IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 29, 2019, accepted October 21, 2019, date of publication October 31, 2019, date of current version December 5, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2950849

Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain

ABDUL RAZAQUE[1], FATHI AMSAAD[2], MEER JARO KHAN[3], SALIM HARIRI[4], SHUJING CHEN[5], CHEN SITING[5], AND XINGCHEN JI[5]

[1]Department of Computer Engineering and Telecommunication, International Information Technology University, Almaty 050000, Kazakhstan
[2]Department of Computing Sciences and Computer Engineering, The University of Southern Mississippi, Hattiesburg, MS 39406, USA
[3]Department of Business Management and Information, International Islamic University Islamabad, Islamabad 44000, Pakistan
[4]Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721, USA
[5]Department of Computer Science, New York Institute of Technology, Nanjing Campus, Nanjing 210046, China

Corresponding author: Abdul Razaque (a.razaque@iitu.kz)

ABSTRACT Recently, an increasing number of cyber-attacks in the medical field has resulted in great losses in the health care industry, since medical information plays an essential role in human health. To introduce a comprehensive survey about possible cyber-attacks and solutions for these attacks, our paper first presents a brief overview of the necessary background of the dataflow in the medical domain and then identifies the vulnerabilities in each stage of the dataflow. Then, according to the weaknesses identified in the medical system, a classification of cyber-attacks is presented. Additionally, the paper presents research on previous work that focuses on solving these cyber-attacks and identifies the strengths and limitations of the solutions for each attack. More importantly, for data storage assurance, our paper discusses several cybersecurity architectures for the medical domain from the existing literature. The countermeasures from previous papers and architectures that are still weak in terms of resource depletion, attack reduction, applicability, etc. are addressed. Finally, the paper discusses and recommends solutions for future work to decrease cyber-attacks in the medical field so that human health can be guaranteed.

INDEX TERMS Dataflow, medical field, cyber-attacks, architectures, cybersecurity, threats, vulnerabilities.

I. INTRODUCTION

Currently, there are increased concerns regarding personal data breaches in the medical field. Boan News [1] reported in 2015 that the top two data breach concerns are in the finance and healthcare sectors, accounting for 49.45% and 28.41% of breaches, respectively. Finance is commonly a target for hackers because the records are filled with pecuniary exchanges. Security measures in the healthcare sector are receiving less attention than those in finance; however, medical data are much more important and sensitive.

Ambrose and Basu [2] express that cyber-attacks are the most frequent causes of medical data breaches. Medical institutions collect and preserve patient data on their systems in databases such as those on their websites, electronic medical recording (EMR) systems, order communication systems (OCS), and picture archiving and communication systems (PACS); thus, data security is closely linked to cybersecurity [3]–[7]. Also, if medical data are in danger, there are detrimental consequences such as patient information leakage, patient misdiagnosis, and mistreatment. These consequences tend to seriously endanger the physical and mental health of patients. With the progress of living standards, demand for better medical systems increases. Yang *et al.* [8] proposed a design for a mobile smart medical system. The system focused on the applicability of mobile smart medical systems and analyzed potential attacks on the system. Hareland [9] designed a medical system considering the multi-lifecycle environment. It focused on medical equipment instead of web applications. By analyzing and expanding the lifetime of medical equipment, patients can receive improved medical healthcare. By following the trend of combining network techniques and medical systems, our paper focuses on cybersecurity and its impact on the medical domain.

Recently, this topic has come under heated discussion. Sun *et al.* [10] fully researched the medical process using emerging Internet-of-Things (IoT) technology and concluded that IoTs technology can reduce treatment time and improve treatment efficiency. However, the paper did not address the

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

influence of medical equipment. Hareland *et al.* [11] proposed a supervisory exchange mechanism to keep the medical system stable and improve the safety level of the system. There are still many issues to discuss regarding cybersecurity in the medical domain.

To study cybersecurity and the medical domain, our paper focuses on the cybersecurity vulnerabilities and relevant protection techniques against these vulnerabilities. We also discuss several cybersecurity systems for the medical domain and classify them based on their type.

