Jahankhani H and Ibarra J, J Forensic Leg Investig Sci 2019, 5: 029
DOI: 10.24966/FLIS-733X/100029

HSOA Journal of
Forensic, Legal & Investigative Sciences

Review Article

Digital Forensic Investigation for the Internet of Medical Things (IoMT)

Hamid Jahankhani * and Jaime Ibarra

Department of cyber security, Northumbria University, UK

Abstract

With the fast growing development of cloud based architecture, smart technology such as Internet of Medical Things (IoMT) and many other new developments of Artificial Intelligence (AI) and Machine Learning (ML) has caused a large increase in data volumes and more complexities in how to handle and manage the data in a more secure and efficient way. This is heightened by the increasing cyber-attacks and range of different types of attack vectors which has become a lucrative and more organised criminal behaviour with ransom ware-as-a-service, as example. It's becoming apparent that even with attention to the various business structures and methods to mitigate cyber security risks such as, continual review of policies/compliance, training, patching, deploying Intrusion Detection and Prevention Systems (IDPS), etc., has not lessened the cyber security breach effect. In fact, more diverse types of cyber-attacks are increasing and growing year on year at a faster rate, particularly in the healthcare industry which accounts for more than 50% of all cyber-attacks. From a client perspective there are of course many advantages of the modern software and system developments and its 'on data demand' type culture that is expected and will benefit in many ways particularly with the more recent developments in Artificial Intelligence and Machine Learning. However, there is a feeling that there is less control on this data usage and its access and concerns over the scale of impacts leading to criminal effects of identity theft and victimisation.

With these points in mind there is a growing motivation for industry to look at guide line on the forensics investigation of the IoMT devices. The aim of this paper is to highlight the needs and the Digital Forensic Investigation Process Model (DFIPM) for IoMT devices in order to assure data privacy.

***Corresponding author:** Hamid Jahankhani, Department of cyber security, Northumbria University, UK, Email: hamid.jahankhani@northumbria.ac.uk

Citation: Jahankhani H, Ibarra J (2019) Digital Forensic Investigation for the Internet of Medical Things (IoMT). Forensic Leg Investig Sci 5: 029.

Received: August 02, 2019; **Accepted:** August 08, 2019; **Published:** August 15, 2019

Introduction

Malicious attackers are enhancing their Tactics, Techniques and Procedures (TTPs) in order to cause security breaches within organisations leading to data theft, manipulation or blackmailing for instance. An article from Forbes (2019) claims that Electronic Health Records (EHRs) can be worth $1,000 (£778) for hackers and therefore the steady increase of cyber-attacks towards the medical sector. One of the most relevant breaches affecting medical processes was the WannaCry ransomware attack over England National Health Service (NHS) that caused a total of 19,000 appointments cancelled and £92 million in investment to remediate and recover from the incident (Field, 2019) [1]. In addition, an article presented by DiGiacomo [2] (2018) presents that in January of 2018 there were reported approximately 115 cyber-attacks, which the one with highest damage rate was over Health South-East RHF, a healthcare organisation that manages hospitals in Norway with a possibility that over 2.9 million users are potentially affected by the breach (Cimpanu, 2018) [3,4].

The research from Catarinucci, et al. (2015) [5] shows how Personal Health Information (PHI) is processed and transmitted via IoT-based devices used for medical purposes (e.g., Wireless Body Area Networks WBAN, Wireless Sensor Networks WSN, biomedical systems, customised mobile applications), supporting the roles of General Practitioners (GPs) to make faster decisions avoiding unnecessary medical appointments with patients. Furthermore, Mittal (2017) [6] predicted an estimated amount of 163.2 million IoT devices aimed to healthcare purposes. IoT presents several challenges in terms of performance and security, and furthermore currently there is no approved standard or framework supporting this new engineering paradigm. Therefore, as a result it complicates the role of security experts and policymakers to deliver the necessary measures that an organisation requires to achieve regulatory compliance.

