Medical and Biological Cybernetics

DOI: https://doi.org/10.15407/kvt212.02.052

KATRAKAZAS P.[1], Ph.D.,
Research Area Manager,
https://orcid.org/0000-0001-7433-786X, e-mail: p.katrakazas@zelus.gr
KALLIPOLITOU Th.[1],
Delivery Manager & Sustainability Expert,
https://orcid.org/0000-0001-5059-4909, e-mail: d.kallipolitou@zelus.gr
KALLIPOLITIS L.[2],
Chief Technology Officer,
https://orcid.org/0000-0002-5689-298X, e-mail: lkallipo@aegisresearch.eu
SPAIS I.[2], Ph.D.,
Senior Project Manager,
Researcher ID: 0000-0002-6167-3247, e-mail: hspais@aegisresearch.eu
[1] Zelus P.C.,
Tatoiou 92, 14452, Metamorfosi, Athens, GR
[2] AEGIS IT Research GmbH,
25 Humboldt Str. Braunschweig, 38106, Germany

ANALYSIS AND DEFINITION OF NECESSARY MECHANISMS TO ENSURE THE SECURITY AND PRIVACY OF DIGITAL HEALTH DATA UNDER A CYBERNETIC DIGITAL INVESTIGATION FRAMEWORK

Introduction: *The recent scale-up of events caused after the Covid-19 pandemic and its subsequent healthcare crisis, highlights the digital forensics importance in a connected health ecosystem. It is therefore safe to assume that there is a growing interest in digital forensics and how they are applied within the existing healthcare ecosystem and under which concept, posing the main research question of the current study.*

The purpose of the paper *is to focuse on defining and developing the necessary mechanisms to ensure the security and privacy of the data disseminated by existing research in both fields of digital health and cybersecurity. A cybernetics-inspired framework is structured based on existing practices and key gaps identified.*

Results: *Five electronic databases, namely Scopus, IEEEXplore, PubMed, DOAJ (Directory of Open Access Journals and arXiV were identified as the main data sources. A State-of-the-Art analysis has been performed to realize the limits of the devices and the machines (including the systems and their elements involved) in the healthcare domain, when these break down so that the investigation will teach us something new that is nontrivial. A highly relevant dimension in our*

approach for a digital forensics driven connected health landscape is based on rigorous and comprehensive feedback take-off methods, which are seemingly lacking.

Conclusion: *The main point of our study is to show that while there might seem an immense multiplicity, a unity can be formulated and vice versa: where something appears as a unit, an unbounded plurality of conditions might be enclosed within it. Moving into a connected health future should be built upon existing accidents so as to mark the upcoming changes that would affect such a system.*

Keywords*: connected health, digital forensics, connected health, cybernetic digital investigation framework, cybersecurity.*

INTRODUCTION

The COVID-19 health crisis and the recent scale-up of events which was accelerated by this healthcare crisis, highlighted the digital forensics importance in a connected health ecosystem. It is therefore safe to assume that there is a growing interest in digital forensics and how they are applied within the existing healthcare ecosystem and under which concept, posing the main research question of the current study.

Digital forensics refers to the practice of amassing and arranging any information found on any type of electronic device for investigative purposes. This area of forensic science is comprised of four key areas: host-, mobile-, network- and cloud-forensics. Each of these four areas provides different types of information, with very little overlap [4]. In brief, host forensics refers to the forensics encompassing everyday devices (e.g., desktop personal computers, servers, and non-specialized sources of data), mobile forensics deal with mobile devices, network forensics refers to the practice of examining information coming from a host or entire network and cloud forensics entails the analysis of cloud services and infrastructure data sources.

Connected health as a definition falls under many fields, where the use of the Internet, sensor and sensing mechanisms, communications, and data analytics are employed towards the support of medical and health-related applications, systems, and engineering technologies [1]–[3]. According to the IEEE IEEE/ACM Conference on Connected Health Applications, Systems, and Engineering Technologies conference "*Connected health is at the convergence of multiple domains and technologies and helps to shape foundational improvements to health delivery. It will revolutionize preventative health and personalized medicine, providing rich medical information never-before available to individuals while driving down healthcare costs.*"

From a definitions' perspective, connected health relies in the digital forensics' investigative mechanisms to assure the integrity, security and privacy mechanisms in medical-related information. Conversely, digital forensics solidifies the connected health framework in terms of preventive capabilities versus cyberattacks and data, device, network corruption and abruption events that would otherwise weaken the offered services.

Therefore, the main research question guiding this study is whether intelligence obtained by both fields has been inter-exchanged and how it has been applied. This targeted approach will allow the evolving on novel and well-defined research foundations in the areas of robust and resilient healthcare systems, explainable and interpretable digital forensics solutions and verifiable

and validated evidence-based discoveries to offer data-driven insights and guidelines for two targeted high-impact domain interventions: acceleration of a trustworthy scientific stimulation towards connected health landscape and to enhance the degree of autonomy and accurate data-driven and research-based methods on cybersecurity event-/fault- detection and prediction that engages the constant incorporation of user-refined domain knowledge.

PROBLEM STATEMENT AND SUGGESTION OF A CYBERNETICS DIGITAL INVESTIGATION FRAMEWORK

The lack of access to open, secure, interoperable, and transparent health data hubs poses significant obstacles to researchers and innovators, such as, SMEs, and healthcare stakeholders towards the deployment of trustworthy data analytics workflows for synthetic data generation, data anonymization and AI modeling in order to promote wellbeing, diagnosis, disease prevention, progression and treatment. This has led to an emerging need for the development of advanced secure cryptographic protocols, high-quality synthetic data generators and data anonymization methods resilient against re-identification attempts, to enable innovators deploy their AI-powered workflows, in a secure way, across decentralized health data hubs. The reduced amount of available training data highlights the emerging need for the development of high-quality synthetic data and robust generative models to address the challenges of today, such as, data confidentiality and data augmentation. Furthermore, the in-applicability of secure, cryptographic techniques [5] that can facilitate the interconnection of decentralized clinical data registries and cohorts obscure the successful deployment of (AI)-powered workflows.

As a matter of fact, the aforementioned factors have a significant negative impact in the capacity of the existing healthcare systems, where the costs and delays for treatment and re-admission are already high. In addition, although the existing data anonymization algorithms incur high levels of information loss, patient privacy is not guaranteed given that the protection of sensitive patient data is considered a fundamental right [6]. Moreover, considering the fact that the most common strategy for knowledge distillation is based on integrative data analysis from multiple dispersed clinical registries and cohorts8, the collection of sensitive data out of premises is not feasible, due to GDPR (General Data Protection Regulation) violations during the sharing of patient data. The greatest impediment to digitalization, according to many organisations, is a lack of cyber-security. Protection, detection, reaction, and investigation are all security functions. Cyber-attack investigation is critical because it may aid in damage reduction and the development of future preventative strategies. Cyber-attack investigations have advanced more than ever before, utilising a mix of intelligence technologies and digital forensics methods. Intelligent tools are just useful when previous information of the software and techniques employed in the cyber-attack is available, i.e., they are not attack-agnostic. As a result, the quantity of never-before-used software and methods used is inversely related to the usefulness of these intelligent instruments. However digital forensic techniques do not have this problem, they lack the capacity to give comprehensive support for a cyber-attack investigation. The reason for this is

because the inspection and analysis stages of the processes, when the real research takes place, are lacking in specifics [7].

This forensic preparedness may be attained by identifying the components and connections that can be employed together. Senior management engagement, training, as well as staff awareness, organisational commitment to forensics, forensic analysis inclined corporate culture, enforcement of suitable forensic policies, and continual analysis as well as optimization of system operations are all suggested by the introduction of a new framework suggested within this paper.

The framework may be used to put up a forensic preparedness capacity for organisations which do not already have one. Organizations can use different factors to find the most important items to consider. Furthermore, the model's links illustrate how the elements discovered contribute to the intended forensic preparation. This architecture may also be adapted and used on a large scale in industry to assure forensic preparedness. This approach also emphasizes the advantages that businesses may get by becoming forensically ready. Organizations may then become compatible with established rules, manage digital evidence responsibly, and respond forensically to issues that arise. The characterization of the desired objectives helps decision-makers in the company make better informed decisions about the advantages of forensic preparedness. The framework for organisational preparedness will guarantee that forensic readiness can be swiftly integrated into a variety of organisational structures. Because of the framework's versatility, forensic preparedness may be built in a variety of organisational sizes.

The work presented here focuses on defining and developing the necessary mechanisms to ensure the security and privacy of the data disseminated by existing research in both fields of digital health and cybersecurity. The framework highlighted in Section 4 is inspired by existing practices and key gaps identified in the investigated papers. Security properties should focus on the integrity, confidentiality, and availability of data at rest, during transport and processing. The techniques and mechanisms that will be used for this purpose may include encryption, access control based on roles and attributes, with privacy-related features integrated into the respective authorization policies. Powerful confidentiality and authentication mechanisms may cover communications between platform peripherals and backend instances. Light mechanisms should be used where needed, based on the analysis of the relevant features and gaps of existing components. In addition to data anonymization techniques, differential privacy and selective blackout and randomization of data techniques can be explored to provide a certified image of the system security stance via assets modeling and security/privacy assessment performed considering their operations to ensure that any omissions/security bugs/potential vulnerabilities are identified and corrected prior to final release of an asset.

METHODOLOGY

Data Sources, Search Methodology and Analysis.

