A systematic review of Security and Privacy issues in the Internet of Medical Things; The role of Machine Learning approaches

Shilan S. Hameed [1,2,*], Wan H Hassan[1], Liza Abdul Latiff[3], Fahad Ghabban[4]

[1] Malaysia-Japan International Institute of Technology (MJIIT), University Teknologi Malaysia, Kuala Lumpur, Malaysia.

[2] Directorate of Information Technology, Koya University, Koya, Kurdistan Region-F.R., Iraq.

[3] Razak Faculty of Technology and Informatics, University Teknologi Malaysia, Kuala Lumpur, Malaysia.

[4] Information Systems Department, College of Computer Sciences and Engineering, Taibah University, Medina, Saudi Arabia

Corresponding author:

Shilan S. Hameed

UTM KL, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia.

Email address: hameed.s@graduate.utm.my

Abstract

Background. The Internet of Medical Things (IoMTs) is gradually replacing the traditional healthcare system. However, little attention has been paid to their security requirements in the development of the IoMT devices and systems. One of the main reasons can be the difficulty of tuning conventional security solutions to the IoMT system. Machine Learning (ML) has been successfully employed in the attack detection and mitigation process. Advanced ML technique can also be a promising approach to address the existing and anticipated IoMT security and privacy issues. However, because of the existing challenges of IoMT system, it is imperative to know how these techniques can be effectively utilized to meet the security and privacy requirements without affecting the IoMT systems quality, services, and device's lifespan.

Methodology. This paper is devoted to perform a Systematic Literature Review (SLR) on the security and privacy issues of IoMT and their solutions by ML techniques. The recent research papers disseminated between 2010 to 2020 are selected from multiple databases and a standardized SLR method is conducted. A total of 153 papers were reviewed and a critical analysis were conducted on the selected papers. Furthermore, this review study attempts to highlight the limitation of the current methods and aims to find possible solutions to them. Thus, a detailed analysis was carried out on the selected papers through focusing on their methods, advantages, limitations, the utilized tools, and data.

38   **Results.** It was observed that ML techniques have been significantly deployed for device and
39   network layer security. Most of the current studies improved traditional metrics while ignored
40   performance complexity metrics in their evaluations. Their studies environments and utilized
41   data barely represent IoMT system. Therefore, conventional ML techniques may fail if metrics
42   such as resource complexity and power usage are not considered.

44   **Keywords**: The Internet of Medical Things, IoMT, Security and Privacy, Machine Learning

Background

A. IoMT and its Classification

47 The Internet of Thing (IoT) is a fast growing technology by which the infrastructures,
48 computerized machines, physical things, applications and individuals are allowed to connect,
49 communicate, capture and exchange information through networking (Farahani et al. 2018; Noor
50 & Hassan 2019). Hence, the Internet of Medical Thing (IoMT) is the application of IoT in
51 medicine and healthcare industry (Alsubaei et al. 2019a; He et al. 2018). It is anticipated that
52 with the implementation of IoMT a significant improvement in the efficiency and standard of
53 treatment is achieved thanks to the steady innovations in IoT including the development in
54 microprocessors, biosensor architecture and evolving 5G technologies (Ahad et al. 2019).
55 However, it is hard to maintain a specific architecture as a baseline due to the variety of devices
56 and their different usage. Consequently, various approaches for the IoT architectures and layers
57 were presented in literature (Sethi & Sarangi 2017; Weyrich & Ebert 2015) such as protocol-
58 based architecture (Burhan et al. 2018; Mosenia & Jha 2016; Weyrich & Ebert 2015) and data
59 processing stages known as edge, fog, and cloud based approaches (Escamilla-Ambrosio et al.
60 2018). In the current review, we present two common architectures of the IoMT. In the first
61 architecture, the IoMT is treated as to be composed of three main elements: (i) network of
62 wireless body sensor, which is device layer, (ii) internet connected smart access points
63 (gateway), which is fog layer, and (iii) cloud computing and big data service, which is cloud
64 layer (Rahmani et al. 2018). The second architecture is simply defined by sensing/device layer,
65 network layer, and server (personal/medical) layer (Sun et al. 2019). However, some researchers
66 have divided the IoMT architecture into more than three layers based on the requirements
67 adopted for a specific application of IoMT (Elrawy et al. 2018; Grammatikis et al. 2019).
68 Furthermore, there are four types of smart medical devices in IoMT that are categorized based on
69 their location of implementation on human body (Nanayakkara et al. 2019). Table 1 shows a
70 brief explanation on the types of IoMT devices and their properties. According to the U.S. Food
71 and Drug Administration (FDA), the IoMT devices can be also classified based on their risk
72 value. Implantable devices such as Implantable cardioverter-defibrillator (ICD),
73 Electrocardiography (ECG), Electromyography (EMG), and Electroencephalography (EEG) are
74 under high-risk category. Hence, they are regulated and certified by FDA. However, non-
75 implantable devices such as fitness trackers, and smart watches are under low-risk category.
76 Therefore, they neither require certification nor regulation by the FDA (Jaigirdar et al. 2019).

77

78   **Table 1:**

79   **The types and characteristics of medical devices used in the IoMT system.**

81   Medical devices and biosensors are responsible for capturing body's vital signs, and transferring
82   a huge real-time raw biological data such as heart rate, brain signal, temperature of the body, and
83   glucose level in blood (Dang et al. 2019). These raw data are accumulated and processed at the
84   personal servers that are either devices located near the patient's body such as mobile phones,
85   medical programmers, and laptops or devices placed far from body such as gateways and routers.
86   Additionally, personal servers usually include a computing analysis facility, which is coupled
87   with a local archiving database in order to store the initial records of the patient. Furthermore, its
88   warning system alerts the patient whenever an abnormality is observed (Newaz et al. 2020). The
89   communication link between body area network (sensors attached to or close to human body)
90   and personal server is usually employed by low-power wireless networking technologies such as
91   Bluetooth or Bluetooth Low Energy (BLE), Near-Field Communication (NFC), Radio-
92   Frequency IDentification (RFID), Zigbee and Z-Wave. Noteworthy, Bluetooth is mostly used in
93   wearable devices, while RFID and NFC are accommodating an ultra-low energy and short-range
94   communication topology. Hence, they are mostly applicable in the implantable devices (Newaz
95   et al. 2020; Sun et al. 2019). In this way, the aggregated data at the personal server is directed to
96   the medical server. Long-range wireless technologies such as Wi-Fi, GSM and LoRa are also
97   used for the connection between the personal server gateway and medical sever.

99   The data analytics are conventionally performed at the cloud. However, cloud computing faces
100   the issues of delay and privacy. For this reason, the term of fog computing at gateways (fog
101   devices) was introduced in 2017 (Rahmani et al. 2018). This approach is used to shift some of
102   the cloud computing works closer to the smart devices aiming at achieving a faster computation
103   with keeping privacy (Dang et al. 2019; Firouzi et al. 2018; Rahmani et al. 2018). It is not
104   deniable that using smart medical devices has made the life easier and healthier. However, there
105   are many safety and security gaps in these devices that put not only the devices at risk but expose
106   a significant risk to the patient's life (Yaacoub et al. 2020)

108   **B. Security and Privacy in the IoMT**
109   The IoMT devices are vulnerable to traditional and zero-day attacks. This is mainly due to the
110   lack of existing security protocols and measures in the fabrication of the devices in addition to
111   the nature of the devices and IoT network. The devices are very tiny, where their computational
112   resources and batteries cannot handle computation of cryptographic and existing heavy security
113   measures. Furthermore, the network of IoMT is heterogeneous, which is composed of different
114   protocols at each layer, making one security solution not applicable to all devices. It was
115   reported in an estimation made by the Statista (The Statistics Portal) that the number of medical
116   IoT devices in the European Union (EU) could reach 25.8 million devices by 2025 (Schneble &
117   Thamilarasu 2019b). In addition to a steady increase in the number of smart medical devices and
118   benefits from the low price of wireless sensors, the security and privacy issues are become the
119   main concern (He et al. 2018). Besides, when internet connected devices are increased, their

120   produced data will eventually increase (Dimitrov 2016; Firouzi et al. 2018; Ma et al. 2017). It
121   was predicted by Statista that IoT devices could produce about 79.4 zettabytes (ZB) by 2025 (S.
122   O'Dea 2020). It is well known that not only the IoMT devices are at risk of cyber-attack, their
123   data are also at a high risk. In fact, privacy issues and data disclosure are the current utmost
124   issues in IoMT infrastructure (Gupta et al. 2020b; Xu et al. 2020)..

125   The IoMT security and privacy requirements are different from the traditional network
126   requirements which are usually referred to as CIA-triad (confidentiality, integrity, and
127   availability). Other metrics such as privacy, and non-repudiation are also essential for the IoMT
128   system (Grammatikis et al. 2019; Nanayakkara et al. 2019; Newaz et al. 2020; Yaacoub et al.
129   2020). The followings are definitions of these metrics used in IoMT system.
130   a)   *Confidentiality*: It limits unauthorized access to certain information and it guarantees the
131   protection of confidential information. Unauthorized access may lead to data leakage and
132   sometimes life-threatening situations (Alassaf & Gutub 2019).
133   b)   *Integrity*: It ensures that the data and reading of devices are not altered, deleted, or
134   injected by unauthorized parties. Attacks on integrity such as false data injection on implantable
135   pacemaker may lead to death (Yaacoub et al. 2020).
136   c)   *Availability*: It ensures that the data, computing elements, and communications are
137   accessible and working continuously when they are required by a service. System service
138   interruption poses danger on patients health, considering a surgery room equipped with wireless
139   medical devices (Sun et al. 2019).
140   d)   *Privacy:* It ensures that privacy rules are enforced by the IoMT system and allows users
141   to access their private details (Mosenia & Jha 2016). The collection of confidential health
142   records must conform with legal and ethical laws of privacy such as the General Data Protection
143   Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA)
144   (Gupta et al. 2020b; Tovino 2016). These rules ensure the protection of private patient data from
145   disclosure. It is important that Electronic Health Records (EHRs) should not be kept beyond the
146   time of their need. Data should not be breached while stored, transmitted, and used (Hassija et al.
147   2019). Due to open communication channels and neglecting data privacy, the possibility of
148   confidential and private details being released, hacked, or compromised is extremely high. This
149   can be compromised through passive attacks or active attacks (Yaacoub et al. 2020).
150   e)   *Non-repudiation*: This metric encompasses the ability of the system to validate the
151   presence or absence of an activity (Mosenia & Jha 2016; Yeh 2016). It ensures that the sending
152   node is granted a delivery receipt and the receiver node is granted a proof on the identity of the
153   sender so that none of them is denied in the process (Newaz et al. 2020).
154   A threat that risks any of the aforementioned pillars of IoMT security and privacy is considered
155   an attack. Table 2 shows the categorized attacks based on the IoMT targeted layer with respect to
156   their impacts on the security requirements of IoMT system. It is worth to mention that despite of
157   the reported attacks the appearance of zero-day attacks is a daily possibility. While these attacks
158   are threatening the privacy of patients, it is also resulted in unbearable financial damage and loss
159   of reputation (Sun et al. 2019). For example, a recent ransomware attack on hospitals in the

160 USA, which infected 400 U.S. sites has resulted in service disruption and data disclosure (Davis
161 2020b). According to a latest analysis by Comparitech, these attacks have cost the healthcare
162 industry over $160 million since 2016 (Davis 2020a). Additionally, it was claimed that attacks
163 on brain implants, lead to death (Rathore et al. 2019). Therefore, with the increased risk of cyber-
164 attack on the IoMT system, the emergence and development of robust security solutions are
165 become a must.
166
167 **Table 2:**
168 **Attacks on different IoMT layers with their respective impact on security requirements.**
169

170 ## C. Machine Learning Techniques and their Evaluation Metrics
171 Machine Learning (ML) is a branch of Artificial Intelligence (AI) which learns from data and
172 experiences without being explicitly programmed (Kubat 2017). ML can play a vital role in
173 IoMT, especially at computing nodes such as cloud/fog computing, for continuous data analysis
174 and producing meaningful information. Recently, ML has been interestingly applied in various
175 areas of IoT and IoMT (Alimadadi et al. 2020; Ardabili et al. 2020; Cui et al. 2018; Durga et al.
176 2019; Pannu 2015; Pramanik et al. 2017; Xiao et al. 2018). ML can be effectively used in many
177 ways to tackle the security issues of the IoMT (Cui et al. 2018; Gupta et al. 2020a; Pandey et al.
178 2020; Pirbhulal et al. 2019), whereas traditional security measures cannot prevent the system
179 from zero-day attacks, and they are resource extensive for the IoMT systems. Advanced ML
180 techniques can learn from massive generated data of IoMT, thereby finding new trends of attacks
181 (Hussain et al. 2020). Hence, data hungry ML techniques can be perfectly tuned with IoMT.
182 There are three main types of ML algorithms which can be used for solving the IoMT security
183 problems, namely **supervised, unsupervised,** and **semi-supervised** algorithms. The ***Supervised***
184 technique deals with labelled data, in which classes or labels are known. There are two forms of
185 supervised learning which are classification and regression (Kubat 2017). Examples of
186 supervised learning are Support Vector Machine, Decision Trees and Neural Network. These
187 methods are used for the **attack and malware detection** purpose such as signature based
188 Intrusion Detection System (IDS) (Eskandari et al. 2020; RM et al. 2020). Since it is not always
189 easy to label the data by human, ***unsupervised techniques*** are utilized to categorize them based
190 on their similar traits (Schneble & Thamilarasu 2019b). Examples of these techniques are K-
191 nearest Neighbor (KNN), Self-Organizing Map (SOM), and Latent Dirichlet Allocation (LDA)
192 (Gupta et al. 2020a). These methods are effective for **anomaly detection** of new attacks (Ahmad
193 et al. 2019; Bostani & Sheikhan 2017; Eskandari et al. 2020). Based on the no free lunch theory,
194 not every unlabeled data is useful for prediction (Rathore & Park 2018). Hence, one can
195 overcome this issue by incorporating some labelled data. ***Semi-Supervised Learning*** is a
196 younger ML sub-field, in which some data are labelled out of a wide number of learning data
197 (Wolfgang 2011). Also, semi-supervised models can be used for attack detection and to avoid
198 adversarial attacks on ML techniques (Miyato et al. 2018; Rathore & Park 2018). In addition to
199 the main classes of ML, a new branch called ***Deep learning (DL)*** has been recently emerged,

200 which is an advanced form of Neural Network. It has several layers of artificial neural network
201 that mimic the working principle of human brain in processing data for detecting objects,
202 recognizing speech, translating languages, and making decisions. DL can perform feature
203 selection/extraction based on its learning process without the need of another method compared
204 to traditional ML techniques that require an additional feature selection (Amanullah et al. 2020).
205 DL comes in different forms, including Convolution Neural Network (CNN), Recurrent Neural
206 Network (RNN), Long-Short Term Memory (LSTM), Auto-Encoders (AE), Boltzmann Machine
207 (BM), Generative Adversarial Networks (GAN), Feed forward Deep Networks (FDN) and Deep
208 Belief Networks (DBN) (Amanullah et al. 2020; Hussain et al. 2020; Saeed et al. 2016). Auto-
209 encoders are usually the best choice of unsupervised learning to be used for anomaly detection
210 (Lopez-Martin et al. 2017).The use of DL for security solutions such as attack detection could be
211 a durable method for slight mutations or new threats due to its ability to extract features
212 (Amanullah et al. 2020; Diro & Chilamkurti 2018; Durga et al. 2019; Ibitoye et al. 2019; Parra et
213 al. 2020; Sollins 2018). On the other hand, the IoMT sensors generate a large amount of data at a
214 fast speed, thereby producing Big data (Cao 2017; Pramanik et al. 2017; Saheb & Izadi 2019)
215 (Marjani et al. 2017). *Big data* refers to the data that are too large and/or complex to be
216 efficiently handled by conventional technologies and tools (Dimitrov 2016; Hameed et al. 2017;
217 Sadoughi et al. 2020; Vinitha et al. 2018). A big data is usually defined by three key features,
218 known as 3Vs, which are volume, velocity and variety (Amanullah et al. 2020; Russom 2011). It
219 was seen in literature that DL and big data have been used together as DL performs better with
220 increasing the amount of data (Gheisari et al. 2017). Very recently, DL and Big Data were used
221 in combination with new technologies of blockchain and reinforcement learning for security
222 purposes in the industrial IoT systems (Aman et al. 2020; Liang et al. 2020; Liu et al. 2018).
223 Concludingly, the ML methods can be employed in different security solutions such as:

224 **Sensor Anomaly Detection in Medical Devices:** Anomaly detection is the process of finding
225 deviations from the normal data. Such anomalies are attributed to the occurrence of phenomena
226 that do not obey a regular process. These irregularities are triggered by abnormal behaviors such
227 as internal assault or false data injection attack (Amanullah et al. 2020), leading to a false reading
228 of the sensors. ML approach in anomaly detection is the most used mechanism for sensor
229 security. Nonetheless, it needs a considerable adoption in order to be implemented in the IoMT
230 (Butun et al. 2015; Hasan et al. 2019).

231 **Authentication and Access Control:** Authentication is the process of ensuring whether the
232 IoMT user is correct, while authorization is associated with the extent of access given to each
233 individual (patient and healthcare provider)(Aghili et al. 2019b). They are the most effective
234 methods to prevent attacks on confidentiality and integrity of the IoMT data (Aghili et al. 2019b;
235 Nguyen et al. 2019; Yang et al. 2018). Different techniques can be combined in the process of
236 authentication and authorization such as cryptography, ML, and lightweight approaches (Aghili
237 et al. 2019b; Shen et al. 2018; Wu et al. 2018). Details about these methods can be found in (Sun
238 et al. 2019).

239   **Intrusion and Malware Detection:**   The most common intrusion detection is network intrusion
240   detection (NIDS) using network traffic analysis. If the log data of sensors and devices are used, it
241   becomes host-based intrusion detection (HIDS) (Aluvalu 2020). Both types of intrusion detection
242   use metrics for finding anomalies (unknown-attacks) and signatures (known-attacks) that do not
243   match with the normal network traffic or sensor data. These detection systems are similar in
244   having an agent for collecting data and a processing unit in the attack detection and reporting the
245   intrusions. However, they are different in: i) Source of data: host-based (Asfaw et al. 2010),
246   network-based (Maleh et al. 2015), hybrid (Ahmad et al. 2019), ii) Method of detection
247   (Abhishek et al. 2018): signature-based (Wang et al. 2018), anomaly-based, and iii) Architecture:
248   centralized, and distributed (Anthi et al. 2018; da Costa et al. 2019). Signature based approaches
249   can easily detect the known attacks but unable to detect new attacks. On the other hand,
250   anomaly-based IDS find anomalous behavior by learning from current data. Therefore, they can
251   detect new attacks, but they are less accurate and computationally expensive (Arshad et al. 2020;
252   Jan et al. 2019; Midi et al. 2017). The recent attacks such as DoS, DDoS and different malware
253   attacks are the most common mitigated attacks by IDSs (Din et al. 2019; Meidan et al. 2018;
254   Roopak et al. 2020).