The rest of the paper is structured as follows. Section II presents contributions of the related reviews and surveys. Section III presents the research methodology. Section IV demonstrates an information flow in the medical domain. Section V defines four different kinds of cybersecurity vulnerabilities in the medical domain and gives a detailed explanation of these vulnerabilities, which can be easily attacked, negatively affecting the medical domain. Section VI presents the different types of attacks due to these vulnerabilities. Section VII presents medical architectures of cybersecurity. Section VIII provides a discussion of the above solutions, and the paper is concluded in section IX.

II. RELATED REVIEWS/SURVEYS, CONTRIBUTIONS

In this section, salient features of existing reviews/surveys are extensively discussed. The medical care has got global popularity over the last decade due to the involvement of IoTs and its heavy reliance on information technology. The cybersecurity of the Medical Care Information system (MCIS) is now a crucial component of reliable, safe and effective medical care delivery. The cybersecurity is one of the greatest threats for IoT-enabled medical devices. Jang-Jaccard and Nepal [143] presented the vulnerabilities in existing software, hardware and network layers. New attack patterns were discussed that affected the emerging technologies such as cloud computing, social media, critical infrastructure smartphone technology.

With advent of the latest technology in the medical domain, there is a great possibility of vulnerabilities and attacks on medical technology. An extensive survey of implantable medical devices including security, privacy risks, and patient safety was produced by Camara *et al.* [107]. Regarding healthcare technologies, a survey of the progress of IoT-enabled health technology was provided by Riazul Islam *et al.* [108]; the review also discusses state-of-the-art network architectures, industry development, and privacy and security characteristics, including security requirements and threat models. Finally, an intelligent collaborative security framework was proposed to reduce security hazards. An interesting survey regarding devices based on wireless body area networks used in the medical field was presented by Al-Janabi et al. [109]. The survey focused on privacy and security requirements for those healthcare devices.

Malasri and Wang [110] presented a survey of healthcare implantable devices and discussed some attacks (eavesdrop and spoofing) on implantable devices. The methodical study of IoT for eHealth was discussed by Ida *et al.* [111]; the study also discussed IoT healthcare security challenges. McMahon *et al.* [112] extensively discussed IoT-enabled medical devices. However, the survey attempted to detect the vulnerabilities of compromised medical devices only. Another good survey presented by Masdari and Ahmadzadeh [113] discussed the authentication taxonomy of the telecare medical system (TMS). Furthermore, the authentication approaches of TMS are compared, and limitations and advantages of TMS are highlighted.

Strielkina *et al.* [114] presented a case study regarding the vulnerabilities of healthcare IoT by using only the Markov model. However, few vulnerabilities were highlighted due to the limitations of the Markov model. A promising review of the medical service field is presented by Alzahrani *et al.* [115]. This review focused on the near-field communication required for healthcare applications. Furthermore, the attack categorization of near-field communication is provided.

Wu *et al.* [116] present a detailed survey on implantable medical devices, with an emphasis on access control approaches for avoiding unauthorized access. Another survey regarding cyber security challenges in healthcare was provided by Kruse *et al.* [117]. Jalali *et al.* [138] presented the bibliometric analysis of the literature on Health care and cybersecurity. This is one of the interesting reviews that highlight the publication-contribution percentage and research gap from the cybersecurity perspective.

The publications involved the non-technological variables, the business community, software development security and physical security. According to this survey, physical security requires more attention because many physical attacks lead to breaches and harm the safety of the patient. McDermott *et al.* [139] conducted survey to determine the potential threat classifications for protecting Electronic Health Record (HER) information. The threats were classified into five categories; portable devices, physical, technical, insider use and administrative. Coventry and Branley [140] discussed the cybersecurity breaches including ransomware attacks on hospitals and health information theft. Furthermore, attacks on entrenched medical devices were deliberated. Fernández-Alemán *et al.* [141] reported the systematic literature review result focusing on the security and privacy of EHR systems. Review further suggested to design the standards and the pronouncement of directives regarding security and privacy for EHR systems. Charlotte [142] presented the overview of IoT and possible cybersecurity threats in general.

After extensively studying these surveys, we determined that all the available surveys are of great importance. However, these surveys either focus on the security and privacy of implantable medical devices from an IoT perspective or authenticate the devices using specific models and case studies. In contrast, our state-of-the-art survey presents the flow of information in the medical domain and the main vulnerabilities of cybersecurity in the medical domain, with a particular focus on information storage and IoT connection.

Furthermore, cyber security attacks regarding dataflow in the medical field are extensively discussed.