Five electronic databases, namely Scopus, IEEEXplore, PubMed, DOAJ (Directory of Open Access Journals and arXiV were identified as the main data sources. The search was conducted using the defined terms (“digital forensic*”

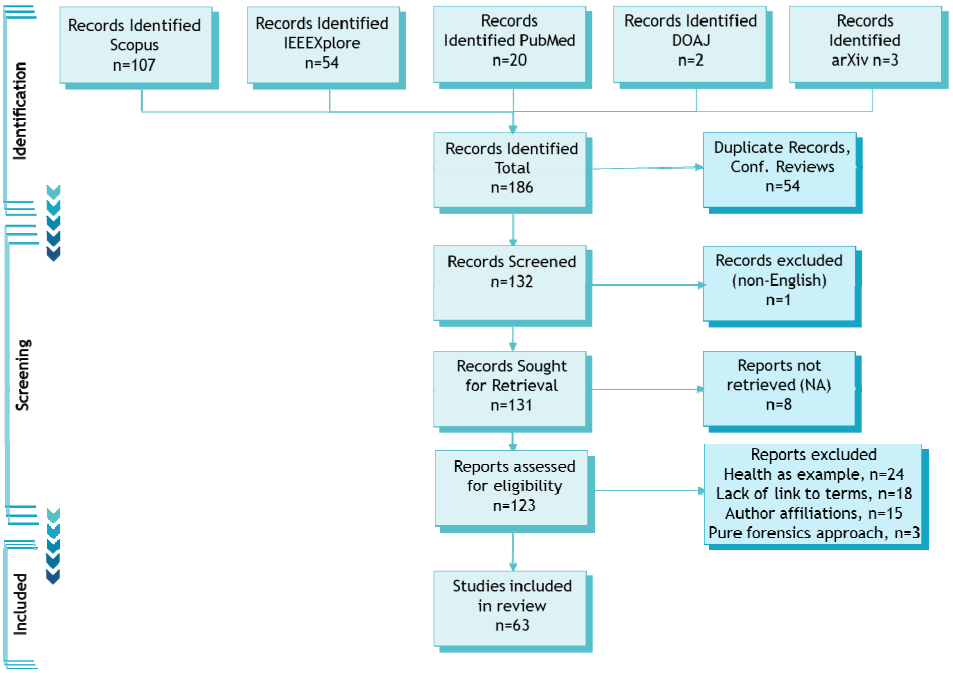

Fig. 1. PRISMA Flowchart of the selection of papers

AND "health*") in the search field of each of these electronic databases. The time frame was set from 2011 to 2021. No other restrictions were applied.

The PRISMA guidelines [8] for conducting a systematic literature review were followed after obtaining the results from all the aforementioned databases. The availability of the articles was defined by the access provided by the HEAL (Hellenic Academic Libraries Link) framework. After an initial analysis of the title and the abstract text of each article, a full-text review was performed on the remaining papers.

This study identified articles which were irrelevant to the field of applying digital forensics in healthcare, so they were also removed. The main reason behind the majority of the records not being eligible to be part of the reviewed corpus (n = 24), was the reference of the term "health" or "healthcare" superficially, e.g., only by-name. Other reasons were the mentioning of either "digital forensics" or "health" in the affiliation of the authors (n = 7 and n = 8 respectively), a pure forensics approach (n = 3) and superficial mentioning of both terms without interconnecting them (n = 18). The chosen articles composed the corpus of this review (n = 63). A final full-text analysis was then performed on each of them, to assess them based on the research question. The results are shown in Figure 1.

Study Selection and Characteristics. The final list of the chosen articles was thoroughly studied to extract their main characteristics, concentrating on whether digital forensics applicability in the healthcare field is provided and towards which area (namely, host-, mobile-, network- or cloud-forensics). The articles presented hereinafter are divided into their relevant forensics field. Articles failing to fit one the aforementioned areas, yet relevant to the research question, will be described under a generic category section.

Host-forensics in Healthcare. Host forensics refers to the process of recognizing, conserving, and examining evidence of attacks in order to identify the perpetrators and document their actions with enough credibility to justify appropriate technological, business, and legal responses. In cases involving multiple hosts and various data sources, it is crucial to collect and analyze health-related data and their artifacts to provide a comprehensive forensic perspective. This is important as data from multiple sources, such as applications, may be used for synchronization and cross-checking.

In [9] the authors test various methods for the analysis (memory, timeline and live analysis) on an up and running machine which fell victim to a targeted attack scenario with a phishing e-mail in a healthcare organization. Authors identified that the trade-off between the various methods highlight that memory should precede the live and final analysis in such cases.

Work in [10] focused on the Picture Archiving and Communication System, to create a baseline of healthcare-wide Threats and Security Objectives, along with suggestions for a guideline for selecting suitable Security Assurance Requirements. Providing a step in the complete cycle of certification under Common Criteria for the healthcare sector.

Protection of decision-relevant data in a generic "doctor-in-the-loop" setup is presented in [11], against manipulations targeting the underlying database in closed-source database management systems. One of the limitations identified in their approach though is that it only works with databases management systems that actually provide transaction safety or data replication and their associated mechanisms.

Authors in [12] present the lessons learned and guidelines for an effective and efficient e-governance structure as implemented in Estonia from a privacy and data control perspective in terms of confidentiality, integrity and availability towards establishing a strong link between privacy and information security in the adoption of smart healthcare at an e-society level.

A conceptual forensic-by-design framework is presented in [13], addressing specific technical and procedural implemenations in nine design and development stages (namely risk assessment, forensic readiness, security-, privacy-, medical-, safety-, software and hardware- requirements, relevant legislation and relevant regulations) for medical cyber-physical systems.

Work in [14] focused on the forensic analysis of software log files, with the intent to improve the quality and adequacy of user activity log files for promoting user nonrepudiation. The research of the author was intended to provide a means to help measure the adequacy and usefulness of activity log file content for forensic analysis and provide forensic-ability metrics as a standard check for software developers to proactively strengthen user activity logging mechanisms to counter repudiation threats.

A holistic anatomy of ransomware attack and assets connected to the hospital network that attack can target to get access and spread malware was investigated in [15], The authors explored vulnerabilities in MRI scanners in Lebanese hospitals, where the attack vectors in which attacker can use to reach the assets were marked and presented for future reference.

Authors in [16] discuss the need for integrating digital forensics into various scenarios involving healthcare providers, point towards the adoption and raise

awareness and prompt discussion surrounding the implementation and use of digital forensics tools, techniques and standards in the medical domain.

A comparison of encryption algorithms for a multipurpose smart card (including the healthcare scenario) is presented in [17]. The authors identified that the elliptical curve cryptography (ECC) algorithm is more suitable than the RSA algorithm for biometric verification and high-speed features. In another perspective, the same authors investigated combinatory algorithms [18] for enhancing the security by proposing an optimized encryption system for the multipurpose smart card.

Authors in [19] discussed the implications for infrastructure forensic readiness in the context of electronic medical record systems and examined several systems, identifying in most cases the lack of a sufficient level of forensic logging capabilities required to assist investigations focusing on privilege abuse. To address this, they proposed an architecture that incorporates an intelligent real-time artifact identification module which can be deployed alongside the EMS and be integrated into cloud forensic logging service.

A blockchain-based forensics-by-design framework for medical devices is proposed by the authors in [20] to manage the access to Internet-of-Medical-Things devices and relevant medical data. The authors worked with the granularity of access and forensics-by-design principles in mind, identifying at the same time the limitations of their work (i.e., integration of key management's services into the framework and its extension to other certificate-less credential management systems).

Authors in [21] discuss the IoT devices' security and forensics aspects, highlighting threats and communication technologies and challenges across the different layers. The authors highlight the need for adopting real-time approaches in the healthcare field among others, where IoT devices might pose life and health risks apart from the sensitive information aspects.

A data retrieval strategy in linearly scalable high-performance NoSQL database was shown in [22]. The authors presented a security analysis model while retrieving the stored e-health data, which were fragmented over multiple servers based on sensitive attributes and their sensitive association. The proposed model was tested in a set of experiments with an efficient query evaluation keeping intact the confidentiality of patients' sensitive attributes.

Authors in [23] proposed an experimental analysis of the quality of Pixel Non Uniformity (PNU) in residual noise of images taken with Scanning Electron Microscope (SEM), to explore the possibility to use a digital forensics technique for source camera identification even with device different from digital cameras. Their experiment showed that the PNU in images taken from SEM devices is less effective for this purpose.

Anthropometric surveying using 3D body scanning was examined and discussed in terms of privacy and security aspects [24]. The authors point that if the issues of data privacy cannot be satisfactorily resolved there may be problems carrying out anthropometric surveys successfully, especially in countries or cultures where modesty is highly valued.

Mobile forensics in Healthcare. Wireless devices are commonly used in healthcare to gather, save, access, present, and send patient data. This enables healthcare professionals to receive and send information immediately while

attending to the patient. However, these portable devices are prone to risks and weaknesses, making it harder to keep patient data secure and maintain their privacy, especially as mobile communication becomes more prevalent in the healthcare industry.

In [25] the authors investigated whether the digital traces from the Apple's Health App can be used for evidential purposes, based on the accuracy of number of steps and distances registered under various walking and running conditions, so as to make a probability statement about different routes that may have been travelled in a case. The authors conclude the health applications can have evidential values

In [26] several popular mHealth applications were analysed in terms of the user activities, their location information and activity timestamps, allowing and facilitating the reconstruction of the users' whereabouts. The authors imply that their findings could be outdated given the new and continuously updated version of these and other mHealth applications and suggest the inclusion of additional artefact categories for the mHealth forensic taxonomy model they proposed.

In [27] examination and development of a disease management programme enhanced with digital forensics capabilities to support people with long term conditions who are cyber-victimised. In this study, a mobile application is adopted as a client-server model for reporting digital evidence of online harassment and stalking, to highlight the need and the means towards collecting and preserving cyber-victimisation incidents.

In [28] the authors investigated two smartwatches, the Samsung Gear 2 Neo and LG G with regards to their forensic analysis. It was shown that useful artifacts can be recovered from the phone of the associated smartwatch, including the set-up date, applications on the watch, timestamps of updates performed, and voice memos that were recorded on the watch, with the Samsung Gear 2 Neo being more forensically sound than the LG G smartwatch.

Authors in [29] forensically focus on the potential of recovering residual data from Android medical applications, with the objective of providing an initial risk assessment of such applications. Their research highlighted that certain smartphone applications, which interact with medical devices, violate the Security and Privacy rules within HIPAA, allowing information to be recovered from these applications including a patient's personal details and their usage of the specific medical device.

The need to integrate mobile devices in terms of increasing the mHealth related cybersecurity education is presented in [30] and their attempts to strengthen their importance via active learning activities, which are meant to be nurtured as skills by future graduates that enter the cybersecurity and digital forensics market.