255   In the process of evaluating ML techniques in terms of accuracy, reliability, and applicability,
256   some special metrics should be considered. Table 3 shows the most used metrics with their
257   definition and formula.

258

259   **Table 3:**
260   **The evaluation metrics used for ML techniques.**

261

262   **D. IoMT Security and Privacy Solutions using Machine Learning.**

263

264   **Research Rationale**
265   The unique nature of the IoMT system with small size devices, heterogeneous network, and
266   diverse protocols, has made the implementation of traditional security frameworks difficult by
267   the medical companies. This in turn makes the IoMT system suspectable to different attacks.
268   Recent advancement in the techniques and technologies of ML has led to achieve fruitful
269   strategies to tackle the issues of IoMT security. However, IoMT system facing more challenges
270   than ordinary network systems.

271   IoMT devices usually generate a large amount of streaming data (Amanullah et al. 2020). The
272   diversity nature of these data along with the limited power and resources of IoMT devices,
273   especially for the implantable medical devices (Sun et al. 2019), impose a high computational
274   burden on the traditional ML techniques, thereby reducing their effective application in the IoMT
275   devices. Hence, new strategies are required to apply the ML approaches efficiently.

276   Consequently, understanding the current security and privacy issues of IoMT system with their
277   respective solutions using ML techniques is essential. Furthermore, it is significant to know the
278   effectiveness of current deployed ML techniques and to understand their solution strength

279   offered to the challenges of IoMT system so far. We found that little attention has been paid in
280   literature to elaborate on these issues. Therefore, in this work, a Systematic Literature Review
281   (SLR) is presented, in which attempts are made to reveal the strong points and limitations of the
282   works performed in this area followed by establishing robust improvement strategies. As such,
283   three research questions can be generated as follows:
284   RQ1: What is the current state of the art and direction of study in IoMT security using ML?
285   RQ2: What kind of tools and data are used for applying ML techniques in IoMT security?
286   RQ3: How ML techniques are effectively applied and what are their limitations?
287   This study is intended for new researchers in the field, and for those who are keen to know about
288   recent advances and limitations in IoMT security issues followed by their solutions using ML
289   approaches.
290

Related Studies

292   In a review performed by Cui et al. (Cui et al. 2018), an overview of ML application in the
293   domain of generic IoT was reported to focus on the main applications of ML and its relevant
294   techniques in IoT. However, the work has partially covered the IoT security solutions with ML.
295   In another study (Tahsien et al. 2020), Tahsien et al. reviewed the architectures of generic IoT
296   and ML-based potential solutions for IoT security. Another comprehensive review on using ML
297   techniques in generic IoT security was also conducted by Hussain et al. (Hussain et al. 2020).
298   The authors discussed major threats to each layer of IoT and reviewed recent works of using ML
299   techniques in securing IoT. Noticeably, the reviewed studies, tools and datasets were not
300   comprehensively elaborated and the IoMT system was not explored. A review study on security
301   and privacy of IoMT was conducted by Sun et al., revealing the security requirements and
302   challenges of IoMT with more focus on authentication and access control (Sun et al. 2019).
303   Moreover, a survey on IoMT security and privacy was carried out by Newaz et al (Newaz et al.
304   2020), in which a detailed discussion was given on the security and privacy threats in healthcare
305   systems. They also presented a subsection on the current solutions for healthcare IoT security.
306   On the other hand, a review on IoMT security issues and limitations with details about the
307   attacks and their impact on IoMT was presented, whereas a special attention was paid on
308   lightweight security solutions (Yaacoub et al. 2020). Concludingly, there have been some
309   reviews found in literature about generic IoT security using ML and DL. However, little
310   attention has been paid to ML applications for the IoMT security and privacy. To this end, the
311   current review is intended to address the role of ML technologies in tackling the issues of IoMT
312   security and privacy. That is by carrying out a comprehensive and systematic review on the
313   related works performed in literature. For this reason, it is difficult to compare our work with the
314   existing surveys. However, a fair relevant comparison of the previous reviews with that of the
315   current study is given in Table 4.
316

Table 4:

318   **Comparison between this survey and other related surveys.**

319
320
Survey methodology
Research Design
323 In the current work, a systematic research design is generated. After creating a list of research
324 questions, searching for relevant papers was started from different databases including IEEE,
325 Web of Science, Springer Link, Scopus, Science Direct. Then, the most specific and relevant
326 papers were extracted to answer the research questions. Later on, the selected papers were
327 comprehensively screened and analyzed. Finally, the results were presented using different
328 methods.

Database Searching and Research Selection
330 A keyword-based search was applied by using different forms and combinations of Machine
331 Learning, The Internet of Medical Things, Security and Privacy and their synonyms. Then, the
332 synonym list was expanded during researching and a Research Information Template (RIT) was
333 generated accordingly, as shown in Fig. 1. Boolean expressions with all the keyword
334 combinations were constructed to form all the searching possibilities. The literature searches
335 were carried out in April 2020, whereas each RIT query string was checked in the respective
336 databases followed by saving the query results. The period affecting this analysis was justified
337 between January 2010 and April 2020. Initially, the full metadata would have been selected for
338 searching and if this option was not available, the common search choice (keyword, title and
339 abstract) was used. The search queries and results returned by the databases are shown in Table
340 5. Noteworthy, a total of 28,155 search results were returned from all the five databases. The
341 titles were then examined for significant and duplicate papers and a total of 500 papers were
342 remained. After that, the papers whose mentioned IoMT/ML/security and privacy were chosen.
343 As such, a total of 153 publications were filtered and the remainder was removed. After going
344 through the full text of the papers, only 43 papers were selected for critical analysis and
345 conducting a careful review of their contents. The rest of the papers were used while discussing
346 the topics related to the background of the study. The selection criteria given in Table 6 were
347 performed equally on the title, abstract, conclusion, and full paper in all stages of screening,
348 while the detailed process of the methodology is shown in Fig. 2.
349
350 **Table 5:**
351   **The searching queries and results achieved from five different databases.**
352
353 **Table 6:**
354   **The selection criteria applied to the reviewed papers.**
355
356 **Figure 1: The keywords used in the Research Information Template (RIT).**
357
358 **Figure 2: The search strategy used for selecting the research papers.**

359

Results and findings

361 In this work, two types of analysis were performed which include a bibliometric analysis and
362 technical analysis, as discussed in the next subsections.

363

Bibliometric Analysis

365 To show the leading countries whose researchers working in the field of IoMT and its security,
366 each individual paper was examined according to the affiliation of authors. It was observed that
367 the USA has made 30% of the papers among 21 affiliated countries, as shown in Fig. 3.
368 Moreover, it was found that research performed on ML applications in the IoMT security has
369 grown steadily from 10 percent in 2015 to a peak value of 80 percent in 2019, as shown in Fig. 4.

370

371

372 **Figure 3: Geographical distribution of the papers.**

373

374

375 **Figure 4: Distribution of the papers by year.**

376

377 It is worth to mention that the majority of the papers were journal article, contributing to 73% of
378 the papers, while 21% of the papers were from conferences of the Institute of Electrical
379 Electronics Engineering (IEEE) and only 6% of the papers were belong to book chapters as seen
380 in Fig. 5. Furthermore, a significant number of papers (64%) was published by the IEEE and
381 17% was published by Elsevier, as seen in Fig. 6.

382

383 **Figure 5: The type of analyzed papers used in the current research.**

384

385 **Figure 6: Distribution of the papers according to the publishers.**

386

387

Studies Technical Analysis

389

Classification of Studies

391 The vast majority of ML related articles were about supervised ML, while the rest of papers were
392 found to report on a combination of supervised and unsupervised ML, with few papers to focus
393 on unsupervised ML. Deep learning was also used in some of the studies, while one study has
394 used big data technology. The papers were further categorized based on the type of medical
395 devices intended to get secured. Almost all studies have focused on the security of wearable
396 devices, while few of them elaborated on the security measures for implantable devices. Only
397 one study was found to focus on securing programmer devices. The targeted IoMT layers in most

398   of the studies were device and sensor layers. Network layer was addressed in some studies, while
399   cloud layer was reported by two paper. Table 7 shows further details on the disseminated studies
400   related to their ML category and types of devices with their targeted layer.
401   The papers were then classified into different subsections based on the approaches taken to
402   tackle the security issues of the IoMT, as was discussed in the background section. In addition,
403   an in-depth assessment was carried out through a critical analysis of the articles, demonstrating
404   the strong characteristics and limitations of each study. In the following sections, we discuss on
405   the findings of the aforementioned analysis.
406   **Table 7:**
407   **Classification of papers based on ML category, medical device, the IoMT layer.**
408
409   **Sensor Anomaly Detection for Medical Devices:** Herein, the review results of the current
410   subsection related research articles are presented and analyzed, while the highlighted limitations
411   of the studies are given in Table 8.
412   In a work performed by Haque et al. (Haque et al. 2015), a sensor anomaly detection system was
413   proposed to differentiate the true from false alarms. The research used a historic data to be
414   compared with the actual sensed data for prediction, whereas majority voting was used for their
415   distinguishing. Consequently, the error was calculated based on dynamic threshold. The
416   proposed method has been implemented in Java environment, supplied by the SMO regression.
417   The results illustrated that the proposed system had a high Detection Rate and low FPR for three
418   medical datasets. Furthermore, referring to the security of signals from deep brain stimulators,
419   the authors in (Abdaoui et al. 2020) built a system for distinguishing false alarms from legitimate
420   ones and classified the attacks using Raspberry Pi3 and deep learning. It was found that deep
421   learning can show an accuracy of about 97% to learn and predict the fake signals. Also, a web-
422   based application was generated using the web engine (Flask) for that purpose.
423   Despite the effective application of ML algorithms, they are generating high computational
424   overhead on the low-power embedded frameworks. Rathore et al. (Rathore et al. 2018c)
425   presented a neural network based MLP solution embedded on an FPGA chip system for securing
426   insulin pump devices that are used by diabetic patients. The authors reported an accuracy of
427   98.1% for their system in distinguishing the fake from genuine glucose measurements. The
428   reliability of whole framework was improved by 18% in the case of securing one device and
429   enhanced by 90% in the case of securing the whole devices.
430   Khan et al. (Khan et al. 2017) proposed a personal server centered (phone based) Markov model-
431   based detection mechanism for the detection of multiple intrusions such as forgery attacks, false
432   data insertions, and data modifications in the ECG data for smart medical devices. The extracted
433   features by DWT method were generated representing a feature set followed by their division
434   into sequences. Each sequence's probability was then calculated. The probability value was used
435   as a benchmark to decide if any changes have occurred. Analyzed results showed that the method
436   has a high detection rate with abnormalities of 5% and 10% in the dataset. However, it has a
437   higher TNR with reduced running time for both 5% and 10% abnormalities.

438 In another study (Gao & Thamilarasu 2017), some ML techniques were used, including decision
439 tree, SVM and K-means, to detect the security attacks in implantable devices. An external
440 detection device was used to monitor the network and the ML classifiers were utilized to detect
441 anomalies on the gateway device for detecting forced device authentication that results in
442 resource depletion of the device. For this purpose, a feature set specific to IMD devices was
443 constructed. Experimental results demonstrated that decision tree-based algorithms achieved the
444 highest detection accuracy, low false positive rate, fast training and prediction speed compared to
445 those of other algorithms.
446 In another study made by Sehatbakhsh et al. (Sehatbakhsh et al. 2018), SYNDROME was
447 proposed. This method can detect code injection attack in a known program which runs on the
448 system in a real time manner. Statistical based methods such as K-S test and external hardware
449 device were used for detecting signal anomaly. The ability of the method was evaluated by
450 implementing control-flow hijack attacks on a real medical device (syringe pump) embedded
451 system. The evaluation results on using four distinct hardware systems have shown that the
452 proposed model can detect all the attacks with 100% TPR and zero false positive, while the
453 detection latency was less than two milliseconds.
454 In a pioneer work carried out by Zhang et al. (Zhang et al. 2013), a security framework was
455 proposed for medical devices monitoring (MedMon). The proposed model was embedded on an
456 external device which listens to all the passed signals coming from or sending to the medical
457 devices by using a multi-layered anomaly detection (behavioral and physical anomalies). The
458 system is useful for those medical devices that do not use encryption. Consequently, the
459 framework either passively notifies the user or actively jams the signal. This solution does not
460 add power overhead on the medical devices without modification to their software and hardware.
461 An insulin delivery device was tested against the proposed method. Results depicted that the
462 system could successfully detect multiple attacks.
463 For the same purpose, a different approach has been proposed by Newaz et al. (Newaz et al.
464 2019) which is based on ML data-driven security framework, called HealthGuard, for detecting
465 three types of malicious activities in a SHS by considering interconnected body function. Here,
466 ML based techniques (Artificial Neural Network, Decision Tree, Random Forest, and k-Nearest
467 Neighbor) were used to interpret the physiological signs in multiple attached SHS instruments
468 and compare them to identify the differences in the person's body functions, thereby
469 differentiating benevolent and malicious behaviors. Moreover, there is no need to have user
470 identification for the medical devices and the framework does not increase any overhead on the
471 sensors while collecting data. The proposed system is trained with physiological data obtained
472 from eight IoMT devices containing 12 genuine events consist of 7 normal patient activities and
473 five disease associated activities. Results showed an accuracy of 91% and F1 score of 90%.
474 Ben Amor et al. (Ben Amor et al. 2020) suggested an anomaly data detection and separation for
475 the mobile smart healthcare. Two steps were implemented in the study, namely a preprocessing
476 step and a real-time processing step. PCA and Correlation Coefficient were used for feature
477 selection and feature extraction. By this, the system can detect false physiological readings and

478   can distinguish between the false and true medical functions. Other researchers (Mohamed et al.
479   2019) attempted to improve the detection efficiency by proposing an intrusion cancellation
480   approach, thereby making the anomaly detection in medical devices efficient. This was achieved
481   by using filters for eliminating noises in the medical data followed by detecting intrusions
482   through statistically analyzed amplitude and frequency. Finally, the detected intrusions were
483   removed to execute the anomaly detection in the medical device for diagnostic purpose. The
484   simulation results applied on two sensor data showed that the system has high TPR and
485   comparable FPR.
486   Anomaly or malfunction sensor reading resulted from defective sensor nodes or produced by
487   fraudulent foreign entities can contribute to medical error and even mortality in patients.
488   Researchers (Salem et al. 2014) suggested a system to identify abnormalities in Wireless Body
489   Area Network (WBAN) for pervasive patient and health surveillance. The proposed software
490   combines advanced data mining and deep learning technologies with existing sensor fusion
491   techniques. The suggested model uses Support Vector Machine (SVM) to identify irregular
492   incidents of the received sensor data. When an anomaly is detected, a regularly updated and
493   regressive prediction model is used to differentiate between the stable and faulty readings
494   resulting in a higher TPR and lower FNR.
495   It was recently (Hau & Lupu 2019) emphasized that identification of fake data injections in low
496   dense Wireless Sensor Networks is important for maintaining the integrity of data, particularly in
497   medical IoT systems. Hence, researchers proposed a framework for detecting false data using
498   anomalies in temporal-attribute correlations between sensor measurements. This method is
499   successful in detecting attacks when more than one sensor is colluding to record coherent
500   measurements (Hau & Lupu 2019). Nevertheless, with an increase in the number of colluding
501   sensors, the detection efficiency degrades to a point that the detection fails when most of the
502   sensors are colluding.
503   Furthermore, researchers (Nagdeo & Mahapatro 2019) have implemented an ML model to
504   separate anomalous data from legitimate sensed data. This research used a combination of ANN
505   with Ensemble LinReg as a detection technique for abnormalities in WBAN sensors. Firstly,
506   normal, and abnormal health records were classified. Secondly, regression methodology was
507   used to recognize the anomaly and real vital data. For the validation purpose, real medical
508   physiological datasets were used. It was concluded that the system was able to effectively detect
509   the anomaly.
510   Additionally, measured data of blood glucose sensor was examined in order to detect adversarial
511   and accidental data modification intrusions (Verner & Butvinik 2017). Here, Otsu's thresholding
512   algorithm was used with extra statistical analysis to create different informative feature vectors.
513   Then, linear SVM with different misclassification parameters were used to classify the feature
514   vectors. The obtained results on huge patient's data showed 100% precision and 99.22% recall.
515   This demonstrated that data modification attacks can be effectively detected by utilizing the ML
516   approach.

517   Furthermore, other research groups (Kintzlinger et al. 2020) presented CardiWall system, which
518   is used for detecting and preventing resource depletion attacks against ICDs at programmer
519   device. The system is a collection of six security layers, exploitation of health experts
520   understanding, statistical techniques and one class SVM as the ML technique. To perform the
521   assessment, data were collected over a time span of four years and 775 benevolent clinical
522   commands were used. These were belonging to hundreds of specific patients and 28 malicious
523   clinical prompts established by two cardiac specialists. The evaluation results showed that only
524   two out of the six layers proposed in CardiWall system have provided a high detection
525   capability. One class SVM was failed to obtain a high detection rate because of the problems
526   related to the datasets and a smaller number of features related to the malicious data.. Noticeably,
527   the system achieved an AUC of 94.7% with a true positive rate (TPR) of 91.4% and false
528   positive rate (FPR) of 1%.
529   Rathore et al. (Rathore et al. 2019) proposed a Long Short-Term Memory, which is a type of
530   recurrent neural network. It was used for predicting and forecasting different signal patterns of
531   Deep Brain Stimulation (DBS). Usually, Rest Tremor Velocity (RTV) is analyzed to know the
532   neurological disorders intensity. In this way, the authors analyzed RTV values for designing and
533   training the neural network. Multiple attacks have been introduced in the DBS context to
534   simulate and distinguish various attack techniques. To assess the performance of the algorithm in
535   terms of accuracy and reliability, real and false observations were listed and estimated at the run
536   time.
537
538   **Table 8:**
539   **Details of published studies on anomaly and attack detection to the sensors/medical**
540   **devices.**
541
542   **Authentication and Access Control:** In this section, results and analysis of the relevant papers
543   on this topic are given, while the main features and limitations of the reported works are
544   summarized in Table 9.

545   Rathore et al. (Rathore et al. 2018b) proposed a biometric verification methodology based on
546   ECG, in which the Legendre polynomial extraction and MLP classifier were used for
547   identification and authorization, aiming at securing the data, network, and application layer. The
548   suggested methodology is the first effort to use ECG signals to exploit MLP in authentication.
549   The results were verified on the ECG dataset and showed that it is possible to achieve 100% test
550   accuracy with 5-degree coefficients when the authorized person is identified.
551   In a research made by Pirbhulal et al. (Pirbhulal et al. 2019), a biometric protection system based
552   on ML technique was introduced, in which the attributes for learning process were derived from
553   ECG signals. Nevertheless, in the testing process, the user is authenticated by using the unique
554   biometric EIs generated from the ECG and the polynomial approximation coefficients. It was
555   concluded that the proposed system can be used for real-time healthcare implementations.

