ICT in Healthcare: the role of IoT and the SECANT solution

M. Caballero*, D. Kavallieros †, A. Spyros †, A. Tavernarakis ‡, A. Tziouvaras §, S. Bonacina¶, K. Chandrarmouli¶, M. Coroiu ‖, L. Chen **, T. Dounia ††, I. Giannoulakis ‡, N. Gligoric[x], E. Kafetzakis ‡, T. Kasig¶, V. Koumaras ††, T. Krousarlis[xiv], K. Lapidaki[xi], A. Markakis[xi], S. Marin ‖, M. Manulis **, S. Menesidou[xiv], S. Nifakos¶, L. Meng**, S. Mhiri[xii], M. Nati[x], K. Ntafloukas[xiii], D. Oniga ‡‡, D. Papamartzivanos[xiv], S. Papastergiou [xiii], K. Sanchez [xiii], C. Sakkas ††, K. Stelliou[xiii], L. Trujillo*, T. Tsikrika †, E. Venegas*, S. Vrochidis †, D. Xydias¶.

*NTT DATA Spain, † Center for Research and Technology, ‡ Eight Bells LTD, § Business and IoT Integrated Solutions Ltd, ¶Department of Learning, Informatics, Management and Ethics, Karolinska Institutet, 171 77 Solna, Sweden, ‖ Polaris Medical, ** University of Surrey, †† INFOLYSIS P.C., ‡‡ Software Imagination & Vision, [x]IOTA Foundation, [xi]Adrestia R&D, [xii] Fundacio Privada I2CAT, Internet I Innovacio Digital a Catalunya, [xiii]Security Labs Consulting Limited, [xiv]Digital Security & Trusted Computing Group, UBITECH.

***Abstract*—The industrial sector is experiencing an unprecedented number of changes in recent years. New models of remote delivery, especially in complex ICT infrastructures such as healthcare, increase the potential impact of cybersecurity breaches to a level that has not been experienced before. This paper presents the SECurity And privacy protectioN in internet of Things devices (SECANT) project, an EU-H2020 project aimed to strengthen the understanding of risks, at both human and technical level through the delivery of a holistic framework for cyber security risk assessment for enhancing the digital security, privacy, and personal data protection in complex ICT infrastructures, such in the healthcare ecosystem. The SECANT platform will implement a collaborative threat intelligence collection, analysis and sharing, an innovative risk analysis specifically designed for interconnected nodes of an industrial ecosystem, a cutting-edge trust and accountability mechanisms for data protection and a security awareness training for more informed security choices. This platform will be demonstrated and validated across four operational pilots reflecting different real-life business cases.**

I. Introduction and related work

The technological advancements of past decades have established a range of new devices to people's lives, with many satisfying the heightened thirst for making our planet smart. COVID-19 pandemic and the need for social distancing have also maximized the need for communication channels between different Information and Communications Technology (ICT) infrastructures, where Artificial Intelligence (AI), Industrial Control Systems (ICS) and Internet of Things (IoT) play an important role. These advancements came with new waves of cyberattacks, raising security and privacy issues.

The healthcare sector, where sensitive information is processed every moment and the race for contact tracing applications has promoted the need for privacy, relies heavily on interconnected IoT solutions. This is a constantly increasing data-driven ecosystem populated by Internet-connected devices, shared medical databases and networks, and it is precisely this interconnected nature and the high criticality of the sector that makes it attractive and profitable to cyberattacks, which range from general-purpose and often indiscriminate ransomware bringing down whole hospitals' networks to highly targeted attacks utilizing advanced backdoor malware. The causes of such incidents are equally diverse, ranging from negligent users, insiders and compromised customer networks, to poorly secured medical devices (mostly legacy) and AI-assisted diagnosis systems. The limited security awareness in the sector and the decentralized nature of the complex ICT infrastructures amplify the situation. Indeed, the prevalence of connected devices creates a fertile ground for cascading cyberattacks [3], [4]. As the number of connected IoT devices worldwide increases, the global security community calls for an increased focus on securing them, especially those involved in the healthcare ecosystem, establishing trust among all the involved entities to avoid damages and monetary losses.

In such a complex cyber risk environment where IoT devices are more necessary than ever to help the European and global population exit the COVID-19 crisis, the SECANT project (https://secant-project.eu/), funded from the European Union's Horizon 2020 programme, aims to complement traditional platform-specific and attack-specific countermeasures developed in the industry, by holistically strengthening the understanding of risks, at both human and technical level. The human factor, which is by default the weakest link, requires intensive cybersecurity education, something that has been expressed repeatedly for more than a decade [12]. On the technical point, the risks need to be understood and codified in ways that can be monitored and prevented not within the boundaries of a single organization in isolation, but across the complete spectrum of interacting IoT devices.

SECANT is a three-year project (September 2021-August 2024) and its main goal is to deliver a holistic framework for cyber security risk assessment for enhancing the digital security, privacy, and personal data protection in complex ICT infrastructures by placing an automated threat detection platform addressed to CERTs/CSIRTs that is capable of identify-

ing threats and attacks, while promoting the situational security awareness as a priority within complex ICT infrastructures, such as the healthcare ecosystem [4], [8]. The SECANT platform will enhance the capabilities of organizations' stakeholders and enable industrial participants to make informed and context-aware decisions regarding cybersecurity, privacy and data protection risks by implementing: (a) collaborative threat intelligence collection, analysis and sharing; (b) innovative risk analysis specifically designed for interconnected nodes of an industrial ecosystem; (c) cutting-edge trust and accountability mechanisms for data protection; and (d) security awareness training for more informed security choices. The proposed solution's effectiveness and versatility will be validated in four realistic pilot use case scenarios reflecting different real-life business cases applied in the healthcare ecosystem .

