to the latest security releases.
* Communication and information transmittal. Regardless of the number of IoT devices the information that is being captured need to be somehow transmitted to the next level for further processing. Authentication and privacy protection should be a fundamental element of IoT security while encryption needs to be applied.
* Unauthorized access to smart devices.
* Security was left aside for some devices, even a couple of years back from vendors that did not take any consideration about security and offered to the public unprotected devices.
* Lack of experience and lack of expertise may be the backdoor to security breaches A smart refrigerator that can report that the milk is finished for a mean consumer is a major step forward, but, on the other hand, this smart device if it’s not properly maintained can be compromised and offer access to other connected devices on the same network.

To solve these challenges, there are hundreds of available solutions for implementation which make things fuzzier; from proprietary protocols in IoT, ZigBee and ZWave, to protocols well established and supported widely like TCP, IP, HTTP or SMTP and open standards from IEEE, IETF or W3C for standardized protocols like 6LowPAN or CoAP.

A set of several studies were considered to stipulate the following summarization for security requirements, challenges, threats and potential solutions ((Farooq, 2015), (Huang, 2015), (Nguyen, 2015), (Commission., n.d.), (Arseni, 2015), (Anon., 2012), (Polk, 2011)).

|  |  |  |
| --- | --- | --- |
| **Type** | **Algorithm** | **Purpose** |
| **Symmetric Encryption** | Advanced encryption standard (AES) | Confidentiality |
| **Asymmetric Encryption** | Rivest Shamir Adelman (RSA)/ Elliptic Curve Cryptography (ECC) | Digital Signatures, Key Transport |
| **Asymmetric Key Agreement** | Diffie-Hellman (DH) | Key Agreement |
| **Hashing** | SHA-1/ SHA-256 | Integrity |

Table 5: Frequently used Cryptographic Algorithms

* 1. **IoT Protocols related to Security.** In the previous chapters a detailed analysis of IoT protocols presented. For the security purpose, I have selected the most appropriate important IoT protocols to be analyzed and compared them. All these protocols are assigned to the transport or application layers of IoT protocol stack.
     1. **DTLS.** Datagram Transport Layer Security (DTLS) is a protocol that provides security for datagrams. The protocol is based on the TLS protocol to offer similar security.

Although it was designed for security. researchers from Royal Holloway, University of London in 2013, managed to recover plaintext from a DTLS connection using the OpenSSL implementation of DTLS when Cipher Block Chaining mode encryption was used.

* + 1. **QUIC.** Quick UDP Internet Connections (QUIC) uses the User Datagram Protocol (UDP) and support a group of composite connections that are present in between two endpoints. QUIC could give the security protection just like Transport Layer Security or like Security Sockets Layer with the feature of minimizing transport latency and no of connections. QUIC is also designed to estimate the bandwidth in either direction so that congestion problem should be avoided.

|  |  |  |
| --- | --- | --- |
| **Features** | **QUIC** | **DTLS** |
| **Layer** | Transport | Transport |
| **Security** | Yes | Yes |
| **Interoperability** | Yes | Partial |
| **Objective** | Composite connections | Communication privacy for UDP |
| **Delivery** | Not guaranteed | Not guaranteed |
| **UDP** | Yes | Yes |

Table 6: Comparison between the two most important security protocols

* + 1. **CoAP.** Constrained Application Protocol (CoAP) is an Internet Application Protocol for controlled devices defined by RFC 7228, extended by RFC7252 for IoT applications. CoAP is designed in such way to avail different devices to operate on a constrained network and between devices on different constrained networks all interconnected by internet. CoAP is also used SMS on mobile communication networks for SMS.

CoAP is designed to translate to HTTP for web integration, to support multicast, offer low overhead, and simplicity, services very critical to IoT. CoAP runs on a variety of devices supporting UDP like protocols.