A study on mobile health and fitness applications from a digital forensics point of view is shown in [31]. The authors argue that they have a more granular approach and better explanation to the content of the geographical data acquisition from these applications, as well as the necessity of the different types of artifacts that are helpful to investigators, so the latter can efficiently find specific pieces of information related to a case.

Work in [32] aimed to evaluate and compare the effectiveness of five base-level classifiers and four ensemble methods in classifying and predicting daily living activities from a wearable accelerometer mounted. The results were

evaluated using precision, recall, and F-measure and indicated that most ML techniques took a reasonable time to build the prediction models.

Medical Internet of Things devices were tested as far as their hijacking attack vulnerability was concerned in [33]. The devices susceptibility to this type of attacks was validated, however limitations were also identified in terms of attackers' proximity to the devices, lack of verification mechanisms on behalf of the device manufacturer's side and lack of confirmation prompt on behalf of the connected smartphone victim-user.

Authors in [34] confirmed the amount of artifacts and data wealth that can be extracted from wearable devices in terms of file names, device users and health-related information. The authors propose that there is a need to study a method for obtaining optimal root privileges for each wearable device, while printed circuit board analysis should be performed for hardware-based data acquisition.

Analysis of three common fitness trackers was performed in [35], where the authors proposed a toll with resulting graphs and tables that can be used in forensic work, highlighting the benefits of such an analysis of fitness trackers for judicature procedure.

A forensic analysis on wearable devices was performed in [36], where several digital forensic software toolkits (namely the FTK Toolkit, Autopsy, GoldenCheetah and FitSDK) were tested in terms of data extraction, interpretation, accuracy and validity.

User data privacy concerns were evaluated in a Fitbit Versa 2 wearable device in [37]. The authors identified that GPS data, health-related information and credit card credentials were easily accessible and stored in plaintext, raising special attention to information pertinent to law enforcement.

Fitness tracker forensics were also examined in [38] along with possible scenarios on how these could be used in hypothetical scenarios in terms of health-related data. As per the previous studies, the authors suggest that analysis of various devices should take place to perfect the data extraction techniques and provide a crucial information source to forensic investigators in related cases.

Authors in [39] proposed a crowdsourced secure logging scheme, which they emulated and then validates its feasibility and efficacy, where the smart devices in the vicinity of the wearable sensor record its communication and ensure its contextual correctness in a lightweight manner, acting as witnesses to the transaction of the sensor.

34 m-health applications were investigated in terms of digital evidence taxonomy in [40]. Important metadata were identified in each lnternet-of-Things layer investigated including the type of activity, location (altitude, longitude and altitude), web bookmarks, DNS query and timestamps, elements able to facilitate evidence correlation.

A reverse engineering and security assessment of three hospital and five stock-and-trade Android applications was performed in [41] with open source tools, towards a mobile forensics investigation and mapping of their vulnerabilities. The authors highlight the need for app developers to become aware and follow best practices for dealing with security and privacy issues of the users.

Network-forensics in Healthcare. The main focus of network forensics is to examine and study all the packets and events that occur on a network, with the goal of detecting any abnormalities or events that could indicate a potential digital attack or

threat. In the healthcare industry, data is particularly sensitive, and log and management files can contain valuable evidence. Therefore, the development of forensic investigation tools has been directed towards utilizing this information in order to effectively investigate and analyze potential threats or attacks.

Study [42] examines a filtering approach to identify a DDoS attack in the Covid-19 era, to efficiently differentiate flash crowd traffic from DdoS in a healthcare network. The authors used statistical methods over a simulation scenario, where the results showed that the proposed approach has precision value, true-negative value, and negative predicate value greater than 95%, indicating the high efficiency of their approach.

The authors in [43] propose a link-pair selection algorithm for choosing an optimal link pair as a baseline for subsequent channel state information (CSI) processing. This was tested on an environment- and scenario-adaptive indoor intrusion detection system with commodity Wi-Fi devices. Its performance was evaluated in real-world scenarios, applying to patient monitoring and elderly healthcare monitoring.

The work in [44] introduces an autonomous log storage management protocol with blockchain mechanisms and access control for an Internet-of-Things (IoT) network, which can be applied to Wireless Body Area Networks (WBAN) for smart healthcare, where wearable sensors encrypt health data before sending it to the coordinators and the healthcare provides for specific services.

IoT Forensic and real-time investigation aspects are brought into the spotlight in [45] where the concept of an IoT environment including its entities and their characteristics, along with their security challenges are discussed. Examples from healthcare sector cyber-attacks are discussed towards the need of having a real-time elements approach in dealing with them.

Authors in [46] compare the state-of-the-art consensus algorithms and communication protocols in IoT blockchain network systems, which are increasingly adopted in the healthcare industry, in order to ensure security, regulation and development policies, which are currently lacking in such networks.

A conceptual design for a cost-effective digital forensic readiness framework in wireless medical networks is presented in [47]. The authors aimed to design an easily implementable and to-be-integrated artefact with Pi-drones into existing wireless networks in the healthcare sector, cross-checking its efficiency and effectiveness by experts who evaluated it. Work in [48] was basically a republishing of [47] with the addition of the design science research paradigm on which the authors based their framework and their consequent findings.

Authors in [49] add context to privacy information access by proposing a new method to realize context constraints and reduce the risks related to privacy disclosure. Their aim is to give an understanding of medical privacy according to the specific circumstances of privacy in health information systems, which provides a reference for the definition of privacy in the medical system.

Internet-of-Things forensics for healthcare are examined as part of the IoT forensics overview in [50], where forensic challenges, frameworks, tools, techniques and open issues and research directions are explored to extend traditional forensics into the IoT domain and stress the need for explicit IoT security regulations and standards to address the ever-growing challenges.

Authors in [51] review the current status of privacy preservation policies used in Electronic Health Records, privacy preserving data mining techniques and analysis and the prioritization to be put in the domain of developing effective and efficient protocols to increase security and privacy preservation.

Cloud-forensics in Healthcare. Cloud forensics is a complicated field that deals with the location of data and the level of access to the infrastructure that supports it. The primary goal of cloud forensics is to obtain digital forensic information from a cloud infrastructure, which involves identifying, preserving, and analyzing evidence of attacks to identify the attackers and document their actions with enough credibility to justify appropriate technological, business, and legal responses. Due to the volatility of health data and issues with data provenance, studies in this area are particularly useful in identifying current limitations and future directions for cloud forensics in healthcare.

The authors in [52] provide a privacy-preserving framework for enabling forensic analytics on encrypted physiological data on sensitive Electronic Medical Records databases no matter they are deployed in cloud service or a private data center. Their development of a generic and scalable framework for proceeding secure similarity search over high-dimensional timeseries medical data is implemented as distributed architecture because of the collocated encrypted index and database.

The authors in [53] propose a scheme focusing on two main parts authentication and role-based access control for a wearable healthcare system to ensure security for patients' data records. This is based on a hybrid cloud solution to minimize the human interaction and give patients more flexibility.

Work in [54] focuses on a user-centric data storage and sharing method in cloud-based medical cyber-physical system to protect the safety and privacy of users' I data which could protect data safety and privacy even when both cloud servers and keys are compromised. The feasibility of this system based on mobile edge computing is tested on a smartphone scenario to prove the improvement of efficiency compared with standard encryption algorithms.

A blockchain based forensic model is introduced in [55] to tackle the challenging task of forensic investigations in an IoT environment, due to the heterogeneous nature of the IoT environment coupled with the integration of the cloud and the network layer. Their proposed model allows any forensic stakeholder to verify the authenticity of the logs they are working with and ensures that innocent people are not framed up and culprits are exonerated by interested parties during a forensic investigation.

A privacy-preserving MapReduce based K-means clustering scheme in cloud computing was proposed in [56], applicable over large-scale datasets like the patients' health records, which should be upgraded in terms of appropriate privacy protection mechanisms when they are outsourced to the public cloud for clustering purposes.

Authors in [57] propose a provable data possession technique (specifically the variant 3 of ECDSA) to be digitally forensic ready, monitoring planning and formulating proactively before the occurrence of any potential security incidents in the area of healthcare data integrity scheme in a cloud environment.

The capabilities of a Raspberry Pi device were explored in [58] in terms of them being network node devices in a cloud big-data enabled healthcare environment for digital forensics purposes in regional secure data process/collect limit issues. The

authors identified both compromising factors and evidential information for securing the device for the purpose of digital forensics investigation.

Authors in [59] explored the main digital forensic challenges related to big data with cloud computing and protection of personal information (and specifically the ones applying to healthcare related data), discussing their impact and exploring problem solving solutions, including the cyber-psychology field.

A cloud-based secure logger for medica devices using the Intel Software Guard Extensions (SGX) and the Trusted Platform Module (TPM) is proposed in [60]. The authors describe the logging system to leverage the use of trusted hardware in an untrusted network and test its detection ability against various attacks attempting to modify or delete logs.

Authors in [61] propose a suite of mechanisms to enhance cloud computing technologies with more assurance capabilities, given the fact that many hospitals outsource their information technology infrastructure to services that are deployed on clouds. A number of steps including mapping laws into evidentiary requirements and targeting these into system-specific evidence descriptions are proposed.

Digital forensic investigation in terms of cyber-physical systems, expanding also in the sector of healthcare is examined in [62], where related challenges are overviewed in terms of the complications posed by the distributed properties of cloud data and the unavailability of physical access to digital artefacts.

An Internet-of-Things architecture and its four layers (perception, network, middleware and application layer) security issues along with proposed solutions are discussed in terms of cyberattacks vulnerability and security issues in [63]. Authors emphasize the need for IoT developers to take into account the different layers characteristics and communication vulnerabilities and consider arrangement on key agreement, authentication and privacy encryption mechanisms.

The biohacking capabilities were highlighted in [64] where the authors presented a Digital Forensic Investigation Process Model along with the considerations of 5G networks due to the massive use of Software Defined Networks and a guideline for forensic investigation on the Internet of Medical Things based on seven processes described on a high-level..