To fulfil this goal the SECANT Consortium, coordinated by NTT Data and supported by CERTH in the Scientific & Technical Management, involves 20 partners from 10 European countries, gathering a multidisciplinary group from research, ICT industry, SMEs, health organizations and CERT partners.

There a significant amount of existing work that relates with certain aspects of the SECANT solution. Threat intelligence platforms such as MISP [9] support the insertion, gathering, and sharing of threat intelligence information, manually through a GUI and automatically through APIs. Furthermore, the H2020 project SANCUS [10] proposes an analysis software that employs uniform statistical sampling, audit and defense processes. Regarding the cyber security training platforms, DOGANA [11] is a framework, which addresses the Social Engineering vulnerability assessment and its inherent challenges on the technical, psychological, ethical, moral and legal domains.

Related work for privacy, data encryption, search and sharing encapsulate various methodologies such as Attribute-based encryption (ABE), Proxy re-encryption (PRE), Searchable Encryption (SE), Honey Encryption (HE) and distributed ledger technology (DLT)-based protection. ABE [16], [15] allows sticky policies in data access control. It encrypts data under a description, so that only user(s) with the secret key matching the description can access it. PRE [19], [20] enables a semi-trusted proxy to convert the encrypted data, to another encryption scheme by using a re-encryption key. SE is employed to securely search encrypted data, and is categorized into public key-based SE [17], which focuses more on integrity check of outsourced data and strong security (but with less efficiency), and symmetric SE [18], guaranteeing efficiency in data search (but with less security). HE [21] is an encryption system against brute-force attacks via outputting a plausible-looking decryption for an arbitrary incorrect key. Despite that the focus on privacy of data shared on DLTs is limited, recent attempts have attempted to leverage emerging technologies such as the IOTA Tangle to promote the concept of self-sovereign sensitive data in case of data generated by IoT devices [25], [26].

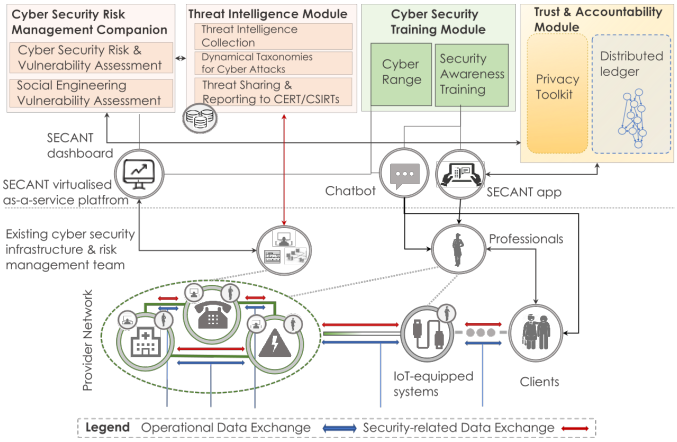

Fig. 1. The SECANT high-level architecture.

II. Main Concept

SECANT introduces a unique architectural structure for best associating modern distributed ledger technologies with novel practices for digital security, privacy, data protection and accountability able to defend the industrial supply chain infrastructure against crippling modern cyber-threats. The interrelation of SECANT's major components is illustrated in Fig. 1, while their high-level summary is highlighted below.

*a) **Threat Intelligence Module (TIM)**:* TIM is responsible for (i) collecting, sharing threat intelligence among SECANT's supply chain stakeholders as well as reporting such intelligence to CERTs/CSIRTs, and (ii) building dynamic taxonomies for cyber-attacks which will be used as a basis for building cybersecurity incident management systems.

TIM is based on MISP, a threat and malware information sharing platform, which will be adjusted to fit the needs of complex ICT infrastructures allowing for the (i) manual collection of cyber threat intelligence (CTI) through a user-friendly GUI, (ii) automatic gathering of CTI from logs and alerts of existing software and hardware security components (i.e. Intrusion Detection/Prevention Systems) through relevant APIs and by periodically crawling and collecting CTI from online sources (e.g., security reports, feeds of CERTs) and (iii) automatic/manual creation of Intelligent Cases based on collected incidents/vulnerabilities/intelligence. Finally, the platform will allow the sharing of all collected information to public databases, and also the automatic reporting to CERTs/CSIRTs to assist in the broader prevention of such threats.

TIM will communicate with other SECANT modules to both provide as well as consume input/data. Specifically, TIM will communicate with: (i) *SECANT's Interoperability Layer (IPL)*, (ii) the *Cyber Security Risk Assessment Companion (CSRAC)*, (iii) the *Technical Vulnerability and Impact Assessment (TVIA)*, and (iv) the *SECANT Dashboard*. The data exchange will facilitate TIM in terms of information gathering, while the other modules will be facilitated regarding the detection as well as the sharing of the gathered CTI. Apart from the internal sources which will be available via the IPL,

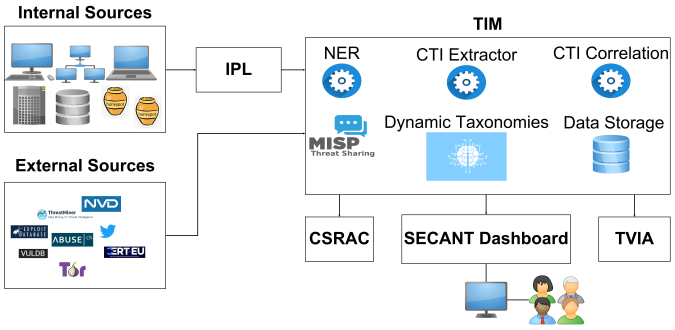

Fig. 2. TIM communication architecture.

