Developing a novel Digital Forensics Readiness Framework for Wireless Medical Networks Using Specialised Logging[*]

Cephas Mpungu[1], Carlisle George[2] and Glenford Mapp[3]

School of Computer Science
Faculty of Science and Technology
Middlesex University, The Burroughs,
London, NW4 4BT, United Kingdom

[1] c.mpungu@mdx.ac.uk; [2]c.george@mdx.ac.uk; [3]c.mapp@mdx.ac.uk

Abstract.

Wireless Medical Networks (WMNs) have always been a vital component for the treatment and management of chronic diseases. However, the data generated by these networks keeps growing and has become a potential target for criminals seeking to capitalise on its sensitivity and value. Wireless networks also happen to be more vulnerable to attacks compared to wired networks. In the event of such attacks, it becomes really difficult to conduct a digital Forensics investigation. This paper investigates and suggests a proactive approach to digital forensics readiness within wireless medical networks by suggesting specialised monitoring and logging mechanisms. The research first identifies threats to wireless medical networks. It then undertakes a trajectory of a systematic review of previously proposed digital forensics frameworks and identifies challenges. Finally, it proposes a conceptual framework for Digital Forensics Readiness (DFR) for wireless medical networks. The paper, therefore, makes a novel contribution to the field of digital forensics. It suggests a more streamlined, robust, and decentralised framework that is partially underpinned by blockchain technology at the evidence management layer. The framework contributes to the enforcement of evidential data integrity whilst also securing wireless medical networks.

Keywords: Wireless medical networks, digital evidence, Digital forensics, Digital Forensics Readiness, digital investigations, incident response.

[*] Mpungu, C., George, C., & Mapp, G. (2023). Developing a Novel Digital Forensics Readiness Framework for Wireless Medical Networks Using Specialised Logging. In: Jahankhani, H. (eds) *Cybersecurity in the Age of Smart Societies. Advanced Sciences and Technologies for Security Applications*. Springer, Cham. https://doi.org/10.1007/978-3-031-20160-8_12

1 Introduction

The world we live in today is transforming rapidly into a digitized network connecting millions of people, businesses, and several vital sectors including healthcare. Healthcare networks have come a long way from the use of papyrus for medical data records [21] to state-of-the-art digitised equipment [4]. This has been bolstered by complex networks harbouring IoT (Internet Of Things) capabilities [51]. As a result, Wireless Medical Networks like Wireless Body Area Networks (WBAN), RFID tagging, GPRS, UTMS, Wireless Area Networks (WANs), Wireless Local Area Networks (WLANs), Wireless Sensor Networks (WSN) and Bluetooth have emerged and continue to evolve [13]. Miniaturized diagnostic equipment and instruments linked to smartphones have instituted a new term in the healthcare paradigm known as 'mHealth' (mobile health).

As the urgent need to manage chronic diseases continues to rise, mHealth technologies and networks have become a sustainable factor in ensuring proper monitored management [58]. The essentiality of IoT-enabled apps has played a vital role in the management of chronic diseases such as diabetes, heart disease and cancer [1]. Examples of these include implantable and wearable medical devices like insulin pumps, glucose monitors, defibrillators, neuro-monitoring systems, and smartwatches [33]. These evolving additions to wireless medical networks (WMNs) have subsequently created a lot of data as well as complexities in handling it. Data privacy enforcers and regulators have also put pressure on the various stakeholders to ensure that healthcare data is processed and managed securely [9, 26].

The Covid-19 pandemic resulted in the healthcare sector experiencing many difficulties. Healthcare facilities that had previously stuck to traditional methods of delivering services had to succumb to poor service delivery due to overwhelming demand for services and cyberattacks. The pandemic also uncovered several healthcare-related system security vulnerabilities [6]. Countries like the USA accused China and Russia of trying to hack into their healthcare research centres [12]. Cybercriminals also capitalised on ransomware, phishing and hacking attacks, amongst others, targeted at healthcare systems [15]. In 2019, Greenfield Hospital (USA) paid $50,000 to hackers as ransom so that 1400 hospital files would be decrypted during a ransomware attack [49]. Kyaw et al. [32] conclude that such incidents are on the rise in the healthcare sector including, even, those that claim to have the very best security technology and resources at their disposal. Protenus [43] publishes up-to-date information on data breaches and in April 2021 reported that over 40 million patient records (worldwide) had been breached in the year 2021. Other security threats to medical systems include Distributed Denial-Of-Service (DDoS) attacks, SQL injections, zero-day attacks, supply chain attacks, human errors, and Man in The Middle attacks (MITM).

The current approach to mitigating these kinds of threats has been more inclined toward security enforcement, disaster recovery and business continuity with less emphasis on Digital Forensics Readiness (DFR) [32]. Aside from external attacks, internal attacks have also been witnessed [16]. This is because most healthcare systems have been designed based on centralised logging mechanisms.

Attacks on medical systems often leave behind traces of evidence concealed within the compromised systems [32, 45, 48]. This paper argues that such attacks on healthcare systems can be mitigated by introducing more robust security mechanisms. The attacks can also be more easily investigated by streamlining the extraction of evidence to identify perpetrators. This paper proposes that these two objectives can be achieved by implementing a DFR framework in WMNs.

2 Background and Literature Review

2.1 Evolution of Healthcare Networks

Technology has evolved at a super-fast speed over the past years, with this also encompassing digital healthcare networks. According to Bhavnani et al. [4], some healthcare Wireless Medical Networks (WMNs) are already thriving with state-of the-art digitised medical equipment and technologies that have since adopted some IoT functionalities. Some examples of these IoT devices include implantable and wearable medical devices such as insulin pumps, glucose monitors, defibrillators, neuro-monitoring systems, and smartwatches [33].

With the emergence of miniaturised diagnostic instruments linked to smartphones, mHealth has developed giving rise to the need for more wireless networks linked to healthcare. The World Health Organisation (WHO) defines mHealth as a component of eHealth (electronic health) that is supported by mobile devices such as patient monitoring devices, mobile phones, PDAs, and other wireless devices [58]. The intersection of mHealth and the 'real world' however has raised new insights and questions into the generation and analysis of data logs collected from these systems [4].

2.2 The Sensitivity of Healthcare Data

Data pertaining to WMNs is of intrinsic value to various stakeholders. This data may include, but not limited to, personal health records (e.g., names, phone numbers, age, medical history, drug prescriptions and home address), network traffic logs, employee records, CCTV footage, authentication records and logistical data. Personal health records are also technically referred to as Electronic Medical Records (EMR). EMR is defined as a collection of medical information pertaining to an individual that is stored digitally on a computer [36]. Examples of EMR are patient history, tests, allergies, treatment plans, medical insurance, and biometric data.

