DOI: 10.1561/9781638285076.ch3

Chapter 3

ERATOSTHENES Project Integrated Solution

By Sokratis Vavilis, Fotis Michalopoulos, Harris Niavis, George Misiakoulis, Konstantinos Loupos, Konstantinos Dafloukas, Jesús García-Rodríguez, Ekam Puri Nieto, Juan Francisco Martínez Gil, Agustín Marín Frutos and Antonio Skarmeta

The Internet of Things (IoT) is transforming our world, connecting countless devices and enabling new levels of automation and data sharing. But this connectivity also creates security risks, as each device becomes a potential target for attackers. Traditional security methods often fall short in protecting these diverse and widespread networks. Many IoT devices have limited resources, making it difficult to implement strong security measures like encryption or complex authentication protocols. The wide variety of devices and communication methods also makes it challenging to establish consistent security standards, as a one-size-fits-all approach simply doesn't work in such a fragmented landscape.

The ERATOSTHENES project aims to solve these problems by creating a new system for managing trust and identities in the IoT. This system is designed to work across an entire network without relying on any central control point, making it more resilient and less vulnerable to attacks that could compromise the whole system. It's automated for efficiency, meaning many tasks are handled automatically without human intervention. It's also transparent for accountability, allowing

actions to be tracked and verified, which helps build trust among users and stakeholders. Importantly, it prioritizes user privacy, giving users control over their data and how it is used. By managing the entire lifespan of IoT devices, from initial setup to eventual decommissioning, this system strengthens trust and security within the network. It also complies with all relevant data protection and cybersecurity regulations, like GDPR and the Cybersecurity Act, ensuring it meets the highest standards for security and privacy.

One of the key challenges is the sheer variety of IoT devices, which makes it difficult to get a clear picture of their security status. Existing methods for establishing trust often lack proper upkeep, and outdated software can be exploited by attackers. This is further complicated by the fact that many IoT devices are "set it and forget it," meaning they are deployed in remote locations or inaccessible environments where regular updates and maintenance are difficult. Another challenge is managing the identities of devices and ensuring user privacy. A lack of security training and proper protocols for both users and devices creates further risks, as users may not be aware of the security implications of connecting their devices, and manufacturers may prioritize functionality over security.

Blockchain technology offers a promising solution for improving IoT security. Its decentralized and tamper-proof nature makes it well-suited for managing trust and identities. Because blockchain records every transaction across multiple computers, it's incredibly difficult to alter or tamper with the data, ensuring its integrity and reliability. The ERATOSTHENES solution includes several key components to address these challenges. The Trust Manager & Broker calculates trust scores for each device based on various factors and manages relationships between devices. The MQTT Broker filters security-related events and stores session data, acting as a central communication hub for security information. The Threat Modelling & Risk Assessment component creates a virtual model of the system to identify potential threats and vulnerabilities. The MUD Manager interprets device information and creates access control lists, determining which devices have access to which resources. The Trust Agent Deployer manages security software on devices, ensuring they are up-to-date and functioning correctly. The Trusted Execution Environment provides a secure area within the device for key services to run, protecting them from tampering. And the Self-Sovereign Identity system gives users control over their data and privacy, allowing them to manage their digital identities and decide how their information is used.

ERATOSTHENES uses privacy-preserving credentials to enhance security during authentication. This allows users to prove their identity without revealing unnecessary personal information. It leverages Physical Unclonable Functions to create unique keys for devices, exploiting tiny physical variations in their hardware. A Distributed Ledger Technology provides a secure infrastructure for storing

and managing critical information, ensuring its integrity and availability. A Cyber Threat Intelligence Sharing Agent helps share security information across the network, allowing different parts of the system to learn from each other and respond to threats more effectively. And a Monitoring and Intrusion Detection System constantly monitors the network for potential threats, using machine learning to identify suspicious activity and anomalies.

The effectiveness of the ERATOSTHENES solution is being tested in three real-world pilot projects. One focuses on securing communication between vehicles and infrastructure, ensuring the safety and reliability of connected cars. Another secures a remote patient monitoring system, protecting sensitive patient data and ensuring the integrity of medical devices. And the third uses unique device IDs and secure data transfer methods to protect industrial networks, safeguarding critical infrastructure and preventing disruptions.