556   In another work carried out by Mawgoud et al. (Mawgoud et al. 2019), an authentication
557   approach was proposed, which is based on SVM. The authentication was established by
558   incorporating both trust management and SVM at the gateway to recognize the frequency of
559   resource-constraint devices and the timing of access. The proposed approach acts to identify
560   several IoMT sensor artifacts based on their pseudo-random exposure in both frequency and time
561   domains. If the value of the time or frequency domain is the same as its distinctive Pseudo-
562   Random Binary Sequence (PRBS), the device will be authenticated by the gateway, in which an
563   average trust value of 1.9 and less than 0.5 value are considered as adversary. Results proved that
564   the method is viable for interacting with the IoMT devices.
565   Furthermore, a study was performed by Barros et al (Barros et al. 2019) aiming at reducing the
566   computational cost, in which the features were extracted from ECG signal by utilizing only
567   fiduciary points measured from the acquisition of the signal. A set of ML techniques such as
568   MLP, RF, SVM and NB were used for the classification purpose. The ECG signal of Stress
569   Recognition Database was employed and it was proved that the method can be used for
570   continuous authentication with lower complexity using less than 10 features.
571   Hospital systems with huge number of patients requires proper authentication method. For that
572   purpose, Zhang et al. (Zhang et al. 2018) proposed a hybrid technique that combines fiducial and
573   non-fiducial features for accuracy improvement for authentication in healthcare systems. Feature
574   selection of 2DPCA was used to enhance the accuracy of Linear Discriminant Analysis (LDA)
575   and improving authentication of smart healthcare along with MapReduce. The PQRST peaks
576   were selected as the main fiducial features. For the ECG user recognition, an incrementing
577   training of the LDA algorithm was considered, utilizing the exposed fiducial and non-fiducial
578   features. The authors reported that detection based on fiduciary feature and Fast Fourier
579   Transform has provided a poor precision. Additionally, they concerned that growing the number
580   of features would lead to additional computing effort.
581   Referring back to the individual authentication for daily use of wearable devices, researchers
582   (Shang & Wu 2019) used photoplethysmography (PPG) signals inspired by hand movements for
583   user authentication on smartwatches. To protect from attackers, the software first senses the
584   beginning and stopping point of any new hand gesture and decides if an attacker is present. This
585   was realized by comparing the features derived from the observed hand movements with those
586   obtained from the regular user. The training samples of the usual consumer have been used to
587   create a local outlier factor (LOF) model. The LOF model has the feature of few parameter
588   modification which helps to easily create a new classifier for a new consumer. In addition, LOF
589   can identify anomalies efficiently. This approach resulted in an overall authentication accuracy
590   of 96:31% and an overall true rejection rate of at least 91:64 % against two forms of attacks.
591   Authors claimed that this software-based solution can be integrated into any smartwatch with
592   PPG sensors for multi-factor authentication.
593   On the other hand, Musale et al. (Musale et al. 2019) proposed a lightweight authentication
594   approach using gait biometric for authenticating users of commercial smart watches. This was
595   realized by extracting the statistical features and person's actions-related features from the

596   collected data of sensors, thereby improving both accuracy and efficiency. For this purpose,
597   techniques such as filters with RF, K-NN and MLP classifiers were used. Results demonstrated
598   that the system could achieve a higher accuracy by having a reduced feature and fewer sensed
599   dataset. This in turn renders the theoretical architecture more realistic and easily accessible to
600   wearable IoT devices with minimal processing resources and energy efficiency.
601   Furthermore, in a study reported by (Vhaduri & Poellabauer 2019), a hybrid approach was
602   implemented for biometric authentication in wearable devices. This was achieved by utilizing a
603   three-combination form of course-grain minute-level biometrics: behavioral (step counts),
604   physiological (heart rate), and hybrid (calorie burn and metabolic equivalent of task). An
605   analysis was performed by using 400 Fitbit consumers data that were obtained from a health
606   research collected over 17 months. A combination of filters (KS-test, PC and SD) with SVM of
607   different settings were used. A high accuracy for both sedentary and non-sedentary with low
608   error rates of 0.05 were achieved when a binary SVM was used. It was also proved that
609   hybridizing the biometrics gives better results even during non-sedentary periods.
610   Mohsen et al. (Mohsen et al. 2019) proposed ECC defined lightweight cooperative
611   authentication scheme to be used in real-time medical wireless sensor networks among
612   physicians/nursing staff, trustworthy databases, sensors and patients. Here, the doctor/nurse can
613   use the system by his/her fingerprint, while patient identity can be verified through continuous
614   monitoring of physiological data (e.g., ECG signals) in every 30 mins to detect the physical theft
615   of the sensor. The server uses PID and ECC feature set as training data and utilizes convolutional
616   neural network. Dynamic identity was applied for user anonymity and mitigating user
617   traceability. Results showed that the scheme is strong against multiple attacks with accepted
618   performance.
619   Moreover, Punithavathi et al. (Punithavathi et al. 2019) proposed a lightweight approach for
620   cloud cancelable biometric authentication. As such, privacy problems related to biometric
621   utilization can be tackled by getting advantage of cancelable biometric templates. A random
622   projection method was used for generating the cancelable fingerprint template. Fingerprint
623   images were chosen anonymously from publicly accessible databases. After pre-processing and
624   feature extraction, the lightweight random projection method was used to create cancelable
625   fingerprint models. However, authors mentioned that the work's scalability in real world has not
626   been tested.
627   Rathore et al. (Rathore et al. 2018a) implemented a lightweight approach for trusted
628   authentication using Dynamic Time Warping (DTW) method. A large database from Physionet
629   was used for validating the method and informative features were extracted from ECG using
630   DTW. It was seen that DTW method showed a higher accuracy compared with that of the non-
631   linear SVM. Additionally, it took less time, while both methods have the same memory
632   complexity.
633   Moreover, Mohsin et al (Mohsin et al. 2019) designed a secure framework for user verification
634   in two stages of patient authentication. In the first stage, merged RFID and finger vein (FV)
635   features were generated to increase the security levels. In the second phase, a combined

636   technique of AES encryption, blockchain, and PSO steganography was used for secure
637   transmission of the data. In the evaluation process, 106 samples were chosen from a database
638   comprising of 6000 samples of FV images. It was seen that the system is strong against spoofing
639   and brute-force attacks, whereby an improvement of 55.56% was achieved in the secure
640   biometric transmission.
641
642   **Table 9:**
643   **The summary of the studies reported on authentication and access control.**
644
645   **Intrusion and Malware Detection**: Herein, the main achieved results on this topic that were
646   reported in literature are given followed by a summarized comparison of the studies, as shown in
647   Table 10.

648   Begli et al. (Begli et al. 2019) designed a security framework for smart healthcare system, which
649   can be specifically useful for protecting wireless sensor network against unauthorized access and
650   network attacks. In their work, a multiagent based layered architecture was first defined. Then,
651   the IDS was applied using SVM, which is proportional to the level of energy and the sensitivity
652   of the available data of each triple group of the agents. Different rules were used for each layer
653   of the multiagent healthcare. Also, attacks related to healthcare, including eavesdropping attacks,
654   were studied in terms of energy usage and computational cost.
655   Moreover, a multivariate correlation analysis was proposed for the IoMT attacks detection (Itten
656   & Vadakkumcheril 2016). Triangular based area maps were utilized for analyzing the incoming
657   data's features to formulate a correlation among various features. It was seen that the learning
658   model has a high rate of time usage with increased classification accuracy. The proposed method
659   can differentiate both known and unknown DoS attacks from normal network traffic.
660   Additionally, in a study made by (Schneble & Thamilarasu 2019a), a massively distributed
661   intrusion detection based on ML was designed and implemented for the Medical Cyber Physical
662   System. Primarily, the notion of Federated Learning was researched to reduce the connectivity
663   and computing expenses associated with conventional ML algorithms. Evaluation was carried
664   out using real patient records against the attacks including DoS, data manipulation and false data
665   injection. Observational findings showed that the proposed system attained a high accuracy of
666   99% and FPR of 1% including a decreased communication network's overhead. Moreover, they
667   proved that the program could cope with unevenly distributed data and is a flexible approach that
668   utilizes the computational power of multiple mobile devices. In another work (Odesile &
669   Thamilarasu 2017), the authors have introduced a mobile agent-based intrusion detection
670   program for WBAN. Different types of sensor agents, and cluster agents are used . Multiple
671   threats were detected in a distributed and hierarchical framework within the healthcare network.
672   ML methods such as NBC, KNN, SVM, RF and DT were applied to sensor nodes for the
673   purpose of providing precise attack detection, followed by choosing an appropriate approach.
674   The system has been tested to be effective in terms of precision and power usage. It was
675   revealed that there is a lack of sufficient researches on the intrusion detection in the medical

676   cyber-physical system (Schneble & Thamilarasu 2019b). Since real time attack detection is
677   critical for medical devices, the volume of data analyzed by the IDS should be reduced to
678   maintain optimal frequency detection. Therefore, an effective IDS was proposed by addressing
679   the problem of feature selection to reduce the data dimensionality (Schneble & Thamilarasu
680   2019b). The findings showed that Laplacian scoring strategies are effective in optimizing the
681   collection of features with reduced resource usage.
682   Furthermore, for the detection of anomaly based intrusion, a stacked autoencoder (SAE) was
683   proposed by He et al. (He et al. 2019). The SAE was used to extract more informative features
684   and eliminate feature dimensions, which resulted in the reduction of detection overhead.
685   RM et al (RM et al. 2020) applied a hybrid PCA-GWO algorithm for feature selection and DNN
686   classifier for classifying the network attacks. The proposed methodology suits the IoMT devices
687   that are using a unique IP. One-Hot encoding scheme was used for pre-processing the input data.
688   Then, PCA and GWO algorithms were sequentially utilized for further data reduction followed
689   by the use of well-known classifiers for prediction. Results showed that the hybrid PCA-GWO is
690   capable of increasing the detection accuracy by 15%. In addition, the training and classification
691   time was reduced by 32%.
692   For the same purpose, researchers (Thamilarasu 2016) used a multi-objective GA algorithm for
693   the feature selection of WBAN network attack detection. The experimental results showed that
694   the proposed algorithm could include the useful features for detecting a specific attack in the
695   detection process, thereby decreasing the computational complexity.
696   Asfaw et al. (Asfaw et al. 2010) presented a datamining-based model to provide a host-based
697   anomaly and attack detection method for pervasive healthcare systems. When a mobile is
698   requesting from the server, its message is recorded and fed to the classification model. Then, the
699   model classifies the record as benign or malicious depending on the previously recorded history.
700   Eventually, the classifier holds the reactions in a passive fashion, maintaining each specific
701   record with the disruptive behavior and hence detecting the anomalous events.
702   In a recent work performed by Manimurugan et al. (Manimurugan et al. 2020), Deep Belief
703   Network (DBN) was proposed for attacks detection in the IoMT. The measurement criteria used
704   in the study were precision, recall, accuracy, and F1-score. The suggested model achieved
705   positive results across all variables compared to the other techniques. It was claimed that this
706   model can be expanded for detecting several forms of attacks against IoT devices and different
707   databases.
708   Alrashdi et al. (Alrashdi et al. 2019) presented a fog-based attack detection (FBAD) architecture
709   by utilizing an online sequential extreme learning machine (EOS-ELM) collection for
710   monitoring of suspicious behaviors in healthcare system. They proved that the proposed
711   architecture is effectively implemented in the decentralized fog-attack detection by comparing its
712   efficiency to other methods. It was revealed that the decentralized architecture surpassed the
713   centralized framework in terms of detection time and accuracy of classification.
714   Wazid et al. (Wazid et al. 2019) surveyed the malware detection methods in the IoMT network
715   using ML approaches. They elaborated on how serious the malware attacks are, especially botnet

716   attacks on the three tiers of security and privacy. In the presence of such attacks, the sensitive
717   data of IoT communication may be disclosed, altered or even may not be available to the
718   authorized users. Hence, in the study various types of malware attacks were explored with their
719   symptoms and a taxonomy for the IoMT security was given. Moreover, ML based malware
720   detection methods were discussed.
721   Furthermore, Fernandez Maimo et al.(Fernandez Maimo et al. 2019) used ML techniques for
722   detecting and classifying ransomware attacks in ICE. The NFV/SDN methods were used to
723   isolate and remove contaminated medical equipment and networks. The method was developed
724   to detect recent malwares such as WannaCry, Petya, BadRabbit and PowerGhost. Techniques
725   such as OC-SVM and Naive Bayes have been proved to detect and classify ransomware infecting
726   ICE with respective accuracy and recall of 92.32% and 99.97% for the OC-SVM in anomaly
727   detection. This is where the Naive Bayes classifier was able to reach a classification accuracy of
728   99.99%.
729   Shakeel et al. (Shakeel et al. 2018) studied a secure data access and transmission in the IoMT
730   through utilizing the Deep-Q-Network (DQN) methodology. Initially, the IoMT system was
731   analyzed by the deep neural network to authenticate and eliminate any possible malware attacks.
732   The traffic attributes of each request were derived and recorded in the database. The output
733   attribute was then analyzed by using the state feature and associated behavior. Then, the deep
734   neural convolution network was used to classify them into malware and regular data. Results
735   showed that the method has achieved a low error of about 0.12 with malware detection rate of
736   98.79%.
737   Furthermore, with the aim of protecting the brain activity data from attacks in Brain–Computer
738   Interface (BCI) systems such as Electroencephalography (EEG) and fraud BCI program (e.g.
739   game), which lets a malicious entity to obtain the user's brain activities, researchers
740   demonstrated that a ML method can anticipate relevant identity characteristics by studying
741   resting-state EEG (rsEEG) records of a person's brain activity (Landau et al. 2020). A complete
742   collection of raw rsEEG tests along with dissociation degree and executive function (EF)
743   assessment indicators were used for 162 subjects in the test. Their study concluded that
744   breaching those identical brain activities are possible if proper security measures are not taken
745   into consideration.
746
747
748   **Table 10:**
749   **Summary of the studies reported on intrusion and malware detection.**
750
751

752   ## Discussion
753   In this section, the main outcomes of the reviewed studies are elaborated and discussed aiming at
754   achieving fruitful answers to each of the research questions, respectively.

RQ1: What is the current state of the art and direction of study in the IoMT security using ML?

One can see from Fig. 7 that 37% of the research articles were devoted to detect anomaly at sensors or medical devices. This indicated that in the past years, the main focus was on detecting the intrusions such as false data injection, resource depletion attacks, behavioral and physical attacks against medical devices. This can be attributed to the fact that these attacks are serious and they lead to significant health issues. For instance, it may lead to death in the case of attacks to the implantable medical devices (Alsubaei et al. 2019b; Hatzivasilis et al. 2019; Yaacoub et al. 2020).

Also, intrusion and malware attack detections received a considerable attention, counting for 35% of the reported studies (7% for malware and 28% for other attacks). Nevertheless, majority of the papers were found to have focused on NIDS. On the other hand, papers that used different strategies to solve the authentication and access control issues were found to take 28%. However, as authentication is computationally heavy for the IoMT devices, the current direction of research is to apply lightweight mechanisms (Aghili et al. 2019a; Wu et al. 2018) by using sensor physiological data to reduce the computation load on the device.

Figure 7: Papers distribution by the direction and problem-solving domain.

RQ 2: What kind of data and tools are used for applying ML techniques in the IoMT security?

Machine Learning methods are data dependent as they learn from these data overtime and decide intelligently based on their learning ability, amount and quality of the data. For this reason, in our study we have paid attention to this matter and we have analyzed all the selected research articles based on the type of data they used for decision making and learning process. It can be seen from Fig. 8 that most of the papers have used historical benchmark data, of which 9% have used network data, while 51% have used sensors and physiological data. This is mainly because most of the methods were to find anomalies in the sensors and to use device authentication as security solution.. On the other hand, 26% of the papers have used simulated or emulated data. However, some of the studies have not given the source of their data or did not mention it at all. For this category, we have given the label not available or not given. This group of papers provides 14% of the whole selected papers.

Figure 8. The type of data used by the researchers to conduct their research.

To further answer the above research question, software and hardware tools used and reported in the reviewed studies are analyzed. Figure 9 shows the used software tools and programs in the reviewed studies. Tools used by the studied works were mainly Network/ Sensor Simulators with ML tools. However, we have excluded those studies that used simulation but did not mention its

795   tool. For this reason, the percentage of the simulation tools is less than expected. Furthermore,
796   25% of the studies did not give the tools used in their studies. The remaining were mainly
797   programming tools for ML purpose. We can see that MATLAB has been used more than the rest
798   of the tools. Python also gained good attention in the current years. In addition, Weka tool has
799   been used frequently, which counts for 9% of the studies. Additionally, Keras and Sckit-learn
800   libraries were used with 8% and 6% by the studies, respectively. Those represent open-source
801   libraries are usually used with Python. Moreover, in the reviewed studies, some works have used
802   testbeds and hardware tools, while few of them reported their tools. Figure 10 shows the number
803   of those tools that have been used. It was found that six types of devices and hardware tools were
804   used and reported in the studies.

805

806   **Figure 9: Software and tools used by the studies.**
807   **Figure 10: Devices and hardware tools used in the studies.**

808

809

810   **RQ 3: How ML techniques are effectively applied by the studies and what**
811   **are their limitations ?**

812   Through a critical analysis of the current works, we can conclude that traditional ML techniques
813   may fail if proper considerations are not given to some metrics such as computational complexity
814   and energy usage. ML performance is reduced when few data are used. However, the IoMT
815   devices are resource limited such as (IMDs) and using a huge data analysis on these devices is
816   resulted in degrading their lifespan. For these reasons, one should take a balance between these
817   two aspects. From our analysis of the reviewed papers, we have found that a small portion of the
818   studies have used lightweight approaches. The pie chart shown in Fig. 11-a illustrates that only
819   14% of the studies have used lightweight approach. Additionally, 12% of the studies have used
820   low complexity approaches, that means it is not exactly lightweight but not heavy. The rest of the
821   studies either did not require this feature in their system or failed to apply it. Furthermore, real
822   time ML techniques are crucial for the IoMT, especially in attack and intrusion detection.
823   Because the IoMT networks are dealing with streaming data and some of the devices never stop
824   from working, a continuous and fast detection of attacks are required. It is seen from Fig. 11-b
825   that 19% of the studies were used real time approach, while 12% of the studies have used low
826   complex approaches that are not exactly real time but have approached it. Nevertheless, the other
827   67% of the works were offline. Additionally, the studies focused on network attack detection
828   paid less attention to distributed attack detection. As can be seen in Fig. 12 that only 12% of the
829   studied have used decentralized models, while the rest were centralized. However, a hybrid of
830   the methods was considered as a better approach.

831

832   **Figure 11: Analysis of the studies in terms of (a) complexity and (b) real time analysis**

833

834   **Figure 12: Details of the studies in terms of placement.**

835

836

837   Based on the studies gaps that were assigned previously, it is found that majority of the studies
838   have focused on improving the traditional evaluation metrics for their ML models such as high
839   (accuracy, recall, precision) and low (FP, FN). However, performance metrics such as memory
840   (space), CPU, time, and energy overhead were neglected. Additionally, most of the techniques of
841   attack detection were performed in an isolated offline environment. However, one should
842   consider simulation/hardware implementation to represent a real IoT setting. Also, decentralized
843   and hybrid approaches are much compatible for the IoMT than centralized one, which was again
844   not common among the studies. Furthermore, we have noticed that the datasets used by the
845   attack and intrusion detection methods were out of date and some of them do not represent the
846   current IoMT system. Moreover, sensitive, and private data usage should be avoided in attack
847   and anomaly detection tasks which was also given a minor attention. Therefore, there should be a
848   trade-off among preserving privacy, high accuracy, and computational complexity. Another
849   challenge that should be considered is the risk of adversarial attacks on ML techniques
850   themselves. An attacker who have enough knowledge on how the ML techniques work with the
851   data can manipulate the data at training or testing stage to fool the ML method. Hence, the
852   proposed methods should be strong enough against the adversarial attacks.