Caution must be taken to ensure that the integrity, confidentiality, and availability (CIA triad) of this data is maintained. Article 9 of the General Data Protection Regulation (GDPR), which is incorporated into the UK Data Protection Act 2018, lists data pertaining to health among "special category data" that should be given more protection. The unauthorised disclosure of such data will lead to data protection violations and the possible discrimination against data subjects [26], in addition to criminal sanctions under S170 of the Data Protection Act 2018. Servers and networks handling logs, personal-health data, and other healthcare-related information should therefore be secured with utmost importance. Measures should also be put in place by data controllers to ensure that logging systems on WMNs are well structured to capture and preserve data that may be of evidential value [13, 32, 46].

2.3 Security Challenges of Wireless Medical Networks (WMNs)

The National Institute of Standards and Technology (NIST) defines vulnerability as any weakness within an organisation's internal controls, system, or its system security procedures [39]. Some researchers within the Digital Forensics (DF) field have discussed vulnerabilities discovered in some wireless medical IoT devices. For example, security experts have demonstrated that some wireless commercially available insulin pumps are prone to hacking attacks [44]. Software radio-based attacks targeted at cardioverter-defibrillators have also been shown to be possible [22]. Flaws in wireless security encryption methods like WPA, WEP and WPA2 have also been discussed by researchers as possible backdoors to cyber-attacks [13, 31].

Beyond hacking threats, other challenges like ransomware attacks [49] and data breaches [16] are increasing. Cusack and Kyaw[13] define such attacks under 'misuse of wireless medical devices' as unauthorised behaviour within the system. Davis [15], discussed some of the biggest healthcare data breaches of 2019. She maintains that phishing attacks and third-party vendors were behind most of these attacks which left over 25 million patient records compromised. Such attacks infringe on the confidentiality, integrity, and availability of healthcare data [34]. Many cyber attacks are instigated internally or externally and exploit identified vulnerabilities within these systems [32].

2.4 Digital Forensics Readiness (DFR)

One of the toughest challenges faced by countries within the European Union (EU) today is ensuring effective compliance with the GDPR Article 33 regarding data breach notifications. It requires organisations to report an incident to the relevant supervisory authority (e.g. the Information Commissioner's Office (ICO) in the UK) "without undue delay and, where feasible, not later than 72 hours after having become aware of it".

This incorporates all aspects of the incident that pertain to its occurrence, what it is, and the damage done [41]. Where the data breach could result in risks to the rights and freedoms of data subjects, the GDPR Article 34 requires communication to the data subjects as well, without undue delay. Realistically speaking, proper compliance with Articles 33 and 34 could be a daunting task to achieve (especially for large networks) as it might entail extensive forensics analysis (needing evidence). Challenges like these, among others, have prompted various researchers to propose the need for DFR within various organisations [13, 23, 29, 47].

DFR is derived from the term Digital Forensics (DF). Vidal and Choo [56], define DFR as an organisation's pro-active approach toward the quick collection of digital evidential data at minimal cost or interruption to its day-to-day business. Rowlingson's definition of DFR is analogous to the one given by Vidal and Choo [48]. Vidal and Choo [56] further clarify that an organisation should be in a position to clearly define this digital evidence. This helps in setting up appropriate teams, programs and infrastructure that facilitate the timely availability of the evidence[25]. DFR is therefore incidence-anticipation and not incidence-response driven [48].

DFR's objectives seek to make the best out of an organisation's environment by collecting digital evidence of credibility whilst minimising the cost of digital forensics during incidence response [14, 53].

2.5 Centralised DFR within Wireless Medical Networks

Cusack and Kyaw [13] proposed a centralised architecture of a DFR system for WMNs with security enforcement abilities as well as a capability to investigate post-events. The researchers delved deep into the architectures of wireless medical technologies and discussed their potential security risks. Their work proposed the addition of drones and a forensic server to an existent wireless network of a hospital information system. It resonates with Rowlingson's suggestion of deploying DFR on top of a system's existent logging mechanism [48].

Kyaw et al. [32] later proposed a modified DFR framework for wireless medical devices (WMedSys) based on the work in Cusack and Kyaw [13], with the aim of streamlining digital forensic investigations. The framework's main objective is to reduce the time and cost of performing a DF investigation. This time the researchers emphasize its conceptual design and its evaluation. Evaluation is done using a thematical expert analysis. The conceptual design consists of a Pi-drone that uses kali Linux Operating System (OS) to scan and capture wireless signals. The captured data is then sent to a Wireless Forensic Server (WFS). Other components of this framework are an Intrusion Detection System (IDS), integrity Hashing Server, Centralised Syslog server, Wireless Access Point (WAP), Remote Authentication Dial-In Service (RADIUS) server and a web server.

Other researchers like Rahman et al. [46] also discussed forensic readiness in WMNs focusing on Wireless Body Area Networks (WBAN). The researchers used the concept of Practical Impact Analysis (PIA) to scrutinise potential WBAN threats and vulnerabilities. Based on their findings, they proposed solutions for implementing a centralised DFR system [46].

2.6 Decentralised DFR Within Wireless Medical Networks

The work of the researchers reviewed in Sect. 2.5 above discussed DFR solutions that utilise a centralised logging mechanism. These researchers proposed frameworks based on the assumption that information system administrators and all those with access to the evidence-log servers can be trusted. This cannot be assumed as human beings are subject to compromise and may also get disgruntled and make irrational decisions leading to the alteration of server logs. Centralised logging models built on a client server architecture are also susceptible to becoming a single point of failure [2].

To address this, researchers like Tian et al. [55] proposed a solution to centralise log management, in the form of a secure digital evidence framework based on blockchain technology for the storage of evidential data. Their proposal, however, was limited by its emphasis on the security of hash files and not the actual evidential logs (data). The proposal in this paper builds on the work of Tian et al. [55] and seeks to improve the use of blockchain in that context.

2.7 Blockchain Technology

Blockchain is defined as a public ledger of transactions distributed and stored on several nodes within a blockchain network [20, 55]. It uses a peer-peer architecture with each constituent node having a copy of the blockchain. It comprises blocks of transactions linked together by cryptographic and distributed consensus algorithms [59]. Each block keeps a record of specific transactions and contains a hash value pointing to the previous block [20]. Blockchain networks can be classified as public, private or consortium (mixed) blockchains [55]. Blockchain is believed to be one of the safest means of storing data and transactions in an immutable form due to its cryptographic and hashing capabilities [3, 20, 42, 55]. Blockchain technology, therefore, ensures auditability, decentralization, immutability, security, and transparency [59]. It is for this matter that researchers like Tian et al. [55] and Pourmajidi et al. [42] have proposed logging frameworks based on blockchain technology.

However, blockchain faces the challenge of scalability. As the blocks of data continue to grow, it creates a need for larger storage facilitation and it might slow down the blockchain network [55, 59]. This is known as blockchain bloat [55]. The work done by Tian et al. [55] suggests a lightweight blockchain to counter this challenge within a digital evidence system.