3.1 Introduction

With its ability to connect billions of objects and provide previously unheard-of levels of automation, data interchange, and ease, the Internet of Things (IoT) is drastically changing our world. IoT devices are influencing every part of our lives and industries, from industrial sensors and connected cars to smart homes and wearable fitness trackers. To guarantee the security and privacy of people and organizations, major security issues brought forth by this broad adoption must be resolved. The enormous growth of the attack surface is one of the main security issues with the Internet of Things. Every connected device is a possible point of entry for bad actors, and because there are so many of them, it is very challenging to properly secure them all. Because IoT systems are scattered and heterogeneous, traditional security solutions—which were created for centralized networks and personal computers—are frequently insufficient. In addition, a large number of IoT devices are built with constrained memory, computing power, and battery life. Because of this, it is difficult to put strong security measures in place without sacrificing functionality or efficiency, such as encryption and authentication procedures. Because of this, attackers looking to take advantage of weaknesses and obtain sensitive information without authorization can easily target these devices. Another major security concern is the heterogeneity of IoT devices. Numerous manufacturers produce these devices, and each has unique communication protocols, software, and hardware. It is challenging to create a single security posture and apply uniform security standards throughout the IoT ecosystem due to this lack of standardization.

The security of data created and sent by IoT devices is another significant worry. Large volumes of data, such as location data, behavioral patterns, and personal

information, are gathered by these devices about users and their surroundings. This data may be intercepted, altered, or misused in the absence of appropriate security measures, which could result in identity theft, privacy violations, and other negative outcomes. These security issues are made worse by the intricacy of IoT ecosystems. Various devices, platforms, and networks are frequently integrated into these ecosystems, resulting in a complex web of relationships and interactions. Access control regulations, data exchange methods, and communication protocols must all be carefully considered in order to secure these interactions. To create uniform security standards and best practices, stakeholders must work together at the ecosystem level. Policymakers, network operators, software developers, and device manufacturers are all included in this. Together, they can build an IoT ecosystem that is more robust and safe. Another crucial component of IoT security is data governance. For the collection, storing, and processing of data produced by IoT devices, organizations must set up explicit policies and processes. This entails putting data anonymization and pseudonymization strategies into practice, getting user consent before collecting data, and adhering to pertinent data protection laws.

IoT security also depends on user awareness and education in addition to these technical precautions. Users must take precautions to protect themselves, such as using strong passwords, updating software, and exercising caution when disclosing personal information online, and be aware of the possible threats connected devices may pose. Although the IoT presents many difficulties, they are not insurmountable. We can maximize the advantages of modern technology while reducing the hazards by adopting a proactive and all-encompassing approach to security. All parties involved—device manufacturers, software developers, network operators, legislators, and users—must work together to accomplish this [1].

3.1.1 The ERATOSTHENES Project

Named after the famous Greek researcher, the ERATOSTHENES project seeks to address the complex security issues affecting the Internet of Things (IoT). It manages the full lifespan of IoT networks and focuses on a holistic approach to security. This ambitious project is part of the European Commission's intelligent security and privacy management program and was given 6 million in funding. ERATOSTHENES focuses on solutions for digital identification and distributed trust management in these intricate networks. Under the coordination of INLECOM INNOVATION in Greece, a broad group of 14 partners from 8 different countries work together on this project. The project begun in October 2021 and will be completed on March 2025. ERATOSTHENES recognizes a number of significant security obstacles impeding the development of an IoT environment that is truly secure.

First of all, it is very challenging to build trust and keep a clear image of the overall security position due to the vast diversity of devices and providers involved in the Internet of Things. The development of a cohesive and safe workplace is hampered by the frequently inadequate effectiveness of current trust-enforcement techniques and standards. Second, a lot of Internet of Things devices don't have frequent firmware updates or security patches installed. They become easy targets for attackers as a result of being exposed to known vulnerabilities and exploits. Thirdly, current procedures for safeguarding the privacy of user and device data frequently lack transparency. Users are frequently kept in the dark about the handling of their data.

Significant challenges are also created by a lack of proper security training and the adoption of security measures for both devices and people. Simply put, a lot of users are unaware of the security risks associated with using linked devices. Lastly, inadequate information exchange with cyberattack response teams, such Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs), impedes quick reaction and security threat mitigation. ERATOSTHENES is creating a unique Trust and Identity Management Framework especially for IoT devices in order to address these issues. This structure functions independently of a central authority and is dispersed throughout the network. It is more robust and less vulnerable to single points of failure because of its dispersed approach [2].

