# Review of Security and Privacy for the Internet of Medical Things (IoMT)

## Resolving the protection concerns for the novel circular economy bioinformatics

George Hatzivasilis, Othonas Soultatos, Sotiris Ioannidis
Institute of Computer Science
Foundation for Research and Technology – Hellas
Heraklion, Crete, Greece
{hatzivas, sultatos, sotiris}@ics.forth.gr

Christos Verikoukis
Telecommunications Technological Center of Catalonia (CTTC)
Barcelona, Spain
cveri@cttc.es

Giorgos Demetriou
Ecole des Ponts Business School
Paris, France
g.demetriou@pontsbschool.com

Christos Iraklis Tsatsoulis
Nodalpoint Systems
Athens, Greece
ctsats@nodalpoint.com

***Abstract*—Day-by-day modern circular economy (CE) models gain ground and penetrate the traditional business sectors. The Internet of Medical Things (IoMT) is the main enabler for this interplay of CE with healthcare. Novel services, like remote sensing, assisting of elder people, and e-visit, enhance the people's health and convenience, while reducing the per-patient cost for the medical institutions. However, the rise of mobile, wearable, and telemedicine solutions means that security can no longer be examined within the neat, physical walls as it was considered before. The problem for a healthcare system further increases as the Bring Your Own Device (BYOD) reality, affects the way that the health services are accommodated nowadays. Both patients and healthcare staff utilize their personal devices (e.g. smart phones or tablets) in order to access, deliver, and process medical data. As the IoMT is materialized and the underlying devices maintain so valuable data, they become a popular target for ransomware and other attacks. In the CE case, the problem is further emerging as several of these assets can be used over-and-over by many actuators. However, medical users and vendors are less aware of the underlying vulnerabilities and spend less on the IoMT security. Nevertheless, the risk from exploiting vulnerabilities can be drastically reduced when the known and relevant controls are placed. This paper presents an overview of the core security and privacy controls that must be deployed in modern IoMT settings in order to safeguard the involved users and stakeholders. The overall approach can be considered as a best-practices guide towards the safe implementation of IoMT systems, featuring CE.**

***Keywords*— *Bioinformatics; e-health; healthcare infrastructure; IoMT; IoT; security; privacy; BYOD; circular economy.***

## I. INTRODUCTION

According to Gartner, the IoT-enabled devices will exceed the $20.4bn by 2020 [1]. These high volumes of interconnected devices constitute an increasingly attractive target for attackers. After the demonstration of several IoT vulnerabilities by researchers and their successful exploitation by attackers (e.g. smart vehicles [2] and smart lights [3]), IoT security has now become an issue of high concern for the main Informatics stakeholders. The figure below depicts the forecasts for the cybersecurity market until 2020, as evaluated by the IoT security report of the Business Insider [4].

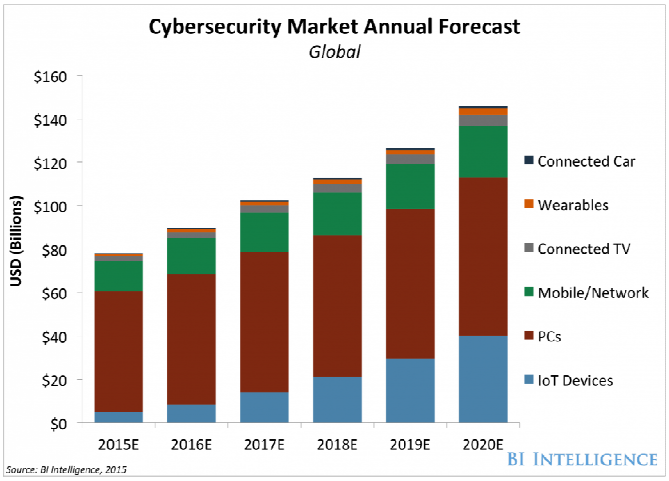


Fig. 1. Cybersecurity market annual forecasts by Business Insider.

Health and health care are going through a total digitalization as multiple intersecting platforms evolve to form a novel operational foundation for health and health care [5], [6]. Transformation and changes occur at a pace determined by stewardship that fosters alignment of technology, science, and culture in support of a continuously changing distributed health system.

Henceforth, CE initiatives start gaining ground in the healthcare sector. The combination of CE and the Internet of Medical Things (IoMT) provides accessibility, low per-patient

cost, fast per patient implementation, and improved efficiency ([7], [8]). Three main application settings are considered in general:

1. **Hospital:** remote diagnostics, predictive maintenance, performance upgrades, recycling and waste management (for general products and specific healthcare assets that contain noxious chemicals)
2. **Home:** decrease the frequent visits to the doctor for patients suffering from chronic diseases, remote monitoring for specific patient types (i.e. diabetics, heart patients, etc.) and automatically alerting, assist of elder or disable persons in order to reside in their home without requiring the 24-hour assistance of nursing personnel.
3. **Body sensors:** monitor the user's health, examine behavior modification, provide freedom while inspecting their health state, and promote best health practices to improve life.

On the other hand several challenges are raising, including high infrastructure cost, strain on existing networks, Bring Your Own Device (BYOD) policies, lack of standardization, regulatory uncertainties, and of course, security and privacy issues.