Blockchain is still a new technology and yet it has attracted a lot of attention from various researchers, industries, and some governments. Estonia (Europe) for example, was the first nation to implement blockchain technology within its production systems. The country opted for a technology known as KSI blockchain, similarly used by USA and NATO [28]. The KSI blockchain in Estonia supports the property, healthcare, succession, and business registries. It also facilitates its digital court system [28]. Similarly, the European Union (EU) is undertaking a blockchain research program known as MyHealthMyData (MHMD). The program aims to ensure interoperability between individuals, healthcare providers, and biomedical industries [19].

3 A New Framework for DFR in Wireless Medical Networks (WMNs)

3.1 Introduction

Most organisations invest a lot of money in securing their networks, but this may not necessarily stop security incidents from occurring. Therefore, the framework proposed by this research assumes that an incident might occur regardless of an implementation that ensures a risk assessment of low probability. The design seeks to enforce the security of WMNs whilst also ensuring forensic readiness, hence aligning itself with the characteristics of a good DFR system identified by previous researchers like Tan [53] and Rowlingson [48].

Figure 1 illustrates the structure of the proposed DFR in the context of a generic WMN. It consists of three major layers: (i) Data Collection Layer (DCL), (ii) NetworkLayer (NL), and (iii) Evidence Management Layer (EML). The design of the framework takes into consideration five major guidelines identified by Rowlingson [48]:

1. Identification of possible sources of evidential data within a generic healthcare wireless network structure. This is implemented at the Data collection Layer.
2. Outlining of the technical and legal requirements for the proper and streamlined collection of digital evidence. These requirements are implemented and maintained at all three layers.
3. Identification and set up of resources for the proper collection of legally admissible evidence to meet the legal and technical requirements. This is mostly enforced at the EML and partly at the DCL.
4. Ensuring that all monitoring systems can detect major incidents. This is implemented at the DCL using the Incident Detection System (IDS) module.
5. Establishing the requirements that warrant a digital forensic investigation.

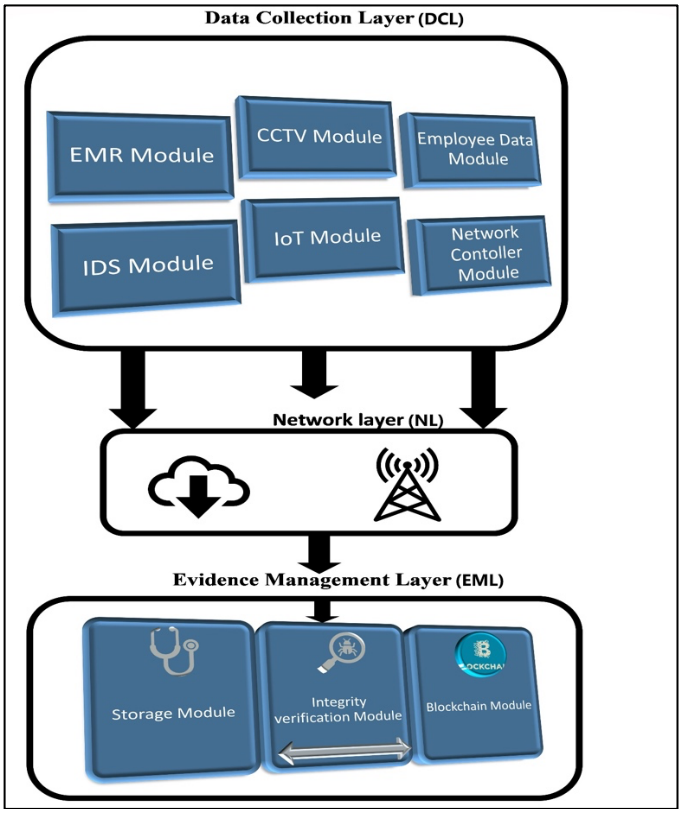

Figure 1. Proposed WMN DFR framework.

3.2 Data Collection Layer (DCL)

The DCL consists of six major modules. These modules were identified as the main sources of evidential data within wireless medical networks by the researcher. These include: Electronic Medical Records (EMR) module, Employee Data Module, IoT Module, CCTV Module, Network Controller Module, and the Intrusion Detection System (IDS) Module. The DCL consists of modules that are implemented and configured to meet the requirements of availing potential evidential data. The collection of logs from these modules can be implemented in about three ways:

1) The utilisation of existing logging agents within the modules.
2) Adjustment/reconfiguration of existing logging agents within the modules.
3) Configuring new logging agents within the modules.

Some potential sources of evidential data considered during the design of this framework include firewalls, switches, wireless access points, proxy servers, DHCP servers, DNS servers, routers, VPN terminators, system logs, IoT devices and CCTV cameras, amongst others.

The **Employee Data Module** collects information relating to employees' day to day activities like patient-diagnosis data, employee-patient interactions, key card logins, etc. and stores them within an MYSQL database. This database(db) is linked to other relational databases like Employee Records db, Medical IoT devices db and Electronic Medical Records db using a Relational Database Management System (RDBMS). The choice to use MYSQL for RDBMS by the researcher is based on its cross-platform support, open-source nature, and compatibility with the Linux operating system.

The **Electronic Medical Records Module** is a database of personal records pertaining to patients e.g. patient history, tests, allergies, treatment plans, medical insurance, and biometric data. This kind of data could be a rich source of evidential data related to medical negligence and fake insurance claims.

IoTModule is used as a central collection point for all IoMT (Internet of Medical Things) data that could be a source of evidential data. Examples of IoT devices include insulin pumps, glucose monitors, cardioverter-defibrillators, and neuro-monitoring systems.

The **Network controller Module** in the framework is configured using Cisco DNA Center software. A Network controller is hardware or software that implements intermediation between an organisation's needs and its network infrastructure [10]. The choice to use Cisco DNA Center is based on its interoperability, easy setup and resilience attributes. A software implementation also eliminates the need to purchase specialised Network controller hardware. The module streamlines the collection of potential evidential data from network hardware like routers, switches, and wireless access points. The Network Controller software is also paramount for the enforcement of security and tweaking network configurations.

The **CCTV Module** is a collection point for all video footage uploaded from the various surveillance cameras within the hospital premises. This kind of data comes in handy when placing suspects at a crime scene.

The **Intrusion Detection System (IDS) Module** of the framework is configured to monitor malicious or policy violation activity and log data to a SIEM (Security Information and Event Management System). This data can be generated from antivirus logs, proxy servers, database audits and application servers. The IDS can be further configured, and rules set to detect bad IPs, URLs, and elimination of false positives [52]. The rules and configurations are then tightened by setting alerts to the incident response team e.g. through SMS and email whenever incidents are detected. Figures 2 and 3 show the flow of data from the DCL to the EML.