The following fundamental ideas guided the design of the framework:

- **Automation**: It reduces the human strain of security management by streamlining procedures for greater efficiency.
- **Auditability**: It facilitates security audits and ensures accountability by enabling transparent tracking and verification of actions.
- **Privacy**: It gives people more control over how their information is utilized and prioritizes their data privacy.

This framework seeks to strengthen trust, protect identities, and improve the overall resilience of the IoT ecosystem by efficiently managing the lifecycle of IoT devices, from initial deployment to decommissioning. Crucially, the framework will be constructed in accordance with pertinent laws, including the Cybersecurity Act, GDPR, and the NIS Directive, guaranteeing that it satisfies moral and legal requirements for data security and protection.

3.1.2 Challenges and Opportunities

Many IoT devices, such basic sensors or smart lightbulbs, are made with little memory and processing capability. Because of this, it is challenging to apply strong

security measures, such as robust encryption, without compromising their efficiency or functionality. Similar to attempting to place a large security door on a tiny garden shed, it may not be feasible or even feasible. Additionally, some IoT devices have out-of-date software or no built-in security safeguards, leaving them vulnerable to manipulation, data breaches, and illegal access. Imagine someone accessing your security camera feed to snoop on you or breaking into your smart thermostat and turning up the heat.

Another level of complication is introduced by the IoT ecosystem's fragmented structure. Because of the wide variety of platforms, communication protocols, and devices, it is challenging to create uniform security requirements. The components may not fit together correctly, much like when you try to assemble a puzzle with pieces from various sets. It is difficult to guarantee security and compatibility throughout the IoT ecosystem due to this lack of standards. Lax restrictions don't always help, and some manufacturers regrettably put new features and usefulness ahead of security. Users' privacy is jeopardized and they become open to attacks.

In addition to these fundamental difficulties, there are a number of other important problems that must be resolved in order to secure IoT networks and devices. Numerous devices can be taken over by hackers, who can then use them to launch botnet attacks, which are large-scale attacks. These assaults have the potential to destroy vital infrastructure, steal data, and interfere with internet services. Concerns over the usage and security of the personal data collected by numerous IoT devices, including location data, browsing history, and health information, have been raised. This data may be intercepted, misused, or sold to third parties without your permission if appropriate security measures are not in place. For data transferred between devices to be protected, secure communication routes are necessary. Imagine your voice commands being sent over the internet by your smart speaker, unencrypted, so that anyone might listen in. To maintain confidentiality and stop unwanted access to private data, strong encryption is essential. To confirm the identification of users and devices, authentication procedures are required. This guarantees that only authorized individuals may operate your devices and stops unwanted access. Imagine someone breaking into your house without your knowing by using your smart lock.

It is essential to manage who can access and use IoT devices. To guarantee that users have control over their data and devices, this involves putting user consent procedures and access control policies into place. Security may also be jeopardized by flaws in the production and delivery procedures. Consider a malevolent actor tampering with devices before they are delivered to customers, introducing malware or backdoors that could be used later. Hackers can easily crack the weak encryption used by some devices. In addition to endangering your data, this enables hackers to intercept and alter device-to-device connections. It can be exceedingly difficult

to maintain security over a wide network of different devices. To efficiently monitor and regulate access, identify threats, and handle incidents, centralized security management technologies and procedures are needed. The low resources of many IoT devices limit their capacity to identify intrusions. Because of this, they are susceptible to complex attacks that get beyond established defenses. Customers find it challenging to select secure equipment due to the absence of defined security testing and certification procedures. Customers are now responsible for researching and comprehending the security features of any device they buy, which can be a difficult undertaking. Most concerning of all is the possibility that compromised IoT devices may be exploited as entry points to assault entire networks, endangering everything. When it comes to vital infrastructure, such as power grids or healthcare systems, this is particularly troubling. Strong security measures are vitally necessary in these locations to avoid possibly devastating outcomes [3].

3.1.2.1 The Heterogeneous Landscape of IoT Security Challenges

The way we live, work, and engage with the world is being revolutionized by the Internet of Things (IoT), which is creating a complex web of interconnected devices. However, the cost of this interconnection is a complicated security environment that is always growing and changing. Securing this digital frontier is extremely difficult because to the wide variety of devices, specs, and suppliers that make up the IoT ecosystem. Consider a busy metropolis with a wide variety of structures, each with its own distinct architecture, security measures, and occupants. This is akin to the IoT landscape, where billions of devices with varying functionalities and security postures coexist. Because of this heterogeneity, it is quite challenging to fully comprehend the security threats that exist in an IoT network. It's similar to attempting to judge a city's level of security based on a few isolated buildings. The IoT ecosystem's wide range of devices are produced by numerous manufacturers and sellers, each with unique design principles, security procedures, and update schedules. This lack of standardization and coordination creates a fragmented security landscape where establishing trust becomes a significant hurdle. How can you be certain that a linked car from one manufacturer complies with the same security regulations as a smart refrigerator from another? The quick development of the Internet of Things frequently outpaces the capabilities of current trust protocols and standards. Many devices are installed with out-of-date firmware or software, which leaves them vulnerable to attacks. It's similar to having a city full of structures with antiquated security, which makes them prime targets for burglars.