TIM will gather CTI data from external sources by crawling and scraping online security related resources, and feeds of CERTs/ CSIRTs and security companies. The communication between TIM and the other SECANT components, including external sources, is depicted in Fig. 2.

TIM will operate on the basis of taxonomies for cyber-attacks. The aim is to enrich the platform's stored threat information, while also providing the basis for building incident management systems. More specifically, existing taxonomies will be adjusted by adding, removing, or updating their predicates and entries to more accurately reflect cyber-attacks against complex ICT infrastructures. To this end, all components of the ICT ecosystem, as well as their pathways and dependencies, will be identified and enumerated based on expert's feedback and reviews of recent attacks. The toolkit will enable these manually adjusted taxonomies to be dynamically adjusted whenever new information is inserted into the database. To this end, the toolkit will first provide suggestions for predicates and entries of the available taxonomies by trying to correlate that information with data already assigned to specific entries of the taxonomy, based on machine learning techniques (e.g., clustering) as well as on techniques that extract domain specific terms and relationships between the concepts that these terms represent. If none of the existing entries in the taxonomies are representative of the new information, the platform will either expand the existing taxonomies by suggesting a new predicate or a new entry inside an already existing predicate with a name and description, or will adjust an already existing predicate/entry.

*b) **Cyber Security Risk Assessment Companion (CSRAC)**:* SECANT will develop the Cyber Security Risk Assessment Companion (CSRAC) component which will facilitate decision making and effective and timely response to detected cyber security risks. In order to avoid the fast propagation of vulnerabilities that can trigger cascading cyberattacks, the SECANT Connected Organizations Cyber Risk Assessment Engine (CO-CRAE) will integrate data regarding cyber-attacks and vulnerabilities, collected from the existing cyber-security infrastructure of different stakeholders through the SECANT's TIM. Risk models adapted to the particular characteristics of connected organizations will be analyzed and included in the cyber risk assessment, which will focus on cascading cyber-attacks and vulnerabilities propagation risk assessment. Thus, the CSRAC will evaluate the impact of vulnerabilities and attacks detected depending on its severity and the potential assets affected in case of propagation. Finally, users will be able to interact with the CSRAC via the SECANT Dashboard which will allow them to perform cyber risk assessments and present them with recommendations of countermeasures and other mitigation actions in a user-friendly manner.

The SECANT module for Human vulnerability assessment will build a HVA for the typical environment and sophisticated ICT infrastructures by configuring initial work such as DOGANA in the field, and developing new functions for the configuration and maintenance of configurable landing sites. The HVA framework's Social Driven Vulnerability Assessment module will be enhanced to include analysis of the online social engineering attack surface as an additional technique to analyze companies' vulnerabilities to SE attacks during the information collection and analysis stage. As a result, the project will develop a Human Vulnerability Assessment module that will use OSINT and social engineering to assess and test privacy and security. Ergo, the module will be completely matched with the two primary tactics for combating Social Engineering (SE), namely, simulation of SE attacks and awareness training to improve users' ability to recognize and respond to such attacks. Finally, as an additional technique of lowering the possibility for SE assaults on its users, HVA will expand its work on data collection and analysis related to the online social engineering attack surface. This will include a module for identifying the organization's digital footprint, which will be gleaned from its home page and social media profiles, as well as identifying employees of the organization among its social media affiliates (e.g., twitter followers) and looking for other OSINT documents, containing references to the organization and the evaluated profile.

The SECANT module for Technical Vulnerability Assessment (TVA) would be responsible for discovering and dynamically isolating vulnerabilities in complex ICT infrastructures. The TVA will discover vulnerabilities based on multiple indicators (domain names, IP addresses, file hashes, or log indicators) produced by Artificial Intelligence (AI) algorithms using data from existing telemetry modules and threat intelligence from the SECANT platform. When a vulnerability is discovered, the TVA will notify security analysts via the SECANT Dashboard and display related information on the vulnerability's discovery point (i.e., vulnerability name, system components or services affected and potential impact).Using the SECANT Dashboard, the analyst will be able to learn more about the vulnerability and isolate the affected component, preventing additional contamination across the supply chain until a security measure is implemented. As the threat's intelligence module's dataset grows over time, the accuracy of the AI algorithms will improve, minimizing the risk of false positives (e.g., out of context vulnerabilities or malformed indicators). The TVA will deliver targeted dynamic vulnerability assessment and testing processes developed for each type of

stakeholders that embed suitable scenarios and test cases, thus reducing the overhead required to assess the security posture of the complex ICT infrastructures.