The rest paper is organized as: Section 2 mentions the related work in the field of IoT security and privacy. Section 3 details the main solutions for accomplishing end-to-end (E2E) security from the device-end to the backend infrastructure. Section 4 presents the protection mechanisms that retain privacy and/or anonymity. Finally, Section 5 concludes this work.

## II. Related Work

Several surveys have been presented in the last years regarding IoT security and privacy. Security is the main concern ([9], [10]) with privacy protection becoming also significant ([9], [11]). BYOD is another important factor [12] that must be tackled towards the protection of modern CE and e-health scenarios.

Digital technologies (i.e. big data, Internet of Things (IoT), personal health record (PHR), risk assessment, high performance computing, and cloud) offer new opportunities to transform healthcare systems. It is expected that connected medical devices, the so called the IoTM, have the potential to increase patient safety and efficiency into healthcare [7], [8].

However, cyber-security has become a strategic issue for healthcare facilities [13]. Branded as easy targets with obsolete defenses and poor information systems and information technologies organization, hackers do not hesitate to attack them in order to get any profit they can: paralyzing the systems using ransomware, hacking into hospitals' databases and selling patients' information to the highest bidder, threatening to release private information, cutting off their power supply, etc.

Moreover, IoMT could further increase the attack surface of modern e-health. Recently, Johnson and Johnson announced that its digital insulin pumps are vulnerable to cyberattacks [14]. The problem was stated by an independent security expert that analyzed the communication interfaces of the devices, after using it as patient for some time. While the possibility of exploiting the vulnerability is low, relevant products constitute a growing and influential trend in modern healthcare technology (e.g. pacemakers and defibrillators). Such equipment represents a new type of risk. Thus, risk analysis is essential for a healthcare system in order to obtain a clearer view regarding the provided security and privacy properties.

Thus, security and privacy concerns represent a strong threat to participate in, and therefore the success of, the sociotechnical health ecosystem. Today, it is evident that the need for security to comply with all current requirements and regulations and retain an ability to evolve is a necessity to meet future needs, legal requirements and technical challenges.

This paper surveys the state-of-the-art solutions in the field. It acts as a practical guide for developing modern IoT and IoMT applications, taking also into account the inheriting aspects of CE in the healthcare domain. The review covers the protection mechanisms that must be acquired from the device to the cloud ends (E2E), and from the processing, transmission, and storing of data to the reuse or disposal of the involved equipment.

## III. Security

Several methodologies and standards are established in order to assist the secure development of a system. Popular and widely-used techniques for specifying security include the Common Criteria Evaluation Methodology (CEM) [15] and the Open Source Security Testing Methodology Manual [16].

The three main cyber security principles for any type of security control are referred to as the **Confidentiality, Integrity, Availability (CIA)** principles. Confidentiality is the property where information is not disclosed to users, processes, or devices unless they have been authorized to access the information. Integrity is the property whereby information has not been modified or destroyed in an unauthorized manner. Availability is the property of being accessible. Each of these three principles involve relevant protection mechanisms, which are described in the following table, as they are derived from the abovementioned standards and related research efforts [17].

Surveys regarding security, architecture, and enabling technologies in the IoT domain are presented in ([18], [19], [20]), while a taxonomy of the related security attacks is proposed in [21]. The guidelines for secure IoT development, as also suggested by large computer and software vendors (e.g., Microsoft, IBM, Siemens, Gemalto, etc.), include the following three security areas:

- **Device security:** mechanisms and techniques for protecting the device itself, once it is deployed in the field.
- **Connectivity security:** mechanisms and techniques for guarantying that the transmitted data between the IoT devices and the IoT Hub/Gateway is confidential and tamper-proof.
- **Cloud security:** mechanisms and techniques for safeguarding data while it is transmitted to, and is stored in the cloud.

Popular IoT platforms, like the Microsoft Azure IoT suite [22] and the IBM Watson IoT Platform [23], tackle these issues and provide the mainstream security solutions. In the following, we provide an overview of state-of-the-art IoT security grouped in under the three main areas listed above.

### A. Device Security

Device security implements the different aspects for authenticating a device in an IoT application. Two main components are required for this purpose:

- A *unique identity key* or *security token* for each device. The device utilizes this key in order to authenticate and communicate with the IoT gateway.
- An *on-device X.509 certificate* and *private key* for authenticating the device to the IoT gateway. The authentication procedure must guarantee that this private key is not known outside the device at any time, thus achieving a higher level of protection.

In typical device operation, the device token provides authentication for each transaction that is made by the device to the IoT gateway. Thus, the symmetric key is associated to each transaction. The X.509-based procedure enables the authentication of the device at the physical layer during the establishment of the TLS connection (connectivity security). The certificate contains information that is related to the devices, like its ID, and other organizational details.

The security token can be also used alone, without requiring the X.509 authentication, but in a less secure setting. The choice between the two methods is determined by the availability of the adequate resources on the device end (e.g. store the private key securely) and the level of authentication security that is needed by the application.

### B. Connectivity Security

Connecting IoT devices over the Internet poses threats for data confidentiality and integrity. It is, thus, important to ensure that all the transmitted data between the devices and IoT gateways and from there to the cloud is encrypted.