853

854

Limitations

856   The underlying drawbacks of this research are: i) Selection bias: This study focuses on literature
857   research, which may have unintentionally omitted most recent non-scholarly advancements or
858   scholarly articles that yet to be published at the time of preparing this study. ii) Publication bias:
859   Some of the studies may have been discarded since their full paper was not accessible. iii)
860   Descriptive bias: Despite the efforts made to present the background comprehensively, this SLR
861   is combining many topics that may need someone to refer to the external sources for a deep
862   understanding.

863

Conclusions

865   In this study, a comprehensive Systematic Literature Review (SLT) was given about the IoMT
866   security and privacy issues and how Machine Learning (ML) methods are used for solving them.
867   By examining the content of the study, including methods, good features, limitations, tools, and
868   datasets, the designated research questions were answered. Findings of this study showed that
869   ML techniques are effective in addressing the IoMT security issues with promising results.
870   Majority of the studies was devoted to device layer or body area network security since attacks
871   on devices such as IMDs are seriously affecting the patient's health and life. The security
872   solutions for such devices were sensor anomaly detection and device authentication and access
873   control. Furthermore, securing the network layer was seen among the studies that used attack and
874   malware detection strategies.

875 Moreover, the tools and environment of the current works are a combination of network
876 simulators and ML tools with more focus on the latter. Additionally, there is a lack of relevant
877 datasets, especially in the intrusion detection. Most of the studies focused on improving the
878 common ML algorithms evaluation metrics such as high accuracy and low FPR. However, since
879 the IoMT devices are characterized with shortage in power and small memory and processor,
880 there should be a balance between security and maintaining resources lifespan during the
881 adaption of these solutions. We have concluded that traditional ML techniques may fail if proper
882 consideration is not given to some metrics such as resource complexity, time complexity, and
883 energy usage. It was noticed that a vast majority of the studies ignored these criteria in the
884 evaluation of their proposed models. Therefore, ML techniques are vital in the application of the
885 IoMT security. However, future studies should focus on how to use ML in a proper way to
886 concede the nature of the IoMT.
887

References

889 Abdaoui A, Al-Ali A, Riahi A, Mohamed A, Du X, and Guizani M. 2020. Secure medical treatment with
890   deep learning on embedded board. *Energy Efficiency of Medical Devices and Healthcare*
891   *Applications*: Elsevier, 131-151.
892 Abhishek NV, Lim TJ, Sikdar B, and Tandon A. 2018. An intrusion detection system for detecting
893   compromised gateways in clustered IoT networks. 2018 IEEE International Workshop Technical
894   Committee on Communications Quality and Reliability (CQR): IEEE. p 1-6.
895 Aghili SF, Mala H, Kaliyar P, and Conti M. 2019a. SecLAP: Secure and lightweight RFID authentication
896   protocol for Medical IoT. *Future Generation Computer Systems* 101:621-634.
897   https://doi.org/10.1016/j.future.2019.07.004
898 Aghili SF, Mala H, Shojafar M, and Peris-Lopez P. 2019b. LACO: Lightweight Three-Factor Authentication,
899   Access Control and Ownership Transfer Scheme for E-Health Systems in IoT. *Future Generation*
900   *Computer Systems* 96:410-424. https://doi.org/10.1016/j.future.2019.02.020
901 Ahad A, Tahir M, and Yau KA. 2019. 5G-Based Smart Healthcare Network: Architecture, Taxonomy,
902   Challenges and Future Research Directions. *IEEE Access* 7:100747-100762.
903   10.1109/ACCESS.2019.2930628
904 Ahmad B, Jian W, Ali ZA, Tanvir S, and Khan MSA. 2019. Hybrid anomaly detection by using clustering for
905   wireless sensor network. *Wireless Personal Communications* 106:1841-1853.
906 Al Shorman A, Faris H, and Aljarah I. 2019. Unsupervised intelligent system based on one class support
907   vector machine and Grey Wolf optimization for IoT botnet detection. *Journal of Ambient*
908   *Intelligence and Humanized Computing*:1-17.
909 Alassaf N, and Gutub A. 2019. Simulating Light-Weight-Cryptography Implementation for IoT Healthcare
910   Data Security Applications. *International Journal of E-Health and Medical Communications* 10:1-
911   15. 10.4018/ijehmc.2019100101
912 Alimadadi A, Aryal S, Manandhar I, Munroe PB, Joe B, and Cheng X. 2020. Artificial Intelligence and
913   Machine Learning to Fight COVID-19. American Physiological Society Rockville, MD.
914 Alrashdi I, Alqazzaz A, Alharthi R, Aloufi E, Zohdy MA, and Ming H. 2019. FBAD: Fog-based attack
915   detection for IoT healthcare in smart cities. 2019 IEEE 10th Annual Ubiquitous Computing,
916   Electronics & Mobile Communication Conference (UEMCON): IEEE. p 0515-0522.

917   Alsubaei F, Abuhussein A, and Shiva S. 2019a. A Framework for Ranking IoMT Solutions Based on
918   Measuring Security and Privacy. In: Arai K, Bhatia R, and Kapoor S, eds. *Proceedings of the Future*
919   *Technologies Conference*. Cham: Springer International Publishing Ag, 205-224.
920   Alsubaei F, Abuhussein A, and Shiva S. 2019b. Ontology-Based Security Recommendation for the
921   Internet of Medical Things. *IEEE Access* 7:48948-48960. 10.1109/access.2019.2910087
922   Aluvalu R. 2020. Intrusion Detection System for the IoT: A Comprehensive Review. Proceedings of the
923   11th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2019):
924   Springer Nature. p 235.
925   Aman AHM, Hassan WH, Sameen S, Attarbashi ZS, Alizadeh M, and Latiff LA. 2020. IoMT amid COVID-19
926   pandemic: Application, architecture, technology, and security. *Journal of Network and Computer*
927   *Applications*:102886.
928   Amanullah MA, Habeeb RAA, Nasaruddin FH, Gani A, Ahmed E, Nainar ASM, Akim NM, and Imran M.
929   2020. Deep learning and big data technologies for IoT security. *Computer Communications*
930   151:495-517.
931   Anthi E, Williams L, and Burnap P. 2018. Pulse: an adaptive intrusion detection for the internet of things.
932   Ardabili SF, Mosavi A, Ghamisi P, Ferdinand F, Varkonyi-Koczy AR, Reuter U, Rabczuk T, and Atkinson
933   PM. 2020. Covid-19 outbreak prediction with machine learning. *Available at SSRN 3580188*.
934   Arshad J, Azad MA, Amad R, Salah K, Alazab M, and Iqbal R. 2020. A Review of Performance, Energy and
935   Privacy of Intrusion Detection Systems for IoT. *Electronics* 9:629.
936   Asfaw B, Bekele D, Eshete B, Villafiorita A, and Weldemariam K. 2010. Host-based anomaly detection for
937   pervasive medical systems. 2010 Fifth International Conference on Risks and Security of Internet
938   and Systems (CRiSIS): IEEE. p 1-8.
939   Bahşi H, Nõmm S, and La Torre FB. 2018. Dimensionality reduction for machine learning based iot botnet
940   detection. 2018 15th International Conference on Control, Automation, Robotics and Vision
941   (ICARCV): IEEE. p 1857-1862.
942   Barros A, Rosário D, Resque P, and Cerqueira E. 2019. Heart of IoT: ECG as biometric sign for
943   authentication and identification. 2019 15th International Wireless Communications & Mobile
944   Computing Conference (IWCMC): IEEE. p 307-312.
945   Begli M, Derakhshan F, and Karimipour H. 2019. A layered intrusion detection system for critical
946   infrastructure using machine learning. 2019 IEEE 7th International Conference on Smart Energy
947   Grid Engineering (SEGE): IEEE. p 120-124.
948   Ben Amor L, Lahyani I, and Jmaiel M. 2020. AUDIT: AnomaloUs data Detection and Isolation approach
949   for mobile healThcare systems. *Expert Systems* 37:e12390.
950   Bostami B, Ahmed M, and Choudhury S. 2019. False Data Injection Attacks in Internet of Things.
951   *Performability in Internet of Things*: Springer, 47-58.
952   Bostani H, and Sheikhan M. 2017. Hybrid of anomaly-based and specification-based IDS for Internet of
953   Things using unsupervised OPF based on MapReduce approach. *Computer Communications*
954   98:52-71.
955   Burhan M, Rehman RA, Khan B, and Kim B-S. 2018. IoT elements, layered architectures and security
956   issues: A comprehensive survey. *Sensors* 18:2796.
957   Butun I, Kantarci B, and Erol-Kantarci M. 2015. Anomaly detection and privacy preservation in cloud-
958   centric Internet of Things. 2015 IEEE International Conference on Communication Workshop
959   (ICCW): IEEE. p 2610-2615.
960   Cao L. 2017. Data science: a comprehensive overview. *ACM Computing Surveys (CSUR)* 50:1-42.
961   Chakraborty A, Alam M, Dey V, Chattopadhyay A, and Mukhopadhyay D. 2018. Adversarial attacks and
962   defences: A survey. *arXiv preprint arXiv:181000069*.
963   Cui L, Yang S, Chen F, Ming Z, Lu N, and Qin J. 2018. A survey on application of machine learning for
964   Internet of Things. *International Journal of Machine Learning and Cybernetics* 9:1399-1417.

965   da Costa KA, Papa JP, Lisboa CO, Munoz R, and de Albuquerque VHC. 2019. Internet of Things: A survey
966   on machine learning-based intrusion detection approaches. *Computer Networks* 151:147-157.
967   Dang LM, Piran M, Han D, Min K, and Moon H. 2019. A survey on internet of things and cloud computing
968   for healthcare. *Electronics* 8:768.
969   Davis J. 2020a. Ransomware Attacks Cost Healthcare Sector At Least $160M Since 2016. *Available at*
970   *https://healthitsecurity.com/news/ransomware-attacks-cost-healthcare-sector-at-least-160m-*
971   *since-2016* (accessed 11/1/2020.
972   Davis J. 2020b. US Ransomware Attacks Doubled in Q3; Healthcare Sector Most Targeted. *Available at*
973   *https://healthitsecurity.com/news/us-ransomware-attacks-doubled-in-q3-healthcare-sector-*
974   *most-targeted* (accessed 2/1/2021.
975   Dimitrov DV. 2016. Medical internet of things and big data in healthcare. *Healthcare informatics*
976   *research* 22:156-163.
977   Din IU, Almogren A, Guizani M, and Zuair M. 2019. A Decade of Internet of Things: Analysis in the Light
978   of Healthcare Applications. *IEEE Access* 7:89967-89979. 10.1109/access.2019.2927082
979   Diro AA, and Chilamkurti N. 2018. Distributed attack detection scheme using deep learning approach for
980   Internet of Things. *Future Generation Computer Systems* 82:761-768.
981   Durga S, Nag R, and Daniel E. 2019. Survey on machine learning and deep learning algorithms used in
982   internet of things (IoT) healthcare. 2019 3rd International Conference on Computing
983   Methodologies and Communication (ICCMC): IEEE. p 1018-1022.
984   Elrawy MF, Awad AI, and Hamed HF. 2018. Intrusion detection systems for IoT-based smart
985   environments: a survey. *Journal of Cloud Computing* 7:21.
986   Escamilla-Ambrosio P, Rodríguez-Mota A, Aguirre-Anaya E, Acosta-Bermejo R, and Salinas-Rosales M.
987   2018. Distributing computing in the internet of things: cloud, fog and edge computing overview.
988   *NEO 2016*: Springer, 87-115.
989   Eskandari M, Janjua ZH, Vecchio M, and Antonelli F. 2020. Passban IDS: An intelligent anomaly based
990   intrusion detection system for IoT edge devices. *IEEE Internet of Things Journal*.
991   Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, and Mankodiya K. 2018. Towards fog-driven IoT
992   eHealth: Promises and challenges of IoT in medicine and healthcare. *Future Generation*
993   *Computer Systems* 78:659-676.
994   Farroha J. 2019. Security Analysis and Recommendations for AI/ML Enabled Automated Cyber Medical
995   Systems. In: Ahmad F, ed. *Big Data: Learning, Analytics, and Applications*. Bellingham: Spie-Int
996   Soc Optical Engineering.
997   Fernandez Maimo L, Huertas Celdran A, Perales Gomez AL, Garcia Clemente FJ, Weimer J, and Lee I.
998   2019. Intelligent and dynamic ransomware spread detection and mitigation in integrated clinical
999   environments. *Sensors* 19:1114.
1000 Firouzi F, Rahmani AM, Mankodiya K, Badaroglu M, Merrett GV, Wong P, and Farahani B. 2018. Internet-
1001   of-Things and big data for smarter healthcare: From device to architecture, applications and
1002   analytics. Elsevier.
1003 Gao S, and Thamilarasu G. 2017. Machine-learning classifiers for security in connected medical devices.
1004   2017 26th International Conference on Computer Communication and Networks (ICCCN): IEEE. p
1005   1-5.
1006 Gheisari M, Wang G, and Bhuiyan MZA. 2017. A survey on deep learning in big data. 2017 IEEE
1007   international conference on computational science and engineering (CSE) and IEEE international
1008   conference on embedded and ubiquitous computing (EUC): IEEE. p 173-180.
1009 Grammatikis PIR, Sarigiannidis PG, and Moscholios ID. 2019. Securing the Internet of Things: Challenges,
1010   threats and solutions. *Internet of Things* 5:41-70.
1011 Gupta R, Tanwar S, Tyagi S, and Kumar N. 2020a. Machine learning models for secure data analytics: A
1012   taxonomy and threat model. *Computer Communications* 153:406-440.

1013   Gupta S, Venugopal V, Mahajan V, Gaur S, Barnwal M, and Mahajan H. 2020b. HIPAA, GDPR and Best
1014   Practice Guidelines for preserving data security and privacy-What Radiologists should know.
1015   European Congress of Radiology-ECR 2020.
1016   Hameed SS, Hassan R, and Muhammad FF. 2017. Selection and classification of gene expression in
1017   autism disorder: Use of a combination of statistical filters and a GBPSO-SVM algorithm. *PloS one*
1018   12.
1019   Haque SA, Rahman M, and Aziz SM. 2015. Sensor anomaly detection in wireless sensor networks for
1020   healthcare. *Sensors* 15:8764-8786.
1021   Hasan M, Islam MM, Zarif MII, and Hashem M. 2019. Attack and anomaly detection in IoT sensors in IoT
1022   sites using machine learning approaches. *Internet of Things* 7:100059.
1023   Hassija V, Chamola V, Saxena V, Jain D, Goyal P, and Sikdar B. 2019. A survey on IoT security: application
1024   areas, security threats, and solution architectures. *IEEE Access* 7:82721-82743.
1025   Hatzivasilis G, Soultatos O, Ioannidis S, Verikoukis C, Demetriou G, Tsatsoulis CI, and Ieee. 2019. Review
1026   of Security and Privacy for the Internet of Medical Things (IoMT) Resolving the protection
1027   concerns for the novel circular economy bioinformatics. *2019 15th International Conference on*
1028   *Distributed Computing in Sensor Systems*. New York: Ieee, 457-464.
1029   Hau Z, and Lupu EC. 2019. Exploiting Correlations to Detect False Data Injections in Low-Density Wireless
1030   Sensor Networks. Proceedings of the 5th on Cyber-Physical System Security Workshop. p 1-12.
1031   He D, Qiao Q, Gao Y, Zheng J, Chan S, Li J, and Guizani N. 2019. Intrusion Detection Based on Stacked
1032   Autoencoder for Connected Healthcare Systems. *IEEE Network* 33:64-69.
1033   He D, Ye R, Chan S, Guizani M, and Xu Y. 2018. Privacy in the Internet of Things for smart healthcare.
1034   *IEEE Communications Magazine* 56:38-44.
1035   Hei X, Du X, Wu J, and Hu F. 2010. Defending resource depletion attacks on implantable medical devices.
1036   2010 IEEE global telecommunications conference GLOBECOM 2010: IEEE. p 1-5.
1037   Hussain F, Hussain R, Hassan SA, and Hossain E. 2020. Machine learning in IoT security: current solutions
1038   and future challenges. *IEEE Communications Surveys & Tutorials*.
1039   Ibitoye O, Shafiq O, and Matrawy A. 2019. Analyzing adversarial attacks against deep learning for
1040   intrusion detection in IoT networks. 2019 IEEE Global Communications Conference
1041   (GLOBECOM): IEEE. p 1-6.
1042   Itten A, and Vadakkumcheril GT. 2016. ENHANCED INTRUSION DETECTION SYSTEM IN MEDICAL CYBER
1043   PHYSICAL SYSTEMS USING MULTIVARIATE CORRELATION ANALYSIS.
1044   Jaigirdar FT, Rudolph C, and Bain C. 2019. Can I Trust the Data I See? A Physician's Concern on Medical
1045   Data in IoT Health Architectures. Proceedings of the Australasian Computer Science Week
1046   Multiconference. p 1-10.
1047   Jan SU, Ahmed S, Shakhov V, and Koo I. 2019. Toward a lightweight intrusion detection system for the
1048   internet of things. *IEEE Access* 7:42450-42471.
1049   Khan FA, Haldar NAH, Ali A, Iftikhar M, Zia TA, and Zomaya AY. 2017. A continuous change detection
1050   mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments. *IEEE*
1051   *Access* 5:13531-13544.
1052   Kintzlinger M, Cohen A, Nissim N, Rav-Acha M, Khalameizer V, Elovici Y, Shahar Y, and Katz A. 2020.
1053   CardiWall: A Trusted Firewall for the Detection of Malicious Clinical Programming of Cardiac
1054   Implantable Electronic Devices. *IEEE Access* 8:48123-48140.
1055   Kubat M. 2017. *An introduction to machine learning*: Springer.
1056   Landau O, Cohen A, Gordon S, and Nissim N. 2020. Mind your privacy: Privacy leakage through BCI
1057   applications using machine learning methods. *Knowledge-Based Systems*:105932.
1058   Li Q, Li W, Wang J, and Cheng M. 2019. A SQL Injection Detection Method Based on Adaptive Deep
1059   Forest. *IEEE Access* 7:145385-145394.