The Human Vulnerability Assessment (HVA) module of SECANT will extend work done in projects like DOGANA that provides a framework's Social Driven Vulnerabilities Assessment module to include an awareness point of view and support for the design, reuse and launching of landing websites. The HVA module will be able to validate and test the privacy and security using OSINT, OpenUEBA and social engineering. This way the module will be fully aligned with the two main strategies for tackling Social Engineering (SE), namely the simulation of SE attacks and awareness training to increase users' ability to identify and react to such attacks. Finally, HVA will further extend the work on information gathering and analysis regarding the online social engineering attack surface, as an additional method of reducing the potential for SE attacks on its users.

The Technical Vulnerability Assessment (TVA) module of SECANT will be in charge of identifying and dynamically isolating vulnerabilities in complex ICT infrastructures. TVA will use input from existing telemetry modules and threat intelligence from the SECANT platform and will detect vulnerabilities based on various indicators (i.e., domain names, IP addresses, file hashes, or log indicators), which will be derived by novel Artificial Intelligence (AI) algorithms. Once a vulnerability is detected, the TVA will notify the security analysts through the SECANT Dashboard and will present related information around the detection point of the vulnerability (i.e., vulnerability name, system components or services affected and potential impact). The analyst, using the SECANT Dashboard, will be able to acquire more information regarding the vulnerability and to isolate the infected component to prevent further contamination within the supply chain until a security mechanism is applied. The accuracy of the AI algorithms will be further improved as the dataset of the threat intelligence module increases over time, thus reducing the likelihood of false positives (e.g., out of context vulnerabilities or malformed indicators). The TVA will deliver targeted dynamic vulnerability assessment and testing processes developed for each type of stakeholders that embed suitable scenarios and test cases, thus reducing the overhead required to assess the security posture of the complex ICT infrastructures.

SECANT will also investigate the extension of mission-aware impact assessment models to incorporate information from intrusion detection systems and other security and safety events, by adding two layers to the existent VTAC model (Virtual Terrain Assisted impact assessment for Cyber-attacks). A physical layer will be introduced to include incidents detected on medical devices and a supply chain layer to include known incidents reported by dependent entities of the supply chain. Within the Impact Assessment Module (IAM), input from the assessment of existing threats and vulnerabilities will be used to simulate the potential impact of identified cyber threats and vulnerabilities on the complex ICT infrastructures. TVA and IAM will constitute SECANT's Technical Vulnerability and Impact Assessment (TVIA) module. The architecture of the Cyber Security Risk Assessment CSRAC and its different components are depicted in the CSRAC architecture in Fig. 3.

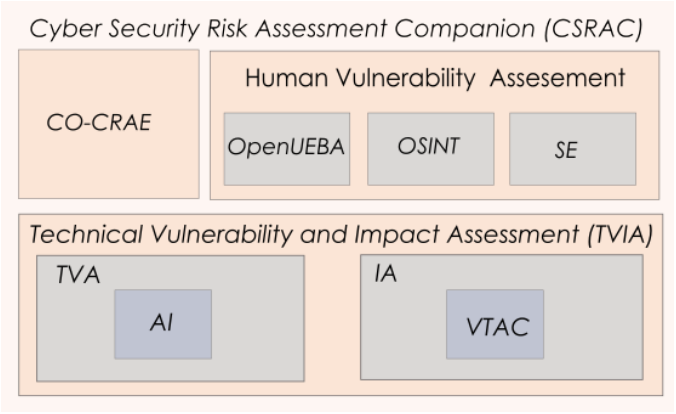

Fig. 3. CSRAC architecture.

c) ***Cyber Security Training Module (CSTM)****:* SECANT will deliver an effective Cyber Range OCR platform for modelling and emulating the complex ICT infrastructures (e.g., online services, applications, security mechanisms), which will operate as a sandbox for emulating network-wide attacks and forensic, eliminating the risk of data loss or adverse impact on running components. The cyber range will leverage on established and emerging virtualization technologies, enabling ultra-fast and automated system and network configuration deployments by using both managed infrastructure services (e.g., AWS, Google Cloud Platform, Microsoft Azure) and local deployment (e.g., based on VMWare vSphere, OpenStack, Kubernetes). Additionally, concepts from AI and ML will be used to create a completely non-scripted simulation experience (e.g., emulating both attackers and defenders and specific end users).

The cyber range platform includes the following functionalities: (i) capability to have multiple users with each of them working either independently over the same replicated infrastructure (or on different infrastructures) or cooperating as a team on a single target; (ii) easy to use catalogue for setting up training scenarios (via drag and drop or via description models); (iii) load balancing among VMs, network and host capture; (iv) remote screens supervision and traffic capture; (v) capability of remotely executing actions on VMs and scriptable actions; (vi) traffic generation; (vii) custom network links emulation (e.g., latency, throughput, loss); (viii) connection with real network devices in hybrid scenarios (e.g., a mix of emulated and real devices, etc.); and (ix) virtualized SIEM (Security Information and Event Management) component, grouping security information and event management functionalities for the real-time monitoring and notification of security events of the system.