TABLE I
SECURITY ASPECTS AND PROTECTION MECHANISMS

| Aspect | Protection mechanism | Description |
|---|---|---|
| Confidentiality | Confidentiality | Guarantees that a processed asset is not becoming known outside the interacting entities |
| | Authentication | Challenges credentials on the basis of identification and authorization |
| | Resilience | Preserves protection in case of failure |
| Integrity | Integrity | Guarantees that the interacting entities know when an asset has been changed |
| | Subjugation | Guarantees that transactions occur based on a defined process, removing freedom of choice and liability in the case of disclosure |
| | Nonrepudiation | Prevents the interacting entities from denying their role in an interaction |
| Availability | Continuity | Preserves interactivity in the case of failure |
| | Alarm | Informs that an interaction is happening or has happened |
| | Indemnification | Includes a contract between the asset owner and the interacting entity. It may also involve warnings as a precursor of legal action and public legislative protection |

The IoT gateway utilizes the security tokens to authenticate devices and services. The process is managed automatically by the IoT platforms. The seamless communication is supported by relevant protocols, such as the Advanced Message Queuing Protocol (AMQP), MQTT, and HTTP [24], and is safeguarded by the security mechanisms that are implemented by each one of them. Nevertheless, these underlying solutions process the security tokens in different ways and the correct usage should be inspected in each specific case. This is a technical issue and concerns the correct mapping of the token-related information to each protocol's data format. For example, the MQTT connection request utilizes the device ID in the username and the security token in the password field, while HTTP includes the valid token in the authorization request header. Also, some application settings need the user to generate the security tokens and use them directly. Examples of these scenarios include the direct use of AMQP, MQTT, or HTTP surfaces.

The IoT gateway maintains an identity registry for the secure storage of device identities and security keys. Distinct devices or groups of them can be added to an allow or block list, achieving complete control over device access. The high-level device provisioning includes the following steps:

- Associate an identifier at the physical device (i.e., the device identity and/or X.509 certificate) at the manufacturing or commissioning phases
- Create a relevant entry at the gateway's identity registry
- Securely store the X.509 certificate thumbprint in the registry

On the other hand, the device must also authenticate the

gateway. In the ordinary setting, a root certificate, which is included in the device software development kit SDK, is utilized for authenticating the gateway's credentials. Although the root certificates are long-lived, they can also expire or be revoked. Thus, a secure procedure must be foreseen for updating the root certificate on the device end or, otherwise, the IoT devices may be subsequently unable to connect to the IoT gateway or the cloud services.

Finally, the Internet connection between the devices and the gateway is generally protected by the SSL/TLS 1.2 standards. Old versions of each protocol may also be supported for backward compatibility (i.e., TLS1.1, TLS 1.0).

### *C. Cloud Security*

Cloud computing suffers from a number of security issues that overlooking them may lead to catastrophic consequences. As seen on [25] and [26] the main security vulnerabilities can be categorized as bellow:

- **Shared technologies:** As seen in [27] and [28] an attacker can exploit shared memory technologies to gain access to unauthorized content such as encryption keys.
- **Data breach:** Personal data containing sensitive information such as credit card information can be lost or worse can be leaked.
- **Account/service hijacking**: If login credentials are lost or leaked can lead to attackers gaining access to critical areas of services and could potentially compromise confidentiality, integrity and availability.
- **Denial of Service (DoS):** As seen in [29] cloud infrastructure mechanisms cope with DoS attacks by providing scaling up its resources but this firstly provides the attacker with more resources to achieve his malicious goals and secondly can this type of attack can have monetary impacts.
- **Malicious insiders:** A company's employee can leverage his position to access sensitive information of the hosted services.

As a first line of defence to prevent the physical access attacks is obviously a high level physical security at the data-centres. Furthermore, a scheme using XACML [30] can be used to limit access of employees to decrease the possibility of an insider attack.

To prevent side channel attacks as proposed in [31], KAISER can be used in order to achieve kernel space isolation. Moreover, Intel trusted execution technology provides a trusted way of loading and executing the Virtual Machine Monitor (VMM) or the OS kernel has a serious limitation as described in [32] which is that the attacker can easily bypass it if he has physical access to the servers.

Hashizume et al. [33] use misuse patterns to describe the environment, conditions and sequences of an attack based on co-residence between malicious and legitimate virtual machines. The misuse patterns act as a repository which may then be used by developers for security measures against the attacks. Also, Intrusion Detection Systems (IDS) that monitor and detect malicious activity in a system can be used to prevent intrusions. However due to the high complexity of the cloud a Hybrid Intrusion Detection System can be used [34].

To prevent data breaches and to guarantee data confidentiality and integrity on the channels and so prevent Sniffing and Spoofing Attacks the basic solution is to use an encrypted network protocol that encrypts all the traffic from the source to the destination over the whole trip. SSL and TLS can be used to prevent leakage of sensitive information through communication encryption. Another standard commonly used by CPs is IPsec, a protocol suite for securing IP communications implementing network-level authentication and encryption for each IP packet. Usually these mechanisms protect network traffic to the edge of the cloud network, VPN and its techniques as SSH and IPsec tunnels are used to defend traffic between servers within the cloud network.

### *D. Other Security Modules*

Except from the main devices, networks, and platforms, also other key products can be necessary for a modern IoT ecosystem. These include products related to security protection and solutions for providing tamper resistant in devices including subscriber identification modules (SIM), trusted platform modules (TPM) and hardware security modules (HSM).