1060   Liang W, Huang W, Long J, Zhang K, Li K-C, and Zhang D. 2020. Deep reinforcement learning for resource
1061   protection and real-time detection in IoT environment. *IEEE Internet of Things Journal*.
1062   Liu CH, Lin Q, and Wen S. 2018. Blockchain-enabled data collection and sharing for industrial IoT with
1063   deep reinforcement learning. *IEEE Transactions on Industrial Informatics* 15:3516-3526.
1064   Lopez-Martin M, Carro B, Sanchez-Esguevillas A, and Lloret J. 2017. Conditional variational autoencoder
1065   for prediction and feature recovery applied to intrusion detection in iot. *Sensors* 17:1967.
1066   Ma Y, Wang Y, Yang J, Miao Y, and Li W. 2017. Big Health Application System based on Health Internet of
1067   Things and Big Data. *IEEE Access* 5:7885-7897. 10.1109/ACCESS.2016.2638449
1068   Maleh Y, Ezzati A, Qasmaoui Y, and Mbida M. 2015. A global hybrid intrusion detection system for
1069   wireless sensor networks. *Procedia Computer Science* 52:1047-1052.
1070   Manimurugan S, Almutairi S, Aborokbah MM, Chilamkurti N, Ganesan S, and Patan R. 2020. Effective
1071   Attack Detection in Internet of Medical Things Smart Environment using a Deep Belief Neural
1072   Network. *IEEE Access*.
1073   Marjani M, Nasaruddin F, Gani A, Karim A, Hashem IAT, Siddiqa A, and Yaqoob I. 2017. Big IoT data
1074   analytics: architecture, opportunities, and open research challenges. *IEEE Access* 5:5247-5261.
1075   Mawgoud AA, Karadawy AI, and Tawfik BS. 2019. A Secure Authentication Technique in Internet of
1076   Medical Things through Machine Learning. *arXiv preprint arXiv:191212143*.
1077   McMahon E, Williams R, El M, Samtani S, Patton M, and Chen H. 2017. Assessing medical device
1078   vulnerabilities on the Internet of Things. 2017 IEEE International Conference on Intelligence and
1079   Security Informatics (ISI): IEEE. p 176-178.
1080   Meidan Y, Bohadana M, Mathov Y, Mirsky Y, Shabtai A, Breitenbacher D, and Elovici Y. 2018. N-BaIoT–
1081   network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervas Comput 17
1082   (3): 12–22.
1083   Midi D, Rullo A, Mudgerikar A, and Bertino E. 2017. Kalis—A system for knowledge-driven adaptable
1084   intrusion detection for the Internet of Things. 2017 IEEE 37th International Conference on
1085   Distributed Computing Systems (ICDCS): IEEE. p 656-666.
1086   Miyato T, Maeda S-i, Koyama M, and Ishii S. 2018. Virtual adversarial training: a regularization method
1087   for supervised and semi-supervised learning. *IEEE transactions on pattern analysis and machine
1088   intelligence* 41:1979-1993.
1089   Mohamed MB, Meddeb-Makhlouf A, and Fakhfakh A. 2019. Intrusion cancellation for anomaly detection
1090   in healthcare applications. 2019 15th International Wireless Communications & Mobile
1091   Computing Conference (IWCMC): IEEE. p 313-318.
1092   Mohsen NR, Ying B, and Nayak A. 2019. Authentication Protocol for Real-Time Wearable Medical Sensor
1093   Networks Using Biometrics and Continuous Monitoring. 2019 International Conference on
1094   Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and
1095   IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData): IEEE. p
1096   1199-1206.
1097   Mohsin A, Zaidan A, Zaidan B, Albahri O, Albahri A, Alsalem M, and Mohammed K. 2019. Based
1098   blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework
1099   for patient authentication. *Computer Standards & Interfaces* 66:103343.
1100   Mosenia A, and Jha NK. 2016. A comprehensive study of security of internet-of-things. *IEEE Transactions
1101   on Emerging Topics in Computing* 5:586-602.
1102   Mozaffari-Kermani M, Sur-Kolay S, Raghunathan A, and Jha NK. 2014. Systematic poisoning attacks on
1103   and defenses for machine learning in healthcare. *IEEE journal of biomedical and health
1104   informatics* 19:1893-1905.
1105   Musale P, Baek D, Werellagama N, Woo SS, and Choi BJ. 2019. You walk, we authenticate: Lightweight
1106   seamless authentication based on gait in wearable IoT systems. *IEEE Access* 7:37883-37895.

1107   Nagdeo SK, and Mahapatro J. 2019. Wireless Body Area Network Sensor Faults and Anomalous Data
1108   Detection and Classification using Machine Learning. 2019 IEEE Bombay Section Signature
1109   Conference (IBSSC): IEEE. p 1-6.
1110   Nanayakkara N, Halgamuge M, and Syed A. 2019. Security and Privacy of Internet of Medical Things
1111   (IoMT) Based Healthcare Applications: A Review.
1112   Newaz A, Sikder AK, Rahman MA, and Uluagac AS. 2020. A Survey on Security and Privacy Issues in
1113   Modern Healthcare Systems: Attacks and Defenses. *arXiv preprint arXiv:200507359*.
1114   Newaz AI, Sikder AK, Rahman MA, and Uluagac AS. 2019. Healthguard: A machine learning-based
1115   security framework for smart healthcare systems. 2019 Sixth International Conference on Social
1116   Networks Analysis, Management and Security (SNAMS): IEEE. p 389-396.
1117   Nguyen DC, Pathirana PN, Ding M, and Seneviratne A. 2019. Blockchain for Secure EHRs Sharing of
1118   Mobile Cloud Based E-Health Systems. *IEEE Access* 7:66792-66806.
1119   10.1109/access.2019.2917555
1120   Noor MM, and Hassan WH. 2019. Current research on Internet of Things (IoT) security: A survey.
1121   *Computer Networks* 148:283-294.
1122   Odesile A, and Thamilarasu G. 2017. Distributed intrusion detection using mobile agents in wireless body
1123   area networks. 2017 Seventh International Conference on Emerging Security Technologies (EST):
1124   IEEE. p 144-149.
1125   Pandey P, and Litoriya R. 2020. Elderly care through unusual behavior detection: A disaster management
1126   approach using IoT and intelligence. *IBM Journal of Research and Development* 64:15:11-15:11.
1127   10.1147/JRD.2019.2947018
1128   Pandey R, Gautam V, Bhagat K, and Sethi T. 2020. A Machine Learning Application for Raising WASH
1129   Awareness in the Times of Covid-19 Pandemic. *arXiv preprint arXiv:200307074*.
1130   Pannu A. 2015. Artificial intelligence and its application in different areas. *Artificial Intelligence* 4:79-84.
1131   Parra GDLT, Rad P, Choo K-KR, and Beebe N. 2020. Detecting Internet of Things attacks using distributed
1132   deep learning. *Journal of Network and Computer Applications*:102662.
1133   Patel N. 2020. Social Engineering As an Evolutionary Threat to Information Security in Healthcare
1134   Organizations. *Jurnal Administrasi Kesehatan Indonesia* 8.
1135   Pirbhulal S, Pombo N, Felizardo V, Garcia N, Sodhro AH, and Mukhopadhyay SC. 2019. Towards Machine
1136   Learning Enabled Security Framework for IoT-based Healthcare. 2019 13th International
1137   Conference on Sensing Technology (ICST): IEEE. p 1-6.
1138   Pramanik MI, Lau RY, Demirkan H, and Azad MAK. 2017. Smart health: Big data enabled health paradigm
1139   within smart cities. *Expert Systems with Applications* 87:370-383.
1140   Punithavathi P, Geetha S, Karuppiah M, Islam SH, Hassan MM, and Choo K-KR. 2019. A lightweight
1141   machine learning-based authentication framework for smart IoT devices. *Information Sciences*
1142   484:255-268.
1143   Qu G, and Yuan L. 2014. Design THINGS for the Internet of Things—An EDA perspective. 2014 IEEE/ACM
1144   international conference on Computer-Aided Design (ICCAD): IEEE. p 411-416.
1145   Rahman MA, and Mohsenian-Rad H. 2012. False data injection attacks with incomplete information
1146   against smart power grids. 2012 IEEE Global Communications Conference (GLOBECOM): IEEE. p
1147   3153-3158.
1148   Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, and Liljeberg P. 2018. Exploiting smart e-
1149   Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future
1150   Generation Computer Systems* 78:641-658.
1151   Rathore H, Al-Ali A, Mohamed A, Du X, and Guizani M. 2018a. DTW based authentication for wireless
1152   medical device security. 2018 14th International Wireless Communications & Mobile Computing
1153   Conference (IWCMC): IEEE. p 476-481.

1154   Rathore H, Al-Ali AK, Mohamed A, Du X, and Guizani M. 2019. A Novel Deep Learning Strategy for
1155   Classifying Different Attack Patterns for Deep Brain Implants. *IEEE Access* 7:24154-24164.
1156   Rathore H, Fu C, Mohamed A, Al-Ali A, Du X, Guizani M, and Yu Z. 2018b. Multi-layer security scheme for
1157   implantable medical devices. *Neural Computing and Applications*:1-14.
1158   Rathore H, Wenzel L, Al-Ali AK, Mohamed A, Du X, and Guizani M. 2018c. Multi-layer perceptron model
1159   on chip for secure diabetic treatment. *IEEE Access* 6:44718-44730.
1160   Rathore S, and Park JH. 2018. Semi-supervised learning based distributed attack detection framework
1161   for IoT. *Applied Soft Computing* 72:79-89.
1162   RM SP, Maddikunta PKR, Parimala M, Koppu S, Reddy T, Chowdhary CL, and Alazab M. 2020. An
1163   effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT
1164   architecture. *Computer Communications*.
1165   Roopak M, Tian GY, and Chambers J. 2020. Multi-objective-based feature selection for DDoS attack
1166   detection in IoT networks. *IET Networks* 9:120-127.
1167   Russom P. 2011. Big data analytics. *TDWI best practices report, fourth quarter* 19:1-34.
1168   S. O'Dea S. 2020. Data volume of IoT connected devices worldwide 2018 and 2025. *Available at*
1169   https://www.statista.com/statistics/1017863/worldwide-iot-connected-devices-data-size/.
1170   Sadoughi F, Behmanesh A, and Sayfouri N. 2020. Internet of Things in Medicine: A Systematic Mapping
1171   Study. *Journal of Biomedical Informatics*:103383.
1172   Saeed A, Ahmadinia A, Javed A, and Larijani H. 2016. Random neural network based intelligent intrusion
1173   detection for wireless sensor networks. *Procedia Computer Science* 80:2372-2376.
1174   Saheb T, and Izadi L. 2019. Paradigm of IoT big data analytics in healthcare industry: a review of scientific
1175   literature and mapping of research trends. *Telematics and Informatics*.
1176   Salem O, Guerassimov A, Mehaoua A, Marcus A, and Furht B. 2014. Anomaly detection in medical
1177   wireless sensor networks using SVM and linear regression models. *International Journal of E-
1178   Health and Medical Communications (IJEHMC)* 5:20-45.
1179   Santagati GE, Dave N, and Melodia T. 2020. Design and Performance Evaluation of an Implantable
1180   Ultrasonic Networking Platform for the Internet of Medical Things. *IEEE/ACM Transactions on
1181   Networking* 28:29-42. 10.1109/TNET.2019.2949805
1182   Schneble W, and Thamilarasu G. 2019a. Attack Detection Using Federated Learning in Medical Cyber-
1183   Physical Systems.
1184   Schneble W, and Thamilarasu G. 2019b. Attack Detection Using Federated Learning in Medical Cyber-
1185   Physical Systems. *IEEE*
1186   Schneble W, and Thamilarasu G. 2019c. Optimal Feature Selection for Intrusion Detection in Medical
1187   Cyber-Physical Systems. 2019 11th International Conference on Advanced Computing (ICoAC):
1188   IEEE. p 238-243.
1189   Sehatbakhsh N, Alam M, Nazari A, Zajic A, and Prvulovic M. 2018. Syndrome: Spectral analysis for
1190   anomaly detection on medical iot and embedded devices. 2018 IEEE international symposium
1191   on hardware oriented security and trust (HOST): IEEE. p 1-8.
1192   Sethi P, and Sarangi SR. 2017. Internet of things: architectures, protocols, and applications. *Journal of
1193   Electrical and Computer Engineering* 2017.
1194   Shafiq M, Tian Z, Bashir AK, Du X, and Guizani M. 2020. IoT malicious traffic identification using wrapper-
1195   based feature selection mechanisms. *Computers & Security*:101863.
1196   Shakeel PM, Baskar S, Dhulipala VS, Mishra S, and Jaber MM. 2018. Maintaining security and privacy in
1197   health care system using learning based deep-Q-networks. *Journal of medical systems* 42:186.
1198   Shang J, and Wu J. 2019. A Usable Authentication System Using Wrist-worn Photoplethysmography
1199   Sensors on Smartwatches. 2019 IEEE Conference on Communications and Network Security
1200   (CNS): IEEE. p 1-9.

1201 Shen J, Chang S, Shen J, Liu Q, and Sun X. 2018. A lightweight multi-layer authentication protocol for
1202   wireless body area networks. *Future Generation Computer Systems* 78:956-963.
1203   https://doi.org/10.1016/j.future.2016.11.033
1204 Sollins KR. 2018. IoT Big Data Security and Privacy vs. Innovation. *IEEE Internet Things J.*
1205 Spiekermann S. 2015. *Ethical IT innovation: A value-based system design approach*: CRC Press.
1206 Stiawan D, Idris M, Malik RF, Nurmaini S, Alsharif N, and Budiarto R. 2019. Investigating Brute Force
1207   Attack Patterns in IoT Network. *Journal of Electrical and Computer Engineering* 2019.
1208 Sun Y, Lo FP-W, and Lo B. 2019. Security and Privacy for the Internet of Medical Things Enabled
1209   Healthcare Systems: A Survey. *IEEE Access* 7:183339-183355.
1210 Tahsien SM, Karimipour H, and Spachos P. 2020. Machine learning based solutions for security of
1211   Internet of Things (IoT): A survey. *Journal of Network and Computer Applications*:102630.
1212 Thamilarasu G. 2016. iDetect: an intelligent intrusion detection system for wireless body area networks.
1213   *International Journal of Security and Networks* 11:82-93.
1214 Tovino SA. 2016. The HIPAA Privacy Rule and the EU GDPR: illustrative comparisons. *Seton Hall L Rev*
1215   47:973.
1216 Tseng TW, Wu CT, and Lai F. 2019. Threat Analysis for Wearable Health Devices and Environment
1217   Monitoring Internet of Things Integration System. *IEEE Access* 7:144983-144994.
1218   10.1109/ACCESS.2019.2946081
1219 Verner A, and Butvinik D. 2017. A machine learning approach to detecting sensor data modification
1220   intrusions in WBANs. 2017 16th IEEE International Conference on Machine Learning and
1221   Applications (ICMLA): IEEE. p 161-169.
1222 Vhaduri S, and Poellabauer C. 2019. Multi-modal biometric-based implicit authentication of wearable
1223   device users. *IEEE Transactions on Information Forensics and Security* 14:3116-3125.
1224 Vinitha S, Sweetlin S, Vinusha H, and Sajini S. 2018. Disease prediction using machine learning over big
1225   data. *Computer Science & Engineering: An International Jouranl (CSEIJ)* 8.
1226 Wang Y, Meng W, Li W, Li J, Liu W-X, and Xiang Y. 2018. A fog-based privacy-preserving approach for
1227   distributed signature-based intrusion detection. *Journal of Parallel and Distributed Computing*
1228   122:26-35.
1229 Wazid M, Das AK, Rodrigues J, Shetty S, and Park Y. 2019a. IoMT Malware Detection Approaches:
1230   Analysis and Research Challenges. *IEEE Access* 7:182459-182476. 10.1109/access.2019.2960412
1231 Wazid M, Das AK, Rodrigues JJ, Shetty S, and Park Y. 2019b. IoMT malware detection approaches:
1232   Analysis and research challenges. *IEEE Access* 7:182459-182476.
1233 Weyrich M, and Ebert C. 2015. Reference architectures for the internet of things. *IEEE Software* 33:112-
1234   116.
1235 Wolfgang E. 2011. Introduction to artificial intelligence. *Translated by Nathanael Black With illustrations
1236   by Florian Mast, Springer-Verlag London Limited*.
1237 Wu F, Li X, Sangaiah AK, Xu L, Kumari S, Wu L, and Shen J. 2018. A lightweight and robust two-factor
1238   authentication scheme for personalized healthcare systems using wireless medical sensor
1239   networks. *Future Generation Computer Systems* 82:727-737.
1240   https://doi.org/10.1016/j.future.2017.08.042
1241 Xiao L, Wan X, Lu X, Zhang Y, and Wu D. 2018. IoT security techniques based on machine learning: How
1242   do IoT devices use AI to enhance security? *IEEE Signal Processing Magazine* 35:41-49.
1243 Xing K, Srinivasan SSR, Jose M, Li J, and Cheng X. 2010. Attacks and countermeasures in sensor networks:
1244   a survey. *Network security*: Springer, 251-272.
1245 Xu G, Lan Y, Zhou W, Huang C, Li W, Zhang W, Zhang G, Ng EYK, Cheng Y, Peng Y, and Che W. 2019. An
1246   IoT-Based Framework of Webvr Visualization for Medical Big Data in Connected Health. *IEEE
1247   Access* 7:173866-173874. 10.1109/ACCESS.2019.2957149

1248   Xu J, Wei L, Wu W, Wang A, Zhang Y, and Zhou F. 2020. Privacy-preserving data integrity verification by
1249   using lightweight streaming authenticated data structures for healthcare cyber–physical system.
1250   *Future Generation Computer Systems* 108:1287-1296.
1251   https://doi.org/10.1016/j.future.2018.04.018
1252   Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, and Chehab A. 2020. Securing
1253   internet of medical things systems: Limitations, issues and recommendations. *Future Generation*
1254   *Computer Systems* 105:581-606. https://doi.org/10.1016/j.future.2019.12.028
1255   Yang Y, Zheng X, Guo W, Liu X, and Chang V. 2018. Privacy-preserving fusion of IoT and big data for e-
1256   health. *Future Generation Computer Systems* 86:1437-1455.
1257   https://doi.org/10.1016/j.future.2018.01.003
1258   Yeh K-H. 2016. BSNCare+: A robust IoT-oriented healthcare system with non-repudiation transactions.
1259   *Applied Sciences* 6:418.
1260   Zhang M, Raghunathan A, and Jha NK. 2013. MedMon: Securing medical devices through wireless
1261   monitoring and anomaly detection. *IEEE Transactions on Biomedical circuits and Systems* 7:871-
1262   881.
1263   Zhang Y, Gravina R, Lu H, Villari M, and Fortino G. 2018. PEA: Parallel electrocardiogram-based
1264   authentication for smart healthcare systems. *Journal of Network and Computer Applications*
1265   117:10-16.

1266
1267

1268

1269
1270

Figure 1

Figure 1: The keywords used in the Research Information Template (RIT).