SECANT goes beyond the static approach employed by the majority of currently available training programs on cybersecurity by investigating novel methodologies to improve the

learning experience and maximize the impact of training. By integrating key gamification concepts into SECANT's Security Awareness Training Platform (SATP) since the design phase of the training scenario, it will be possible to set objectives, steps, keys/flags, and timestamps to measure the performance of trainees in real time and at the end of the training session. Gamification (role playing) of the cyber security awareness training will enhance the long-term motivation of learners and increase the cybersecurity awareness of end users. The focus of the approach will be to move cybersecurity from passive to active learning, thus increasing retention and knowledge transfer to non-skilled end users (e.g., other professionals and clients). The project will test and evaluate the platform extensively with both technical and non-technical experts: (1) for non-technical experts, the evaluation will be related to their perception of user friendliness and ease of use of the interface, and on the explanations to understand the basics of cyber-security; (2) for technical experts, the evaluation will be based on the perceived similarity between the proposed training and the real environment and on the soundness of the proposed technical content; 3) the platform will be also tested with expert-level penetration testers evaluating the technical skills required to pass the trainings.

d) ***Chatbot****:* A chatbot application will be created in the context of the Cybersecurity Training module, developed within SECANT Project and aiming at enhancing the security awareness of both professionals and non-professionals. More specifically, the chatbot will make use of content specifically created for fulfilling the purpose of training and evaluating healthcare personnel reflecting best practices in several cybersecurity topics. The use of the chatbot application will offer its users a rich experience and will incorporate capabilities for their assessment on security related topics providing also feedback for overcoming assessed weaknesses. For example, any interested user, will be able to use the chatbot application to take an assessment test consisting of questions in multiple choice or free text format, receiving an overall score at the end of the assessment and at the same time, the trainings responsible will be able to use the chatbot to redirect the users to related training material for the enhancement of their expertise. This training chatbot will be an enhancement of the chatbot application marketed by INFOLYSIS (Fig. 4) and its adaptation to the needs of SECANT. The training chatbot will be able to (a) establish a two-way communication channel between trainees and instructors, (b) allow registration to specific training sessions, (c) communicate training material in various format (text, images, animations, videos, etc.), (d) provide training through video playback, (e) be used as an alternative communication channel for personalized messaging/notifications sent by the instructors to trainees (f) provide statistical analysis of responses received from trainee assessments, (g) provide statistical graphs for quick insights int the efficiency of training, and (h) provide follow up communication to trainees.

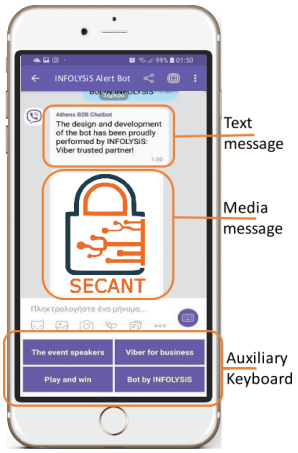

Fig. 4. The Chatbot application.

e) ***Trust and Accountability Module (TAM)****:* SECANT's Trust and Accountability Module (TAM) will deal with: (i) verifying the integrity of data; (ii) establish security of devices and track provenance and integrity of their data; and (iii) tracking the correct access to data. It will be developed as decentralized infrastructure using a Distributed Ledger Technology (DLT).

The IOTA Tangle (i.e. a system of nodes used for confirming transactions) will be used for its lightweight and scalable nature that allows the integration of Internet of Things devices, as well as for its feeless consensus protocol. This highly reduces the barriers for adoption of this technology compared to conventional blockchain platforms. In addition to that, IOTA Streams will be used to protect confidentiality of ledger data, while IOTA Identities will be integrated to remove unreliable centralized Identity Management Systems.

The TAM (depicted in 5) will provide interfaces and APIs towards different data sources. Once access to client's data from a given data repository is authorized, an encrypted immutable certificate, including who is accessing what, under which authorization and for what purpose, will be stored into the IOTA Tangle together with a hash and a sequence number of the data sets. Actual data sets will be transferred off-chain using TAM Accountability APIs, while transfer is logged using the data traceability tool and its integrity verified using the verification tool. This will allow data owners, such as clients, to trustfully track their data accesses and data processors to transparently verify the integrity of data. IOTA Streams will be used to protect the confidentiality of data transactions carrying access certificates associated with a given stakeholder data. The IOTA Tangle will also store decentralized identities and metadata of connected IoT devices (e.g., firmware version, latest security update, last user pseudonymous ID) to track their provenance and to define their Level of Assurance towards third parties using them or including in their systems. After a decentralized device identity is created, a dedicated IOTA Stream associated to it will collect information for each device and immutably store it.

Device Identity Management Tools such as interfaces, visualization and notification tools, will be developed to facilitate the decentralized device identity verification. QR-codes and Near Field Communication (NFC) tag will be used to digitize dummy devices and create their immutable digital twin. Data Validation Tools using Zero Knowledge Proof will be integrated in the TAM northbound layer for privacy-preservation.

f) ***Privacy Toolkit****:* The Privacy Toolkit, illustrated in Fig. 6, elegantly merges advanced encryption technologies to

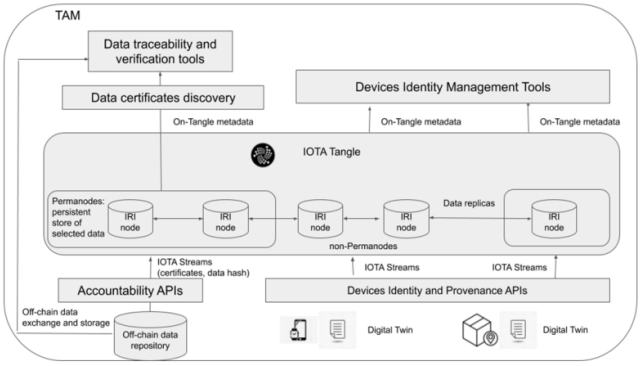

Fig. 5. Overview of the TAM module.