Many mobile IoT devices are now equipped with a subscriber identification module (SIM) – an integrated circuit that stores securely the international mobile subscriber identity (IMSI) number and the corresponding key [35]. This information is utilized for the subscriber's identification and authentication. However, the SIM data are hardcoded on the chip and cannot be altered. Thus, when the operator of a device is changed, the SIM card must be replaced with a relevant card containing the credentials of the new user.

The embedded SIM (eSIM) card solution is proposed in the IoT domain in order to facilitate the M2M communication between devices ([36], [37]). The eSIM module is re-programmable, enabling the remote provisioning of the operator subscription. It is, thus, a vital enabler for M2M connections allowing simple and seamless mobile connection of all types of communicating devices. The card comes in different sizes and shapes. In settings, where there is no need to swap cards, the chip is placed within a device and it is kept protected from heat, humidity, or extreme vibrations. Then, the owner updates the settings remotely when the operator changes, enhancing usability and the physical protection of the equipment. This is a fundamental requirement in several application domains, like precision agriculture, intelligent transportation, and industrial deployments ([38], [2]). Popular eSIM vendors include Gemalto [39] and GSMA [40]. The provided interfaces support a mode of operation that is virtually identical with the current SIM personalization procedures of mobile operators. Another class of M2M SIM ([39], [40]) cards safeguards the identities of devices communicating on cellular networks and implements secure authentication and ciphering.

A TPM constitutes the international standard for secure crypto-processors [41]. TPM is a dedicated microcontroller that protects cryptographic keys in hardware. It is placed on the motherboard and, once enabled; it provides full disk encryption and becomes the "root of trust" for the system, offering authentication and integrity to the boot procedure. TPM can lock/seal the hard drives until the system completes an authentication check or a system verification. It also includes a unique RSA key hardcoded on the chip that is utilized for asymmetric cryptography. Moreover, TPM can generate, maintain, and protect other keys which are utilized by cryptographic procedures. TPM is standardized by ISO/IEC 11889 [42].

The HSM also protects and manages digital keys for strong authentication and offers crypto-processing functionality [43]. In contrast to TPM that is embedded on the motherboard, HSMs are removable. HSMs are deployed as plug-in cards or external devices that are attached to the network server or a computing device. High performance modules are connected to the network using TCP/IP. HSMs are certified by international standards, like Common Criteria [15].

## IV. Privacy

Information security controls alone are not enough for modern settings. In the recent years, protection of privacy has gained high attention, especially in e-health applications.

### A. Private Data

In IoMT applications, high volumes of personal data are exchanged by the underlying systems, rising serious concerns regarding privacy and deriving the application of relevant protection controls imperative for the end users. Therefore, several standards (like the ISO/IEC standards 27018 [44] and 29100 [45]) and regulation efforts (such as the General Data Protection Regulation of European Union – Regulation (EC) 2016/679 [46]) are established, trying to tackle these issues.

This type of knowledge that is referred to a person is defined as **Personal Identifiable Information (PII)** [45]. The data may be categorized as personal sensitive, sensitive, and statistical [45], with the first category demanding the highest privacy protection followed by the sensitive data, while statistical data requires moderate protection with such information becoming often publicly known via survey reports.

Moreover, three actuator types are defined, marshalling the ownership of personal data and the related processing rights [45]. The *PII principal/owner* is the person to whom the data is referred to and must have the total control and legal rights over the data. The *PII contracted processor* is the entity (e.g. person or service) that has been granted the explicit agreement of the PII principal for processing his/her personal data for a specific purpose. The processor is restricted and cannot use the data in a way that will trespass the common agreement with the principal. Nevertheless, in order to deliver the required functionality, the processor may need to disclose the PII to a *third party*. The processor has to obtain the explicit consent from the principal, with the corresponding processing terms and access rights also restricting the usage for the third party. For every violation, the contracted processor and the different third parties are accountable to the PII owner.

TABLE II
Privacy Aspects and Protection Mechanisms

| Aspect | Protection mechanism | Description |
|---|---|---|
| Data collection | Consent | Demands the PII owner's freely given, specific, and informed agreement to the processing of the PII. The PII must not be shared or disclosed to a third party without the owner's consent |
| | Opt-in | Includes a policy or process where the PII owner agrees explicitly to the PII's processing, before relevant consent |
| | Fairness | Guarantees that the PII is collected, used, or disclosed for only the appropriate purposes, implementing the GDPR features of collected data minimization and accuracy |
| Data access | Identifiability | Results in identifying the PII owner, directly or indirectly, based on a given set of PII. It should include identifiability, pseudonymization, or anonymity |
| | Notification | Informs the PII owner that his/hers data are being collected |
| | Auditability | Provides adequate means to identify and control the access of PII data |
| | Challenge compliance (accountability) | Guarantees that the PII owner can hold the PII processors accountable for adhering to all privacy controls, supporting the GDPR properties for lawfulness, fairness, and transparency |
| Data usage | Retention | Guarantees that the PII, which is no longer needed, is not maintained, as a precautionary measure towards the minimization of unauthorized collection, disclosure, or use. |
| | Disposal | Includes mechanisms for destroying or disposing of the PII on demand, including and the 'right to be forgotten' of GDPR |
| | Report | Informs that an interaction with PII is happening or has happened |
| | Break or incident response | Manages a breach of PII |

### B. Protection mechanisms

Privacy threats include malicious or non-malicious events that affect the protected PII (e.g. exploitation of connection vulnerabilities for smart home equipment [47] or private data disclosure from wearable fitness tracking devices [48]. The private data must be protected during the transmission and storage operations. The aforementioned security mechanisms on the previous subsections are deployed for this purpose and ensure the CIA principles.