The entire Mind Map show The keywords used in the Research Information Template (RIT).
The rectangle box at the middle represent the main keywords, then the square boxes
represent the derived similar words from the main words. The oval shaped keywords are
dervied from their previous sequare box keywords
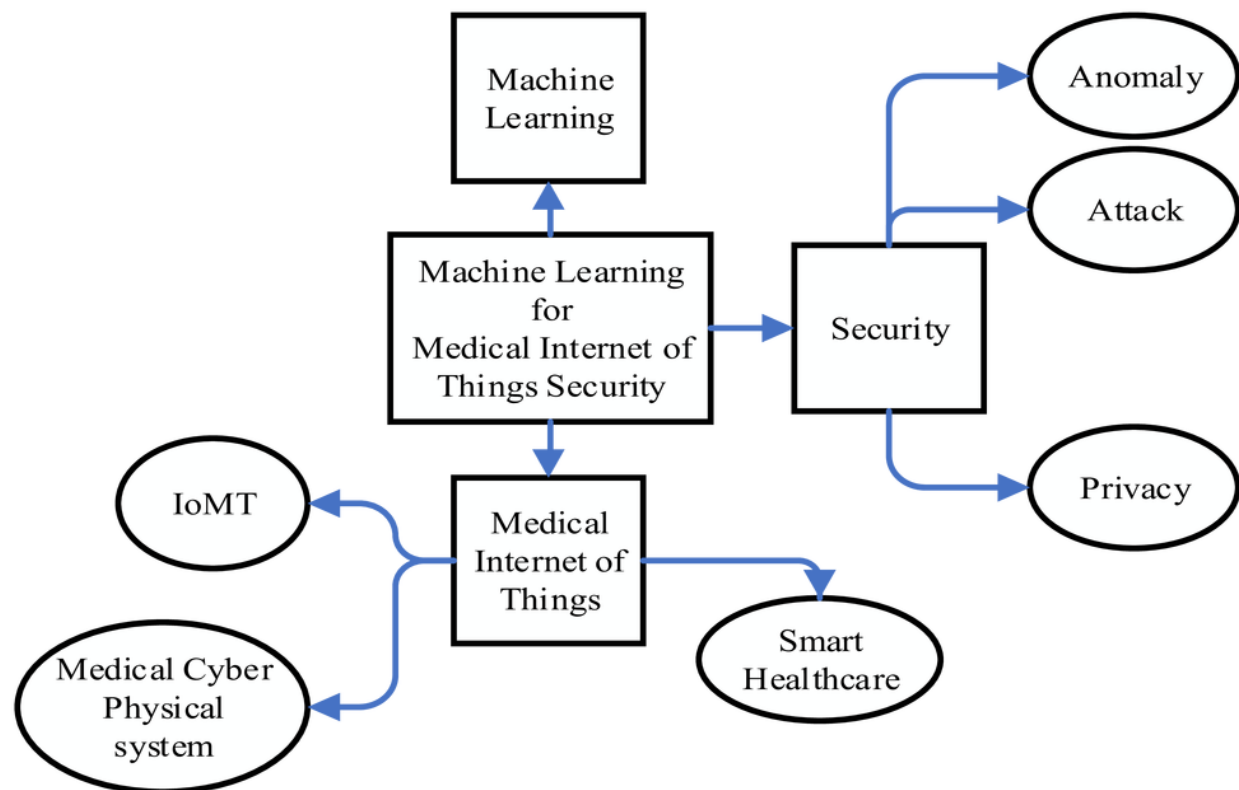
Figure 2

Figure 2: The search strategy used for selecting the research papers based on the PRISMA guideline.

The flow chart represents the procedure of searching in different databases using PRISMA guideline. It starts from top to bottom showing each step of paper selection and fileteration .
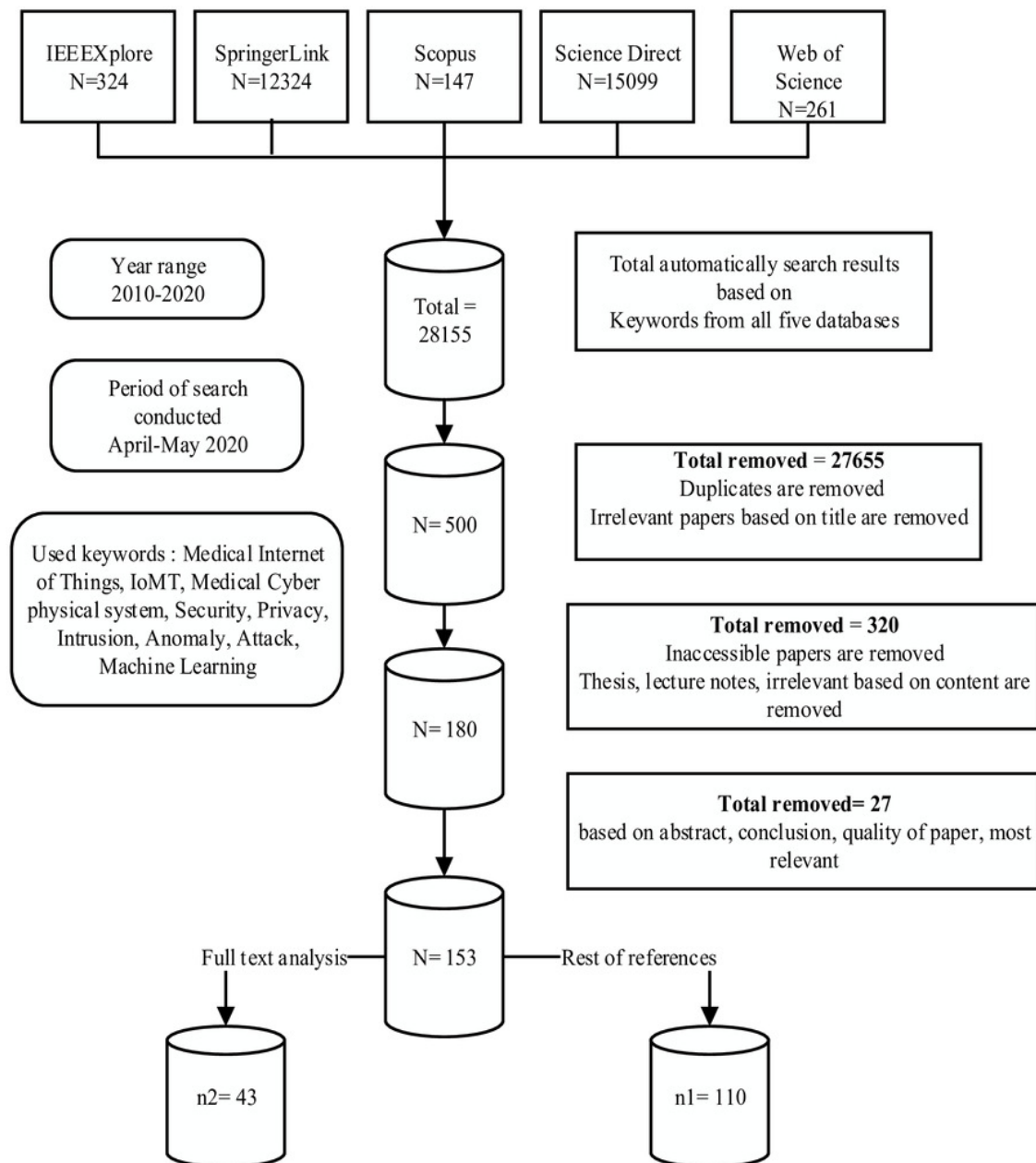
Figure 3

Figure 3: Geographical distribution of the papers.

The pie chart shows the percentage of the papers by each country
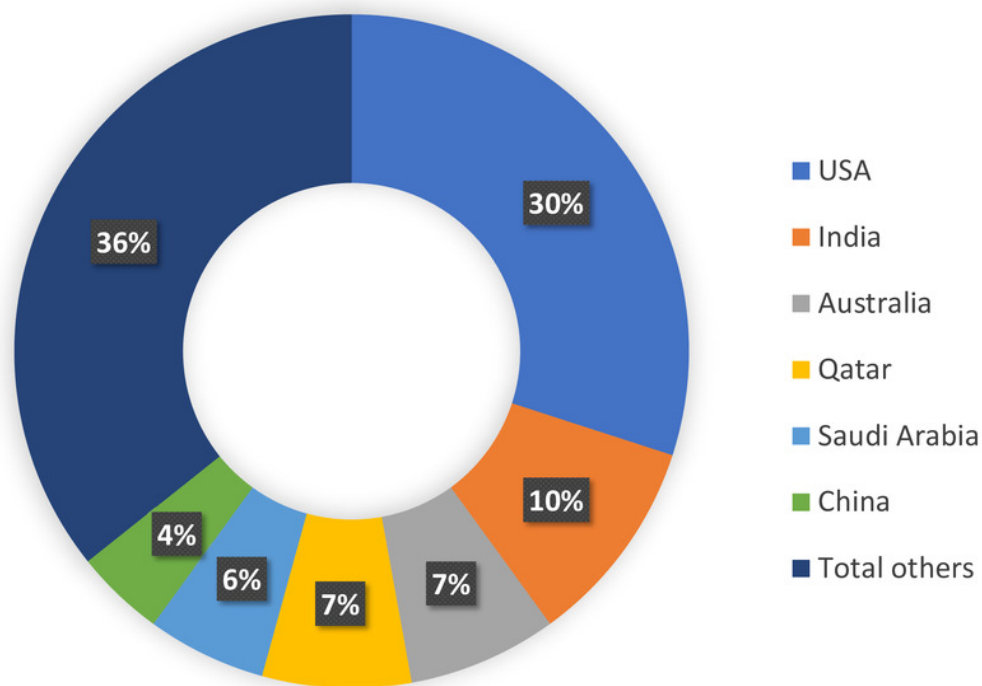
Figure 4

Figure 4: Distribution of the papers by year.

Each Blue Bar represent the number of papers published in each year and orange line shows the percentage of the included reviewed papers in each single year
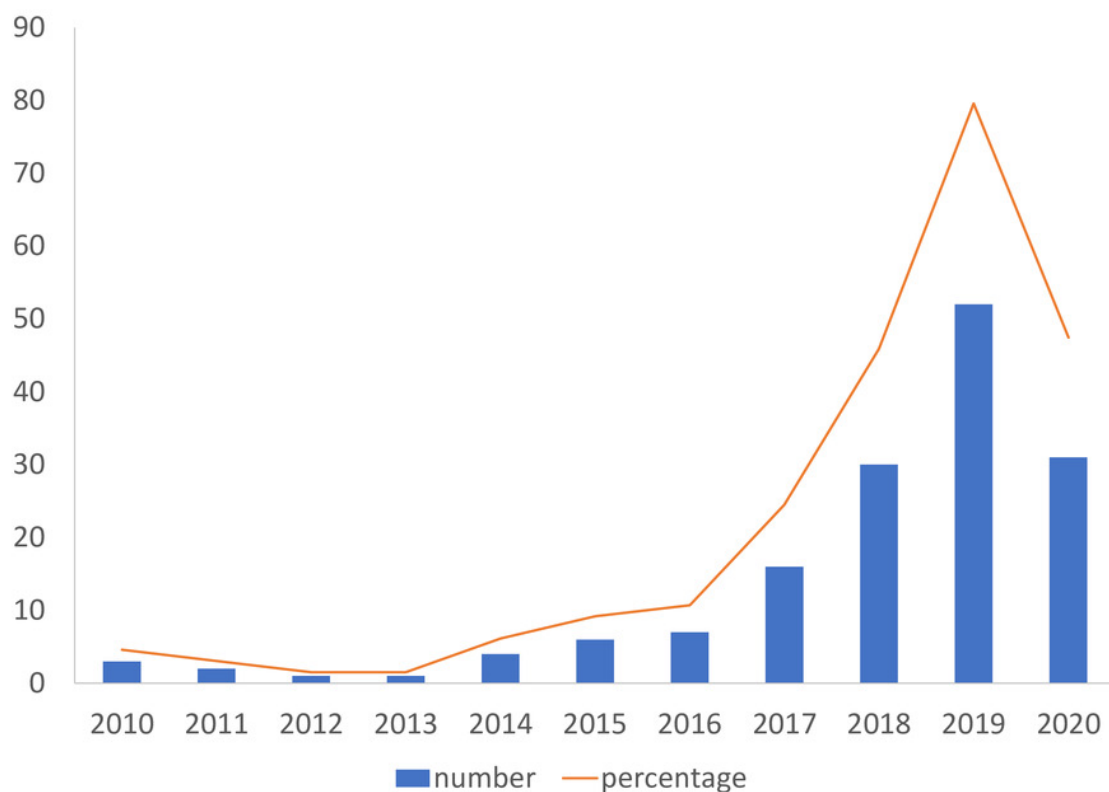
Figure 5

Figure 5: The type of analyzed papers used in the current research.

The pie chart shows the percentage of the analyzed papers in each catgory of Journal, Conference, and Book chapter
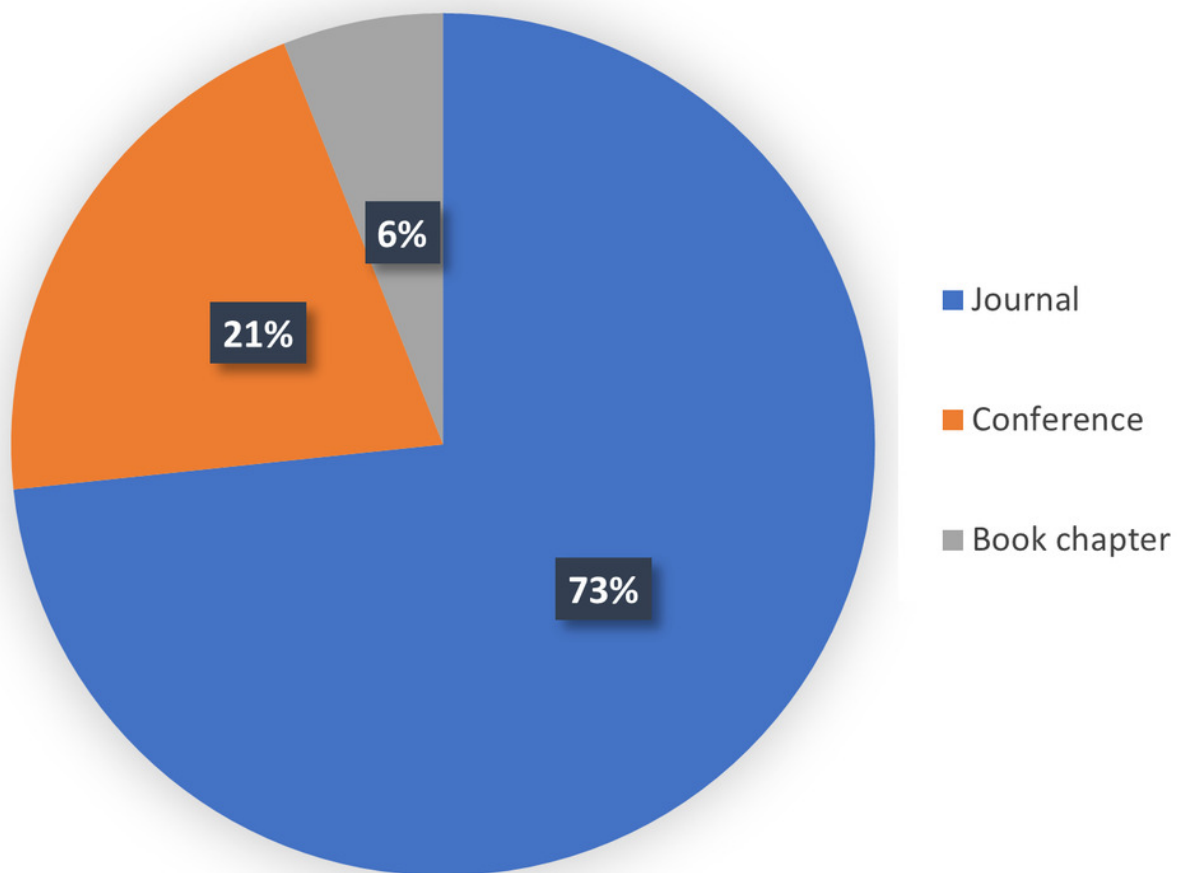
Figure 6

Figure 6: Distribution of the papers according to the publishers.

the pie chart line chart shows the percentage of the analyzed papers which are published by each publisher
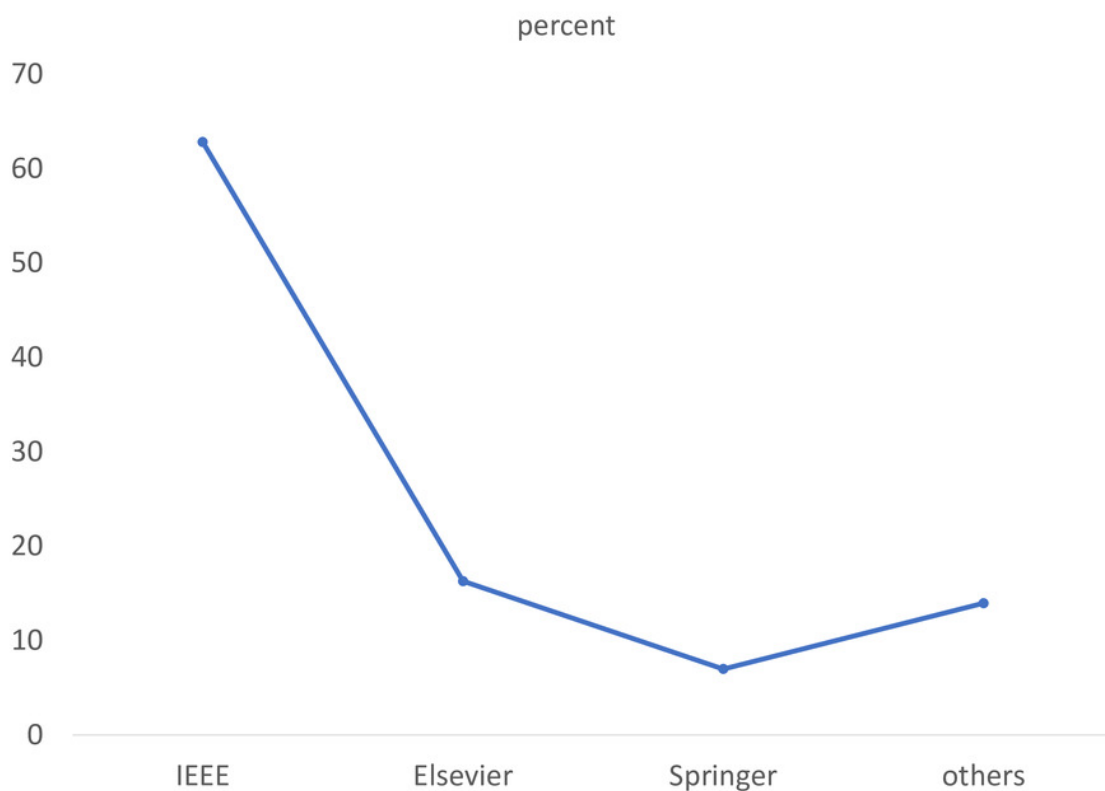
Figure 7

Figure 7: Papers distribution by the direction and problem-solving domain.