The data collected from the DCL is encrypted and forwarded to the Integrity Verification Module (IVM) of the Evidence Management Layer (EML) as shown in Figure. 2. The IVM server is configured primarily to hash the logs and additionally as a Network Time Protocol (NTP) server (for synchronisation of clocks on all servers). Time synchronisation is a key factor for the proper enforcement of data integrity.

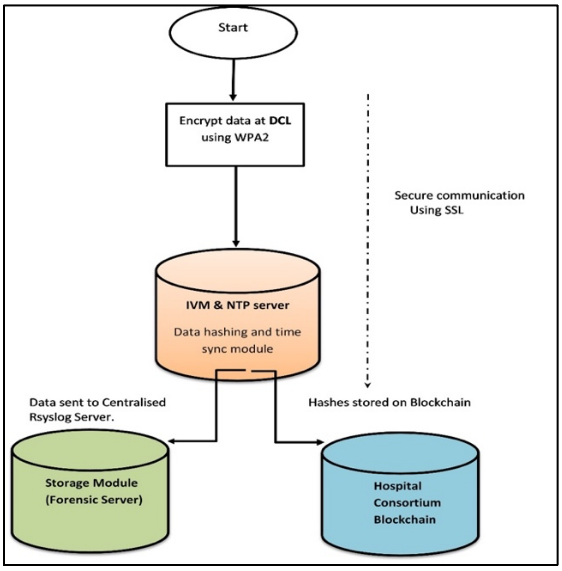
Start
Encrypt data at DCL using WPA2
Secure communication Using SSL
IVM & NTP server
Data hashing and time sync module
Data sent to Centralised Rsyslog Server.
Hashes stored on Blockchain
Storage Module (Forensic Server)
Hospital Consortium Blockchain

Figure 2. Data flowchart from the DCL to the EML

Each data source is hashed and then forwarded and logged/stored onto the Storage Module (Forensic Server) within the EML. The data source's corresponding hash is then stored securely on the consortium blockchain. A consortium blockchain is a combination of a private and public blockchain [55]. The researcher's choice to use a consortium blockchain implementation is supported by the fact that a mixed blockchain facilitates easy and streamlined access to data by all third parties relevant to an investigation (e.g., insurers, lawyers, and forensic investigators). It, therefore, enforces interoperability [18] whilst maintaining data integrity.

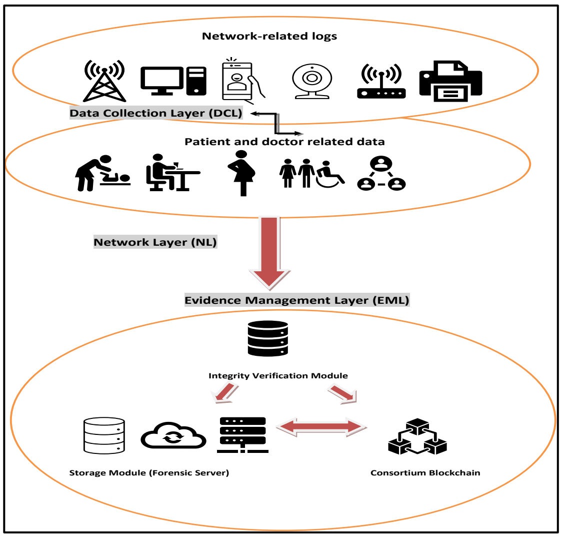
Network-related logs
Data Collection Layer (DCL)
Patient and doctor related data
Network Layer (NL)
Evidence Management Layer (EML)
Integrity Verification Module
Storage Module (Forensic Server)
Consortium Blockchain

Figure 3. Data flow from the DCL to the EML.

As an added layer of security, the IVM and the Forensic Server can be configured as virtual machines residing on hypervisor hardware or software. Hypervisors provide a private network ecosystem where two virtual machines can communicate with each other without the knowledge of the physical network they reside on [30]. The two servers can then be assigned two sets of static IPs, one set for private communications with each other and the other set for communication with other relevant devices on the physical network. With this kind of setup, the network traffic generated between the two servers will remain concealed from the healthcare's physical network.

3.3 Network Layer (NL)

The Network layer consists of communication channels needed for ensuring connection setup between different networks and devices for the secure transfer of data packets. The communication channels are configured using a cryptographic protocol known as Secure Sockets Layer (SSL) or TSL (Transport Layer Security) for the safe transportation of data across the network. SSL helps enforce security and ensure data integrity for TCP/IP communications. The researcher also proposes the use of enhanced security protocols WPA2/3 (WI-FI Protected Access 2/3) Enterprise within the WLAN. This is configured using a RADIUS authentication server. The task of network user access and authentication is handled by the RADIUS server [50].

The IoT medical devices within a hospital's premises will also be configured to use dedicated wireless routers and access points whose SSIDs (Service Set Identifiers) are not broadcast. This adds a layer of security [57] by reducing the attack surface for cybercriminals as they wouldn't know the SSIDs of the wireless routers to attack.

3.4 Evidence Management Layer (EML).

The evidence storage and management module is paramount to ensuring the integrity, availability and confidentiality of potential evidential data. It comprises an Integrity Verification Module (IVM), a Linux Rsyslog server and consortium blockchain nodes. As an added layer of security, these three components should be configured on a separate subnet of the wireless network.

The IVM is run on a Red hat Linux Operating System platform and is configured to serve as a hashing and NTP server. Hashing is necessary for enforcing data integrity, checking data integrity, and speeding up the retrieval of evidential data. This research proposes a SHA-256 cryptographic hashing algorithm. SHA-256 is considered the strongest hashing algorithm and is highly recommended by NIST. The hashed data is forwarded to the centralised logging facility which acts as a forensic server. The hashes are sent to the decentralised storage facility on the consortium blockchain.

The Storage Module (Forensic server) is a centralised logging facility also running Red hat Linux OS. It is configured using Rsyslog. The researcher's choice of Red Hat Linux OS is based on its robust security features like Systemd log management, Security Enhanced Linux (SElinux), advanced AccessControl Lists (ACLs) management and 'Firewalld'. A good logging mechanism should also be supported by data compression and backup capabilities. For this framework, the researcher proposes a periodic archiving and remote backup of the forensic server image on a secure cloud storage. This can be automated by writing scripts on the log server using a facility known as crontab.

Combining local and remote logging helps secure the integrity of the evidential data [48]. Remote logging on the proposed DFR is configured using the Rsyslog facility by editing its configuration file (/etc./rsyslog.conf). Rsyslog also contains a log rotation facility known as logrotate that can be configured using the /etc./logrotate.conf configuration file to align log data retention policies on the server with the laws governing data retention of healthcare-related data. The ICO in the UK maintains that data should be gathered and logged for defined purposes and nothing more [48].