GENERIC LINKING OF HEALTHCARE TO DIGITAL FORENSICS

Authors in [65] extend the healthcare-related rationing practices and strategies to formulate a framework for demand management within digital forensic units related to data categorization and facilitation of comparison techniques to provide a suitable and adaptive assistance basis for digital examinations.

The Delone and Mclean Information Systems Mode 1 was used in [66] to investigate the relationship between the quality and use of health information technologies and their impact on patient care quality from a trusts, security and information privacy control perspectives. The critical importance of effective privacy and security controls was stressed out in terms of transparency, accessibility and cross-checking in terms of enhancing the patient care quality.

A research model for e-health portal adoption intention in terms of privacy and security perspective was analysed in [67] with the twofold intention to increase transparency of information practices, which may increase users' trust and confidence in using new health technologies, such as portals and to provide protection of e-health portals in terms of potential cyberattacks.

Authors in [68] present a metadata analysis informed by digital forensics and trace ethnography to model the overlapping temporal, format-related, and annotation characteristics present in a corpus of repair manual files, in a crowdsourced effort during collaborations between volunteer archivists and professional technicians.

Authors in [69] present a practice for hiding doctor reviews using computed tomography images, keeping medical records unchanged and only, if necessary, accessed by authorized persons, ensuring both patient's privacy and the right treatment without the attention of third parties/attackers.

Work in [70] focused on introducing the Majura schema, a pornography/child exploitation material annotation schema specifically designed to support collaborative development of machine learning tools and techniques to assist digital forensic investigators exposed to child exploitation material and in order to protect their mental health from repeated exposure to such material. A three-stage classifier was trained and validated on data from multiple, isolated, 'real world' criminal cases was built and its performance on multiple, thematically distinct corpora including a completely separate case was documented.

A similar approach was followed in [71] where the authors compared the psychological well-being and coping mechanisms of law enforcement personnel involved either as investigators and/or examiners in child pornography cases. The author stresses out the need for a meaningful support to those individuals and the provision of mental health services to them, without creating a fear of stigmatization.

AGGREGATED RESULTS

As we can see from Table 1, most digital forensics research in the healthcare field lies in the mobile- and host-forensics field, with 17 and 16 number of research studies conducted respectively. Cloud and network forensics in healthcare follow with 13 and 10 studies each, while seven studies fall out of these domains although linking healthcare and digital forensics in their core study.

LIMITATIONS IN CURRENT PRACTICES

A significant number of limitations as identified in the corpus of this study indicates how current digital forensics are struggling towards creating a robust and safe-proof environment for the healthcare ecosystem and the associated healthcare services continuum.

Most studies have either not tested their proposed frameworks or data investigation mechanisms in an outside-of-the-laboratory environment (70% of total studies), which provides ground for fake news given the "unrealistic"

Table 1. *Aggregated List of Studies in Review per category*

Digital Forensics Category	Number of Studies
Host Forensics	16
Mobile Forensics	17
Network Forensics	10
Cloud Forensics	13
Generic Category	7

Table 2. *Application settings of Corpus Studies*

	Studies	Total
Simulations or Lab Environment	[9], [17], [18], [25], [26], [29], [31], [33]–[36], [39]–[42], [56], [58], [60], [69]	19
Conceptual Framework	[10], [11], [13], [14], [16], [19]–[22], [24], [27], [45]–[53], [55], [61]–[64]	25
Real-Case Applied Framework	[12], [15], [23], [28], [30], [32], [37], [38], [43], [44], [54], [57], [59], [65]–[67], [68, p. 19], [70], [71]	19

environment their results are based upon, while only 30% have been either used or tested their approaches in real-case applications or actual settings, as shown in Table 2. This challenge however is tackled by the fact that 42.8% of the studies were published/conducted over the last two years (2020 and 2021) where the Covid-19 pandemic was at its peak. Another positive aspect identified is that the majority of the real-case application-related studies (10 out of 19 studies, 52.8%) was conducted or published on the same period, showing that there was an increased interest in the application of digital forensics in actual healthcare settings and environments.

Another issue identified is the limited application field of the investigated items in healthcare. As indicated in the Introduction section, several issues related to digital forensics gain attention, like the use of deepfakes [72] or the need for biometric authentication system in health monitoring systems based on bio-signal processing so as to prevent health fraud scam [73]. However, there is not a bird eye's view of how digital forensics can actually help a connected health future. While many authors recognize that healthcare organizations face many different challenges, including the adaptation to new and existing regulatory standards, shifting technology landscapes, and the new realities introduced by Covid-19, facing the challenge of managing the potentially devastating effects of cybersecurity attacks is taken in an isolated and idealistic manner in most cases.

For example, identifying the vulnerabilities of fitness trackers, smartwatches and health applications monopolized the interest of authors in the mobile-forensics area (14 out of the 17 identified studies). Although all approaches are valid in terms of digital forensics in the field of healthcare, their field of application is pretty limited and based on several hypotheses which do not actually contribute to the connected health vision but rather split it into its elements. This is of course by any means not a fault of the researchers but to the lack of providing a connected health framework under a digital forensics' perspective. Healthcare organizations are in need of a digital forensics solution which will help them easily identify how cyberattacks occurred so they can quickly meet regulatory compliance and remediate the effects of security incidents as comprehensively as possible.

A crucial limitation in the state of the art is the need for a trusted setup, in the form of trusted parameters selected by a trusted third party. The last decade has therefore seen the rise of the decentralized approach, starting with blockchains. While decentralization was originally oriented to developing

cryptocurrencies, it has then been generalized to smart contracts and is finding its way into an increasing number of applications. Although centralized systems have inherent limitations, poorly designed decentralized systems can easily be worse. Therefore, it makes sense to focus on understanding what kind of privacy-preserving solutions can be provided in (i) cloud and/or (ii) edge and/or (iii) decentralized architectures. To this end, a digital investigations framework for connected health should rely on provable security to design both centralized and decentralized solutions leveraging on private and trusted spaces with the goal of providing a clear picture showing to which extent one can protect security and privacy without compromising effectiveness. Another research line should also consider how to scale and adapt existing methods for secure aggregation in federated learning to the specific scenarios considered in terms of defining an object for investigation. Furthermore, designing ad-hoc secure protocols (boosting thus efficiency) for relevant functions in an on-the-fly framework is a very compelling research problem

Towards a Cybernetic Digital Investigation Framework for Connected Health. Cybernetics as a concept is a term coined to indicate a cooperative process on the control and communication aspects in the animal and the machine, based on Norbert Wiener [74]. By using a cybernetic approach, the aim is to realize the limits of the devices and the machines (including the systems and their elements involved) in the healthcare domain, when these break down so that the investigation will teach us something new that is nontrivial. The digital forensic investigators are always present, as the healthcare system includes them. And this should be a prerequisite, given the new post-Covid-19 era coming. Given that cybernetics is distinctive in accepting the ubiquity of the error and the circularity nature of the link between the actor-agent and the objects or goals in terms of action and communication aspects, creating a cybernetic digital investigation framework in healthcare employs in many ways superb models for a modern, skeptical digital forensic science based on the notion of explanations by humans and exploiting the healthcare devices and mechanisms in an agnostic manner, where cybernetics principles will serve their purposes of investigation (Fig. 2).

One additional reason for using the cybernetics concept is the pursue of a behaviorist approach, by observing and trying to account for behaviors, reflected not only in the mechanical aspects but on the human aspects as well. Through the mechanism of circularity, the elements of the actors-agents and the sub-systems alter in every change of each cycle.

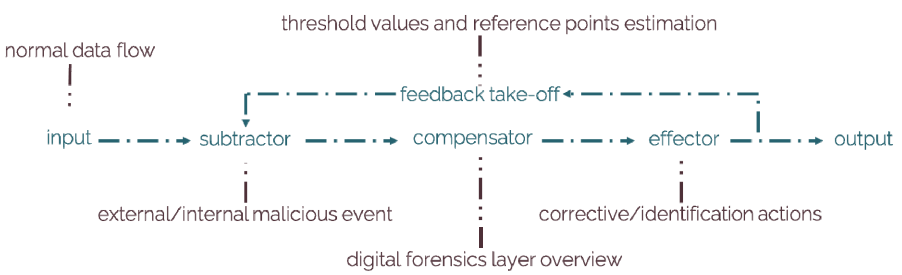

Fig. 2. Bird's Eye View of the Cybernetic Digital Investigation Framework

Thus, the behavior of each change is response to the other. In this sense, the actor-agent's progress around the circle forms a spiraling notion, leading to knowledge of who and what has been involved. Given the circularity of such system, we assume the possibility of similar behavior (or better, similar trends and behavioural patterns) in each element. That way we can correct the error, by creating a pattern as we correct them, extrapolating from several specific cases to develop a general understanding through which to identify or even modify the actors' behavior, we exhibit learning and we modify our learned behavior by continuing to test for errors and adapting accordingly, continuing the learning process.

A highly relevant dimension in our approach for a digital-forensics driven connected health landscape is based on rigorous and comprehensive feedback take-off methods, which are seemingly lacking. Most of the current tools are only applicable locally and to a smaller extent failing to scale and being practical over local, national and international borders. The proposed cybernetic digital investigation framework aims at remaining healthcare-relevant by handling use-cases that come from real-world applications, where normal data flows are (or not) interrupted by either internal or external (malicious) events. Another need, arisen from the plurality of different digital forensics efforts is a unifying framework that offers features that can harness the power of the best tools and solutions available. The feedback take-off mechanism aims to carefully study and estimate the existing threshold values and reference points, not only from an academic aspect but from a practical, solution-oriented approach as well, to select the most promising ones and improve them through integration via a unified feedback and validation mechanism.

In addition, while the current frame of digital forensics is centered on its different areas, pursuing expansion over an area of research will allow a re-estimation of threshold values and reference points to build tailor-made constraint solvers through the assembly of components that is safe and trustworthy by-design. This important dimension is feedback take-off capability of developed corrective and event identification methods and actions, where their effect will be cross-checked to allow for an internal validation loop. Figure 2 depicts the envisioned framework from a bird's eye perspective.