Digital Forensic (DF) investigation is a process that works along with Incident Response in order to extract information from a particular device, system or infrastructure, which is submitted to analysis, preservation and presentation of digital evidence that can be used to identify activities related to security/policy violation or crime. Considering that most of devices are unlikely to show or contain the necessary consent from users (O'Connor, et al., 2017) [7], the limitations that Internet of Things (IoT) present in terms of hardware and software, the complexity in its architecture, no standardisation present, along with the recently enforced European Global Data Protection Regulation (GDPR), the requirement to define a comprehensive and holistic forensic investigation model that ensures data privacy and compliance maintaining most discretion during an investigation in order to protect people during and after a security breach is now required.

Internet of Things in Medicine and Wireless Body Area Networks (WBAN)

The research from Al-Fuqaha, et al. (2015) [8] shows details of the IoT architecture with:

a. ***Objects Layer*** - The objects layer can be recognised as perception layer too, and it is represented by the physical devices of the IoT aimed to collect, process information and execute actions according to the orders from operators. This layer is made up of sensors and actuators that can be used for different actions such as querying location, temperature, pressure, weight, etc. This layer is in charge of starting the big data over the architecture, and it is transferred through secure channels to the Object Abstraction Layer (Al-Fuqaha, A., et al., 2015)

b. ***Object Abstraction Layer*** - This layer transfers the information received from the Objects layer using secure channels addressed to the Service Management layer. An interesting feature that IoT devices present is the fact that data is transferred through different communication protocols such as 3G, GSM, UMTS, RFID, WiFi, Bluetooth, Infrared, ZigBee, etc. In addition, this layer handles processes regarding data management and cloud computing

c. ***Service Management Layer*** - This layer pairs a service with the sender/requester based on names and addresses. It allows IoT software developers to work along with different resources without limitations related to specific hardware requirements. Moreover, this layer performs data processing, decision making and delivers the requested services over the wired network

d. ***Application Layer*** - The application layer provides the services to the end user. The main feature is the capability to provide high-quality and smart services in order to comply with the user's needs

e. ***Business Layer*** - The business layer manages the overall IoT environment including the activities of the system and their services developed (Sethi, P. and Sarangi, S.R., 2017) [9]. It must support operators by deploying graphs, flowcharts, reports in order to build a business model according to the information received from the Application layer. In addition, it should support on decision making-processes based on Data analytics. This layer must monitor and manage the behaviour of the underlying four layers and compare the output information with the expected one in order to enhance the services and preserve users' privacy (Al-Fuqaha, A., et al., 2015)

Looking at correlation with the research from Lee, I. et al. (2012) [10], as shown in Figure 1, medical IoT devices are divided in monitoring devices like heart-rate and oxygen-level sensors, providing information about the physiologic state from the patient; and delivery devices like infusion pumps for instance, which can perform therapy actions in order to enhance the patient's health status. In addition, the information gathered from sensors are sent to different administrative platforms such as Electronic Health Records (HER), pharmaceutical stores, hospitals, private vendors, etc., together with systems that are supported by electronic devices aimed at decision support such as controllers and alarms (Figure 1).

IoT-driven healthcare is allowing a transition from hospital to patient-centric with a model called Patient Centred Care (PCC) having as core component patients and their individual health requirements (Farahani, et al., 2018) [11]. The application of IoT in healthcare is possible thanks to Wireless Body Area Networks (WBAN), allowing to retrieve information from patients without the requirement to be present. WBAN can be wearable or implantable, and the IEEE 802.15.6 has proposed a taxonomy for WBAN depending on its location within the human body and their main tasks for the network. The node is classified into the following:

- ***Implant Node:*** It is planted under the skin or within the body.
- ***Body Surface:*** Place over the skin or 2 cm away from the body.
- ***External Node:*** It does not have contact with the human body and is away a minimum distance of 5 cm.