Nonetheless, there are other specific protection mechanisms for preserving privacy that safeguard the private data during the collection, access, and usage procedures. Typically, the PII owner must be always get informed about the collection of his/her personal data, the entities that can gain access to them, and how this information is going to be used.

The general privacy framework and properties are defined in ISO/IEC standards 27018 [44] and 29100 [45], and the General Data Protection Regulation of European Union – Regulation (EC) 2016/679 [46]. The next table summarizes the main privacy properties and the specialized protection mechanisms, as derived by these initiatives [17].

As concerning IoMT devices specific controls can be deployed [49]. The collection of raw data must be minimized along with the overall data volume that is collected or requested by applications (e.g. minimize sampling rate, amount of data, recording duration, different parameters, etc.). The storage of data have to be confined, enforcing also a short retention period. Thus, maintaining information for longer than necessary must be avoided. Edge computing should be promoted in order to process as much data as possible at the filed layer, hiding data sources and concealing user-related information to adversaries (e.g. user's actual location). Data outght to be anonymized, wherever possible, by removing the PII to decrease the risk of unintended disclosure. Data granularity must be reduced (e.g. disseminate a location-related information and not the exact address) and the storage must be in an encrypted form. Repeating querying for specific data by applications, services, or users that are not intent to act in this manner shall be blocked, and if possible, information over groups of attributes or individuals could be aggregated (e.g. 'the majority of people that visited the examined area in this time interval were young students' this is sufficient information for an advertising application of a nearby shop, without requiring to process raw data from the personal IoT devices).

### C. Identification and Anonymity

The identification of the user is one of the main concerns of every privacy preserving strategy. An adversary may be able to correlate the exchange data with a specific person by integrating different sources of available information. In some cases, the user may wish to preserve his/her anonymity even from the service provider. Thus, the way that the user has access to an application is important for preserving privacy. In general, three types of user access can be implemented that are also determined by the functionality that is requested:

- An *authenticated user* must login the system and use the provided service using its own identity (real or virtual), for example in e-government services or social-media
- A user that access the system utilizing a *pseudonym*
- *Anonymous* usage

In the first case, the service provider knowns the user's identity and the system may intentionally or non-intentionally track the user's activity. The user is aware of this fact and participates with his/her own will. If this type of knowledge is available, it can be utilized not only by the provider but also by a third party or an attacker that will gain access to it. In such cases, the undesired effects need to be circumscribed by established security and privacy controls (e.g. store encrypted data in the database and minimize the pieces of personal information that has to be maintained).

When pseudonyms are utilized, the user cannot be tracked directly. This provides a higher privacy protection that is considered adequate for many applications. However, context knowledge can still make it possible to infer information about the user. For example, from service requests that are made by users that are located in a hospital, we can infer that these people are either employees, patients, or patients' companions. A user that uses an IoT application service from the hospital almost every day, could also be identified as faculty stuff. If the same user also accesses the system frequently from another constantly used location, then we could deduce with a high probability that this other location is his/her home and from it try to figure out the true identity of the user and track back all the service activity to the specific person. Thus, extra protection mechanisms must be deployed as a defence measure, especially for the location-based services (LBS) that are usually provided by the different IoT settings [50].

The main defence strategies include *cloaking areas* [51] and *k-anonymity* ([52], [53]). In cloaking areas, the users' mobile equipment deploys automatic procedures where the pseudonyms of different people are randomly interchanged when they are passing through a specified area. For example, in an IoT environment with smart cars the anonymization areas may be located in the traffic lights or in road crossing, where many cars are met and decrease their speed, allowing the identity change to take place. However, context knowledge can still be inferred [54]. The effectiveness of this solution depends on the density of the anonymization areas and the volume of the participating users over time. The higher the density and the volume, the higher the protection. More advanced schemes are proposed to counter such attacks. Semantic obfuscation techniques intermix the data of semantically diverse domains and reduce the deduced amount of context knowledge [55]. Other protection mechanisms can send dummy location data to the LBS provider instead of the accurate location [56]. Also, the cloaking solution is only applicable to LBS or other services that involve the user's mobility.

With k-anonymity, an intermediate entity between the users and the service is responsible for blurring the identities of at least $k$ users with each other. The users may need to subscribe in this entity and access the functionality even through Internet, overcoming the locality restrictions of the cloaking areas. However, the entity must be considered as a trusted participant by the users' community. In other cases, the functionality can be implemented as a peer-to-peer service, running on the user's devices. On the other hand, this option demands the users' active participation and the willingness to

consume their own resources for the community's benefit. Nevertheless, one main advantage of k-anonymity for system design is the fact that the protection level can be quantified and configured. Increasing the *k* factor, enhances the privacy defence. Combinatorial approaches of both cloaking areas and k-anonymity schemes are also suggested [57], taking advantage of the benefits from both approaches.