Dataflow attacks are characterized into four categories: information collection attacks, database attacks, website attacks and operation device attacks. Finally, the medical architecture of cybersecurity is classified and briefly discussed. The contributions of this paper are as follows:

- Background information and the relationship between the medical field and cybersecurity is introduced to describe the basic information of the article.
- A dataflow model that is efficient for identifying attacks in the medical system is created for the medical domain.
- A classification of cyber-attacks closely related to the medical field is given, and this classification contributes to the analysis of the advantages and limitations of cyber-attack solutions.
- A classification of medical cybersecurity architectures in different systems is given, and this classification can be used to address cybersecurity problems.
- The advantages and drawbacks of various architectures are analyzed with respect to the intelligence medical system, the personal electronic medical system, E-Health archives, the noninvasive ECG sensor system, the implantable imaging system, the comprehensive information system and the hospital information system. Furthermore, we provide reasonable explanations and methods for addressing these problems.
- A comparison of cybersecurity architecture capabilities, which can be helpful for recommending solutions, is presented.
- A brief and detailed conclusion that covers all parts of this survey is provided, and a comprehensive comparison and future expectations in the separate areas are discussed.

III. RESEARCH METHODOLOGY

To conduct this survey, an integrative review approach is used because the purpose is to criticize and synthesize the existing cybersecurity challenges, which affect the medical domain. For example, what types of vulnerabilities could affect the medical domain that leads to several cybersecurity attacks? What is the negative impact of those attacks on the human and physical IoT devices in the medical domain? What possible countermeasures and protection solutions should be considered to avoid such types of cyber-attacks? Because 41% medical companies have over 1000 sensitive and confidential files including credit/debit card numbers and medical records left undefended [133] and 70% medical industry claims that have been greatly affected due to several types of cyber-attacks. The healthcare industry faces the highest number of malicious attacks by the ransomware, which will be multiplied by 2020 [134].

To address these questions, the qualitative analysis and evaluation approaches are applied for accumulating the more creative information. However, the search strategy is not purely systematic and the survey does not cover all blinded peer-reviewed scholarly articles ever published on this topic but focused on the year 2001-2019. The source of collection of the articles is highly transparent and to have been selected from the books, research articles, and other published online materials from the databases of CINAHL, PubMed (Medline), IEEE Digital Library, MetaPress, Science@Direct, Trip Database, ERIC, CORE, arXiv e-Print Archive, Directory of Open Access Journals (DOAJ), ProQuest, Semantic Scholar, Social Science Research Network (SSRN) regarding the cybersecurity issues correlated to software and hardware vulnerabilities, attacks, possible solutions and architectures from the medical domain perspective. The key terms used in the search criteria were based on cybersecurity, Dataflow, medical field, cyber-attacks, architectures, threats, and vulnerabilities.

The search produced samples of 143 articles. As each article was separated by the authors for significance to the goal. Seventy-Six articles were reviewed to determine the top vulnerabilities, attacks, and possible solutions.

As some of the interesting surveys attempt to partially answer to our review questions. However, the existing surveys either focus on the security and privacy of implantable medical devices or just authenticate the devices using specific models and case studies from an IoT perspective. Our suggested quantitative approach enables us to discover whether or not the medical domain is affected due to cyber-vulnerabilities. On the other hand, such vulnerabilities harm the data collection, patient's input data registration processes (e.g. hardware-based data collection and software-based data collection). For our practical sample selection, we chose two hospitals in Kazakhstan, which are almost connected with IoT devices and most of the data collection and registration processes in those hospitals are carried out using IoT.

As such practically a couple of hospital exploration helped in understanding the challenging insights of cybersecurity over the medical domain from a deeper and better perspective. Besides, the information was gathered from the books, research articles, and other published online materials to answer our review questions. The second objective is to merge viewpoints to create new classification/Taxonomy, theoretical model or framework rather than is merely description or overview of the chosen research area. As these developed new conceptual frameworks and theory can contribute to the cybersecurity domain focusing on the medical field.

Third, the survey addresses the development in several medical-enabled systems and current encountered attacks and their possible solutions.