Furthermore, the security threats are increased when these devices are not properly maintained and controlled. Many IoT devices are placed in remote areas or in settings where it is not feasible to perform routine security audits and updates. This exposes them to possible threats and compromises, such as leaving a building's doors

open and unattended. These security problems may have far-reaching effects. IoT devices that have been compromised may be used as springboards for assaults on other networks or devices, the theft of private information, or even the disruption of vital infrastructure. Consider a hacker gaining access to a hospital's network via a weak medical equipment or taking over a traffic light network to wreak havoc. A multi-layered strategy is essential to navigating this dangerous terrain. Manufacturers of devices must put security first while designing and developing their products, adding strong security features and patching vulnerabilities on a regular basis. To safeguard their infrastructure and keep an eye out for questionable activities, network operators must put robust security measures in place. Additionally, users must be aware of the security threats connected to IoT devices and take precautions to keep themselves safe, like creating strong passwords, updating software, and sharing data with others.

3.1.2.2 Identity Management and Training Gaps

When it comes to identity management, the Internet of Things (IoT) poses a special difficulty. The Internet of Things is a huge network of devices, each with its own distinct identity and potential security flaws, in contrast to traditional computer networks where users are the main focus. This brings up important issues regarding the management and security of these identities as well as the protection of user and device privacy. Transparency is frequently lacking in current IoT identity management procedures. Users might not be aware of how their connected devices are gathering, storing, and using their data. In a similar vein, a network's authorization and authentication procedures could be inadequately thought out or executed. This lack of openness damages confidence and makes it challenging to hold people accountable in the event of security breaches.

Imagine living in a smart house with numerous linked devices that are all gathering information about your daily activities and habits. Are you aware of who has access to this data, where it is going, and how it is being used? Users are unaware of the security and privacy implications of their connected devices if identity management procedures are unclear and opaque. The absence of proper security procedures and training for both users and devices exacerbates this problem. Many consumers might not take the required safety precautions because they are ignorant of the security threats connected to IoT devices. Similar to this, a lot of devices are deployed with default settings or lack fundamental security protections, making them open to assaults. Furthermore, a lack of defined protocols and communication channels frequently hinders the efficacy of information sharing with incident response teams, such as Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). This makes it more difficult for everyone to work together to quickly resolve security threats and vulnerabilities. It is comparable

to a neighborhood watch in which nobody is aware of how to call the police in an emergency. Reacting to security events and lessening their effects require efficient information exchange.

A thorough strategy to identity management and security training is required to address these issues. This entails creating transparent and unambiguous identity management procedures that inform users about the collection and use of their data and enable safe, transparent authentication and authorization of devices. In order to educate consumers about the security threats connected with IoT devices and how to protect themselves, it is also necessary to provide them with thorough security training. It is crucial to put strong security standards in place for devices, making sure they have solid security features and are updated frequently to fix vulnerabilities. Lastly, timely information exchange regarding security risks and vulnerabilities would be made possible by the establishment of efficient communication channels with incident response teams. By addressing these challenges, we can create a more secure and trustworthy IoT ecosystem where users can confidently embrace the benefits of connected devices without compromising their privacy or security [4].

3.1.2.3 Blockchain

Blockchain technology provides a glimmer of light within the complicated security environment that the Internet of Things (IoT) presents. Think of blockchain as a digital ledger that is spread over several computers and records and verifies each transaction. Blockchain is a potent tool for boosting security in the IoT ecosystem because of its decentralized and impenetrable nature, which makes it extremely impossible for anyone to change or manipulate the data.