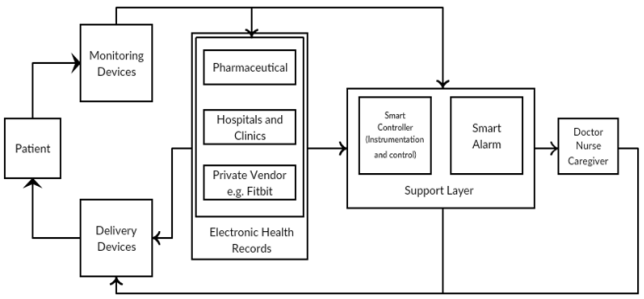

Figure 1: Overview of IoT in Medicine.

In addition, the research from Al-Janabi, S., et al. (2017) [12] presents the architecture of WBAN divided into three tiers. WBAN devices are tied to a certain application and because the human body continuously changes it cannot be defined as a fixed network. Tier-1 consists of intra-WBAN communication, where devices are sending/receiving information to/from a Personnel Server (PS), which acts as a gateway to communicate with local networks. Tier-2 is the bridge between PS and access points (APs), allowing the communication between the local and the wide area network (WAN) however, the AP must be placed in a strategic point allowing emergency services. Finally, Tier-3 allows the communication from the beginning sensor node with the database that normally is allocated within cloud computing environments (Figure 2).

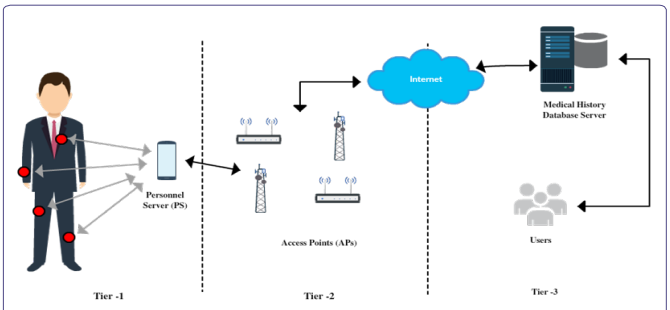

Figure 2: WBAN communication.

Therefore, taking Figures 1 and 2, and the research from Kocabas, et al. (2016) [13], the IoMT architecture can be divided into four layers according as shown in Figure 3. Layer 1 in charge of data acquisition, which involves WBAN (Cavallari, R., et al., 2014) [14] and biomedical sensors, using wireless protocols like WSNs, Bluetooth, ZigBee, etc, video surveillance and mobile networks (Movassaghi, S., et al., 2014) [15]. Layer 2 pre-process the data from sensors because they are limited in resources and due to the amount of information it must be sent to a more sophisticated device, which acts as a gateway in order to transmit the information to the cloud environment. Layer 3 is the cloud granting access to caregivers or patients to their health

information and the ability to predict possible health changes thanks to data analytics and data science. Finally Layer 4 can provide either passive action allowing a better monitoring of the patient's condition, whereas the active action involves order to actuators to provide changes in the medical device (Figure 3).

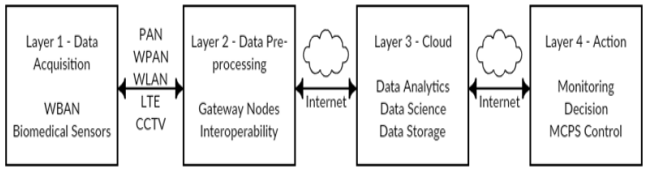

Figure 3: IoMT Architecture.

The Role of Forensic Investigation in IoMT

Forensic investigation is an essential part of incident response in cyber security. Investigators must understand the threats that medical IoT devices are prone such as data exfiltration, data tampering, ransomware, botnets, etc., however, the threat landscape is subject to modifications and it would depend whether the Internet of Things gets standardised or not.

Khan, S., et al. (2017) [16] claim that forensic investigation in the Internet of Things demands solutions from researchers, security and IoT experts, along with cloud computing providers to secure the infrastructure during a security incident. Nowadays, it is a fact that one of the main targets for malicious attackers are EHRs from patients and therefore, investigators must assure privacy to data owners during the investigation process too.

The information in the mind-map in Figure 4, shows the challenges that forensic investigators have when dealing with medical IoTs. Considering that IoT is mainly cloud based, therefore, three stages are recommended for investigation. Firstly the device from users, secondly the network where the information is being transmitted and finally the cloud servers. It is important that the chain of custody is respected so that all digital evidence extracted are reliable, authentic, complete, believable and admissible before it can be presented for judgment.