Anonymous participation requires threshold signature schemes [58]. A community possess valid credentials to a service (i.e., crowdsourcing), which are then processed by the threshold scheme. Each community participant possesses a share of the common secret. In order to decrypt and authenticate the credentials, one would require at least n valid shares. Thus, users send their collected data to the service along with their shares. If the service achieves to authenticate the credentials of the group utilizing n shares, the data from these specific users are considered authenticated and are further processed. The user provides only partial knowledge to the data collector regarding the credentials of such a group. The collector trusts and processes the data, while the unlinkability with the contributor's identity is retained. These schemes can be centralized, decentralized, or hybrid. The protection level can be configured by changing the n parameter of the threshold scheme. One main security concern is the fact that the community signing key dealers must be honest and trustworthy.

On the other hand, anonymous privacy-preserving techniques restrict popular business operations for e-commerce and targeted marketing. Thus, attribute-based credentials (ABC) are proposed as a mean to protect privacy and provide the adequate information to the service provider [58], [59]. In ABC, a cryptographic container stores attribute-related data, similarly with an X.509 certificate. The container is issued by a trusted authority and bounds the ABC owner to a secret key. The user can show only his/her attributes and prove that they are signed by the authority. The selective disclosure feature enables the user to send only an arbitrary attribute subset, like his/hers purchase level that determines discounts or other advantages. As the proof is based on zero-knowledge, the service provider does not learn the secret key of the user. Moreover, some ABC schemes offer multi-show unlinkability that prevent the service from correlating two different showings of the same user.

### *D. Data Destruction*

Another important issue, which is not handled properly in most cases, concerns the data destruction for the equipment that is reused or disposed. If the data are not deleted properly from the non-volatile memory, security and privacy issues raise as the new owner of the machinery can disclose fruitful information regarding the previous user (e.g. health records, credit card info, etc.). The problem is even more imperative in CE scenarios, where the digital assets are meant to be reused and exchanged between the various actuators.

Thus, specific policies are proposed in order to permanently erase the device's data prior its disposal [60], [61], [62]. However, the aforementioned strategies are not always applicable in cases of distributed storage or cloud. Thus, other state-of-the-art solutions are proposed, which utilize cryptography (i.e. ABE schemes) in order to implement self-destruction policies of the maintained data, on-select or after a specified period of time [63].

## V. Conclusion

As the Internet of Medical Things (IoMT) gains ground, the integration with Circular Economy (CE) becomes popular. New business models and services are modelled, materializing, among others, remote sensing, assistance of elder people, and bioinformatics with crowdsourcing and Big Data. This study presents the main defence mechanisms for providing end-to-end security and privacy. This by-design approach protects the user/patient from a high variety of attacks and threats and safeguards the healthcare sector's operation. The paper reviews the state-of-the-art solutions in each layer and describes the potential towards safe functionality. The overall study can act as a best-practices guide for general IoT or specialized IoMT applications, taking also into consideration the CE perspective.

## Acknowledgment

This work has received funding from the European Union Horizon's 2020 research and innovation programme H2020-DS-SC7-2017, under grant agreement No. 786890 (THREAT-ARREST), as well as the Marie Skodowska-Curie Actions (MSCA) Research and Innovation Staff Exchange (RISE), H2020-MSCA-RISE-2017, under grant agreements No. 777855 (CE-IoT) and No. 778229 (Ideal Cities).

## References

[1] Meulen, R., 2017. Gartner says 8.4 billion connected "things" will be in use in 2017, up 31 percent from 2016, Gartner.

[2] Woo, S., Jo, H. J. and Lee, D. H., 2015. A practical wireless attack on the connected car and security protocol fir in-vehicle CAN, IEEE Transactions on Intelligent Transportation Systems, vol. 16, issue 2, pp. 993-1006.

[3] Ronen, E. and Shamir, A., 2016. Extended functionality attack on IoT devices: The case of smart lights, IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, Saarbrucken, Germany, 21-24 March 2016.

[4] Camhi, J., 2015. The IoT Security Report: Securing new connected devices against cyber attacks, BI Intelligence, Business Insider.

[5] Gong, T., Huang, H., Li, P., Zhang, K. and Jiang, H., 2015. A medical healthcare system for privacy protection based on IoT, PAAP, IEEE, Nanjing, China, 12-14 December.

[6] Appari, A. and Johnson, M. E., 2010. Information security and privacy in healthcare: current state of research, International Journal of Internet and Enterprise Management, Inderscience, vol. 6, issue 4, pp. 279-314.

[7] Jha, N. K., 2017. Internet-of-Medical-Things, Great Lakes Symposium on VLSI (GLSVLSI), May, 2017, Banff, Alberta, Canada, pp.7-7.

[8] Islam, S. M. R., Kwak, D., Kabir, MD. H., Hossain, M. and Kwak, K.-S., 2015. The Internet of Things for health care: a comprehensive survey, IEEE Access, IEEE, vol. 3, issue 1, pp. 678-708.

[9] Xi, W. and Ling, L., 2016. Research on IoT privacy security risks, ICIICII, IEEE, Wuhan, China, 3-4 December.