The capacity of blockchain to handle identities and build trust in the Internet of Things is one of its main advantages. On the blockchain, each device and user may have a distinct, verified identity, making authorization and authentication considerably simpler. This stops harmful activity and unauthorized access by limiting network and data access to trustworthy devices and people. Consider it your IoT devices' digital passport system. Every device has a distinct "passport" that is kept on the blockchain, confirming its identification and enabling safe communication with other users and devices. This lowers the possibility of single points of failure and does away with the requirement for a central authority to control IDs. Blockchain can also make it easier for devices to communicate securely with one another. It guarantees that only authorized parties can access and decode data by encrypting and verifying it within the blockchain itself. In the Internet of Things, where sensitive data is continuously transferred between devices, this is essential. Consider a factory with a network of sensors that communicate with one another to keep an eye on and manage the production process. By prohibiting hostile interference and

data modification, blockchain technology can guarantee that this connection is safe and impenetrable.

Additionally, blockchain can provide firmware update integrity. Attackers are unable to alter or install harmful software because these changes are recorded and validated on the blockchain. Given that many IoT devices are placed in remote areas and might not be readily accessible for manual upgrades, this is especially crucial. Blockchain has the potential to offer decentralized governance, data integrity, and user privacy in the Internet of Things in addition to security. Blockchain can provide people more control over their data and how it is used by facilitating safe and transparent data management.

3.2 The ERATOSTHENES Project Technical Scope

3.2.1 Summary of Outcomes

ERATOSTHENES is creating a new system for managing trust and identities in the Internet of Things. This system is designed to work across an entire network of devices without relying on any central control point. This makes it more resilient and less vulnerable to attacks. The system is automated, which means it can handle many tasks automatically, making it more efficient. It's also designed to be transparent, allowing actions to be tracked and verified. This ensures accountability and helps build trust. Most importantly, the system prioritizes user privacy. It gives users control over their data and ensures their privacy is protected. By effectively managing the entire lifespan of IoT devices, from when they are first connected to when they are retired, this system strengthens trust and security within the network. It also makes the entire system more resilient to attacks and disruptions. Finally, the system is designed to comply with all relevant data protection and cybersecurity regulations, ensuring it meets the highest standards for security and privacy [5–7].

3.2.2 Technical Description of Components

3.2.2.1 Dynamic Trust Management

To build trust within the IoT network, the ERATOSTHENES solution uses a special **"Trust Broker" mechanism.** This mechanism has several components that work together to ensure security. Initially, a "trust score" is determined for every device. Similar to a credit score, this number indicates a device's level of reliability. The "trust manager," which also maintains track of device relationships and communicates trust data to the network, performs this computation. It securely stores and distributes this data using a technique known as Hyperledger Fabric. Consider the trust manager as a central repository that collects data about every device and

establishes its level of trustworthiness. Other components of the system are then informed of this information. The "**MQTT Broker**," which serves as a filter for all events pertaining to trust, comes next. It also records the devices that are currently in use and any messages that they may have overlooked.

Think of this broker as a receptionist who manages all trust-related correspondence, both inbound and outbound. It ensures that no crucial signals are missed and that only pertinent information is conveyed. The "**Threat Modelling & Risk Assessment (TMRA)**" module is another crucial component of this process. To find possible risks and determine a risk score for every device, this module builds a virtual model of the system. Additionally, it has the ability to dynamically modify these scores in response to fresh data or system modifications. Consider this module as a security guard that continuously checks the system for possible threats and evaluates each device's risk level.

Last but not least is the "**MUD manager**," which decodes data regarding the device's access requirements from the manufacturer. After that, it generates access control lists (ACLs), which function similarly to digital "permission slips" and specify what each network device is allowed to access. Consider the MUD manager as a permissions administrator who controls which network resources are accessible to which devices. The Trust Broker mechanism offers a thorough method of controlling security and trust in the Internet of Things network by integrating these elements. It guarantees secure communication between trusted devices and restricts access to the network.

The **Trust Agent Deployer** (TAD) is a unique tool used by the **Trust Manager & Broker** (TMB). Consider the TAD as a manager for "trust agents"—small software components that aid in maintaining network device security. The TAD oversees these agents' whole lifecycle, not just their installation. This entails updating them, repairing them in the event that they malfunction, and even swapping them out for more recent, secure models. The TAD continuously collects data from the devices it oversees in order to accomplish this efficiently. It uses this data to make informed decisions about how to control the software on every device. It is comparable to a gardener who continuously checks on their plants to ensure they are receiving enough nutrients, sunlight, and water. The TAD simultaneously maintains a list of every trust agent that is available. This enables it to select the appropriate agent for every device according to its unique requirements and attributes. Each item is paired with the ideal trust agent to ensure its safety, much like a dating service. When trust agents malfunction or are compromised, the TAD is also essential in repairing them. It can either replace them completely with a new, updated version or return them to a safe state. It's like a mechanic who can repair a damaged car part or replace it with a brand new one. To put it briefly, the TAD acts as a committed protector for the trust agents, making sure they are always operating properly and

safeguarding the devices in the network. This helps maintain the overall security and trustworthiness of the IoT ecosystem.