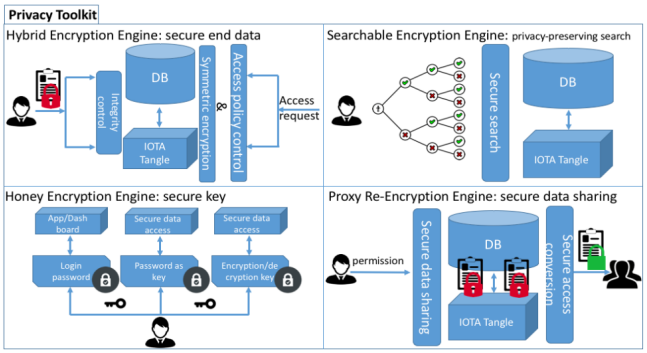

Fig. 6. Overview of the SECANT Privacy Toolkit.

mediate all access to information flowing through the TAM.

The Privacy Toolkit will make use of hybrid encryption mechanisms, employing symmetric encryption, Hash-based Message Authentication Code (HMAC) [14], Attribute-Based Encryption (ABE) [15][16], Searchable Encryption (SE) [17][18] and Proxy Re-Encryption (PRE) [19][20] to: (i) enhance the security of devices by issuing a hardcoded, hardware-level symmetric key used to encrypt and decrypt information flow; (ii) guarantee the integrity and confidentiality of data by using a combination of symmetric encryption and HMAC; (iii) provide expressive data sharing capabilities and access control without loss of confidentiality and flexibility by leveraging ABE and symmetric encryption; (iv) provide privacy-preserving search over encrypted data without loss of data security and user privacy by using advanced SE. We will consider on-chain and off-chain searchable encrypted index structure. The chain will convert the most frequent metadata/search keyword/mode into the "secret information" which can be embedded into a binary tree structure and store the location of information on the ledger on the leaves of the structure. The index structure will build up a strong link with the ledger so that the data searcher may only need to execute a privacy-preserving search over the structure to locate the leaf and then it will obtain the location information of data on ledger. To synchronize the real-time ledger expansion, a new type of dynamic SE mechanism will allow an encrypted index structure growing with the ledger. SE will offer fine-grained expressive search services, e.g., formula, range, and regular language search. (v) Protect data security but also minimize the use of data sender's operational resources by incorporating PRE, a novel encrypted data sharing mechanism. PRE provides data sharing and key management for decentralized network infrastructures. It enables a semi-trusted proxy, such as a gateway, to convert ciphertext intended for a party to another encryption of the same plaintext, which can be decrypted by someone else. The conversion leaks no information to the proxy. SECANT will use it to further share encrypted data recorded online on the fly.

SECANT will leverage Honey Encryption (HE) [21], a novel scheme against the brute-force attack even when low-entropy keys are chosen by users. It can "fool" attackers by leveraging the randomized encoder to output a plausible-looking decoy message for an arbitrary incorrect key. SECANT will deploy HE in securing system login passwords for the SECANT Dashboard, App and other management systems. Using HE, only a valid password holder can correctly login to the systems while malicious attackers will be unable to succeed with brute-force attacks.

SECANT will also employ Password-Based Encryption (PBE) [22] for accessing client's records. It will combine HE with PBE so that a client may use login password as encryption/decryption key for the personal data. SECANT will design a secure level to safeguard sensitive information via advanced encryption but also provide another protection level via securing the keys. Eventually, SECANT will provide secure solutions for personal secret information, e.g., identity, via the use of HE.

*g) **Digital Identity Management Module**:* Traditional identity management systems adopt the centralized approach, with a design already witnessed several limitations and weaknesses regarding security, privacy, and scalability. The negative side of centralized models is that identity providers have full control over individuals' identity, and identity owners are incapable of preventing any misuse of their identities [27]. Sensitive data are exposed on daily basis in breach incidents caused by weak security of centralized databases. There are numerous weak points in the centralized approach, one of them being exchange of data when users register or access the services, when the data are shared or stored without following the best practice or standards.

SECANT's Digital Identity Management (DIM) module allows the unequivocal identification of professionals, clients and instruments of an organization. Its integration with SECANT's TAM would allow it to record and trace all the interactions made between different entities, maintaining absolute certainty of the identity of the client or professional involved.

SECANT will also develop a Self-Sovereign Identity (SSI) solution, which is capable of digitizing entities with a Level of Assurance (LoA) of the required level. This type of identity will provide the capacity to own customer self-identity and share only the data customer needs to share in each case. Fig. 7 shows how SSIs works. First, an issuer creates a verifiable

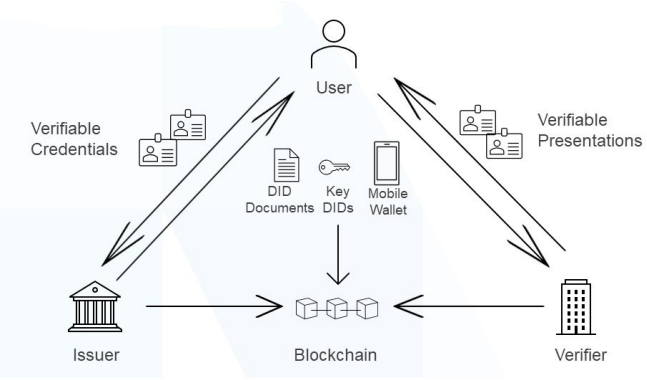

Fig. 7. Self-sovereign identity

credential on the blockchain. This credential is registered in the user's wallet, allowing it to be shared when needed. When the user wants to use it, he sends that verifiable presentation to the verifier and the verifier checks it on the blockchain.