[10] Abie, H. and Balasingham, I., 2012. Risk-based adaptive security for smart IoT in eHealth, BodyNets, 24-26 February, Oslo, Norway, pp. 269-275.

[11] Tank, B., Upadhyay, H. and Patel, H., 2016. A survey on IoT privacy issues and mitigation techniques, ICTCS, Udaipur, India, 4-5 March, Article no. 2, pp. 1-4.

[12] Miller, K. W., Voas, J. and Hurlburt, G. F., 2012. BYOD: security and privacy considerations, IT Professional, IEEE, vol. 14, issue 5, pp. 53-55.

[13] Stathiakis, N., Chronaki, C. E., Skipenes, E., Henriksen, E., Charalambus, E., Sykianakis, A., Vrouchos, G., Antonakis, N., Tsiknakis, M. and Orphanoudakis, S., 2003. Risk assessment of a cardiology eHealth service in HYGEIAnet, Computers in Cardiology, IEEE, 21-24 Sept., Thessaloniki, Greece, pp. 201-204.

[14] Rockoff, J. D., 2016. J&J warns insulin pump vulnerable to cyber hacking – OneTouch Ping uses unencrypted radio signal, The Wall Street Journal, 4 October, 2016.

[15] ISO/IEC 15408, 1996-2018. Common Criteria for Information Technology Security Evaluation, ISO/IEC.

[16] ISECOM, 1988-2018. Open Source Security Testing Methodology Manual, ISECOM.

[17] Hatzivasilis, G., Papaefstathiou, I. and Manifavas, C., 2016. Software security, privacy and dependability: metrics and measurement. IEEE Software, IEEE, vol. 33, issue 4, pp. 46-54.

[18] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. and Zhao, W., 2017. A survey of Internet of Things: architecture, enabling technologies, security and privacy, and applications, IEEE Internet of Things Journal, IEEE, vol. 4, no. 5, pp. 1125-1142.

[19] Andrea, I., Chrysostomou, C. and Hadjichristofi, G., 2015. Internet of Things: security vulnerabilities and challenges, ISCC, IEEE, 6-9 July, Larnaca, Cyprus, pp. 180-187.

[20] Bekara, C., 2014. Security issues and challenges for the IoT-based smart grid, COMMCA, Elsevier, vol. 34, issue 2014, pp. 532-537.

[21] Nawir, M., Amir, A., Yaakob, N. and Lynn, O. B., 2013. Internet of Things (IoT): taxonomy of security attacks, ICED, IEEE, Phuket, Thailand, 11-12 August 2016, pp. 321-326.

[22] Betts, D., Street, C. and Diogenes, Y., 2018. Internet of Things security architecture. Microsoft Azure documentation.

[23] IBM, 2018. About Watson IoT Platform. IBM Cloud Docs.

[24] Hatzivasilis, G., et al., 2018. The Industrial Internet of Things as an enabler for a Circular Economy Hy-LP: A novel IIoT Protocol, evaluated on a Wind Park's SDN/NFV-enabled 5G Industrial Network. Computer Communications – Special Issue on Energy-aware Design for Sustainable 5G Networks, Elsevier, vol. 119, pp. 127-137.

[25] Jansen, W. and Grance, T., 2011. Guidelines on Security and Privacy in Public Cloud Computing, Director, vol. 144, issue 7, pp. 800–144.

[26] Fernandes, D. A. B. et al., 2014. Security issues in cloud environments: a survey, International Journal of Information Security, vol. 13, issue 2, pp. 113–170.

[27] Kocher, P. et al., 2018. Spectre Attacks: Exploiting Speculative Execution. Available at: http://arxiv.org/abs/1801.01203 .

[28] Lipp, M. et al., 2018. Meltdown. Available at: http://arxiv.org/abs/1801.01207 .

[29] Deshmukh, R. V. and Devadkar, K. K., 2015. Understanding DDoS attack & its effect in cloud environment, Procedia Computer Science. Elsevier Masson SAS, vol. 49, issue 1, pp. 202–210.

[30] Oasis, 2005. eXtensible Access Control Markup Language, OASIS Standard, (February), p. 141.

[31] Gruss, D. et al., 2017. KASLR is dead: Long live KASLR, Springer, LNCS, vol. 10379, pp. 161–176.

[32] Wojtczuk, R. and Rutkowska, J., 2009. Attacking Intel Trusted Execution Technology, Bios, pp. 1–6.

[33] Hashizume, K., Yoshioka, N. and Fernandez, E. B., 2011. Three Misuse Patterns for Cloud Computing, Security Engineering for Cloud Computing, pp. 36–53.

[34] Rajendran, P. K., Muthukumar, B. and Nagarajan, G., 2015. Hybrid intrusion detection system for private cloud: A systematic approach, Procedia Computer Science. Elsevier Masson SAS, vol. 48, issue C, pp. 325–329.

[35] Palattella, M. R. et al., 2016. Internet of Things in the 5G era: enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, IEEE, vol. 34, no. 3, pp. 510-527.

[36] Park, J., Lee, J. and Lee, K., 2017. Method for changing MNO in embedded SIM on basis of dynamic key generation and embedded SIM and recording medium therefor, US Patent, US Grant US9775024B2.

[37] Vesselkov, A., Hammainen, H. and Ikalainen, P., 2015. Value networks of embedded SIM-based remote subscription management, Conference of Telecommunication, Media and Internet Techno-Economics (CTTE), IEEE, 9-10 November, Munich, Germany.

