**CHAPTER-2**

**INTRODUCTION**

The Internet of medical things (IoMT) is an integrated embedded system of software, hardware, network access, and sensor/actuators [1, 2]. As these systems are more sophisticated and interfere with critical healthcare operations, due to which it raises many security and privacy issues. However, IoMT technology revolves at a greater speed, yet majority of devices are resource-constrained and limits us from considering the high-end mechanism for security and privacy perspectives. Regardless of having multiple protocols and standards for IoMT ecosystems, it lacks in security and privacy issues [3]. In addition, the classical cloud-centric healthcare systems have inherent problems like a single point failure, lack of transparency, low level of control over personal data, and high latency. Because of less availability of medical service professionals, the healthcare industry is unable to provide critical healthcare services to large number of patients [4] during pandemic time. These particular technical challenges are achievable with the help of a perfect combination of protocols, mechanisms, and enhanced system architecture. The remote patient monitoring system (RPMS) helps the healthcare service providers to eliminate unnecessary engagement of professionals in regular consultancy and provides more time for understanding the patient’s health issues to improve the patient health status. It is suggestible to have a parallel supporting system to automate primary healthcare services to handle pandemics with limited healthcare professionals. The blockchain technology is a decentralized distributed ledger system which provides smart-contracts, and exhibits traceability, transparency in digital asset management [7]. The transactions in blockchain are represented as blocks linked together to form a chain of blocks. If one block or transaction is forced to alter, then we need to change the entire chain header information of that blockchain. The transaction integrity is maintained by using Merkel tree mechanism. However, use of blockchain technology for IoMT or H-CPS is not straightforward due to several deficiencies in the original blockchain, such as lack of scalability and high computational demand [8]. The smart-contracts automates event-driven actions without intervention of a third party to provide a cost-effective automation solutions [9]. In order to mitigate large data storage problem of blockchain, we have adopted a distributed data storage system (DDSS) named as Inter Planetary File System (IPFS) [10]. The chosen DDSS provides a content-centric peer-to-peer faster data sharing. It uses data caching and file versioning to maintain multiple documents with same name. However, when a large size file is uploaded to DDSS, it breaks the file into multiple objects of 256kb and connects all these objects to an empty object to retrieve the complete file using Distributed Hash Tables (DHTs) [11].

**2.1 LITERATURE SURVEY:**

### 1. Title: [Security and privacy for the internet of medical things enabled healthcare systems: A survey](https://ieeexplore.ieee.org/abstract/document/8936335/)

**Author**: Y sun

**Abstract**: With the increasing demands on quality healthcare and the raising cost of care, pervasive  
healthcare is considered as a technological solutions to address the global health issues. In  
particular, the recent advances in Internet of Things have led to the development of Internet  
of Medical Things (IoMT). Although such low cost and pervasive sensing devices could  
potentially transform the current reactive care to preventative care, the security and privacy  
issues of such sensing system are often overlooked. As the medical devices capture.

### 2. Title: [PMsec: Physical unclonable function-based robust and lightweight authentication in the Internet of Medical Things](https://ieeexplore.ieee.org/abstract/document/8752409/)

**Author:** VP Yanambaka

**Abstract:** Various commercial off-the-shelf components are available for the development of  
communication-enabled consumer electronics devices. This opens new doors to attackers  
who can take advantage of various vulnerabilities to attack the entire network and  
compromise the integrity of the system and the environment. If a malicious device enters the  
environment and the attacker gains access to the server or transmits malicious data to the  
server or cloud, the entire network can be jeopardized.

### 3. **Title**: [Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations](https://ieeexplore.ieee.org/abstract/document/8688434/)

# Author: En Cheng

**Abstract:** The security issue impacting the Internet-of-Things (IoT) paradigm has recently attracted  
significant attention from the research community. To this end, several surveys were put  
forward addressing various IoT-centric topics, including intrusion detection systems, threat  
modeling, and emerging technologies. In contrast, in this paper, we exclusively focus on the  
ever-evolving IoT vulnerabilities. In this context, we initially provide a comprehensive  
classification of state-of-the-art surveys, which address various dimensions of the IoT

### 4. Title: [Ultra low power ECG processing system for IoT devices](https://link.springer.com/content/pdf/10.1007/978-3-319-97016-5.pdf)

# Author: Guihua Er

**Abstract**: The Internet of Things (IoT) represents a set of interconnected smart objects and people at any time and at any place. The IoT incorporates wide spectrum that can impact businesses, healthcare, social and political aspects. It is a platform that extends from sensors, local processors, wireless transmitters, and central management stations

### 5. Title: [Health-CPS: Healthcare cyber-physical system assisted by cloud and big data](https://ieeexplore.ieee.org/abstract/document/7219371/)

# Author: CW Tsai

**Abstract**: The advances in information technology have witnessed great progress on healthcare technologies in various domains nowadays. However, these new technologies have alsomade healthcare data not only much bigger but also much more difficult to handle and  
process. Moreover, because the data are created from a variety of devices within a short  
time span, the characteristics of these data are that they are stored in different formats and  
created quickly, which can, to a large extent, be regarded as a big data problem..