The consortium blockchain is a mixture of a private and public blockchain distributed on several nodes using a peer-to-peer network. This kind of configuration ensures a better consensus mechanism in comparison to a private blockchain. It also offers a more decentralisation setup compared to a private setup [40]. To solve the issue of blockchain bloat, the blockchain is only used to store the data hashes and to provide a secure interface for access and handling of evidential data. The stakeholders that may need access to the evidential data go beyond the scope of just healthcare employees. They include insurance companies, private GPs, forensic investigators, courts of law, government compliance officers and lawyers. A mixed blockchain setup allows for this kind of varied access whilst also enforcing the data integrity of evidential data.

Different stakeholders (authorised to access the evidential data) like the hospital, insurance companies and government institutes can share the blockchain development costs to suit the DFR requirement. Companies like Hashed Health are already offering distributed ledger solutions within the Healthcare sector tailored to the needs of their clients [24]. The researcher proposes the use of smart contracts for the streamlined and transparent access of evidential data by all the relevant stakeholders. Smart contracts are software/program codes written to execute actions when fed inputs or when a specific event is triggered [38, 54]. Smart contracts can also be programmed to enforce private/public key-oriented registrations, access control rules and interfaces for various stakeholders pertaining to healthcare data. Smart contracts rely on the “if–then” logic of programming and help ensure immutability, security, privacy, reduced costs and automation [38]. The blockchain interface of the proposed framework will constitute a smart contact configuration that checks the public/private key of a user and grants them access to evidential data based on Access Control Rules (ACLs) set by the Rsyslog server System administrator. For example, a digital forensics Investigator would be assigned access to all logs on the server whilst a medical insurance company investigator would be limited to accessing only logs pertaining to their client. A smart contract configuration is also set up to trigger alerts to the incident response team when nefarious activity is detected within the Evidence Management Layer. The proposed consortium blockchain is meant to be accessible by all parties relevant to an investigation (e.g. law enforcement investigators, lawyers, digital forensics investigators, and medical insurers, amongst others). Verification, management, and retrieval of evidence are therefore executed at the blockchain interface module.

4 Digital forensics investigation process using the proposed framework.

The conceptual design of the proposed framework is partly inspired and guided by previous (validated) research and best practices within the field of DFR (e.g. [37, 55]). It aims to simplify and streamline the process of retrieval and submission of admissible evidential data by a forensic investigator as much as possible. This is further reflected in the researchers' choice to use highly customisable software of high repute like Red Hat Enterpise Linux (RHEL), Rsyslog, Cisco DNA Center and MYSQL. The open-source nature of RHEL and MYSQL also optimises the attributes of scalability, integrated-management and interoperability needed for this framework. Figure 4 illustrates the digital forensic investigation process-flow within the proposed DFR framework.

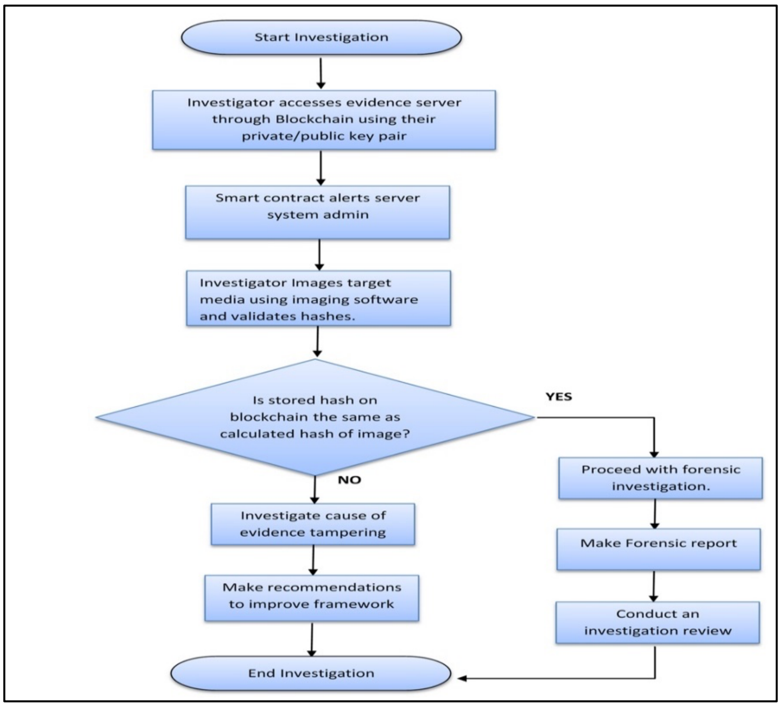
Start Investigation
Investigator accesses evidence server through Blockchain using their private/public key pair
Smart contract alerts server system admin
Investigator Images target media using imaging software and validates hashes.
Is stored hash on blockchain the same as calculated hash of image?
YES
NO
Proceed with forensic investigation.
Make Forensic report
Conduct an investigation review
Investigate cause of evidence tampering
Make recommendations to improve framework
End Investigation

Figure 4. Digital Investigation protocol on the proposed DFR framework

5 Evaluation of proposed framework

5.1 Introduction

This section focuses on the evaluation of the proposed DFR framework using two approaches, a standard-based approach, and a scenario-based approach.

5.2 Standards-based evaluation

The standards-based evaluation entails investigating whether the framework conforms to relevant guidelines for proper DFR planning and implementation provided by the International Organisation for Standardisation (ISO/IEC 27,043:2015). The guidelines utilise models that are idealised to represent common incidents encountered during investigations. The ISO/IEC 27,043:2015 defines the three categorical groups of readiness processes as planning, implementation, and assessment process groups [27]. Evaluation of the framework is done based on the planning process group. The implementation and assessment process groups are beyond the scope of this research.

The planning process group comprises six major steps:

1. Definition of scenarios
2. Identification of potential evidential data sources.
3. Pre-incident planning, gathering, storage and handling of potential evidential data.
4. Pre-incident analysis of potential evidential data planning.
5. Incident detection planning.
6. System architecture definition.

5.2.1 Definition of Scenarios

Scenario definition is important to help conceptualise simulations of incidents that may trigger a digital forensic investigation or audit of the wireless medical network. A risk assessment is conducted by the incident response team to identify potential vulnerabilities and threats within the WMN. The scenarios can then be defined based on the risk assessment analysis and also based on the current threats facing healthcare networks. The researcher used scenarios like past ransomware attacks on the NHS [35], internal data breaches, DDOS attacks as well as hacking cases during the COVID-19 season. Identification of scenarios enlightens the technical and system administration team on the requirements of achieving digital forensics readiness.

Evaluation results: Appropriate scenarios were identified to guide the design of the proposed framework based on current security threats to wireless medical networks cited in media and articles and a literature review of relevant work. This met the scenario definition requirement.