Description and Key Concepts. Based on the primitive second-order cybernetic system and on the theory of objects which is founded on both circularity and observing, a self-observing circular system is hereinafter proposed in which observing involves a switching condition between being observed and observing. This system is inspired by the theoretical approach presented in [75], where the entities which interchange the role of (self-)observed and (self-)observing are named Objects (O). This interchange of roles generates a timeframe (t_b) and empty slots, where O is (self-)observed, meaning it is not (self-)observing, so another Object could fill the vacant (observing) slot, observing it (Fig. 3). Using temporal synchronicity logical arrangements can be established to give external observers the chance to enter both into observing and observed slots to establish relationships between (observations of) Objects, thus satisfying the prerequisite for logic, representation and communication principles as dictated by cybernetics principles.

This continuous and circular switching between (self-)observing and (self-) observed generates time, as the back and forth switching of the same Object between the slot of observing and being observed, transforms it into an oscillator (a time generator). This time of course is under relevant terms, meaning that it may span across different time scales (e.g., minutes, days or even years). As this switching leaves empty slots, the resulting vacancies may be filled by other Objects. That means that another Object can act as an external observer and may observe the previous (or another) Object. For this to happen, the two Objects must have a degree of synchronicity in order that the empty slot can be filled.

This coming together of the two oscillators allows an external observation to be made. Coming together in partial synchronicity of several oscillators allows logical relationships between the observations of various Objects. For example, if the times of observation by an externally observing Object of two other Objects is exactly the same, there is a logical identity, which may be used either to establish the relationship "same" or to have one of the two Objects "represent" the other. Therefore, the basics of observation of one Object by another, and of how Objects can be related together, become inherent in these structures named Objects.

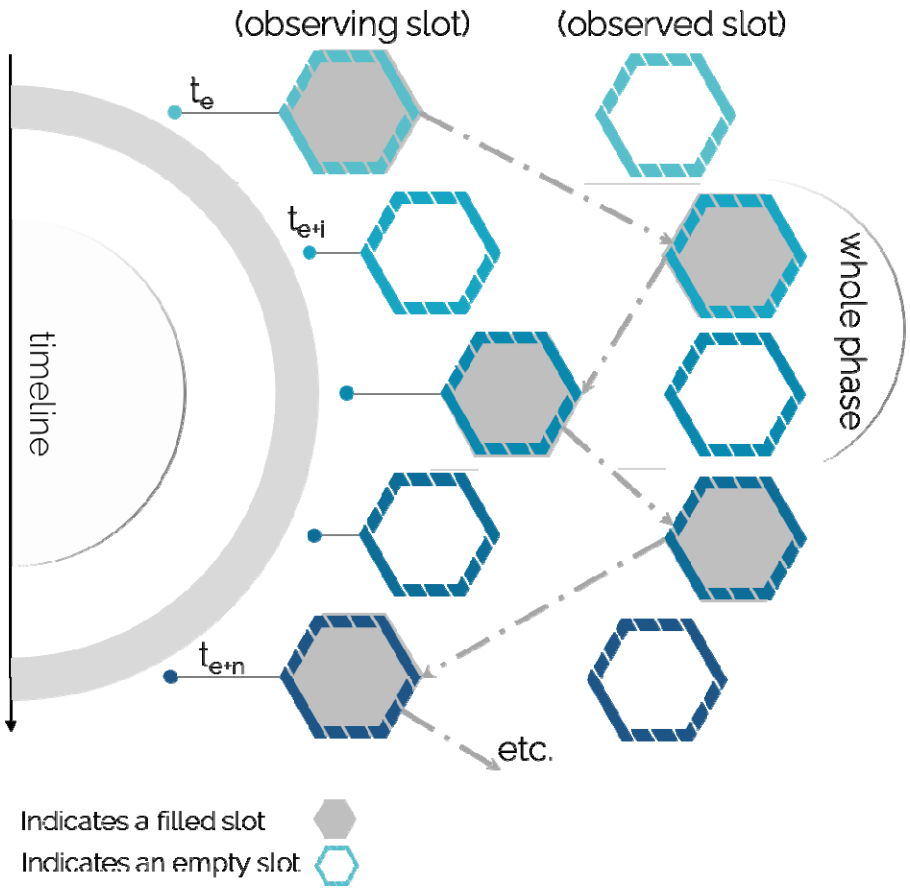

Fig. 3. Schematic Representation of an Object (adapted by [75])

A schematic representation of an Object is presented in Figure 3 (adapted by [75]). As the timeline progresses from top to bottom, a grey slot indicates that it is "filled" by an Object, while a white one that it is vacant. The sequence where a filled (self-)observing slot switches to fill a (self-)observed slot and back again is indicated by the dotted arrows. When a (self-)observed slot is empty, another Object may observe through it. A whole phase is marked when the same Object reaches for a second time the phase of being (self-)observing.

Framework Paradigm. While at a conceptual stage, the practicalities of our framework can be seen via deploying the results of the current study. Given the theoretical framework presented in the previous section, an Object in our case can be a wearable, an application, or a medical device, with the actors-agents being the digital forensic investigators, the cyberattackers and the healthcare departments. In constructing the timeline events between the entities, the main aim of the relationships and characterization of the systems would be to increase the robustfulness and trustworthiness of the healthcare system, in it offering provable security, safety and reliability guarantees.

Inspired by the limitations and challenges identified in the cloud forensics area and especially in work performed in [52], [54], [55], [61], [62] we present a conceptual architecture which can be enhanced by enabling multi-party computation (MPC) to involve the distribution of the health data across multiple nodes and authorities, where each node and authority has its own rules and data sharing policies.

While privacy relates to any rights one has to control their personal information to ensure that only the minimal information required for a computation is disclosed, security, on the other hand, refers to how these computations are protected in the presence of adversaries so that the outputs are correct according to the inputs and the functionality that is behind the computation. Instead of naively relying on signed privacy disclosure agreements, one should as much as possible protect confidential data so that it is released only during those computations that inherently need them. This is precisely the goal of the challenging submodule named "Privacy" that will include interesting research directions. The "Privacy" submodule aims at providing a satisfactory trade-off between effectiveness and confidentiality.

By deploying the suggested framework, one can leverage privacy-enhancing cryptography to protect data so that they remain available only to the owner and to the computations that strictly need them. No player in the system is supposed to obtain more information than what is strictly required for its role. Obtaining such an extreme form of data protection requires some advanced tools that go way beyond the naïve use of digital signatures and private/public-key encryption. The most relevant one is multi-party computation (MPC), but other tools as zero-knowledge proofs and differential privacy can be integrated as well. In detail:

- MPC is a cryptographic tool that consists of allowing data owners to jointly compute functions of their private data so that: (a) the outputs are correctly computed and known only to those players in the system that are supposed to receive them while at the same time they remain hidden to anyone else; (b) the confidentiality of every input used in the joint computation is preserved except for what can be inherently inferred by whoever sees the output and knew already some other inputs before the computation even took place.

- ZK-proofs: Zero-Knowledge (ZK) proofs allow the owner of some confidential data to make claims about the output of public functions of such data while keeping data confidential.
- Differential Privacy (DP) tries to go beyond some unavoidable privacy leak of MPC. Indeed, the output of a joint computation might inherently reveal too much information about the data owner. Such possible privacy breach can be mitigated using DP that aims at anonymizing data before they are used in a distributed computation. Unlike previous modules, here the impact on effectiveness is not just based on measuring the overhead in terms of performance, but also in terms of quality of the aggregated data. Indeed, when anonymizing data through differential privacy there is also a loss in data quality.

By leveraging MPC jointly with ZK, and DP the framework can produce a layer of computations over confidential data that provides resilience to adversarial behaviors both in terms of correctness of the computation and on protection of confidentiality. Again, no additional layer with such desirable features can come without cost. Therefore, focus should be given on carefully measuring the pros of confidentiality and integrity of the computations with the cons of reduced effectiveness due to loss of performance and data quality. An important parameter that should be considered is the degree of decentralization that can be achieved, considering the corresponding loss of the impact on effectiveness. Indeed, a decentralized system would minimize the use of the trusted space with the purpose of maintaining security and privacy even in the presence of a fault in the trusted space. Obviously, the computations in the trusted space would be reduced and consequently more expensive and less expressive computations among private spaces would be required.

The methodology that can be used to assess the validity of the protocols that will be constructed along with their analyses is known as "provable security". By deploying the suggested framework, we consider another methodology that is a de-facto standard in cryptography: the ideal/real-world paradigm. When adopting this methodology, the definitions consist of specifying an ideal world that is clearly invulnerable by inspection and assessing the developed methodology. Considering Objects as two dimensions to measure the quality of a computation over (possibly confidential) data. The first dimension will be the effectiveness. The second dimension will be robustness of the computation in terms of resilience to adversaries trying to compromise security and privacy. Another element that will be considered is the transparency of the system. The rise of blockchain technology has shown that transparency can be achieved while reliably computing on data. Such settings can be explored when considering decentralizations with the goal of giving weight to transparency. To further validate our approach, creation of “what if” [76] scenarios involving data controllers and processors to assess if MPC leads to GDPR avoidance, no legal benefits or there exists data protection by design (DPbD) can already be seen to “fit” the description of our suggested framework.

The application of such a framework will fundamentally change how connected health systems are engineered in the real world. The researched techniques and investigation processes will provide the highest possible degree of assurance, with the certainty of mathematical proof, while being cost-competitive with traditional

low- to medium-assurance systems. Verified research is a reality in the healthcare field thus work should be done on creating a societal shift towards mainstream adoption. To present our approach, we construct two more paradigms based on the state-of-the-art review presented here.

Paradigm I: As mentioned earlier in the Limitations section fitness trackers were investigated the most in the mobile forensics research. This gives a chance to obtain observations of an Object (a fitness tracker) from different perspectives creating at the same time a timeframe of the investigation process and establish relationships.