* + 1. **MQTT.** Message Queue Telemetry Transport (MQTT) is a light-weight messaging protocol specially designed for IoT and M2M communication introduced by Andy Stanford-Clark and Arlen Nipper in 1999. designed for constrained devices and low-bandwidth, high latency, or unreliable networks. The requirements were to minimize bandwidth and device resource requirements, while making sure reliability and assurance of delivery will be catered as well. These make MQTT ideal for IoT and M2M environment. Security was also implemented in V3.1 where username and password could be passed. Encryption is implemented with SSL.

MQTT working model is based on Publisher/Subscriber mode (see Figure 6: MQTT working model) which means that a publisher makes available a set of information through a broker, who makes this information accessible to the ones that are interested in (subscribers).

Figure 4: MQTT working model

* + 1. **JSON.** JavaScript Object Notation or JSON uses human-readable text to transmit data objects consisting of attribute–value pairs and array data types, it was introduced by Douglas Crockford in 2000 and defined by RFC 7159. It is a very commonly used for asynchronous communication and is a language independent. It was originally derived from JavaScript, but many programming languages are handling JSON-format data structures.
    2. **CBOR.** Concise Binary Object Representation (CBOR) is a binary data format based on JSON and defined by RFC 7049, that results in compact message size. It is used for the CoAP Internet of Things protocol.

1. **Security Mechanisms for IoT systems**
   1. **Blockchain Technology.** Blockchain is a decentralized, distributed, immutable and shared ledger that keeps track of assets and transactions on a peer-to-peer network (P2P) [9].

One of the most important concepts of blockchain is blocks. Each block contains an encrypted value containing the block information preceding it.

Transactions are a small task unit usually stored in public records within a block. Records are usually added to the blockchain after obtaining the approval of most users participating in the blockchain network [10]. The data processed in the distributed ledger is recorded in the ledger with the consent of all participants in the network. This is called a consensus mechanism.

The first of the features that make Blockchain valuable is the decentralization structure. In a blockchain network, data appears as a distributed ledger database. The same data are kept simultaneously on all other stakeholders in the network. With all these features, blockchain technology provides the highest level of traceability by all stakeholders.

Another important contribution of blockchain technology is the transparency it adds to business processes. This increases the trust between stakeholders and ensures accountability. It allows all stakeholders to monitor the blockchain network in real-time.

Data privacy is an important feature of restricted blockchain networks. In restricted blockchain networks, only users authorized by the node's administrator can view data. This ensures that data coming to the blockchain network is protected.

The public key structure of blockchain networks, which protects data modification, largely eliminates integrity problems. The participants and the consensus mechanism of a blockchain network are other factors that increase data security.

Smart contracts are pieces of code that define the business processes between stakeholders in blockchain networks.

Blockchain technology is used on many digital currencies including widespread Bitcoin and Ethereum cryptocurrencies using smart contracts. In the field of corporate blockchain applications, Hyperledger Fabric network is frequently used.

* 1. **Background.** At [11], an approach is presented to integrate IoT and blockchain technologies into supply chain processes. The study proposes a Blockchain-based distributed logistics platform that involves adding actors in a supply chain to the system as a node. A virtual copy of a transported property is created with IoT devices on the proposed platform. Other data such as the location, temperature, and humidity of the transported goods are monitored via the virtual copy and recorded on the blockchain.

At [12], it is explained that the most important benefit in saving data from IoT devices to a blockchain network using smart contracts is that these data can be evaluated and reported to the sender or receiver automatically. The smart contract running in the system corrects the temperature values coming from the sensors and saves them to the blockchain. Mobile clients communicate with the server using the REST API. Customers can control the data in the system through these mobile clients.

At [13], a blockchain-based network monitoring and management architecture is proposed. The administrators in the network indirectly control the network devices by recording the changes in the device configuration on the blockchain, where they control the updates in the configurations of the network devices.

At [14], it is aimed to control and configure IoT devices using blockchain. The proposed system includes a smartphone and three raspberry pi. The three-raspberry pi in the system act as a meter, air conditioner, and light bulb, respectively. The user can adjust the policy in the system via the smartphone. Configuration changes made via the smart device are recorded on the Ethereum network.