5.2.2 Identification of Potential Evidential Data Sources

The step of identification of potential evidential data sources is informed by the scenario-definition process. For example, a scenario of a data breach on personal health data by authorised personnel informs this step that electronic medical records (EMR) are vulnerable to attacks. EMR is therefore identified as a potential data source. Emphasis can then be put on logging authorized personnel activities within the systems as well as logging EMR metadata information for analysis during an investigation. Access control lists on this kind of sensitive data can also be enforced and monitored keenly.

***Evaluation results**:* The proposed DFR identified five major modules as the main sources of evidential data within wireless medical networks by the researcher. These include: Electronic Medical Records (EMR) module, Employee Data Module, IoT Module, CCTV Module, Network Controller Module, and the Intrusion Detection System (IDS) Module. The identified modules met the requirement of potential data sources.

5.2.3 Pre-Incident Planning, Gathering, Storage and Handling

The step of pre-incident planning, gathering, storage and handling of potential evidential data was defined in the proposed DFR. This was defined within the EML. It comprises an Integrity Verification Module (IVM), a Linux Rsyslog server, and consortium blockchain nodes. The IVM enforces integrity, the Linux Rsyslog server centrally manages evidential log data and the consortium blockchain enforces the confidentiality, integrity, and availability of evidential data.

Evaluation results: The requirement was met by the above-proposed modules for the framework.

5.2.4 Pre-Incident Analysis of Potential Evidential Data Planning

Pre-incident analysis of potential evidential data planning is achieved by the proposed model at the SIEM (Security Information and Event Management System) of the IDS module. This event analyzer implemented at the logging-agent level is configured to alert the incident response team about suspicious activity within the WMN.

Evaluation results: The SIEM of the IDS in the proposed DFR met this requirement.

5.2.5 Incident Detection Planning

Incident detection planning is handled at the IDS module by configurations made by the systems administrators, network administrators and network engineers. These are also part of the incident response team and DFR team and liaise with the forensic investigators during an investigation.

Evaluation results: The IDS in the proposed DFR met this requirement.

5.2.6 System Architecture Definition

The system architecture definition has been partially achieved in the framework proposal. The operating system and logging format of the evidence log server have been identified. The operating system of the IVM is defined, and the type of blockchain and the database management system have also been identified and justified. However, the network architecture has not been fully defined because the proposed framework is based on a generic wireless medical network.

Evaluation results: The system architecture definition requirement was partially met.

5.3 Scenario-based evaluation.

A scenario can be defined as a prediction made about a sequence of events [11]. Scenario-based evaluation of the proposed framework was done by first identifying common security threats to wireless medical networks. These include (but not limited to) Distributed Denial-Of-Service (DDoS) attacks, human errors, Man in The Middle attacks (MITM), ransomware attacks, malware, data breaches, and hacking. The researcher then identified the kind of data that needs to be logged to sustain digital forensics investigations and audits of WMNs.

Scenario 1: Unauthorised access
A disgruntled employee Mike, having financial challenges, is suspected of accessing and copying the personal medical records of HIV patients. The employee plans to anonymously contact the patients and ask for money or release their medical records online.

Investigation Process:
The investigator will make use of CCTV footage data to help place the suspect at the scene of crime. Logs generated by the IDS module like computer MAC address, IP address and User login credentials will also provide evidence proving unauthorised access. The metadata of the accessed HIV medical records will also be a rich source of evidence for proof of unauthorised access and timeline analysis. Table 1 summarises the data source modules of the framework and logged data that are utilised for this investigation.

Table 1 Investigation process for unauthorised access.

Logging Agent on DFR framework	**Data Logged**	**Benefit to Investigator**
CCTV module	Time-stamped footage of suspect accessing hospital computer	• Will link the CCTV timestamp to other evidential metadata. • Placing the suspect at the crime scene
IDS Module	SMS alert to the incident response team, MAC address and IP of the device, medical data accessed metadata, login user credentials, key card login.	• Account login details of employee and key card logins • Metadata of accessed records.
The server containing medical records.	Registry files, personal data access time, copy and paste activity, external device attachment	• Server metadata proving unauthorised activity.

Scenario 2: Alteration of log files.
The disgruntled employee connives with an assistant system administrator known as Patrick and asks him to delete all the logs on the server that could implicate him. Mike blackmails Patrick and threats to tell his wife about his affair with the receptionist at the hospital. The systems admin, afraid of losing his marriage, deletes all the CCTV footage and logs that implicate Mike in the crime. The systems admin forgets to delete the backup copies of the server in the cloud.

Investigation Process:
Smart contracts customised within the consortium blockchain alert the incident response team about nefarious activity on the log server. Once an investigation is commissioned, the backup copy of the server is imaged and compared against the current server image for traces of discrepancies. The Integrity Verification Module also contains an index of the history of all log ids and hash ids which can be used for further cross-references to prove alteration activity. Table 2 summarises the data source modules of the framework and logged data that are utilised for this investigation.

Table 2. Investigation process for log alteration.

Logging Agent on DFR framework	Data Logged	Benefit to Investigator
Blockchain module	The hashes of the deleted logs and CCTV footage.	• Smart contracts alert the incident response team about the deletion of data corresponding to the hashes on the blockchain.
Backup server	A full backup image of the server that was compromised by the assistant systems admin	• Restoration of the server backup image from the cloud is used to identify the logs that were deleted using their corresponding hashes.
Integrity Verification Module (IVM)	Index of log ids and hash ids	• The IVM module is used to map the compromised data hashes onto the restored logs from the backup.

Scenario 3: Hacking.
A hacker obtains access to personal healthcare information intending to sell it to the highest bidder.

Investigation Process:
Unauthorised access alerts triggered by the IDS and blockchain smart contracts alert the incident response team. Investigator images logs generated by the IDS module to

obtain rogue IP and MAC address of the external threat agent device. Table 3 summarises the data source modules of the framework and logged data that are utilised for this investigation

Table 3 Investigation process for hacking.

Logging Agent on DFR framework	Data Logged	Benefit to Investigator
Blockchain Module	Unauthorised access login attempts	• Smart contracts alert the Incident response team of attempted access by an unauthorised agent
IDS Module	SMS alert to data to the incident response team, MAC address and IP of the external device.	• SMS alert to the incident response team • IP and MAC address of the rogue device

Scenario 4: Malware attack.

Malware is any software that is designed with the intent to damage a computer, network, server, or client. The term is derived from the terms ‘malicious’ and ‘software’. In this scenario, an employee is suspected of unintentionally installing malware by clicking on a link sent through email.

Investigation Process:

The investigator images IDS module logs to identify malicious file-based signatures after an alert is sent to the incident response team by the IDS module. The investigator will then compare the hashes of the suspicious file signatures to the NIST database used by law enforcement. Table 4 summarises the data source modules of the framework and logged data that are utilised for this investigation.

Table 4 Investigation process for malware attack.