In more detail, we may assume as an Object (O) the Xiaomi Mi Band tracker, which was researched in three studies [34], [35], [38]. In [35], [38] the Xiaomi Mi Band 2 (O_2) is presented, while the Xiaomi Mi Band 4 (O_4) is investigated in [34]. We create two different objects (based on the different version of the tracker) so as to investigate (a) whether a whole phase has been completed and (b) whether we can deduce some relationships related to the nature of the Object. Following the principles of the theoretical framework, three actors-agents are considered: the device manufacturers (DM), the digital forensics researchers (DF) and the healthcare organizations (H) testing the device. Depicting the oscillator time points related to the Objects into the framework for a better overview (Fig. 4), we can see that:

(a) the DM point-of-view remains in the observing slot (at least for the time being in both timelines, t_2 and t_4);

(b) the DF and H perspectives create a knowledge base (observed slot) that can assist in formulating relations that may characterize both Objects;

(c) the one thing missing to complete a phase and move into the next level of the framework approach, is the integration of the results from both DF and H perspectives into the device (be it from a hardware or a software approach).

That would transit the state of the object from being observed to the observing once again, meaning that the feedback received updates its status.

As it seems, the DM perspective remains mainly in the observing slots, leaving other actors (DF and H) to assess the object and consequently initiating a reactivation of the observing slot and a new oscillation based on another or newer version of the Object.

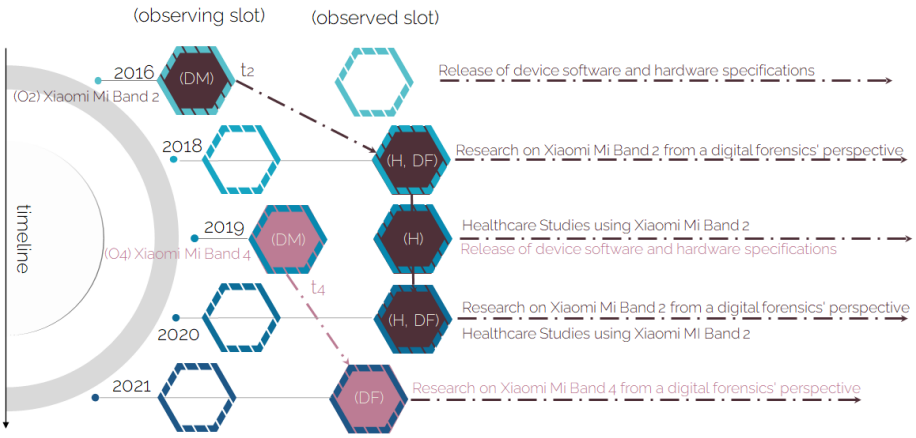

Fig. 4. An example application of the suggested framework in selected literature

This is driven by market needs and changes, customer needs and financial reasons, however it clearly shows the lack of feedback control mechanisms in the contemporary era, where actors most likely choose to start anew instead of revisiting existing products and upgrading/updating their functionalities by taking into account existing research.

Paradigm II: The previous approach stands also true when we examine the Wireless Body Area Network (WBAN) as an Object. Following the same steps with the Xiaomi Mi Band device, WBANs are examined in four studies [44], [47], [48], [53]. As all of them remain at a conceptual level and not being part of the actual healthcare system, a whole phase is still not marked, although solutions in this area might seem closer to realization as indicated in [77], [78].

These two paradigms highlight what is currently lacking in existing efforts towards connected health and digital forensics by design approaches: not only the evidence needed to support and prove the health and privacy/security aspect, but the feedback take-off needed to drive further progress in this field. These actions should be undertaken not only from the DM perspective, but also from the DF and H viewpoints in our paradigms, meaning that all involved stakeholders should be activated in order to put the relevant knowledge into meaningful evidence-based and soundproof updates and upgrades of the existing systems.

CONCLUSION

The actual integration of the suggested framework within the digital forensics and linked health joint domain has to be established. Even though the recent Covid-19 outbreak might have accelerated things, the present research revealed that there is a theoretical relationship between digital forensics and healthcare. Furthermore, the threat of fake news and widespread public distrust of pharmaceutical companies and news organisations have underlined the need for a digital forensics system of health data. Identification as well as recognition of fabricated clinical evidence, validation of clinical research results, as well as validation of medical reports, just like any housing agreement, should be the core component of such an approach, upon which integrated entities could perhaps devise a device-agnostic reliable and smart ecosystem.

The framework presented in this current research aspires to contribute through the interlinking of diverse, de-centralized Objects, as these are defined in the previous section, in a secure way, avoiding the problems of managing structural data heterogeneities. This will facilitate the connected health data interoperability and will enable the development of data modeling and advanced curation methods that will contribute to enhance the productivity of health innovators exploiting rich data and information registries, as well as the quality of services offered to the patients and relevant stakeholders. In line with the transformation of health and care in the digital single market and cross-border innovation objectives, our framework highlights and promotes the activities for contributing to providing secure mechanisms for data generation and facilitating data interoperability to address patients' safety and empowerment through data value innovation.

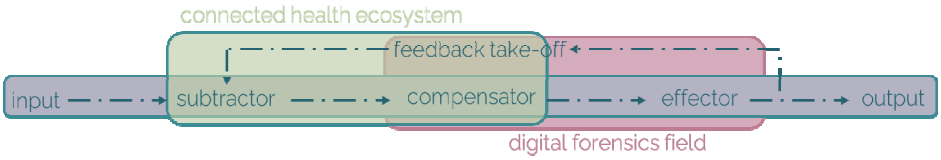

Fig. 5. Mutual Benefit Areas in Systemic Overview of Digital Forensics-enabled Connected Healthcare

This report makes the point that opportunities to gather data and give solutions are thriving. Cyberattacks might be used as a launching pad for healthcare facilities, technologies, or concepts, revealing what and how is weak and of interest to enemy groups. The primary notions represented by the suggested cybernetics digital research framework are not all that dissimilar with those of digital forensics and connected health. It is more of a little departure from the parent concepts, since its elements are drawn from the subject, than anything altogether different. A close parallelism can be shown schematically (Fig. 5) where one notion begins and the other concept finishes.

The main point of our study is to show that while there might seem an immense multiplicity, a unity can be formulated and vice versa: where something appears as a unit, an unbounded plurality of conditions might be enclosed within it. Moving into a connected health future should be built upon existing accidents so as to mark the upcoming changes that would affect such a system (Fig. 5). Isolated events of digital forensics interest should inform such a foundation in a verified and validated manner, driven by existing and future research works. Developing a comprehensive healthcare domain-informed digital forensics-driven framework for a trustworthy connected health landscape in tomorrow's smart city will enhance the intelligence and increase the degree of autonomy and safety of these systems so as to support operations of critical nature in a cross-sector manner.

REFERENCES

1. K. Colorafi. Connected health: a review of the literature. *mHealth*. vol. 2, Apr. 2016, p.13 doi: 10.21037/mhealth.2016.03.09.
2. C. Kuziemsky, R. M. Abbas, N. Carroll. Toward a Connected Health Delivery Framework. *2018 IEEE/ACM International Workshop on Software Engineering in Healthcare Systems (SEHS)*, May 2018, pp. 46–49.
3. C. S. Pattichis, A. S. Panayides. Connected Health. *Front. Digit. Health*, vol. 1, 2019, p.1 doi: 10.3389/fdgth.2019.00001.
4. C. Horan and H. Saiedian. Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *J. Cybersecurity Priv.* vol. 1, no. 4, Art. no. 4, Dec. 2021, doi: 10.3390/jcp1040029.
5. S. Kumar, A. K. Bharti, and R. Amin. Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. *Secur. Priv.* vol. 4, no. 5, p. e162, 2021, doi: 10.1002/spy2.162.
6. N. J. Podlesny, A. V. D. M. Kayem, C. Meinel. Towards Identifying De-anonymisation Risks in Distributed Health Data Silos. *Database and Expert Systems Applications*, Cham, 2019, pp. 33–43. doi: 10.1007/978-3-030-27615-7_3.
7. A. Adel. A Conceptual Framework to Improve Cyber Forensic Administration in Industry 5.0: Qualitative Study Approach. *Forensic Sci.*, vol. 2, no. 1, Art. no. 1, Mar. 2022, doi: 10.3390/forensicsci2010009.