IV. INFORMATION FLOW IN THE MEDICAL SECTOR

In recent years, cybersecurity threats have greatly increased within the medical domain. Major insurance organizations such as Premera Blue Cross, Anthem, and Excellus have observed that malicious hackers have tried to hack millions of patient records in their systems [12]. Despite numerous benefits to health care services, Sametinger et al. [13] pointed

out that the availability of the Internet in medical devices allows hackers to obtain delicate patient information and infect Internet-enabled medical devices with malware, thus imperiling human lives. A model of the dataflow in the medical domain is depicted in Figure 1.

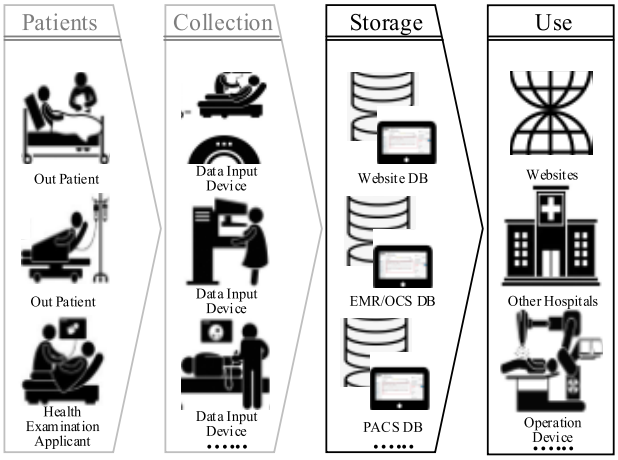

FIGURE 1. Dataflow model of the healthcare sector.

The information-sharing process is essential for the delivery of care, as the observations and actions of one healthcare provider often inform those of another. Therefore, the sensitive nature of medical information in the health domain means that the data must be secured. If data are destroyed or tampered with during information sharing, incorrect parameters may cause doctors to make incorrect decisions or perform inappropriate procedures. Therefore, it is important to analyze the dataflow in the medical field to determine cybersecurity vulnerabilities. To analyze the relationship between cybersecurity and personal health, this paper first analyzes how dataflow works in hospitals. The dataflow process model is composed of the following four phases:

- **Patient Registration:**The doctor usually acts according to the patient's principal claim to perform a preliminary exam. All the information the doctor obtained is input into the computer.
- **Data Collection:** Patients undergo laboratory tests such as X-rays and blood tests, and hospitals acquire data from these medical tests.
  - **Data Storage**: Doctors collect data from patients and input them into the specially devised database.
  - **Medical Data Application:** Doctors read the information stored in the medical database and perform the appropriate procedure on the patient. During this process, the data goes through four steps, encountering various devices and networks; thus, each step has the possibility of being attacked by hackers. Collecting the data is of high prominence because input data registration experiences several types of vulnerabilities and attacks [14]. The patient's input data registration requires hardware-based data collection and software-based data collection. As the software-based data collection requires low cost and high flexibility. On the other hand, hardware-based data collection is highly significant, but they are not flexible and have a high cost. The hardware-based devices experience more vulnerabilities particularly in the medical domain \as explained by Lin *et al.* [15]. These vulnerabilities need to be addressed prior to patient input data registration. However, this paper focused on data storage and data usage from a vulnerability and attack perspective, and input data registration will be addressed in the future.

V. VULNERABILITIES OF CYBERSECURITY IN MEDICAL DOMAIN

According to Figure 1, the medical data flow through four steps, flowing from patient to practical usage, and each step requires cybersecurity [16]–[18]. The analysis of this article is divided into two parts: information storage and IoT connection. From the first step in the collection of data, the potential risk of being attacked exists in consumer products for external medical devices, wearable devices, and internally IoT-enabled medical devices [19]. Such devices can sense the electrical, chemical, and thermal signals from the patient's body. As a result, these devices can directly sense and gather patient information through biomedical signals [20].

The process of signal transmission makes it relatively simple for data to be disrupted and stolen. Once the attacker hacks into the terminal device, the accuracy and reliability of data cannot be guaranteed. After data acquisition, the security of Internet access also needs to be emphasized. To realize the rapid transmission and sharing of different types of sensor signal information, the IoT has adopted a variety of network access technologies, such as mobile Internet and Wi-Fi.

The heterogeneity of the network access layer provides location management for terminals, which causes security problems, such as security authentication and access control, when communicating between networks. Due to the lack of a unified standard for cross-platform network security systems, the network is vulnerable to cross-heterogeneous network attacks [21]. Besides, the restrictions on access passwords for the database are not strictly for securing data.