Logging Agent of DFR framework	Data Logged	Benefit to Investigator
IDS Module	• IDS module is configured to detect file-based signatures and send alerts to incident response team. • IDS is also configured to detect unauthorised data movement and malicious file signatures.	• Extracted files are scanned with antivirus software. • The investigator can compare suspicious hashes against the NIST hash (updated) database used by law enforcement and forensics experts.

5.4 Conclusion

The proposed digital forensics readiness framework for wireless medical networks makes a novel contribution to the field of digital forensics. The research builds on the work done by [32] and Tian et al. [55] to propose a tamper-proof digital forensics readiness framework for wireless medical networks. It proposes a logging mechanism with an additional layer of security that utilises a consortium blockchain technology for integrity enforcement.

The standard-based evaluation discussed in this chapter shows that the proposed WMN DFR framework addresses the requirements highlighted within the planning readiness process group defined by the ISO/IEC 27,043:2015 standard. Furthermore, the scenario-based evaluation which focused on security threats faced by the healthcare sector demonstrated the effectiveness of the framework. Therefore the proposed DFR framework provides possible solutions to current security threats (e.g. unauthorized access, log alterations hacking, and malware attacks) based on its logging mechanism.

References

1. Albesher A (2019) IoT in health-care: recent advances in the development of smart cyberphysical ubiquitous environments. Available at: https://www.researchgate.net/publication/331642487_IoT_in_Health-care_Recent_Advances_in_the_Development_of_Smart_Cyber-Physical_Ubiquitous_Environments. Last accessed 19 July 2022

2. Atlam H, Alenezi A, Alassafi A, Wills G (2018) Blockchain with internet of things: benefits, challenges, and future directions.Available at: https://eprints.soton.ac.uk/421529/1/Published_Version.pdf. Last accessed 19 July 2022

3. Belchior R, Correia M, Vasconcelos A (2019) JusticeChain: using blockchain to protect justice logs. In: Lecture notes in computer science (online) pp 318–325. Available at: https://link.springer.com/chapter/10.1007%2F978-3-030-33246-4_21. Last accessed 19 July 2022

4. Bhavnani P, Narula J, Sengupta P (2016) Mobile technology and the digitization of healthcare. Eur Heart J 37(18):1428–1438. https://doi.org/10.1093/eurheartj/ehv770

5. Bsigroup.com (2014) BS 10008 Electronic information management (online) Available at: https://www.bsigroup.com/en-GB/bs-10008-electronic-information-management/. Last accessed 19 July 2022

6. Burgess M (2020) Hackers are targeting hospitals crippled by coronavirus. Available at https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing. Last accessed 19 July 2022

7. CDC(2019) About chronic diseases (online)Available at: https://www.cdc.gov/chronicdisease/about/index.htm. Last accessed 19 July 2022

8. Cabinet Office (2016) Security policy framework (online) GOV.UK. Available at https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework. Last accessed 19 July 2022

9. Cellan-Jones R (2020) Coronavirus: England's test and trace programme breaks GDPR data law. The BBC.Available at: https://www.bbc.co.uk/news/technology-53466471. Last accessed 19 July 2022

10. Cisco (2020) What is a network controller? (online) Available at: https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-a-network-controller.html. Last accessed 19 July 2022
11. Collinsdictionary.com (2019) Definition of scenario (online) Available at: https://www.collinsdictionary.com/dictionary/english/scenario. Last accessed 19 July 2022

12. Corera G (2020) Coronavirus: US accuses China of hacking coronavirus research. The BBC. Available at: https://www.bbc.co.uk/news/world-us-canada-52656656. Accessed 21 July 2020

13. Cusack B,KyawA(2012) Forensic readiness for wireless medical systems.Available at https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1107&context=adf. Last accessed 19 July 2022

14. DWP Forensic Readiness Policy (2018) DWP forensic readiness policy Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886724/dwp-forensic-readiness-policy.pdf. Last accessed 19 July 2022

15. Davis J (2019) The 10 biggest healthcare data breaches of 2019*,* So far. Available at https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2019-so-far. Last accessed 19 July 2022

16. Ehlinger S (2017) Former employee reportedly steals mental health data on 28,434 Bexar County patients. The San Antonio Express-News. Available at: https://www.expressnews.com/business/local/article/Former-employee-reportedly-steals-mental-health-12405113.php. Last accessed 19 July 2022

17. Endicott-Popovsky B, Frincke D, Taylor C (2007) A theoretical framework for organizational network forensic readiness. Available at: https://www.researchgate.net/publication/42803345_A_Theoretical_Framework_for_Organizational_Network_Forensic_Readiness. Last accessed 19 July 2022

18. England.nhs.uk. (no date) NHS England. Interoperability (online) Available at https://www.england.nhs.uk/digitaltechnology/connecteddigitalsystems/interoperability/. Last accessed 19 July 2022

19. Europa.eu. (2020) CORDIS|European commission (online) Available at: https://cordis.europa.eu/project/id/732907. Last accessed 19 July 2022

20. Furneaux N (2018) Investigating cryptocurrencies: understanding the technology. Wiley, IN. Last accessed 19 July 2022

21. Gillum R (2013) From papyrus to the electronic tablet: a brief history of the clinical medical record with lessons for the digital age. https://doi.org/10.1016/j.amjmed.2013.03.024

22. Halperin D, Heydt-Benjamin T, Ransford B, Clark S, Defend B, Morgan W, Fu K, Kohno T, MaiselW(2008) Pacemakers and implantable cardiac defibrillators: software radio attacks and zero-power defenses. Available at: https://scholarworks.umass.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1067&context=cs_faculty_pubs Last accessed 19 July 2022

23. Harbawi M, Varol A (2017) An improved digital evidence acquisition model for the Internet of Things forensic I: a theoretical framework. In: 2017 5th international symposium on digital forensic and security (ISDFS). https://doi.org/10.1109/ISDFS.2017.7916508

24. Hashed Health. (2020). *About*. (online) Available at: https://hashedhealth.com/about/ (Last accessed: 19 July 2022).