The pie chart show the direction of studies. The percentage of the papers for each direction of study is given in the chart
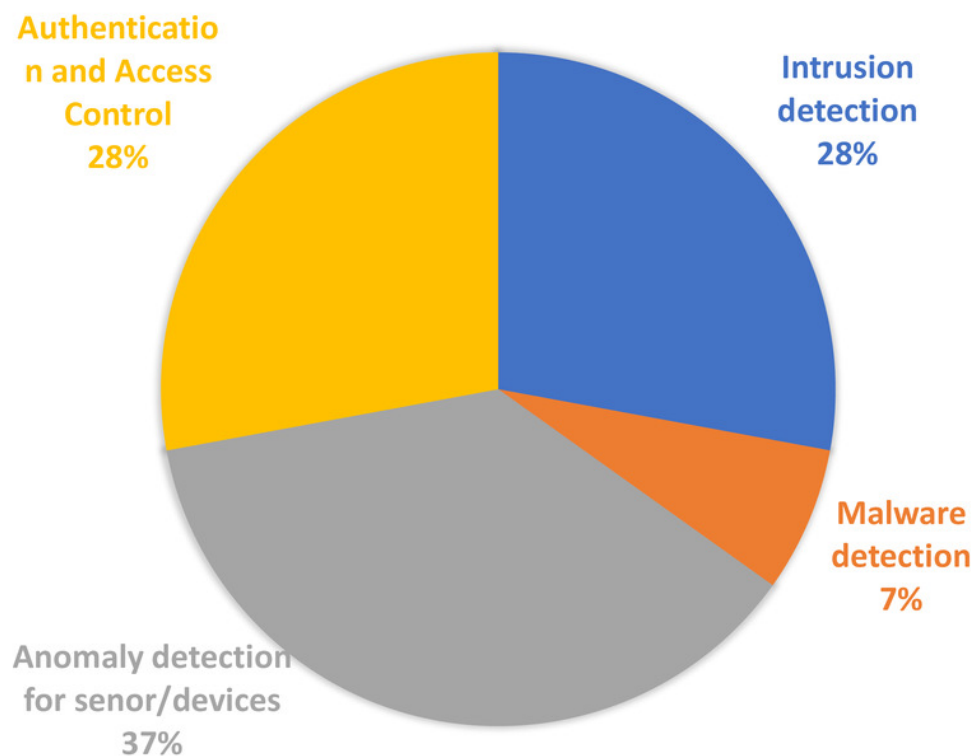
Figure 8

Figure 8. The type of data used by the researchers to conduct their research.

The pie chart shows the percentage of the papers in terms of the type of the data used for their analysis
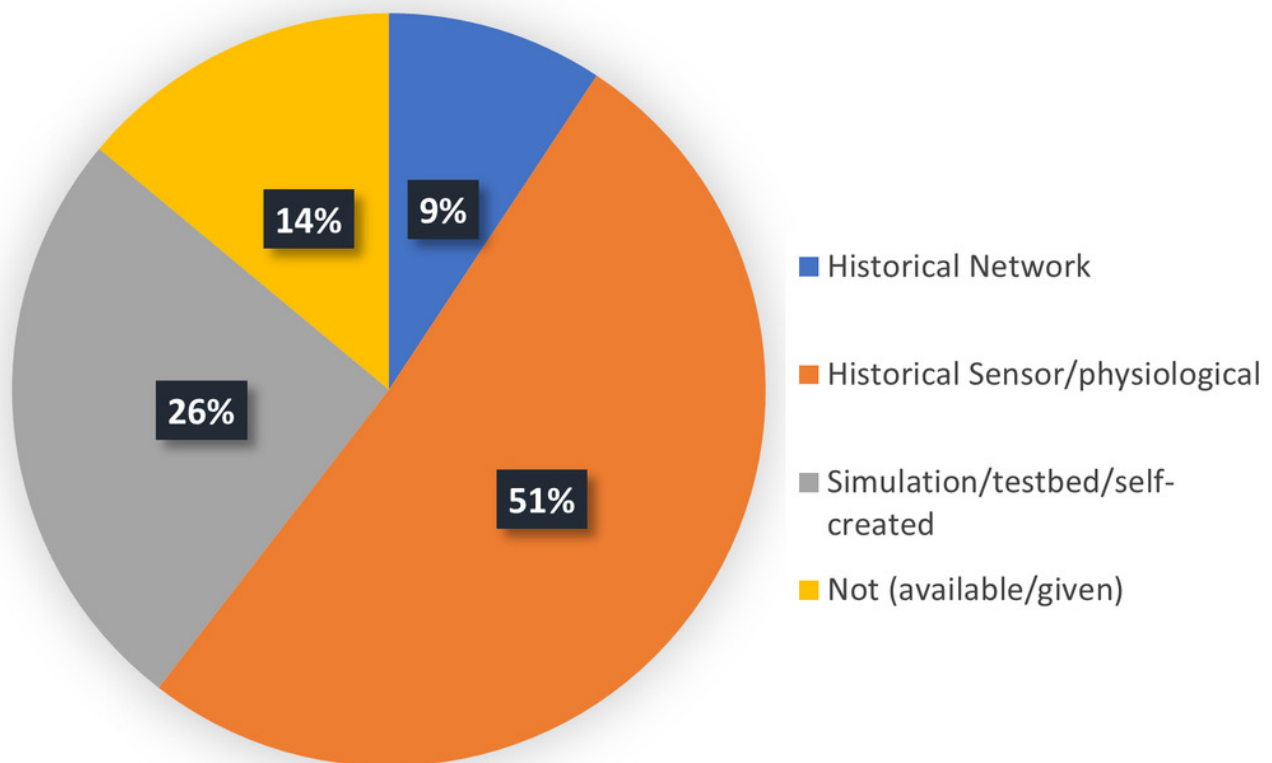
Figure 9

Figure 9: Software and tools used by the studies.

The pie chart shows the percentage of different tools and software which are used by the reviewed studies
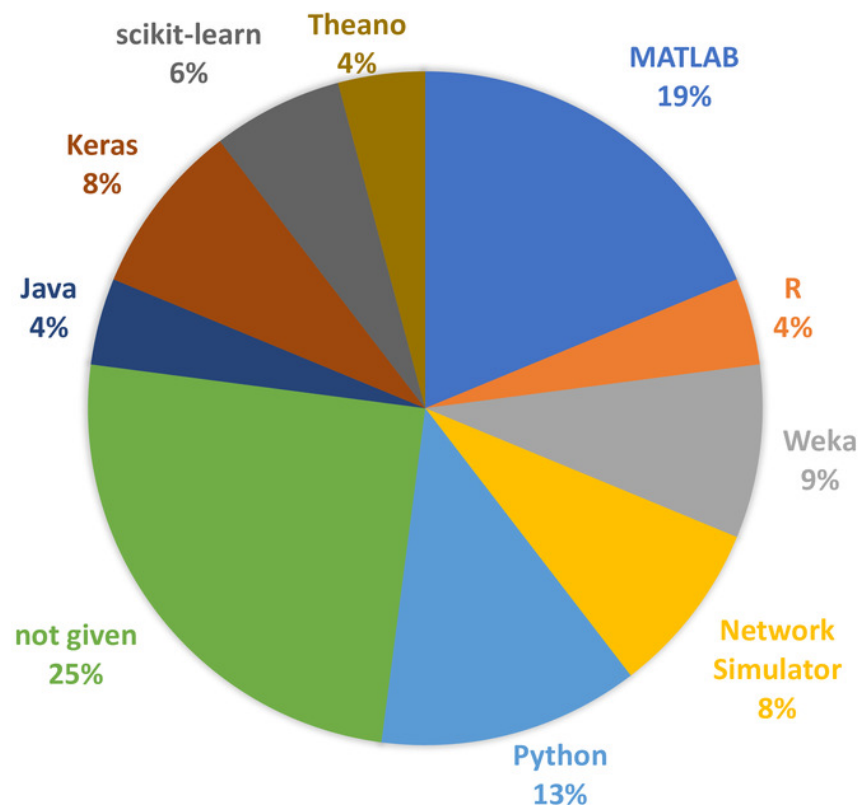
Figure 10

Figure 10: Devices and hardware tools used in the studies.

The bar chart shows the number of hardware tools used by the analyzed studies .
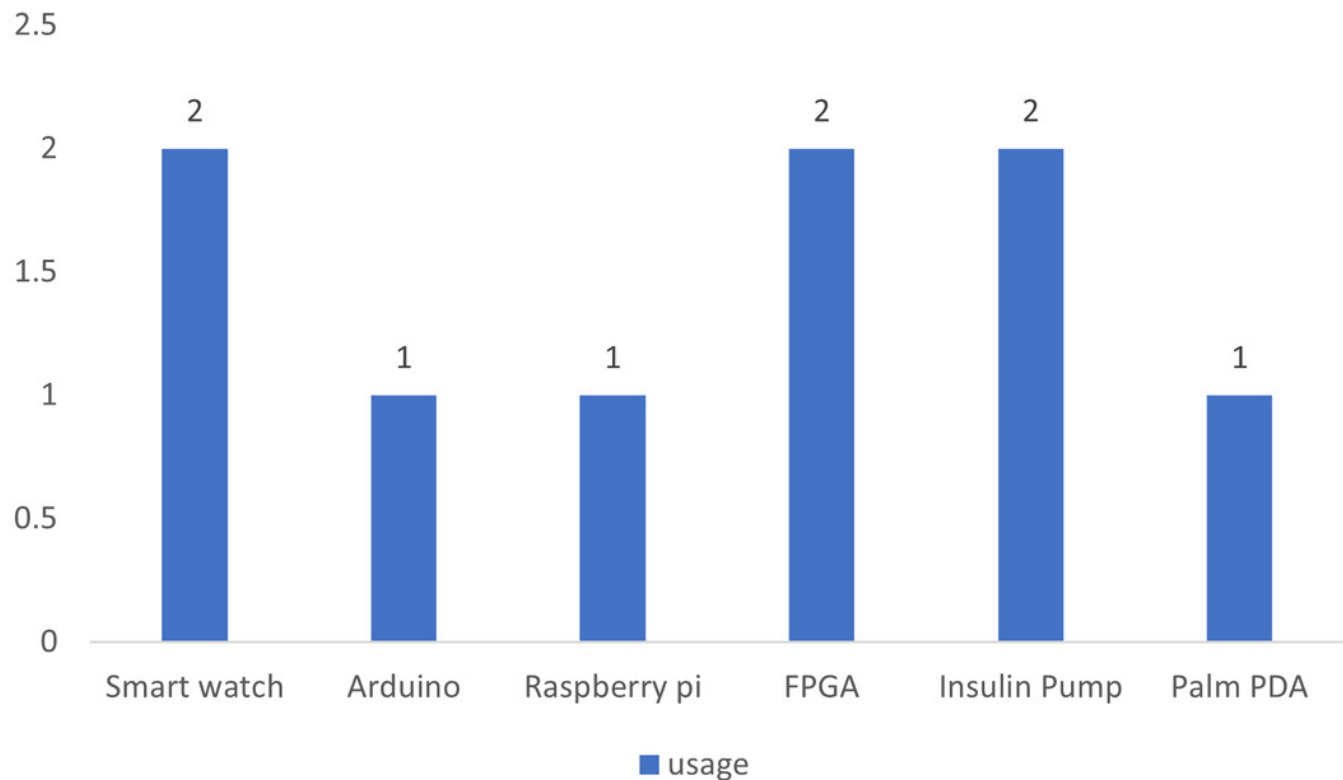
Figure 11

Figure 11: Analysis of the studies in terms of (a)complexity and (b) real time analysis

The pie chart (a) shows the percentage of the papers in terms of complexity {lightweight, heavy, low complex} The pie chart (b) shows the percentage of the analyzed papers based on their real time feature {real time, not real time (heavy), low time complex)}
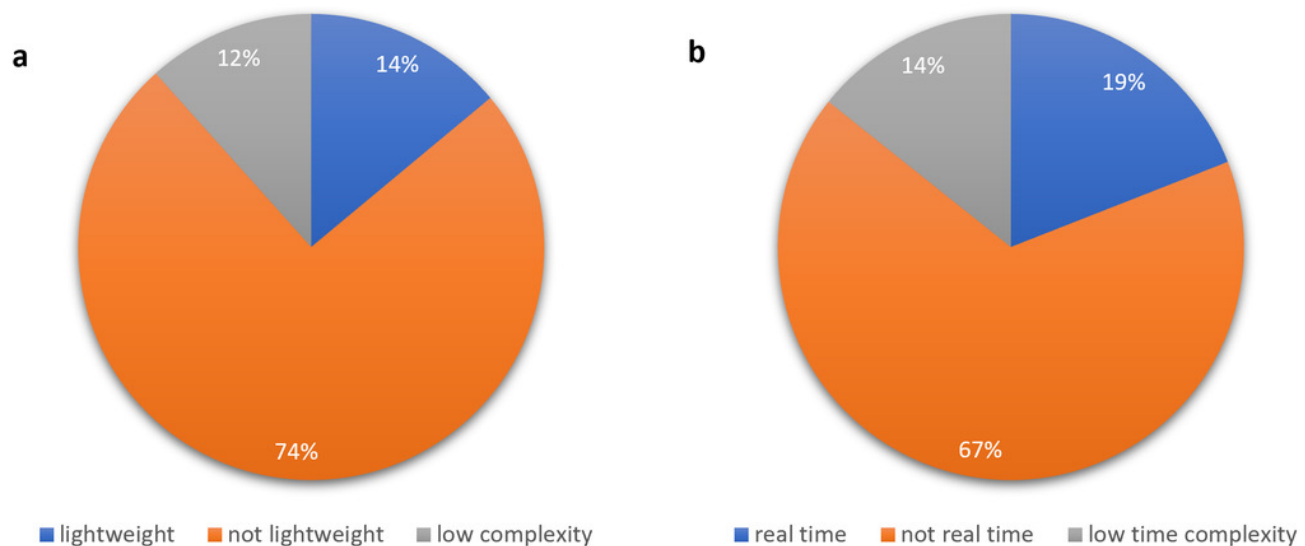
Figure 12

Figure 12: Details of the studies in terms of placement.

the chart shows the percentage of the papers based on their placement
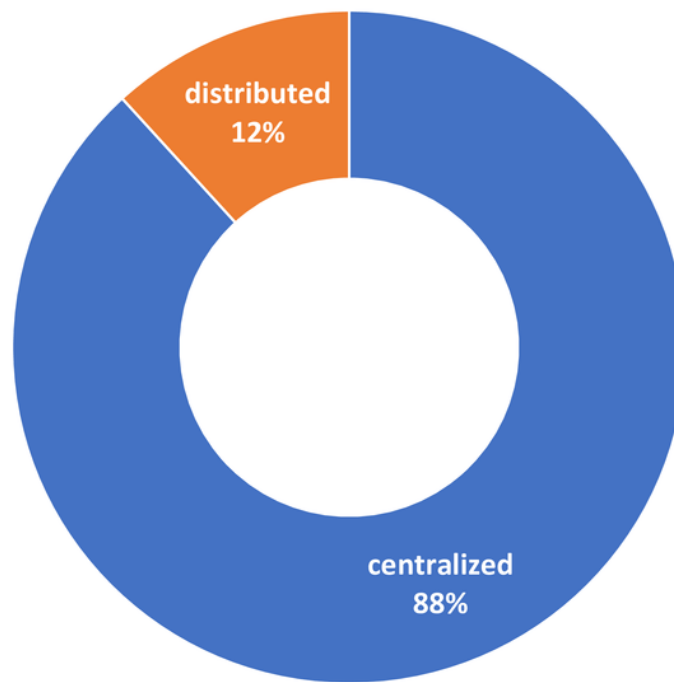
Table 1: The types and characteristics of medical devices used in the IoMT system.

Each row represent different type of medical device and each column represents characteristic of that device

1 Table 1:
2 The types and characteristics of medical devices used in the IoMT system.

Device type	Placement	Example	Risk Value	Ref.
Implantable	H Within the human tissues	deep brain implants, heart pacemaker and insulin pump	High	(Santagati et al. 2020)
Wearable	On the human body	smart watches, fitness devices	Low	(Tseng et al. 2019)
Ambient	Outside the human body	elderly monitoring devices in smart home	Low	(Pandey & Litoriya 2020)
Stationary	Inside hospitals	medical image processing devices of MRI and CT-Scan	Low	(Nanayakkara et al. 2019; Xu et al. 2019)

4
5
6
7
8
9
10
11
12

Table 2: Attacks on different the IoMT layers with their respective impact on security requirements

Each row reprsenst different type of attack and the rows show their targeted layer, Impact, and Refrenece

1   Table 2:
2   Attacks on different the IoMT layers with their respective impact on security requirements.

Attacks	Impact	Ref.
Targeted layer: Server/Database layer		
Malware attack	Integrity, Availability	(Wazid et al. 2019)
Ransomware attack	Integrity, Availability	(Fernandez Maimo et al. 2019)
SQL injection	All	(Li et al. 2019, Gupta et al. 2020)
Social Engineering (Reverse Engineering, Shoulder-surfing)	All	(Yaacoub et al. 2020) (Patel 2020) (He et al. 2018)
Brute Force	Confidentiality, Integrity	(Stiawan et al. 2019)
Adversarial Machine Learning attacks (Causative (Poisoning and Evasion attacks), Exploratory)	Confidentiality, Integrity	(Ibitoye, Shafiq and Matrawy 2019), (Mozaffari-Kermani et al. 2014, Mosenia and Jha 2016), (Chakraborty et al. 2018)
Targeted layer: Network layer		
Denial of Service (DoS) and Distributed DoS (DDoS)	All	(Gupta et al. 2020, Yaacoub et al. 2020) , (Al Shorman, Faris and Aljarah 2019)
Man in the Middle (MIM) attack	Confidentiality, Integrity	(Yaacoub et al. 2020)
Eavesdropping attack	Confidentiality, Non-repudiation, Privacy	(Gupta et al. 2020) (McMahon et al. 2017)
Replay attack	Confidentiality, Integrity	(Spiekermann 2015, Yaacoub et al. 2020)
botnet attack	Availability, Confidentiality	(Bahşi, Nõmm and La Torre 2018)
Mirai attack	Availability, Confidentiality	
Jamming	Availability	(Sun, Lo and Lo 2019)
flooding	Availability	(Gupta et al. 2020, Shafiq et al. 2020, Yaacoub et al. 2020)
Packet Analysis attacks	Integrity, Confidentiality, Non-repudiation, Privacy	(Tseng, Wu and Lai 2019)
Targeted layer: Device/sensor layer		
Physical Sensor/ Node tampering	All	(Xing et al. 2010)
False data Injection	Integrity, Confidentiality, Non-repudiation, Privacy	(Rahman and Mohsenian-Rad 2012, Bostami, Ahmed and Choudhury 2019, Farroha 2019, Newaz et al. 2020)
Resource Depletion Attacks (Battery drain, Sleep deprivation, Buffer overflow)	Availability	(Hei et al. 2010), (Mosenia and Jha 2016) , (Gupta et al. 2020)
Side-channel	Confidentiality, Non-repudiation, Privacy	(Zhang, Raghunathan and Jha 2013, Newaz et al. 2020)
Hardware Trojan	All	(Qu and Yuan 2014, Mosenia and Jha 2016)
Eavesdropping	Confidentiality, Non-repudiation, Privacy	(Gupta et al. 2020) (McMahon et al. 2017)

Table 3: The evaluation metrics used for ML techniques.