Figure 4: Digital Forensics Challenges in IoMT.

Although, cloud environment has provided a great support for businesses simplifying the system and network administration, it has also increased the risks in terms of security and privacy. Furthermore, its infrastructure has become more complex to perform forensic investigation.

The challenges that cloud forensics presents are:

- ***Identification:*** It refers to the possible evidence that requires to be gathered for the investigation, which demands collaboration from stakeholders and Cloud Service Providers (CSPs). One of the main challenges presented are the physical location of devices and jurisdiction. Cloud systems can be located at any place throughout the world which can mean for investigators the possibility of dealing with national or regional laws in terms of data acquisition out of bounds (Quick, et al., 2013) [17]. In addition, other important features that cloud provides are decentralised data and redundancy, meaning that there is more than one location for file retrieval, including logs and therefore, the complexity to destroy evidence from the cloud (Ruan, K., et al., 2013) [18]. However, some CSPs have their own log formatting, complicating the task of pulling forensic data. Another important aspect is encryption, which is nowadays important for privacy purposes; however, the encryption algorithms used can mean an important challenge for this and the next phases.

- ***Preservation:*** The main goal is to preserve the integrity of digital evidence that could likely contribute to the overall investigation following the definition from ISO 27037 (2012) [19,20]. However it presents significant challenges, starting with: 1) Chain of Custody (CoC), where it is highlighted the importance of the maintenance of it following guidelines set such as the Association of Chief Police Officers (ACPO) [21] guideline. Principle 3 of the ACPO claims the requirement of keeping record of all processes done (ACPO, 2012). However, this guideline is not adapted for cloud environments (Pichan, et al., 2015) [22], even worse for Internet of Things architectures; 2) Evidence segregation: cloud is featured for multi-tenancy, presenting difficulties in the isolation and preservation of evidence without involving other tenants that are using the same resources; 3) Distributed Storage: Cloud computing is elastic and its data can be stored into many different hosts located worldwide; 4) Data Volatility: Information transmitted to cloud servers are volatile because of its nature such as structured, semi-structured, non-structured, etc., therefore investigators struggle with the preservation and collection of data that could support on building a reliable CoC and Data Integrity: It is important that data collected is accurate and not tampered during its transmission and while being retained by storage services.

- ***Collection or Data Acquisition:*** CSA defines collection as the process to collect items that likely have potential evidence, while acquisition refers to imaging/replicating a copy of the information under specific parameters (CSA, 2013a). Although cloud offers simplified administration, from the investigation standpoint the inaccessibility is the main due to its nature. Access to cloud storage is not possible, while is a client-server environment is guaranteed (Pichan, et al., 2015). Other challenge is trust, which has been highlighted by many researchers (Birk and Wegener, 2011[23]; Daryabar et al., 2013 [24]; Hay and Nance, 2008 [25]; Zawaod and Hasan, 2013 [26]; Hay et al., 2011) [27]. For evidence to be

validated it requires an established level of trust on the layers that compose the architecture of the cloud system. Multiple VMs, sharing same physical resources, allowing to host multiple users at the same time and the information can get across multiple data centres. This feature can mean that privacy of users must be taken into account due to the shared infrastructure. In addition, it means the collection of higher amounts of data implying higher time consumption that could lead to the investigation to get discarded (Ruan, et al., 2013). When information gets collected, it can be encrypted and the time to its decipher could be further than the deadline assigned. The architecture of cloud leads to jurisdiction challenges as mentioned beyond, because of its location investigators could deal with internal regulations that could not allow them to collect the digital evidence required to support the overall investigation.