The solution is composed of the following elements: (i) Digitization Portal: used to generate and manage corporate and individual identities by organizations. It will also allow issuing, revoking and managing the credentials of each identity; (ii) Wallet App: used for the user to manage and control their own identity. Furthermore, the user can save, verify and share his identity credentials; (iii) Integration API: for the communication of the identity module with the DLT and the different stakeholder systems.

In order to create a consistent and legally compliant solution, it is necessary to develop Decentralized Identifiers (DID). SECANT decentralized identities will be based on the decentralized Identity or Self-Sovereign Identity (SSI) - a new method for identity management and authentication based on W3C Standard. It removes the centralized aspects and puts the Identity subject in full control over its own identity. Decentralized identity provides a solution for the increasing amount of database breaches, the lack of trust.

This identity will be indexed to the DLT that allows identity verification. DIDs are standardised by the W3C standard. This framework will guide the definition of all the attributes associated with a given digital identity. This will be expressed by verifiable credentials, signed by other parties in the ecosystem. Verifiable credentials are a standard format for the digital representation of credentials that are cryptographically secure, verifiable through machines, and that guarantee privacy by enabling methods such as minimum disclosure. Verifiable presentation are a pack of claims extracted from one or more verifiable credentials from the same or different issuers.

The regulation requires that the digital identity solution be catalogued under a LoA, which marks the level of trust customers have regarding the digitized identity. This level varies from 0 to 4 based on the systems used to digitize the entity. For example, to deal with the administration it is necessary to obtain a level of 3 or 4. Typically, the systems that define a high value of LoA also have a significant cost of installation and use for organizations and users. However, for the purposes of the SECANT project, a level of 2 is deemed satisfactory. LoA will be automatically derived and verified based on the credential collected by each identity, who signed them and assert their ownership.

*h) **SECANT Dashboard and End User Application**:* SECANT will provide a dashboard and a mobile application as the main interfaces through which end users can interact with the platform. The SECANT Dashboard will be the main point of interaction between cybersecurity professionals and the SECANT platform. Through the SECANT Dashboard a cyber security professional will be able to (i) access a knowledge base of cyber security and social engineering vulnerabilities collected by the Threat Intelligence Module and (ii) assess the impact of vulnerabilities as they propagate throughout the ICT infrastructure.

More specifically, the Case Management process will be facilitated by the dashboard, via which cybersecurity professionals will be able to collaboratively examine a new case/incident, report functionalities of the created case to CERTs/CSIRTs, comment on it, and update details regarding its potential propagation through the supply chain and potential countermeasures to reduce its impact. SECANT End User Application on the other hand, targets the clients and other professionals. This mobile application will allow non-expert end users to familiarize themselves with best practices and common pitfalls of cyber security through the Security Awareness Training module. Additionally, the SECANT app will allow end users to monitor information relevant to them as it flows through the supply chain via the Trust and Accountability module. The monitoring capabilities offered by the app will allow end users to easily identify how the information they received has been handled (e.g., who interacted with it, when and where was it created, which devices have been used) so their trust towards other stakeholders of the supply chain can be increased.

*i) **SECANT Platform**:* One of the main objectives of SECANT is to integrate the individual technologies and components described above into a unified cyber security risk management platform that will provide an automated threat detection platform addressed to CERTs/CSIRTs, identifying possible threats and attacks, while promoting the situational security awareness amongst its users as a priority through a powerful training module. The SECANT platform and modules will be integrated based on each component's background technologies in a virtualised platform as-a-service type of solution. The platform will be released in two iterations- an initial prototype and a second one based on the results of testing and validation in the operational environments of the demonstration partners. After and during development each component will be tested in more steps: (i) functional tests, (ii) modular tests, inter-modular tests, (iii) technical assessment of the outcome, (iv) recommendations for the final platform refinements, and (v) fine tuning and overall optimization. Functional and end to end tests of the integration of the SECANT modules will be provided in a controlled environment before actual deployment at pilots. The first

prototype of SECANT platform will be further tested and validated in four uses cases, in operational environment and improvements will be embedded in the second version of the platform. At the end of the project the final result will be an operational cyber security risk management platform for connected ICT ecosystems, addressing cyber security possible threats, privacy, data protection and accountability needs, in a dynamic and flexible way.

III. Use cases

The SECANT plafofrm will be validated through four different Pilot Use Cases that are aiming (i) to validate SECANT's ability to improve transportation safety and ensure zero-error delivery of patients transported using time-constraint Emergency Medical Services (*Protecting the connected ambulance of the future*), (ii) to validate SECANT's efficiency to deal with cascading effects of cyber threats and with propagated vulnerabilities in connected healthcare infrastructures, as well as in remote healthcare settings (*Cyber security for connected medical devices and mobile applications* [23], [24]), (iii) To validate the capabilities of SECANT to ensure privacy, data protection and accountability when operational data is being exchanged within the healthcare supply chain (*Health data protection in the healthcare supply chain*) and (iv) to validate the capabilities of SECANT's cyber security training modules and critical infrastructure cyber range (*Cyber Security training*). These Pilot Use Cases will be further discussed on separate papers that are under preparation.