[38] Hatzivasilis, G., Papaefstathiou, I. and Manifavas, C., 2017. SCOTRES: secure routing for IoT and CPS. IEEE Internet of Things (IoT) Journal, IEEE, vol. 4, issue 6, pp. 2129-2141.

[39] Gemalto, 2015. Cellular connectivity management solution for consumer electronics devices, Gemalto documentation.

[40] GSMA, 2017. The importance of embedded SIM certification to scale the Internet of Things, GSMA documentation, pp. 1-12.

[41] Chen, C., Raj, H., Saroiu, S. and Wolman, A., 2014. cTPM: a cloud TPM for cross-device trusted applications, 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2-4 April, Seattle, WA, USA, pp. 187-201.

[42] ISO/IEC 11889, 2015. Trusted platform module library, ISO/IEC.

[43] Paverd, A. J. and Martin, A. P., 2012. Hardware security for device authentication in the smart grid, International Workshop on Smart Grid Security (SmartGridSec), Springer, LNCS, col. 7823, pp. 72-84.

[44] ISO/IEC 27018, 2014. Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors, ISO/IEC.

[45] ISO/IEC 29100, 2011. Privacy Framework, ISO/IEC.

[46] European Parliament, 2016. Regulation (EU) 2016/679, European Union.

[47] Apthorpe, N., Reisman, D. and Feamster, N., 2016. A smart home is no castle: privacy vulnerabilities of encrypted IoT traffic, Workshop on Data and Algorithmic Transparency (DAT), New York, USA, 19 November.

[48] Zhou, W. and Piramuthu, S., 2014. Security/privacy of wearable fitness tracking IoT devices, CISTI, IEEE, Barcelona, Spain, 18-21 June, pp. 1-6.

[49] Perera, C., 2017. Privacy guidelines for Internet of Things: a cheat sheet, Technical report, New Castle University, UK, pp. 1-9.

[50] Chen, Z., Xia, F., Huang, T., Bu, F. and Wang, H., 2013. A localization method for the Internet of Things, The Journal of Supercomputing, Springer, vol. 63, issue 3, pp. 657-674.

[51] Buchanan, W. J., Kwecka, Z. and Ekonomou, E., 2013. A privacy preserving method using privacy enhancing techniques for location based services, Mobile Networks and Applications, vol. 18, issue 5, pp. 728-737.

[52] Moque, C., Pomares, A. and Gonzalez, R., 2012. AnonymousData.co: a proposal for interactive anonymization of electronic medical records, Procedia Technology, Elsevier, vol. 5, issue 2012, pp. 743-752.

[53] Yamaguchi, R. S., Hirota, K., Hamada, K. and Takahashi, K., 2012. Applicability of existing anonymization methods to large location history data in urban travel, IEEE International Conference on Systems, Man, and Cybernetics, IEEE, 14-17 October, COEX, Seoul, Korea, pp. 997-1004.

[54] Niu, B., Zhu, X., Li, Q., Chen, J. and Li, H., 2015. A novel attack to spatial cloaking schemes in location-based services, Future Generation Computer Systems, Elsevier, vol. 49, issue 2015, pp. 125-132.

[55] Ullah, I. and Shah, M. A., 2016. A novel model for preserving location privacy in Internet of Things, ICAC, IEEE, 7-8 September, Colchester, UK, pp. 1-6.

[56] Sun, G., Chang, V., Ramachandran, M., Sun, Z., Li, G., Yu, H. and Liao, D., 2017. Efficient location privacy algorithm for Internet of Things (IoT) services and applications, Journal of Network and Computer Applications, Elsevier, vol. 89, issue 2017, pp. 3-13.

[57] Yu, R., Bai, Z., Yang, L., Wang, P., Move, O. A. and Liu, Y., 2016. A location cloaking algorithm based on combinatorial optimization for location-based services in 5G networks, IEEE Access, vol. 4, issue 2016, pp. 6515-6527.

[58] Alcaide, A., Palomar, E., Montero-Castillo, J. and Ribagorda, A., 2013. Anonymous authentication for privacy-preserving IoT target-driven applications, Computers & Security, Elsevier, vol. 37, issue September 2013, pp. 111-123.

[59] Alpar, G. et al., 2016. New directions in IoT privacy using attribute-based authentication, ACM International Conference on Computing Frontiers (CF), ACM, Como, Italy, 16-19 May, pp. 461-466.

[60] Bergren, M. D. and Murphy, E. A., 2005. Data Destruction. The Journal of School Nursing, vol. 21, issue 4, pp. 243-246.

[61] Yan, Q., Xue, M., and Xu, Z. 2013. Disposal of waste computer hard disk drive: data destruction and resources recycling, Waste Management & Research, SAGE, pp. 559-567.

[62] Dong, H., Kun, S., and Yu, C., 2009. Research on secure destruction of digital information, International Conference on Apperceiving Computing and Intelligence Analysis, IEEE, Chengdu, China, pp. 356-359.

[63] Xiong, J., et al., 2013. A secure document self-destruction scheme: an ABE approach, International Conference on High Performance Computing and Communications, IEEE, Zhangjiajie, China, pp. 59-64.