- ***Examination / Data Analysis:*** The NIST defines this step as the usage of tools and techniques to the collected data in order to extract the relevant information while maintaining its integrity along with the analysis of the results obtained that could answer the questions that lead to the collection of the information (Kent, et al., 2006) [28]. One of the main challenges for investigators is that there is not a standardised framework for logging. Generally, cloud providers have their own policies and formats for log recording (AWS Security Centre A, 2013b, 2014; Google, 2014) [29-31]. Other challenge is the time lining that could contribute to the reconstruction of the sequence of events for building a reliable CoC and delivering a comprehensive explanation to a jury. Digital evidence must be authentic, complete, reliable, admissible and especially believable (Reilly, et al., 2010) [32]. Evidence in cloud can get spread through multiple devices, including mobile, wearable and implantable devices. The research from Ruan et al. (2011) showed that CSPs sometimes exchange services between themselves, leading to a convoluted array of an intra-cloud level dependency chain.

- ***Reporting / Presentation:*** The NIST defines this phase as the process which involves the description of actions performed, and the required tasks to be taken for the improvement of policies, procedures, guidelines, tools and other features of the forensic process (Kent et al., 2006). The main challenges are: 1) Jurisdiction: When presenting the details of the investigation, the law in each nation is different and the research from Ruan et al. (2013) points out the lack of international cooperation for cross nation data access and exchange; 2) CoC: Demonstrating a CoC in cloud environments is more complex than in traditional forensic investigation processes, therefore the need of following a reliable and updated guideline for evidence collection and CoC construction, and; 3) Compliance: If the investigators are keen to get the evidence shown validated by the court, following a standard procedure for forensic investigation is necessary. Some examples are the ACPO and the International Organisation on Computer Evidence (IOCE) (Pichan et al., 2015). However there is not present an approved international standard that could support forensic investigation worldwide, and in the UK the ACPO guideline is outdated because it does not show guideline for cloud environments, even worse for IoT.

User devices are important during an investigation when talking about IoT, and it is more relevant when devices are used for medical purposes. Nowadays IoT devices present several security and privacy issues that creates concern on security experts on whether the device is reliable or not. In addition, a smart devices can be used as a node to perform pivoting techniques in order to get access to the main target. For example, information that was stolen in a casino got successful due to a fish tank that possessed internet connectivity according to the article published by Forbes (Matthews, 2017) [33].

It is unavoidable that smart devices are creating more attack vectors for malicious hackers in order to bypass security layers and get access to their main targets. IoT presents great future for medicine, allowing the usage of either wearable or implantable devices; however, these devices can be hacked or incriminated by malicious attackers by using them as source of attack leading to the prosecution of owners. In addition, IoT presents diverse architectures in terms of hardware and software. One of the common ones in terms of hardware are the Arduino and Raspberry Pi, while for software, the Operating System (OS) Contiki has a software named Cooja used for the simulation of IoT environments. Nevertheless, from the investigative context it is necessary to be clear how to trace back the source of the crime in order to form a believable CoC. This leads to questions such as:

- "Is it necessary to have contact with the provider of the components from the device?" e.g. microprocessor provider.
- "How data is being collected and transmitted from device to cloud?"
- "What are the protocols used in the IoT context for this device?" "Are they compatible with traditional TCP/IP networks?"
- "Was the involved device either a victim or a criminal?"

Moreover, there are ethics involved during the investigation period. For instance, legally users can simply deny the request of retrieving the device for investigation as they are the owners of their information and they can establish their boundaries.

Conclusion

There has been significant increase in the volume and diversity of cyber attacks over the last few years. Attack formations have become more complicated, progressing from script kiddies to crime-for-hire (Ransomware-as-a-Service) and sophisticated hackers. However, attack success relies on the victim acting as the catalyst to initiate the chain of events. Therefore, one of the most complex part to contain or control in handling cyber security risks is the human element.

No matter what amount of training or programme in organisations is used to heighten the intent by malicious outsiders it looks evident that social engineering such phishing attacks will still increase due to human nature of curiosity. Intrusion Detection and Prevention Systems (IDPS) will help but also opens the debate on adding the layer of security through block chain and protecting high value data (sensitive or personal data) so even if attacks have succeeded there are other hurdles to overcome requiring defeating encryption.