Consider certain IoT devices to have an integrated, safe vault. This "vault," known as a **Trusted Execution Environment** (TEE), guards against unauthorized parties accessing or altering crucial software components. This safe vault is used by several components of the ERATOSTHENES system. This secured environment, for instance, is where the "Advanced Data Protector," which protects sensitive data, operates. This vault is also where components of the system that handle trust and digital identities function. The TEE improves the system's overall security by offering this safe area. It serves as a fortress, preventing attacks on vital operations and guaranteeing their secure operation. Although trust, identities, and data protection are not directly managed by the TEE, these tasks are indirectly supported by it by offering a safe environment in which its essential components operate. It ensures the stability and security of the entire building, acting as a foundation.

3.2.2.2 Advanced Identity Management

ERATOSTHENES puts users in control of their own digital identities and data. It does this through a system called "**Self-Sovereign Identity**" (SSI), which you can think of as a digital ID card that you own and control. This SSI system has two main parts:

1. **SSI Management:** This part lives on a central server and helps create and manage user identities. It works with a special tool called the "Ledger uSelf Broker" to do this. Imagine this as the office where you would go to get your ID card issued.
2. **SSI Agent:** This part lives directly on your IoT device. It allows your device to use its digital ID card to interact with the system securely. Think of this as the card reader that checks your ID card.

The **Trusted Execution Environment** (TEE), a secure section of your device, is where the SSI Agent operates to further increase security. This guarantees that all of your personal data is safe and available only in this restricted area. Keeping your ID card kept in a safe is analogous to that. Additionally, the TEE employs cutting-edge data protection mechanisms to provide an additional degree of security, guaranteeing that your private data is only accessible within the safe hardware environment. It is comparable to having a security guard guard your safe.

ERATOSTHENES employs cutting-edge technologies to safeguard your identity and private data. One of these devices functions similarly to a unique ID card, revealing only the information that is strictly required and concealing the rest. A method known as "**privacy-preserving Attribute-Based Credentials**" (p-ABC) is used to do this. Consider having to provide proof of age in order to attend a movie

theater. You can use this unique ID card to merely demonstrate that you are of legal age without disclosing your name, address, or other personal information, as opposed to presenting your full driver's license with all of your personal information. Additionally, the system makes use of a technology known as "**Distributed Ledger Technology**" (DLT), which functions similarly to an open public record book. Important data, including as public keys and credential types, are kept in this record book, but your personal information is not. ERATOSTHENES employs a unique module that enables safe authentication without disclosing extraneous information in order to further improve privacy. It functions similarly to a secret code that verifies your identification without disclosing any personal information.

Privacy is safeguarded during the identity management process thanks to the cooperation of this module with other system components. Another important function is played by the public record book (DLT), which offers transparent and safe means of exchanging information without jeopardizing your privacy. ERATOSTHENES also employs other instruments to bolster security. It's similar to having several levels of security, such as a distinct fingerprint for every device and a unique system to safeguard private data. Combining these cutting-edge methods, ERATOSTHENES develops an identity management system that protects your personal information in the Internet of Things and provides you control over your data. Identity information security is a top priority for ERATOSTHENES, particularly when it comes to retrieving such data from your Internet of Things devices. To protect this data, it makes use of a unique part known as the **Advanced Data Protector** (ADP).

Think of the ADP as a secure storage container on your device, specifically designed to protect your identity data. This container utilizes your device's built-in security features to ensure your information is encrypted and stored safely. This secure storage is important for backing up your identity data to a separate server. However, because the ADP is so focused on security, it makes it a bit tricky to simply export your information. To make backup and recovery easier, ERATOSTHENES is enhancing the ADP. The goal is to find a balance between keeping your data secure and making it accessible when you need to recover it.

Unique and unpredictable keys are essential for strong security, and ERATOSTHENES employs a new method known as PUFs (Physical Unclonable Functions) to accomplish this. PUFs provide unique and unclonable keys by exploiting small, random physical variances within each device, such as variations in the material it is built of. It's similar to how every device has a distinct fingerprint. The IoT devices themselves are referred to as "low-level" entities in the ERATOSTHENES system, while the central components that oversee the system are referred to as "high-level" entities. Imagine it like employees and managers in a business.