At [15], it is pointed out that blockchain's decentralized and change-resistant nature can be used to solve some of the problems faced by the nature of IoT. The authors present a cloud and fog-based solution to solve this problem. In the study, the Intel Edison Arduino card is used as the IoT device, and the blockchain works separately on the fog and the cloud. In the experiments, the IoT device writes data to the blockchain via a Python server.

* 1. Identification, Authentication, and Authorization the MQTT publisher running on the Hyperledger Fabric API server [16] must transact with a previously defined authorized user within the Hyperledger Fabric organizations. At the same time, additional authentication is provided by using the username and password fields provided by MQTT for authorization. With this identification provided by the Hyperledger Fabric user identification and MQTT protocol (Figure 2), the data sent through the protocol will be authenticated, and unauthorized access to the data will be prevented. In addition, the optional MQTT TLS support makes it easy to encrypt messages and authenticate clients using authentication protocols.

Graphical user interface, application

Description automatically generated

Figure 5: IoT Integration to Hyperledger Network [16]

1. **.**

# Bibliography

|  |  |
| --- | --- |
| [1] | K. Ashton, "That ‘internet of things’ thing," *RFID journal,* vol. 22, no. 7, pp. 97-114, 2009. |
| [2] | Wikipedia, "Enigma machine," 2022. [Online]. Available: https://en.wikipedia.org/wiki/Enigma\_machine. |
| [3] | Y. Cherdantseva and J. Hilton, "Information Security and Information Assurance," *Standards and Standardization: Concepts, Methodologies, Tools, and Applications,* 2015. |
| [4] | ITU-T, "Overview of the Internet of things," I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n, 2012. |
| [5] | K. K. Vaigandla, R. K. Karne and A. S. Rao, "A Study on IoT Technologies, Standards and Protocols," *IBMRD's Journal of Management & Research,* vol. 10, no. 2, pp. 7-14, 2021. |
| [6] | T. Salman and R. Jain, "A Survey of Protocols and Standards for Internet of Things," *Advanced Computing and Communications,* vol. 1, no. 1, 2017. |
| [7] | G. Mavridis, "Security mechanisms for Internet of Things (IoT)," University of East London, Greece, Piraeus, 2017. |
| [8] | R. v. d. Meulen, "Newsroom Press Releases," 2017. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. |
| [9] | N. E. Ioini and C. Pahl, "A Review of Distributed Ledger Technologies," *On the Move to Meaningful Internet Systems. OTM 2018 Conferences Confederated International ,* vol. 11230 , pp. 277-288, 2018. |
| [10] | G. W. Peters and E. Panayi, "Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money," 2015. |
| [11] | N. Rožman, R. Vrabič, M. Corn, T. Požrl and J. Diaci, "Distributed logistics platform based on Blockchain and IoT," *Procedia CIRP,* Vols. 81,, pp. 826-831, 2019,. |
| [12] | T. Bocek, B. B. Rodrigues, T. Strasser and B. Stiller, "Blockchains everywhere - a use-case of blockchains in the pharma supply-chain," *IFIP/IEEE Symposium on Integrated Network and Service Management (IM),* pp. 772-777, 2017 . |
| [13] | K. Košťál, P. Helebrandt, M. Belluš, M. Ries and I. Kotuliak, "Management and Monitoring of IoT Devices Using Blockchain," *Sensors for Information Technology, Electronics and Mobile Communication,* vol. 19(4), p. 856, 2019. |
| [14] | S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform," *19th International Conference on Advanced Communication Technology (ICACT). Global IT Research Institute - GiRI,* pp. 464-467, 2017 . |
| [15] | M. Samaniego and R. Deters, "Blockchain as a Service for IoT," *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),* pp. 433-436, 2016. |
| [16] | K. O. Toka, Y. Dikilitaş, T. Oktay and A. Sayar, "Securing Iot with Blockchain," *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences,* vol. 46, pp. 529--532, 2021. |