This paper has attempted to highlight the challenges of the existing IoMT forensic investigation models by identifying the multiple architectures that IoT interacts with, and showing the gaps for their different forensic investigation processes. Any IoMT forensics investigation framework or model must ensure a high quality CoC including detailed reporting. Finally, having Information Governance

procedures to perform precise tasks and deliver high quality investigation is paramount. Creation of "Smart Contracts" that would allow investigators to adhere to the SLAs agreed along with regulatory compliance will protect the rights of digital citizens.

References

1. Field M (2019) WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled.
2. DiGiacomo J (2018) Data Beach Statistics For 2018 Plus Totals From 2017.
3. Cimpanu C (2018). Hacker Might Have Stolen the Healthcare Data for Half of Norway's Population.
4. Columbus L (2019). 2018 Roundup Of Internet Of Things Forecasts And Market Estimates.
5. Catarinucci L, De Donno D, Mainetti L, Palano L, Patrono L, et al., (2015) An IoT-aware architecture for smart healthcare systems. IEEE 6: 515-526.
6. Mittal S (2019) IoT Ecosystem: How the IoT Market will Explode by 2020.
7. OConnor Y, Rowan W, Lynch L, Heavin C (2017) Privacy by Design: Informed Consent and Internet of Things for Smart Health. Procedia Computer Science 113: 653-658.
8. Al Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M (2015) Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials 4: 2347-2376.
9. Sethi P, Sarangi SR (2017) Internet of things: architectures, protocols, and applications. Journal of Electrical and Computer Engineering Page no: 1-25.
10. Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E, et al., (2012) Challenges and research directions in medical cyber–physical systems. Proceedings of the IEEE 1: 75-90.
11. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, et al., (2018) Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. Future Gener Comp Sy 78: 659-676.
12. AlJanabi S, AlShourbaji I, Shojafar M, Shamshirband S (2017) Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. Egyptian Informatics Journal 2: 113-122.
13. Kocabas O, Soyata T, Aktas MK (2016) Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics.3: 401-416.
14. Cavallari R, Martelli F, Rosini R, Buratti C, Verdone R (2014) A survey on wireless body area networks: Technologies and design challenges. IEEE Communications Surveys & Tutorials 3: 1635-1657.
15. Movassaghi S, Abolhasan M, Lipman J, Smith D, Jamalipour A (2014) Wireless body area networks: A survey. IEEE Communications Surveys & Tutorials 3: 1658-1686.
16. Khan S, (2017) The Role of Forensics in the Internet of Things: Motivations and Requirements. IEEE Internet Initiative eNewsletter.
17. Quick D, Martini B, Choo R (2013) Cloud storage forensics. Syngress.
18. Ruan K, Carthy J, Kechadi T, Baggili I (2013) Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation 1: 34-43.
19. CSA. Mapping the forensic standard ISO/IEC27037 to cloud computing (2013).
20. ISO 27037. Guidelines for identification, collection, acquisition and preservation of digital evidence (2012).
21. ACPO. ACPO good practice guide for digital evidence (2012).
22. Pichan A, Lazarescu M, Soh ST (2015) Cloud forensics: Technical challenges, solutions and comparative analysis. Digital Investigation 13: 38-57.
23. Birk D, Wegener C (2011) Technical issues of forensic investigations in cloud computing environments. In 2011 Sixth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering Page No: 1-10.
24. Daryabar F, Dehghantanha A, Udzir NI, Bin Shamsuddin S, Norouzizadeh F (2013) A survey about impacts of cloud computing on digital forensics. International Journal of Cyber-Security and Digital Forensics 2: 77-95.
25. Hay B, Nance K (2008) Forensics examination of volatile system data using virtual introspection. ACM 3: 74-82.
26. Zawaod S, Hasan R (2013) Cloud Forensics: A Meta-Study of Challenges, Approaches, and Open Problems. Distributed, Parallel, and Cluster Computing.
27. Hay B, Nance K, Bishop M (2011) Storm clouds rising: security challenges for IaaS cloud computing. IEEE Page No: 1-7.
28. Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response. NIST Special Publication 14: 800-886.
29. AWS Security Centre A. Amazon web services: overview of security process (2014).
30. AWS Security Centre A. Logging in AWS. (2013).
31. Google's approach to it security, a google White paper (2014).
32. Reilly D, Wren C, Berry T (2011) Cloud computing: Pros and cons for computer forensic investigations. IJMIP 1: 26-34.
33. Matthews L (2019) Criminals Hacked A Fish Tank To Steal Data From A Casino.