The clients (devices) can only interact with specific managers (system components) after they've been registered and authorized. This registration process happens during manufacturing to ensure the devices are secure from the start. Each device uses special applications to connect securely with the system. These applications are like secure communication channels that ensure only authorized devices can connect. They are also tailored to each specific device, preventing counterfeits and duplicates. For highly sensitive devices, these applications can even self-destruct if they detect any tampering, adding an extra layer of protection. It's like a secret agent destroying their communication device if it falls into the wrong hands. The system can also be combined with other security measures to protect against various attacks, like someone trying to inject malicious code or manipulate the device's software. The flexible design of ERATOSTHENES allows for customized security applications for each device. It can even be fully automated, making it work like a security service that constantly protects the system. In essence, ERATOSTHENES leverages PUFs and other security measures to create a robust and adaptable security ecosystem for the IoT. This ensures that devices are authenticated, communication is secure, and sensitive data is protected from unauthorized access and tampering.

3.2.2.3 Lifecycle Consideration of IoT Devices

"**Distributed Ledger Technology**" (DLT), a unique technology used by ERATOSTHENES, functions similarly to a shared and secure digital ledger. This blockchain-based technology facilitates the seamless operation of many system components. Consider this digital record book as a primary repository for sharing and storing vital information. This includes details regarding cyberthreats, trust scores, and device IDs. This shared record book is used by various system components, such as the Trust Manager and Identity Manager, to access and maintain their data. Because Hyperledger Fabric provides the necessary security, flexibility, and storage capacity, ERATOSTHENES employs it expressly for this purpose.

Different portions, referred to as "channels," within this shared record book correspond to various system components. Additionally, there is a dedicated channel that facilitates information exchange between various regions. It's similar to having safe communication and information sharing amongst various departments inside a business. Additionally, ERATOSTHENES makes use of special agents who exchange data regarding cyberthreats. By gathering information from many sources and disseminating it to other areas of the system, these agents serve as messengers.

Consider these agents as interconnected security personnel who work together to maintain the system's security. To enable other guards to respond, they collect information about possible threats and disseminate it to them. These agents operate in two ways: they gather data from external sources and from within the system,

such as an intrusion detection system. Other components of the system are then given access to this data in order to enhance their security protocols.

3.2.2.4 Intrusion Detection for IoT

Additionally, this security system employs a method known as "federated learning" to detect attacks on network edge devices. Consider a system of security cameras that communicate with one another to provide a comprehensive view of the situation. As a result, the system is better equipped to learn and adjust to emerging threats. In order to keep the entire community secure, everyone shares their observations, just as in a neighborhood watch.

These elements work together to form a potent threat analysis and detection system. They make it simple to monitor and react to security occurrences by offering unified warnings via a common interface. Security staff can swiftly evaluate and react to any situation thanks to a central security hub that gets notifications from all of the network's cameras and sensors.

Through a communication link, the system also exchanges data with other components of the ERATOSTHENES security system. This makes it possible to react to any risks that are identified in a coordinated manner. It functions similarly to a direct channel of communication between the security cameras, the central hub, and the ground-based security staff, guaranteeing that everyone is aware of any security breaches and can cooperate to resolve them.

3.3 Results Validation and Use Cases

The deployment of all technological components (as previously mentioned) into three industrial use cases is part of the robust integration and deployment stage that the various technologies of the ERATOSTHENES security stack are presently undergoing. These pilots operate as hands-on tests to confirm the ERATOSTHENES solution's operational and technical efficacy. Below is a discussion of the three pilots:

V2X Communication Security: Vehicle-to-Everything (V2X) communication in a regulated setting is the main focus of the first pilot. It looks at two important use cases: standardized software update procedures for connected cars and cybersecurity protocols. The pilot will illustrate the difficulties in establishing confidence in V2X communication, especially while software updates are being implemented. Next, it will demonstrate how ERATOSTHENES technology can identify malevolent actors, detect network anomalies, and keep systems resilient to cyberattacks. The project's capacity to resolve security issues and guarantee the dependability of V2X communication infrastructure is highlighted by this trial.

Remote Patient Monitoring: A remote patient monitoring system for long-term conditions like COPD or diabetes is the focus of the second trial. By enabling patients to control their diseases and get care from home, this method encourages self-care and lowers the number of hospital visits. The Personal Health Gateway, which is situated in each patient's home, is a crucial part of this study. Data from a variety of medical sensors is gathered by this gateway and safely sent to cloud-based services for monitoring and analysis.