IV. Conclusion

This paper has presented the SECANT project and its approach to tackle cyber threats coming from the unprecedented number of changes in the healthcare sector in recent years: the new models of remote delivery, the increasing use of IoT devices acting as sensors for monitoring and diagnostics; and the low levels of security awareness.

SECANT will deliver to all actors and stakeholders involved in the healthcare value chain a novel, flexible and scalable risk assessment platform for all types of healthcare supply chain organizations and businesses; a platform offering tools to provide cybersecurity and privacy enhancing services, holistic risk analysis and treatment, trust and accountability, as well as security training for experts and non-expert users. Ultimately, SECANT will contribute decisively towards improving the readiness and resilience of the organizations against the crippling modern cyber-threats, increasing the privacy, data protection and accountability across the entire interconnected ICT ecosystem, and reducing the costs for security training in the European market.

Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 101019645.

References

[1] S. Boddy and J. Shattuck, *The Hunt for IOT: The Growth and Evolution of Thingbots Ensures Chaos*, F5 Labs, Seattle, Washington, USA, 2018.
[2] G. Cleary, M. Corpin, O. Cox, H. Lau, B. Nahorney, D. O'Brien, ... & C. Wueest, *Symantec internet security threat report*, 2018.
[3] *2021 HIMSS Healthcare Cybersecurity Survey Report*, January 2022. Available at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey
[4] *Black Book Market Research. State of the Healthcare Cybersecurity Industry*, October 2020. Available at: https://blackbookmarketresearch.com
[5] L. Irwin, *List of data breaches and cyber attacks in June 2020 –– 7 billion records breached*, June 2020. Available at: https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-june-2020
[6] Statista, *The Internet of Things IoT units installed base by category from 2014 to 2020 (in billions)*
[7] ECSO, *Healthcare Sector Report: Cyber security for the healthcare sector*, March 2018. Retrieved from https://www.ecsorg.eu/documents/uploads/healthcare-sector-report-032018.pdf
[8] NCC Group, *Research Insights*, March 2018. Available at https://www.nccgroup.trust/uk/about-us/resources/research-insights-us-healthcare/
[9] https://www.misp-project.org/
[10] https://www.sancus-project.eu/
[11] https://www.dogana-project.eu
[12] IBM, *2018 Cybersecurity Trends in Healthcare*, March 2018. Available at https://www.ibm.com/blogs/insights-on-business/healthcare/2018-cybersecurity-trends-healthcare/
[13] K. Arapi (2018). *The Healthcare Industry: Evolving Cyber Threats and Risks*, Doctoral dissertation, Utica College, 2018
[14] Krawczyk H, Bellare M, Canetti R. *HMAC: Keyed-hashing for message authentication*, 1997.
[15] Bethencourt J, Sahai A, Waters B. *Ciphertext-policy attribute-based encryption*, 2007 IEEE symposium on security and privacy (SP'07). IEEE, 2007: 321-334.
[16] Goyal V, Pandey O, Sahai A, et al. *Attribute-based encryption for fine-grained access control of encrypted data*, Proceedings of the 13th ACM conference on Computer and communications security. 2006: 89-98.
[17] Boneh D, Crescenzo G D, Ostrovsky R, et al. *Public key encryption with keyword search*, International conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2004: 506-522.
[18] Curtmola R, Garay J, Kamara S, et al. *Searchable symmetric encryption: improved definitions and efficient constructions*, Journal of Computer Security, 2011, 19(5): 895-934.
[19] Liang K, Au M H, Liu J K, et al. *A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing*, Future Generation Computer Systems, 2015, 52: 95-108.
[20] Liang K, Au M H, Liu J K, et al. *A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing*, IEEE Transactions on Information Forensics and Security, 2014, 9(10): 1667-1680.
[21] Juels A, Ristenpart T. *Honey encryption: Security beyond the brute-force bound*, Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin, Heidelberg, 2014: 293-310.
[22] Kaliski B. *PKCS# 5: Password-based cryptography specification version 2.0*, 2000.
[23] Nifakos, S., Chandramouli, K., Nikolaou, C.K., Papachristou, P., Koch, S., Panaousis, E., Bonacina, S. *Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review*, Sen- sors 2021, 21, 5119. https://doi.org/10.3390/s21155119.
[24] Zakim D, Brandberg H, El Amrani S, Hultgren A, Stathakarou N, et al. *Computerized history-taking improves data quality for clinical decision- making—Comparison of EHR and computer-acquired his- tory data in patients with chest pain*. PLOS ONE 16(9): e0257677, 2021, https://doi.org/10.1371/journal.pone.0257677
[25] Brogan, J., Baskaran, I., & Ramachandran, N. (2018). Authenticating Health Activity Data Using Distributed Ledger Technologies. Computational and Structural Biotechnology Journal, 16, 257-266.
[26] Hawig, D., et al. (2019). Designing a Distributed Ledger Technology System for Interoperable and General Data Protection Regulation–Compliant Health Data Exchange: A Use Case in Blood Glucose Data. J Med Internet Res, 21(6).
[27] https://www.mdpi.com/1424-8220/20/2/483