Journal of Anesthesia & Clinical Care

Journal of Addiction & Addictive Disorders

Advances in Microbiology Research

Advances in Industrial Biotechnology

Journal of Agronomy & Agricultural Science

Journal of AIDS Clinical Research & STDs

Journal of Alcoholism, Drug Abuse & Substance Dependence

Journal of Allergy Disorders & Therapy

Journal of Alternative, Complementary & Integrative Medicine

Journal of Alzheimer's & Neurodegenerative Diseases

Journal of Angiology & Vascular Surgery

Journal of Animal Research & Veterinary Science

Archives of Zoological Studies

Archives of Urology

Journal of Atmospheric & Earth-Sciences

Journal of Aquaculture & Fisheries

Journal of Biotech Research & Biochemistry

Journal of Brain & Neuroscience Research

Journal of Cancer Biology & Treatment

Journal of Cardiology: Study & Research

Journal of Cell Biology & Cell Metabolism

Journal of Clinical Dermatology & Therapy

Journal of Clinical Immunology & Immunotherapy

Journal of Clinical Studies & Medical Case Reports

Journal of Community Medicine & Public Health Care

Current Trends: Medical & Biological Engineering

Journal of Cytology & Tissue Biology

Journal of Dentistry: Oral Health & Cosmesis

Journal of Diabetes & Metabolic Disorders

Journal of Dairy Research & Technology

Journal of Emergency Medicine Trauma & Surgical Care

Journal of Environmental Science: Current Research

Journal of Food Science & Nutrition

Journal of Forensic, Legal & Investigative Sciences

Journal of Gastroenterology & Hepatology Research

Journal of Gerontology & Geriatric Medicine

Journal of Genetics & Genomic Sciences

Journal of Hematology, Blood Transfusion & Disorders

Journal of Human Endocrinology

Journal of Hospice & Palliative Medical Care

Journal of Internal Medicine & Primary Healthcare

Journal of Infectious & Non Infectious Diseases

Journal of Light & Laser: Current Trends

Journal of Modern Chemical Sciences

Journal of Medicine: Study & Research

Journal of Nanotechnology: Nanomedicine & Nanobiotechnology

Journal of Neonatology & Clinical Pediatrics

Journal of Nephrology & Renal Therapy

Journal of Non Invasive Vascular Investigation

Journal of Nuclear Medicine, Radiology & Radiation Therapy

Journal of Obesity & Weight Loss

Journal of Orthopedic Research & Physiotherapy

Journal of Otolaryngology, Head & Neck Surgery

Journal of Protein Research & Bioinformatics

Journal of Pathology Clinical & Medical Research

Journal of Pharmacology, Pharmaceutics & Pharmacovigilance

Journal of Physical Medicine, Rehabilitation & Disabilities

Journal of Plant Science: Current Research

Journal of Psychiatry, Depression & Anxiety

Journal of Pulmonary Medicine & Respiratory Research

Journal of Practical & Professional Nursing

Journal of Reproductive Medicine, Gynaecology & Obstetrics

Journal of Stem Cells Research, Development & Therapy

Journal of Surgery: Current Trends & Innovations

Journal of Toxicology: Current Research

Journal of Translational Science and Research

Trends in Anatomy & Physiology

Journal of Vaccines Research & Vaccination

Journal of Virology & Antivirals

Archives of Surgery and Surgical Education

Sports Medicine and Injury Care Journal

International Journal of Case Reports and Therapeutic Studies

Herald Scholarly Open Access, 2561 Cornelia Rd, #205, Herndon, VA 20171, USA.
Tel: +1 202-499-9679; E-mail: info@heraldsopenaccess.us
http://www.heraldopenaccess.us/