Disposable IDs for Industrial Network Security: The third pilot, which aims to secure connected devices, data transfer, and analytics in dynamic and heterogeneous industrial networks, is focused on Industry 4.0 applications. This project, called "Industry 4.0 (disposable IDs)," uses PUFs and DLT in tandem to create secure, one-of-a-kind disposable IDs for every device. By serving as unique device fingerprints, these IDs allow for safe network identification. By guaranteeing strong device identification and improving data security and reliability, this novel method fortifies the industrial network's overall security architecture.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101020416. The authors acknowledge the research outcomes of this publication belonging to the ERATOSTHENES (101020416) project consortium.

References

[1] K. Loupos, B. Caglayan, A. Papageorgiou, B. Starynkevitch, F. Vedrine, C. Skoufis, S. Christofi, B. Karakostas, A. Mygiakis, G. Theofilis, A. Chiappetta, H. Avgoustidis, George Boulougouris – COGNITION ENABLED IOT PLATFORM FOR INDUSTRIAL IOT SAFETY, SECURITY AND PRIVACY – THE CHARIOT PROJECT, IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), IEEE XPLORE, 11–13 September 2019, Limassol, Cyprus, DOI: 10.1109/CAMAD.2019.8858488.

[2] K. Loupos, A. Papageorgiou, A. Mygiakis, B. Caglayan, B. Karakostas, T. Krousarlis, F. Vedrine, C. Skoufis, S. Christofi, G. Theofilis, H. Avgoustidis, G. Boulougouris, A. Battaglia, M. Villiani – COGNITIVE PLATFORM FOR INDUSTRIAL IOT SYSTEM SECURITY, SAFETY AND PRIVACY,

Embedded World 2020 Conference and Exhibition, 25–27 Feb. 2020, Nuremberg, Germany.

[3] K. Loupos – INTEGRATED SOLUTION FOR PRIVACY AND SECURITY OF IOT DEVICES IN CRITICAL INFRASTRUCTURES, Critical Infrastructure Protection and Resilience Europe (CIPRE 2020), 6–8 Oct. 2020, Bucharest, Romania.

[4] K. Loupos, C. Kalogirou, H. Niavis, A. F. Skarmeta, E. Torroglosa-Garcia, A. Palomares, H. Song, P.E. Brun, F. Giampaolo, D. V. Landuyt, S. Michiels, B. Podgorelec, C. Xenakis, M. Bampatsikos, K. Krilakis – A HOLISTIC APPROACH FOR IOT NETWORKS' IDENTITY AND TRUST MANAGEMENT – THE ERATOSTHENES PROJECT, 4th Workshop on Internet of Things Security and Privacy (WISP), Global IoT Summit 2022, Dublin, June 2022.

[5] O. Vermesan, M. Coppola, M. Diaz Nava, A. Capra, G. Kornaros, R. Bahr, E. Darmois, M. Serrano, P. Guillemin, K. Loupos, L. Karagiannidis, S. McGrath – New Waves of IoT Technologies Research – TRANSCENDING INTELLIGENCE AND SENSES AT THE EDGE TO CREATE MULTI EXPERIENCE ENVIRONMENTS, Internet of Things – The Call of the Edge – Everything Intelligent Everywhere, River Publishers, DK, October 2020, ISBN: 9788770221962, e-ISBN – 9788770221962.

[6] K. Loupos, C. Kalogirou, H. Niavis, A. F. Skarmeta, E. Torroglosa-Garcia, A. Palomares, H. Song, P.E. Brun, F. Giampaolo, D. V. Landuyt, S. Michiels, B. Podgorelec, C. Xenakis, M. Bampatsikos, K. Krilakis – A HOLISTIC APPROACH FOR IOT NETWORKS' IDENTITY AND TRUST MANAGEMENT – THE ERATOSTHENES PROJECT, Lecture Notes in Computer Science book series (LNCS,volume 13533), DOI: 10.1007/978-3-031-20936-9_27.

[7] A. M. Frutos, J. G. Rodríguez, A. Skarmeta, K. Loupos, S. Vavilis, F. Michalopoulos – IDENTITY AND TRUST ARCHITECTURE FOR DEVICE LIFECYCLE MANAGEMENT, Future Generation Computer Systems, Volume 162, January 2025, Science Direct, Elsevier