8. M. J. Page. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, vol. 372, p. n71, Mar. 2021, doi: 10.1136/bmj.n71.
9. A. Shaaban, N. Abdelbaki. Comparison Study of Digital Forensics Analysis Techniques; Findings versus Resources. *Procedia Comput. Sci.* vol. 141, pp. 545–551, Jan. 2018, doi: 10.1016/j.procs.2018.10.128.
10. K. Hovhannisyan, P. Bogacki, C. A. Colabuono, D. Lofù, M. V. Marabello, B. E. Maxwell. Towards a Healthcare Cybersecurity Certification Scheme. Jun. 2021, doi: 10.1109/CyberSA52016.2021.9478255.
11. P. Kieseberg, B. Malle, P. Frühwirt, E. Weippl, A. Holzinger. A tamper-proof audit and control system for the doctor in the loop. *Brain Inform.* vol. 3, no. 4, Art. no. 4, Dec. 2016, doi: 10.1007/s40708-016-0046-2.
12. J. Priisalu, R. Ottis. Personal control of privacy and data: Estonian experience. *Health Technol.* Vol. 7, no. 4, pp. 441–451, Dec. 2017, doi: 10.1007/s12553-017-0195-1.
13. G. Grispos, W. B. Glisson, K.-K. R. Choo. Medical Cyber-Physical Systems Development: A Forensics-Driven Approach. *2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Jul. 2017, pp. 108–113. doi: 10.1109/CHASE.2017.68.
14. J. King. Measuring the forensic-ability of audit logs for nonrepudiation. *35th International Conference on Software Engineering (ICSE)*, May 2013, pp. 1419–1422. doi: 10.1109/ICSE.2013.6606732.
15. R. A. Nabha, H. Sbeyti. Exploiting Vulnerabilities Of MRI Scanner Machine: Lebanon Case Study. *8th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2020, pp. 1–7. doi: 10.1109/ISDFS49300.2020.9116449.
16. G. Grispos, K. Bastola. Cyber Autopsies: The Integration of Digital Forensics into Medical Contexts. *IEEE 33rd International Symposium on Computer-Based Medical Systems (CBMS)*, Jul. 2020, pp. 510–513. doi: 10.1109/CBMS49503.2020.00102.
17. M. Savari, M. Montazerolzohour, Y. E. Thiam. Comparison of ECC and RSA algorithm in multipurpose smart card application. *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Jun. 2012, pp. 49–53. doi: 10.1109/CyberSec.2012.6246121.
18. M. Savari, M. Montazerolzohour, Y. E. Thiam. Combining encryption methods in multipurpose smart card. *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Jun. 2012, pp. 43–48. doi: 10.1109/CyberSec.2012.6246120.
19. M. Chernyshev, S. Zeadally, Z. Baig. Healthcare Data Breaches: Implications for Digital Forensic Readiness. *J. Med. Syst.* Vol. 43, no. 1, p. 7, Nov. 2018, doi: 10.1007/s10916-018-1123-2.
20. V. Malamas, T. Dasaklis, P. Kotzanikolaou, M. Burmester, S. Katsikas. A Forensics-by-Design Management Framework for Medical Devices Based on Blockchain. *IEEE World Congress on Services (SERVICES)*, Jul. 2019, vol. 2642–939X, pp. 35–40. doi: 10.1109/SERVICES.2019.00021.
21. H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, G. B. Wills. Security, cybercrime and digital forensics for IoT. Intelligent Systems Reference Library. Springer International Publishing, 2019. doi: 10.1007/978-3-030-33596-0_22.
22. K. Kumari, S. Saha, S. Neogy. Cost Based Model for Secure Health Care Data Retrieval. *Security in Computing and Communications*. Vol. 969, S. M. Thampi, S. Madria, G. Wang, D. B. Rawat, and J. M. Alcaraz Calero, Eds. Singapore: Springer Singapore, 2019, pp. 67–75. doi: 10.1007/978-981-13-5826-5_5.
23. A. Bruno, G. Cattaneo. Experimental Analysis of the Pixel Non Uniformity (PNU) in SEM for Digital Forensics Purposes. *Pervasive Systems, Algorithms and Networks*. Vol. 1080, C. Esposito, J. Hong, and K.-K. R. Choo, Eds. Cham: Springer International Publishing, 2019, pp. 313–320. doi: 10.1007/978-3-030-30143-9_26.

24. S. Bindahman, N. Zakaria, and N. Zakaria. 3D body scanning technology: Privacy and ethical issues. *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, Jun. 2012, pp. 150–154. doi: 10.1109/CyberSec.2012.6246113.
25. J. P. van Zandwijk, A. Boztas. The iPhone Health App from a forensic perspective: can steps and distances registered during walking and running be used as digital evidence? *Digit. Investig.* Vol. 28, pp. S126–S133, Apr. 2019, doi: 10.1016/j.diin.2019.01.021.
26. A. Azfar, K.-K. R. Choo, L. Liu. Forensic Taxonomy of Popular Android mHealth Apps. *ArXiv150502905 Cs*, May 2015, Last accessed: Oct. 26, 2021. Online. URL: http://arxiv.org/abs/1505.02905
27. Z. A. Alhaboby. Understanding the Cyber-Victimisation of People with Long Term Conditions and the Need for Collaborative Forensics-Enabled Disease Management Programmes. *Cyber Criminology*, H. Jahankhani, Ed. Cham: Springer International Publishing, 2018, pp. 227–250. doi: 10.1007/978-3-319-97181-0_11.
28. I. Baggili, J. Oduro, K. Anthony, F. Breitinger, G. McGee. Watch What You Wear: Preliminary Forensic Analysis of Smart Watches. *10th International Conference on Availability, Reliability and Security*, Aug. 2015, pp. 303–311. doi: 10.1109/ARES.2015.39.
29. G. Grispos, T. Flynn, W. Glisson, K.-K. R. Choo. Investigating Protected Health Information Leakage from Android Medical Applications. *ArXiv210507360 Cs*, May 2021, Last accessed: Oct. 27, 2021. Online. URL: http://arxiv.org/abs/2105.07360
30. H. Chi. Integrate mobile devices into CS security education. *Proceedings of the 2015 Information Security Curriculum Development Conference*, New York, NY, USA, Oct. 2015, pp. 1–4. doi: 10.1145/2885990.2885991.
31. C. Hassenfeldt, S. Baig, I. Baggili, X. Zhang. Map My Murder: A Digital Forensic Study of Mobile Health and Fitness Applications. *Proceedings of the 14th International Conference on Availability, Reliability and Security*, New York, NY, USA, Aug. 2019, pp. 1–12. doi: 10.1145/3339252.3340515.
32. M. Akour, S. Banitaan, H. Alsghaier, K. A. Radaideh. Predicting Daily Activities Effectiveness Using Base-level and Meta level Classifiers. *7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, pp. 1–7. doi: 10.1109/ISDFS.2019.8757487.
33. T. Flynn, G. Grispos, W. B. Glisson, W. Mahoney. Knock! Knock! Who is There? Investigating Data Leakage from a Medical Internet of Things Hijacking Attack. Jan. 2020, Last accessed: Oct. 31, 2021. Online. URL: https://shsu-ir.tdl.org/handle/20.500.11875/3199
34. S. Kim, W. Jo, J. Lee, T. Shon. AI-enabled device digital forensics for smart cities. *J. Supercomput.* Jul. 2021, doi: 10.1007/s11227-021-03992-1.
35. F. Hantke, A. Dewald. How can data from fitness trackers be obtained and analyzed with a forensic approach? *IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, Sep. 2020, pp. 500–508. doi: 10.1109/ EuroSPW51379.2020.00073.
36. Á. MacDermott, S. Lea, F. Iqbal, I. Idowu, B. Shah. Forensic Analysis of Wearable Devices: Fitbit, Garmin and HETP Watches. *10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, Jun. 2019, pp. 1–6. doi: 10.1109/NTMS.2019.8763834.
37. Y. H. Yoon, U. Karabiyik. Forensic Analysis of Fitbit Versa 2 Data on Android. *Electronics*. Vol. 9, no. 9, Art. no. 9, Sep. 2020, doi: 10.3390/electronics9091431.
38. S. Kang, S. Kim, J. Kim. Forensic analysis for IoT fitness trackers and its application. *Peer--Peer Netw. Appl.* Vol. 13, no. 2, pp. 564–573, Mar. 2020, doi: 10.1007/s12083-018-0708-3.
39. M. Siddiqi, S. T. Ali, V. Sivaraman. Forensic Verification of Health Data From Wearable Devices Using Anonymous Witnesses. *IEEE Internet Things J.* Vol. 7, no. 11, pp. 10745–10762, Nov. 2020, doi: 10.1109/JIOT.2020.2982958.
40. N. Rahman, M. Thariq. A digital evidence taxonomy of m-health apps in iot environment. Jun. 2020.

41. N. Phumkaew, V. Visoottiviseth. Android Forensic and Security Assessment for Hospital and Stock-and-Trade Applications in Thailand. *15th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, Jul. 2018, pp. 1–6. doi: 10.1109/JCSSE.2018.8457347.
42. Z. Zhou, A. Gaurav, B. B. Gupta, H. Hamdi, N. Nedjah. A statistical approach to secure health care services from DDoS attacks during COVID-19 pandemic. *Neural Comput. Appl.*, pp. 1–14, Sep. 2021, doi: 10.1007/s00521-021-06389-6.
43. W. Zhuang, Y. Shen, L. Li, C. Gao, D. Dai. Develop an Adaptive Real-Time Indoor Intrusion Detection System Based on Empirical Analysis of OFDM Subcarriers. *Sensors*. Vol. 21, no. 7, Art. no. 7, Jan. 2021, doi: 10.3390/s21072287.
44. C.-L. Hsu, W.-X. Chen, T.-V. Le. An Autonomous Log Storage Management Protocol with Blockchain Mechanism and Access Control for the Internet of Things. *Sensors*. Vol. 20, no. 22, Art. no. 22, Jan. 2020, doi: 10.3390/s20226471.
45. N. H. N. Zulkipli, A. Alenezi, G. B. Wills. IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. *2nd International Conference on Internet of Things, Big Data and Security*, Oct. 2021, pp. 315–324. Last accessed: Oct. 27, 2021. Online. URL: https://www.scitepress.org/PublicationsDetail.aspx?ID=fpfedOeeepw=&t=1
46. L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, Y. Yang. A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling. *ACM Comput. Surv.* Vol. 53, no. 1, p. 18:1-18:32, Feb. 2020, doi: 10.1145/3372136.
47. A. Kyaw, B. Cusack, R. Lutui. Digital Forensic Readiness In Wireless Medical Systems. *29th International Telecommunication Networks and Applications Conference (ITNAC)*, Nov. 2019, pp. 1–6. doi: 10.1109/ITNAC46935.2019.9078005.
48. A. K. Kyaw, Z. Tian, B. Cusack. Design and Evaluation for Digital Forensic Ready Wireless Medical Systems. *IoT Technologies for HealthCare*. Vol. 314, N. M. Garcia, I. M. Pires, and R. Goleva, Eds. Cham: Springer International Publishing, 2020, pp. 118–141. doi: 10.1007/978-3-030-42029-1_9.
49. Z. Wu, X. Qi, G. Liu, L. Fang, J. Liu, J. Cui, 'An extend RBAC model for privacy protection in HIS. *6th International Symposium on Digital Forensic and Security (ISDFS)*, Mar. 2018, pp. 1–6. doi: 10.1109/ISDFS.2018.8355328.
50. M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E. K. Markakis. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Commun. Surv. Tutor.* Vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.
51. A. Kumar, R. Kumar. Privacy Preservation of Electronic Health Record: Current Status and Future Direction. *Handbook of Computer Networks and Cyber Security*, B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, Eds. Cham: Springer International Publishing, 2020, pp. 715–739. doi: 10.1007/978-3-030-22277-2_28.
52. X. Liu, X. Yuan, J. Liu. Towards Privacy-Preserving Forensic Analysis for Time-Series Medical Data. *17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2018, pp. 1664–1668. doi: 10.1109/TrustCom/BigDataSE.2018.00247.
53. E. Al Alkeem, C. Y. Yeun, M. J. Zemerly. Security and privacy framework for ubiquitous healthcare IoT devices. *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, Dec. 2015, pp. 70–75. doi: 10.1109/ICITST.2015.7412059.
54. H. Qiu, M. Qiu, M. Liu, G. Memmi. Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0. *IEEE J. Biomed. Health Inform.* Vol. 24, no. 9, pp. 2499–2505, Sep. 2020, doi: 10.1109/JBHI.2020.2973467.
55. P. Agbedanu, A. D. Jurcut. BLOFF: A Blockchain based Forensic Model in IoT. *ArXiv210308442 Cs*, pp. 59–73, 2021, doi: 10.4018/978-1-7998-7589-5.ch003.