Each row represents a metric and the columns show their description, and formula

1   Table 3:
2   The evaluation metrics used for ML techniques.

Metric	Description	Formula
Accuracy	Determines the performance of the model in recognizing all classes, respectively	$Acc = \dfrac{TP + TN}{N}$
Sensitivity (Recall)	Measures the completeness, which is the percentage of positive predicted samples to the positive samples in dataset is depicted.	$Sensitivity = \dfrac{TP}{TP + FN}$
Specificity (Precision)	Shows the exactness, in which the percentage of correctly positive predictive samples to all positive predictive samples by the model are calculated.	$Specificity = \dfrac{TP}{TP + FP}$
False Positive Rate (FPR)	Measures the number of those normal network behaviors which are calculated as attack.	$FPR = FP/(FP + TN)$
Performance overhead	It is the calculation of any combination of (memory, CPU, energy) overhead taken by the ML techniques to perform a task.	*Big(o)notation for time and space complexity and Energy unit for energy usage*
Where TP is True Positive, TN is True Negative, N is total number of samples, FP is False Negative FP is False Positive		

Table 4: Comparison between this survey and other related surveys.

Each row show different related study and columns show their features

1   Table 4:

2   Comparison between this survey and other related surveys.

Year	Ref.	IoT domain	Architecture	Threats	ML methods	Big data	ML for IoMT security	Systematic analysis
2018	(Cui et al. 2018)	Generic	NA	NA	Discussed	NA	NA	NA
2020	(Tahsien et al. 2020)	Generic	IoT architecture	IoT attacks	Discussed	NA	NA	NA
2020	(Hussain et al. 2020)	Generic	NA	IoT attacks	Discussed	Big data at cloud	NA	NA
2019	(Sun et al. 2019)	IoMT	IoMT architecture	IoMT Security requirement	NA	NA	Partially discussed	NA
2020	(Newaz et al. 2020)	IoMT	IoMT architecture	IoMT attacks	NA	NA	Partially discussed	NA
2020	(Yaacoub et al. 2020)	IoMT	IoMT architecture	IoT attacks	NA	NA	NA	NA
-	This study	IoMT	IoMT architecture	IoMT Attacks	Discussed	Discussed	Discussed	Comprehensive and Systematic Review

Table 5: The searching queries and results achieved from five different databases.

Each row shows different queries used for all databases and the columns show their results

1   Table 5:

Searching texts versus databases	IEEE Xplore	Springer Link	Scopus	Science Direct	Web of Science
Machine Learning AND Medical Internet of Things AND Security	89	3431	63	2459	33
Machine Learning AND Medical Internet of Things AND Privacy	37	1093	43	1494	31
Machine Learning AND Medical Internet of Things AND Intrusion	6	336	2	445	3
Machine Learning AND Medical Internet of Things AND Attack	13	1225	2	1203	18
Machine Learning AND IoMT AND Security	9	81	3	929	5
Machine Learning AND IoMT AND Privacy	8	44	3	78	6
Machine Learning AND IoMT AND Intrusion	0	8	1	21	1
Machine Learning AND IoMT AND Attack	0	33		64	5
Machine Learning AND Medical Cyber Physical system AND Security	30	481	5	1038	11
Machine Learning AND Medical Cyber Physical system AND Privacy	8	429	3	693	4
Machine Learning AND Medical Cyber Physical system AND Intrusion	6	321	3	301	4
Machine Learning AND Medical Cyber Physical system AND Attack	9	494	0	699	11
Machine Learning AND Smart healthcare AND Security	57	1971	12	2134	52
Machine Learning AND Smart healthcare AND Privacy	25	1012	3	1901	36
Machine Learning AND Smart healthcare AND Intrusion	7	334	1	431	21
Machine Learning AND Smart healthcare AND Attack	20	1031	3	1209	20
Total including duplicates	**324**	**12324**	**147**	**15099**	**261**

2   The searching queries and results achieved from five different databases.

Table 6: Selection criteria of the papers at final stage

each row represent a criadera for selecting the papers and the coloumn shows the responce

1   Table 6:
2   Selection criteria of the papers at final stage

Criteria#	Questions	Answer
1	Does the paper relevant to the topic?	Y/N
2	Does the work propose a machine learning related solution and method to solve a problem in the IoMT security and/or privacy?	Y/N
3	Is the paper published in scholarly journals, conferences, books?	Y/N

Table 7: Classification of papers based on ML category, medical device, and the IoMT layer.

The table shows a matrix represntation of the paper's classification to different categories

1   Table 7:

2   Classification of papers based on ML category, medical device, and the IoMT layer**.**

ML category - medical device category	IoMT layer- Ref
Supervised ML - Implantable, wearable	**Sensor layer-** **{** (Haque, Rahman and Aziz 2015) ,(Abdaoui et al. 2020) (Rathore et al. 2018), (Khan et al. 2017), (Gao and Thamilarasu 2017), (Newaz et al. 2019), (Ben Amor, Lahyani and Jmaiel 2020), (Mohamed, Meddeb-Makhlouf and Fakhfakh 2019), (Salem et al. 2014), (Hau and Lupu 2019), (Nagdeo and Mahapatro 2019), (Verner and Butvinik 2017) **}** **All layers-**(Rathore et al. 2018b)
Supervised ML- Wearable, smart watches, smart fitness	**Device layer-** **{**(Pirbhulal et al. 2019), (Mawgoud et al. 2019), (Barros et al. 2019), (Zhang et al. 2018), (Shang & Wu 2019), (Musale et al. 2019), (Vhaduri & Poellabauer 2019), (Mohsen et al. 2019), (Rathore et al. 2018a) **}** **Network layer-** **{**(Begli, Derakhshan and Karimipour 2019), (Itten and Vadakkumcheril 2016), (Schneble and Thamilarasu 2019), (Odesile and Thamilarasu 2017), (RM et al. 2020), (Asfaw et al. 2010), (Alrashdi et al. 2019), (Wazid et al. 2019), (Fernandez Maimo et al. 2019)} **Cloud layer-** {(Punithavathi et al. 2019), (Landau et al. 2020)}
Unsupervised ML-Implantable, wearable	**Sensor layer-** **{**(Ben Amor, Lahyani and Jmaiel 2020),(Sehatbakhsh et al. 2018), (Zhang, Raghunathan and Jha 2013), (Verner and Butvinik 2017)**}**
Unsupervised ML-Wearable	**Device layer-** **{**(Zhang et al. 2018), (Shang & Wu 2019), (Musale et al. 2019), (Vhaduri & Poellabauer 2019), (Mohsin et al. 2019)**}** **Network layer-** **{**(Schneble and Thamilarasu 2019), (He et al. 2019),(RM et al. 2020), (Thamilarasu 2016), Fernandez Maimo et al. 2019)**}**
Unsupervised ML-ICD, Programmer	**Device layer-** (Kintzlinger et al. 2020)
Deep learning-Wearable	**Device layer-{** (RM et al. 2020), (Manimurugan et al. 2020), (Shakeel et al. 2018), (Rathore et al. 2019), (Mohsin et al. 2019) **}**
Big data-Wearable	**Device layer-**(Zhang et al. 2018)

Table 8: Details of published studies on anomaly and attack detection to the sensors/medical devices

each row represent each paper under category anomaly and attack detection to the

sensors/medical devices and the columns show their characteristics that are used for

evaluating them

2   Table 8:
3   Details of published studies on anomaly and attack detection to the sensors/medical devices

Ref.	Methods	Detection type	Good features	Limitations	Tools	Dataset info.
(Haque, Rahman and Aziz 2015)	SMO	Anomaly detection	- high detection rate - low FPR	- high computation overhead	Weka	-10 real datasets -(MIMIC)data
(Abdaoui et al. 2020)	Deep Learning	Anomaly based false alarm detection	-real time -high accuracy	- high computation overhead - high FPR	Tensor flow and Keras in Python	John Radcliffe Hospital data
(Rathore et al. 2018)	neural network-based MLP	Anomaly based false alarm detection	-real time -energy efficient -high accuracy -reliable	- high memory requirement due to training overhead	NI myRIO FPGA-based MLP	UCI Diabetic dataset
(Khan et al. 2017)	DWT and Marcov model	Anomaly based false data detection	-high detection rate -high TNR -real time	- detection rate decreases when there is too much attack - high FNR and FPR	MATLAB	The ECG dataset from MIT-PHYSIOBANK
(Gao and Thamilarasu 2017)	Decision tree, SVM and K-means	Anomaly-based attack detection	- high accuracy - low FPR - low training time - low prediction time	- no validation - memory, battery usage is not considered - fails in detecting insider attack	Castalia	Simulation data
(Sehatbakhsh et al. 2018)	(K-S test) on external hardware device	malware Anomaly detection	-high TPR -low FPR -low detection latency -no overhead on the medical device	- external device needs maintenance and the device itself could be hacked (stolen or lost)	Open Syringe Pump Arduino UNO, Nios-II, OlimexA13, and TS-7250	Testbed data
(Zhang, Raghunathan and Jha 2013)	a model is embedded on an external device	multi-layered anomaly detection.	- zero overhead on battery - real time - multiple attacks detection - hybrid detection	-protecting only integrity - external device needs maintenance and it could be hacked (stolen or lost) - lack of behavioral anomaly detection experiment	USRP Glucose monitoring and insulin delivery systems	Testbed data
(Newaz et al. 2019)	ANN, DT, RF, and k-NN	Anomaly detection Uses medical device data	-high accuracy -high F1 -No overhead on the sensors - uses body functioning data	- high training overhead - performance overhead not calculated.	MATLAB	A set of heath dataset from different sources
(Ben Amor, Lahyani and Jmaiel 2020)	PCA and Correlation Coefficient	Anomaly based faulty sensor data detection.	- real time - lightweight - improved accuracy - improved FPR	-energy, CPU usage is not considered -lacks attack detection at server and transmission	AUDITmodule Java and R languages	MIMIC database
(Mohamed, Meddeb-Makhlouf and Fakhfakh 2019)	Statistical signal amplitude calculation	Anomaly based intrusion cancellation	- using more than one type of Sensor type - high TPR	- not lightweight -not real time -high performance overhead	MATLAB	real medical ECG and EMG datasets
(Salem et al. 2014)	Classifiers (SVM, RF, K-NN, Decision Trees) and Regression	Anomaly detection for sensor physiological data	- low detection time - high TPR - low FNR	-not lightweight -performance overhead not calculated	Weka	MIMIC dataset
(Hau and Lupu	Time series	Anomaly based false	-High detection for	-long detection time	Not given	MIMIC

2019)	approach temporal-attribute correlations	data injection attack detection	single sensor -acceptable detection for moderate sensors	-disable when many sensors increase (collusion)		dataset
(Nagdeo and Mahapatro 2019)	combined ANN with Ensemble LinReg	Classification of anomalous and faulty sensor physiological data	- high TPR - low FPR	Not real-time Not lightweight Unknown dataset source Performance overhead not calculated	Weka	ECG dataset
(Verner and Butvinik 2017)	Otsu's Thresholding, and Linear SVM	sensor data modification detection	- high precision - high recall - can be used for other IoT domains	-not real-time -not lightweight -Performance overhead not calculated	MATLAB	(JDRF) (CGM) Clinical Trial dataset
(Kintzlinger et al. 2020)	statistical and One class SVM	Rule and knowledge based anomaly attack detection	- high TPR - low FPR - high accuracy - real time	-layers III-V is useless - heavy training overhead - performance overhead not calculated - learns from only benign data	Not given	Self-created clinical data
(Rathore et al. 2019)	Deep Learning classifier	Attack prediction	-classify different attacks -reduced training time	-not lightweight -accuracy not given	Keras with Theano in Python	Parkinson tremor dataset from Physionet

Table 9: The summary of the studies reported on authentication and access control.

each row represent each paper under category authentication and access control and the
columns show their characteristics that are used for evaluating them

1   Table 9:
2   The summary of the studies reported on authentication and access control.

Ref.	Methods	Good Features	Gaps and limitation	tools	Data info
(Rathore et al. 2018b)	Legendre approximation and MLP	-High testing accuracy	-High computational overhead for IMD. -Not able to detect unknown attacks.	MATLAB Keras Theano	ECG-ID dataset
(Pirbhulal et al. 2019)	MLP	-Efficient -Light weight	-Evaluation not given. -Lacks validation metrics. -MLP is memory intensive.	Not given	Not given
(Mawgoud et al. 2019)	SVM and trust management	-Low resource consumption -Lower detection time	-Performance overhead not calculated. -Lacks measuring the cryptography security strength of the algorithm.	Not given	Not available
(Barros et al. 2019)	MLP, RF, SVM and Naïve bayes	-Low complexity -High accuracy	- Performance overhead not calculated -High Training overhead -Reduced accuracy due to feature selection -Not easy to implement with different sensors	Weka	Stress Recognition in Automobile Drivers database
(Zhang et al. 2018)	2DPCA, LDA, and MapReduce	-Improved accuracy -Improved efficiency	-Performance overhead not calculated. -High training overhead - Not suitable for tiny IoT devices	Hadoop	MIT-BIH Database
(Shang & Wu 2019)	LOF model	-Improved accuracy in acceptance and rejection	-Not accurate when user's behavior not stable. -Different performance on different brands of smartwatch -Sensors should be attached to body tightly. -Performance overhead not calculated	Samsung smartwatchTizen OS 3.0	Self-created
(Musale et al. 2019)	Statistical filers, RF, KNN, and MLP	-Lightweight -Higher accuracy -User-friendly -Easily deployable	- performance overhead not calculated. - No attack model is considered for gait authentication. - Environment can affect its accuracy. - Authentication fails if the user is far from smart home. - Its accuracy decreases in the case of increasing the users	Motorola (smartphone) python	Self-created
(Vhaduri & Poellabauer 2019)	A combination of filters ((KS)-test, PC, SD based filter) and SVM	-Use of hybrid biometric. -High accuracy -Low error rate	-Degradation of Non-Sedentary performance for highly active periods. -Need for retraining. -Cannot detect online attacks -performance overhead not calculated.	MATLAB	NetHealth Study Dataset
(Mohsen et al. 2019)	Cryptography, convolutional Neural network (CNN)	-End to end security -Strong against multiple attacks -Lightweight - Real time	-Communication overhead is still high for medical devices. -High training overhead. - Performance overhead not calculated. -Some attacks may still occur in that 30 min of monitoring gap ex; sensor may be relocated and returned	Not available	Not available
(Punithavathi et al. 2019)	a lightweight random projection technique	-Low complexity -Lightweight -High recognition accuracy	-Rejection rate not calculated. -memory, energy usage is not calculated. -Missing attack validation	OpenCV 3.6 in Python 3.4.	DB1 and DB2 of FVC2002 and FVC2004
(Rathore et al. 2018a)	Dynamic Time Warping (DTW)	-Lightweight -Efficient -High accuracy -Less complex	-Missing validation against attacks -Acceptance and Rejection rate not calculated. -Heavy for implantable devices	LabVIEW MathScript RT Module	ECG-ID dataset
(Mohsin et al. 2019)	PSO, Blockchain, AES	-Higher secure transmission -Strong against spoofing and brute-	-Key distribution in AES adds extra load on the channels. -Block chain is a heavy and resource extensive	Not given	MMCBNU_6000 database

		force attacks -High accuracy			

Table 10: Summary of the studies reported on intrusion and malware detection.

each row represent each paper under category intrusion and malware detection, the columns
show their characteristics that are used for evaluating them

2   Table 10:
3   Summary of the studies reported on intrusion and malware detection.

Ref.	Method	Type of Intrusion detection	Good features	Gaps and Limitations	Tools (software& hardware)	Datasets
(Begli, Derakhshan and Karimipour 2019)	SVM	Anomaly and signature-based IDS	-High detection accuracy -Satisfied detection time	- High memory overhead - Low detection rate in misuse analysis -Outdated dataset	R program	NSL-KDD
(Itten and Vadakkumcheril 2016)	a multivariate correlation analysis	Hybrid Anomaly and rule based IDS	- Improved accuracy. - Detecting known and unknown attacks.	- High learning overhead - Unclear implementation - Validation process not given	Not given	Not given
(Schneble and Thamilarasu 2019)	Federated Learning	Anomaly based false data injection, data modification, DoS IDS	-Multiple attack detection -High accuracy - Low FPR - Flexible	- Reduced accuracy and increased FPR in some cases - Weak against adversarial attacks	- Sci-kit Learn's on Raspberry Pi's. - MATLAB	- MIMIC dataset from PhysioNet - ECG
(Odesile and Thamilarasu 2017)	Hierarchical and distributed classifiers (NBC, KNN, SVM, RF and DT)	Anomaly based IDS	- High accuracy - Low energy consumption	- High training time for some methods - High FPR	Castalia WBAN	Self-created simulated data
(Schneble and Thamilarasu 2019)	feature selection (Laplacian scoring)	Signature based intrusion detection.	- Reduced the detection time. - Reduced performance overhead	- Accuracy reduced upon selecting more features. - Lacks detail of selected features.	Not given	MIT-BIH Arrhythmia dataset
(He et al. 2019)	SAE is used for feature selection	Signature based intrusion detection. HIDS	- Improved accuracy and detection overhead	- High training overhead - Not lightweight	Not given	real CHS Source not given
(RM et al. 2020)	Feature selection using PCA and GWO with DL classifier	Signature based IDS NIDS	-high accuracy low training and testing time	- High Memory and CPU overhead. - Limited to only IP based devices.	Not given	NSL-KDD
(Thamilarasu 2016)	multi-objective genetic algorithm (GA)	-Signature based IDS -HIDS	-F selection reduced the complexity	- Not lightweight - Detection time and training time not given.	MATLAB	Self-created by simulation
(Asfaw et al. 2010)	Data mining-based Association rule mining	-Anomaly based HIDS	-Ability to detect anomalous activity.	- Lacks model evaluation - Using many resources	-J2ME -Java Servlets -MySQL Server -Palm PDA	Self-created
(Manimurugan et al. 2020)	Deep Belief Network (DBN)	-Anomaly based NIDS.	-High accuracy -High precision, F1, and recall.	- FPR and performance overhead neglected. - -High training overhead	MATLAB	CICIDS2017 dataset

(Alrashdi et al. 2019)	Ensemble an online sequential extreme learning machine (EOS-ELM)	-Anomaly based NIDS.	- Lower latency compared with cloud-based. - Reduced attack detection time	-Memory and CPU usage are not considered	-Python (scikit-learn, Tensorflow, Keras, Numpy, HDF5)	NSL-KDD dataset
(Wazid et al. 2019)	Machine Learning, Data mining, Blockchain	-Signature and Anomaly based Malware detection.	Discussed current IoMT malware detection	Most papers are generic IoT especially Smart phone-based solutions.	Not given	Not given
(Fernandez Maimo et al. 2019)	NFV / SDN, OC-SVM , and Naïve Bayes	-Anomaly and signature-based Ransomware detection.	- Real time - Can detect recent malware attacks. - Short detection time	- Not lightweight - performance overhead not calculated	- OpenICE - OpenStack - OpenDaylight - Python language - Scikit-learn v0.20.0	Self-created real testbed dataset
(Shakeel et al. 2018)	Deep-Q-Network (LDQN)	-Signature based malware detection.	- High detection rate - Low error - Low energy consumption	- FPR, Memory usage are not considered. - Training overhead is high	NS2 simulator	Simulated data
(Landau et al. 2020)	Different ML techniques	-Privacy attack detection.	-Improved performance -Larger datasets used	- Still low accuracy - high error rare	Not given	rsEEG data