25. ISACA(2014) Importance of forensic readiness.Available at: https://www.isaca.org/resources/isaca-journal/past-issues/2014/importance-of-forensic-readiness. Last accessed 19 July 2022

26. Ico.org.uk. (2019) Special category data (online) Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawfulbasis-for-processing/special-category-data/. Last accessed 19 July 2022

27. Iso.org. (2020) (online) Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27043:ed-1:v1:en. Last accessed 19 July 2022

28. Karm A (2019) Estonia–the digital republic secured by blockchain estonia -the digital republic secured by blockchain Estonia-the digital republic secured by blockchain PwC1 (online)Available at: https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf. Last accessed 19 July 2022

29. Kebande V, Venter H (2014) A cloud forensic readiness model using a botnet as a service. Available at: https://www.researchgate.net/profile/Natalie_Walker4/publication/263617788_Proceedings_of_the_International_Conference_on_Digital_Security_and_Forensics_DigitalSec2014/links/0f31753b5cd085c06a000000/Proceedings-of-the-International-Conferenceon-Digital-Security-and-Forensics-DigitalSec2014.pdf#page=25. Last accessed 19 July 2022

30. Komperda T (2012) Virtualization security [online]. Available at: https://resources.infosecinstitute.com/topic/virtualization-security-2/. Last accessed 19 July 2022

31. Kumkar V, Tiwari A, Tiwari P, Gupta A, Shrawne S (2012) Vulnerabilities of wireless security protocols (WEP and WPA2). Available at: https://www.researchgate.net/publication/266005431_Vulnerabilities_of_Wireless_Security_protocols_WEP_and_WPA2.Last accessed 19 July 2022

32. Kyaw A, Cusack B, Lutui R (2019) Digital forensic readiness in wireless medical systems. In: 2019 29th international telecommunication networks and applications conference (ITNAC). Auckland, New Zealand, pp 1–6. https://doi.org/10.1109/ITNAC46935.2019.9078005

33. LenkW(2020)Wireless mobile medical devices. Available at: https://sites.tufts.edu/eeseniordesignhandbook/2015/wireless-mobile-medical-devices/. Last accessed 19 July 2022

34. NHS Digital (2018) Protecting patient data—NHS digital (online) Available at: https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/protecting-patient-data. Last accessed 19 July 2022

35. NHS services hit by cyber-attack (2017) BBC news (online). Available at: https://www.bbc.co.uk/news/health-39899646. Last accessed 19 July 2022

36. National Cancer Institute. (2011). *NCI Dictionary of Cancer Terms*. (online) Available at: https://www.cancer.gov/publications/dictionaries/cancer-terms/def/electronic-medical-record. (Last accessed: 19 July 2022)

37. National Institute of Standards and Technology (2006) Guide to integrating forensic techniques into incident response: publication 800–86. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Last accessed 19 July 2022

38. Neuburger J, Choy W, Milewski K (2020) Smart contracts: best practices. (online) Available at: https://prfirmpwwwcdn0001.azureedge.net/prfirmstgacctpwwwcdncont0001/uploads/dc2c188a1be58c8c9bb8c8babc91bbac.pdf. Last accessed 19 July 2022

39. Nieles M, Dempsey K, Pillitteri VY (2017) An introduction to information security. Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf. Last accessed 19 July 2022

40. OpenLedger Insights (2019) What are consortium blockchains, andwhat purpose do they serve? (online) Available at: https://openledger.info/insights/consortium-blockchains/. Last accessed 19 July 2022

41. Park S, AkatyevN, JangY,Hwang J, KimD,YuW, ShinH,Han C, Kim J (2018)Acomparative study on data protection legislations and government standards to implement digital forensic readiness as mandatory requirement. https://doi.org/10.1016/j.diin.2018.01.012

42. Pourmajidi W, Miranskyy A (2018) Logchain: blockchain-assisted log storage (online) IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/8457918. Last accessed 19 July 2022

43. Protenus (2021) 2021 breach barometer (online) Available at: https://www.protenus.com/resources/2021-breach-barometer/Last accessed 19 July 2022

44. Radcliffe J (2011) Hacking medical devices for fun and insulin: breaking the human scada system. Available at: https://cs.uno.edu/~dbilar/BH-US-2011/materials/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Last accessed 19 July 2022

45. Rahman N, Glisson W, Yang Y, Choo K (2016) Forensic by-design framework for cyberphysical cloud systems. EEE Cloud Computing 1(3):50–59

46. Rahman A, Ahmad R, Ramli S (2014) Forensics readiness for Wireless Body Area Network (WBAN) system (online) IEEE Xplore. Available at: https://ieeexplore.ieee.org/document/6778944. Last accessed 19 July 2022

47. Raju B, Geethakumari G (2016) An advanced forensic readiness model for the cloud environment. In: 2016 international conference on computing, communication and automation (ICCCA). Noida https://doi.org/10.1109/CCAA.2016.7813819.

48. Rowlingson R (2004) A ten step process for forensic readiness. Available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf. Last accessed 19 July 2022

49. Ryckaert V (2019) Hackers held patient data ransom, so Greenfield hospital system paid $50,000, The Indianapolis Star. Available at: https://eu.indystar.com/story/news/crime/2018/01/17/hancock-health-paid-50-000-hackers-who-encrypted-patient-files/1040079001/. Last accessed 19 July 2022

50. SecureW2 (2020) WPA2-enterprise and 802.1x simplified. [online] Available at: https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified. Last accessed 19 July 2022

51. Somasundaram R, ThirugnanamM(2020) Review of security challenges in healthcare internet of things. https://doi.org/10.1007/s11276-020-02340-0

52. Studio Fiorenzi Security & Forensics (2017) GDPR & Forensics Readiness-English (online) Available at: https://www.slideshare.net/AlessandroFiorenzi/gdpr-forensics-readiness-english. Last accessed 19 July 2022

53. Tan J (2001) Forensic readiness (online) CiteSeer. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.480.6094&rep=rep1&type=pdf. Accessed 04 Aug 2020

54. Thompson E (2019) Three ways smart contracts are used in healthcare. Available at: https://uk.finance.yahoo.com/news/three-ways-smart-contracts-used-120013678.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAB2Bc57lNL-hL55sY-VBV-schgWWyDxqgEOx40lhZSWQDfis2VIALKJ-d-AyHK6GEGXHag1SY5Lpr09EQntC-IxsCLTx75ejZz3lsqTMRxxUEBHE-HFHfCcbNsPNsubeQtdYLpU1btexvS7tgTmzPVSC-l-rrTbTDonRC1FNHMSR. Last accessed 19 July 2022

55. Tian Z, Li M, Qiu M, Sun Y, Su S (2019) Block-DEF: a secure digital evidence framework using blockchain. Information Sciences (online). Available at: https://www.sciencedirect.com/science/article/pii/S002002551930297X?via%3Dihub. Last accessed 19 July 2022

56. Vidal C, Choo K (2015) ‘The cloud security ecosystem. Available at: https://www.sciencedirect.com/book/9780128015957/the-cloud-security-ecosystem. Last accessed 19 July 2022

57. Wallace K (2020) Configuring security—wireless networking essential training video tutorial| LinkedIn Learning [online]. Available at: https://www.linkedin.com/learning/wireless-networking-essential-training/configuring-security-2?u=42408908. Accessed 30 March 2021

58. World Health Organisation (2011) mHealth, New horizons for health through mobile technologies. Available at: https://apps.who.int/iris/handle/10665/44607. Last accessed 19 July 2022

59. Zheng Z, Xie S, Dai H, Chen X, Wang H (2017) An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData Congress). (online)Available at: https://ieeexplore.ieee.org/document/8029379. Last accessed 19 July 2022