56. J. Yuan, Y. Tian. Practical Privacy-Preserving MapReduce Based K-Means Clustering Over Large-Scale Dataset. *IEEE Trans. Cloud Comput.* Vol. 7, no. 02, pp. 568–579, Apr. 2019, doi: 10.1109/TCC.2017.2656895.
57. I. Jayaraman, A. Stanislaus Panneerselvam. A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. *J. Ambient Intell. Humaniz. Comput.* Vol. 12, no. 5, pp. 4911–4924, May 2021, doi: 10.1007/s12652-020-01931-1.
58. X. Feng, B. Onafeso, E. Liu. Investigating Big Data Healthcare Security Issues with Raspberry Pi. *IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*, Oct. 2015, pp. 2329–2334. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.344.
59. X. Feng, Y. Zhao. Digital Forensics Challenges to Big Data in the Cloud. *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Jun. 2017, pp. 858–862. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.132.
60. H. Nguyen. Cloud-Based Secure Logger for Medical Devices. *IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, Jun. 2016, pp. 89–94. doi: 10.1109/CHASE.2016.48.
61. A. Gehani, G. F. Ciocarlie, N. Shankar. Accountable clouds. *IEEE International Conference on Technologies for Homeland Security (HST)*. Nov. 2013, pp. 403–407. doi: 10.1109/THS.2013.6699038.
62. F. Khan. A detailed study on Security breaches of Digital Forensics in Cyber Physical Systems. *Sixth HCT Information Technology Trends (ITT)*. Nov. 2019, pp. 38–43. doi: 10.1109/ITT48889.2019.9075094.
63. A. Abdullah, H. Kaur, R. Biswas. Universal Layers of IoT Architecture and Its Security Analysis. *New Paradigm in Decision Science and Management*. Singapore, 2020, pp. 293–302. doi: 10.1007/978-981-13-9330-3_30.
64. J. Ibarra, H. Jahankhani, J. Beavers. Biohacking Capabilities and Threat/Attack Vectors. *Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity*, H. Jahankhani, S. Kendzierskyj, N. Chelvachandran, and J. Ibarra, Eds. Cham: Springer International Publishing, 2020, pp. 117–131. doi: 10.1007/978-3-030-35746-7_7.
65. B. Rappert, H. Wheat, D. Wilson-Kovacs. Rationing bytes: managing demand for digital forensic examinations. *Polic. Soc.*, vol. 31, no. 1, pp. 52–65, Jan. 2021, doi: 10.1080/10439463.2020.1788026.
66. V. Kisekka, J. S. Giboney. The Effectiveness of Health Care Information Technologies: Evaluation of Trust, Security Beliefs, and Privacy as Determinants of Health Care Outcomes. *J. Med. Internet Res.* Vol. 20, no. 4, p. e107, Apr. 2018, doi: 10.2196/jmir.9014.
67. V. Kisekka, S. Goel, K. Williams. Disambiguating Between Privacy and Security in the Context of Health Care: New Insights on the Determinants of Health Technologies Use. *Cyberpsychology Behav. Soc. Netw.* Vol. 24, no. 9, pp. 617–623, Sep. 2021, doi: 10.1089/cyber.2020.0600.
68. J. A. Hodges. Forensically reconstructing biomedical maintenance labor: PDF metadata under the epistemic conditions of COVID-19. *J. Assoc. Inf. Sci. Technol.*, Apr. 2021, doi: 10.1002/asi.24484.
69. S. Karakus, E. Avci. Application of Similarity-Based Image Steganography Method to Computerized Tomography Images. *7th International Symposium on Digital Forensics and Security (ISDFS)*, Jun. 2019, pp. 1–4. doi: 10.1109/ISDFS.2019.8757521.
70. J. Dalins, Y. Tyshetskiy, C. Wilson, M. J. Carman, D. Boudry. Laying foundations for effective machine learning in law enforcement. Majura – A labelling schema for child exploitation materials. *Digit. Investig.* Vol. 26, pp. 40–54, Sep. 2018, doi: 10.1016/j.diin.2018.05.004.

71. K. C. Seigfried-Spellar. Assessing the Psychological Well-being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations. *J. Police Crim. Psychol.* Vol. 33, no. 3, pp. 215–226, Sep. 2018, doi: 10.1007/s11896-017-9248-7.
72. T. W. Jing, R. K. Murugesan. Protecting Data Privacy and Prevent Fake News and Deepfakes in Social Media via Blockchain Technology. *Commun. Comput. Inf. Sci.* Vol. 1347, pp. 674–684, 2021, doi: 10.1007/978-981-33-6835-4_44.
73. A. Bruno, G. Cattaneo, U. Ferraro Petrillo, P. Capasso. PNU Spoofing: a menace for biometrics authentication systems? *Pattern Recognit. Lett.* Vol. 151, pp. 3–10, 2021, doi: 10.1016/j.patrec.2021.07.008.
74. N. Wiener. Cybernetics; or, Control and communication in the animal and the machine. New York: M.I.T. Press, 1961.
75. R. Glanville. Cybernetics: Thinking Through the Technology. *Traditions of Systems Theory*. Routledge, 2013.
76. L. Helminger, C. Rechberger. Multi-Party Computation in the GDPR. *Priv. Symp. 2022 - Data Prot. Law Int. Converg. Compliance Innov. Technol. DPLICIT*, 2022.
77. M. Roy, C. Chowdhury, N. Aslam. Security and Privacy Issues in Wireless Sensor and Body Area Networks. *Handbook of Computer Networks and Cyber Security*, B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, Eds. Cham: Springer International Publishing, 2020, pp. 173–200. doi: 10.1007/978-3-030-22277-2_7.
78. A. Vyas, S. Pal. Preventing Security and Privacy Attacks in WBANs. *Handbook of Computer Networks and Cyber Security*, B. B. Gupta, G. M. Perez, D. P. Agrawal, and D. Gupta, Eds. Cham: Springer International Publishing, 2020, pp. 201–225. doi: 10.1007/978-3-030-22277-2_8.

Received 29.01.2023

Катраказас П.[1], доктор філософії,
Менеджер наукового напряму,
https://orcid.org/0000-0001-7433-786X, e-mail: p.katrakazas@zelus.gr
Каллiполіту Т.[1],
Менеджер з доставки та експерт зі сталого розвитку,
https://orcid.org/0000-0001-5059-4909, e-mail: d.kallipolitou@zelus.gr
Каллiполітіс Л.[2],
Головний технічний директор,
https://orcid.org/0000-0002-5689-298X, e-mail: lkallipo@aegisresearch.eu
Спейс І.[2], доктор філософії,
Старший менеджер проєкту,
Researcher ID: 0000-0002-6167-3247, e-mail: hspais@aegisresearch.eu

[1] Zelus P.C.,
Tatoiou 92, 14452, Metamorfosi, Athens, GR

[2] AEGIS IT Research GmbH,
25 Humboldt Str. Braunschweig, 38106, Germany

АНАЛІЗ І ВИЗНАЧЕННЯ НЕОБХІДНИХ МЕХАНІЗМІВ ДЛЯ ПІДТРИМКИ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ЦИФРОВИХ ДАНИХ ПРО ЗДОРОВ'Я У КІБЕРНЕТИЧНІЙ СИСТЕМІ ЦИФРОВИХ РОЗСЛІДУВАНЬ

Вступ: *Нещодавнє збільшення масштабів подій, спричинених пандемією Covid-19, та зумовлена цим криза в галузі охорони здоров'я підкреслюють важливість цифрової криміналістики у пов'язаній екосистемі охорони здоров'я. Тому можна з упевненістю припустити, що є зростання інтересу до цифрової криміналістики і до того, як ці методи застосовуються в сучасній екосистемі охорони здоров'я, що зумовлює головне питання поточного дослідження.*

Мета *роботи полягає в тому, щоб зосередитися на визначенні та розробленні необхідних механізмів для підтримання безпеки та забезпечення конфіденційності даних, які поширюються в рамках наявних досліджень у сферах цифрової охорони здоров'я та кібербезпеки. Структуру, натхненну кібернетикою, створено на основі чинних практик і виявлених ключових прогалин.*

Результати: *П'ять електронних баз даних, а саме Scopus, IEEEXplore, PubMed, DOAJ та arXiV, було визначено як основні джерела даних. Було проведено найсучасніший аналіз (State-of-the-Art — як витвір мистецтва), щоб зрозуміти обмеження пристроїв та комп'ютерних систем (включно з залученими системами та їхніми елементами) у сфері охорони здоров'я, коли вони виходять з ладу, щоб розслідування навчило нас чомусь новому, нетривіальному. Дуже важливий аспект нашого підходу до ландшафту пов'язаної системи охорони здоров'я, керованого цифровою криміналістикою, базується на жорстких і комплексних методах отримання зворотного зв'язку, яких, здається, наразі бракує.*

Висновки: *Головна мета нашого дослідження полягає в тому, щоб показати, що за умови наявності величезної множинності, єдність може бути сформульована, і навпаки: якщо щось виглядає як одиниця, в ньому може міститися необмежена множина умов. Рух до майбутньої пов'язаної системи охорони здоров'я має базуватися на результатах аналізу виявлених нещасних випадків у її функціонуванні, щоб позначити майбутні зміни, які позитивно вплинуть на функціонування цієї системи.*

Ключові слова: *пов'язана система охорони здоров'я, цифрова криміналістика, пов'язане здоров'я, кібернетична цифрова структура розслідування, кібербезпека.*