The existing medical database system generally adopts user connection information and simple encryption to prevent illegal users from accessing database passwords. However, in C/S mode, the client still has a username and password to access the database, and these identifiers can be simply cracked or maliciously changed [22]. Hospital networks can be visited by individuals. Although the circulation and sharing of information are unimpeded for the user's convenience, a lack of authentication will lead to data risks. The classification of cybersecurity vulnerabilities in the medical domain is shown in Figure 2.

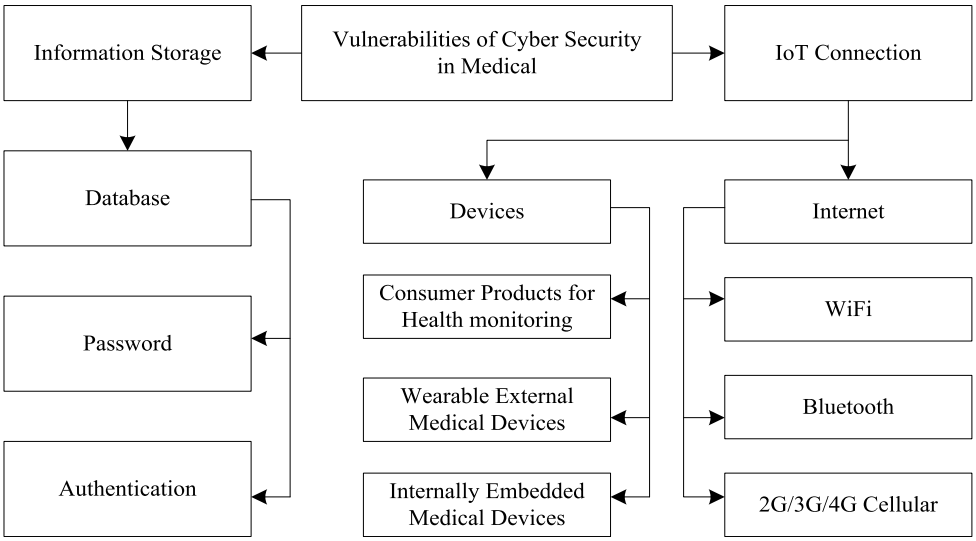

FIGURE 2. Main vulnerabilities of cybersecurity in the medical domain.

A. **Information Storage:** It causes the vulnerability in the medical domain when storing the data into database. As, information storage is principal component of fundamental distributed computation [126]. The information storage is quantified that can directly be used in the exploring the patient's information. However, information storage process is not fully safe due to storage of information on the cloud. As a result, patient's privacy and security are borderline. The hacker's easy access to IoT provides ample opportunity to crack the password and get access to medical information [127]. On the other hand, the weaker authentication methods for medical devices particularly sensor nodes are paramount security concerns [128].

B. **IoT Connection:**IoT connection brings several troublesome for nature and humans, but this troublesome can be worse if the medical commotion is involved especially when medical staff is carrying out routine activities and tasks for the patients' operations and other recovery processes [129]. IoT connections could be affected due to carriers such as Wi-Fi, Bluetooth, cellular technology and the Internet [130]. Most hospitals have been moved from local data storage to cloud storage. Besides, these hospitals believe that doing experiments with IoT devices not only helps to diagnose the patients efficiently, but also gather the information through those connected devices accurately. However, these connections are barely secure and extremely vulnerable to several forms of attacks [131]. These attacks find the vulnerabilities in the embedded devices, health-monitoring consumption products, wearable external and internal medical devices. As such vulnerabilities lead to desecration of doctor-patient confidentiality and privacy [132]. Exchange of delicate and sensitive information is pretty common in the IoT networks, as information exchange should be based on stable connections, but practically it is not possible. As a result, data leakage and loss of such significant information occur.

VI. CYBER ATTACK FOR DATAFLOW IN THE MEDICAL FIELD

Based on the analysis of medical dataflow and the vulnerabilities of cybersecurity in the medical domain systems, this section focuses on four main attacks that impact people's health: information collection attacks, database attacks, website attacks and operation devices attacks (see Figure 3).

A. INFORMATION COLLECTION

1) INFORMATION COLLECTION ATTACK

In this increasingly digital society, medical treatment is also becoming digital. When a patient wants to know what is wrong with his/her health, he/she must first check-in at the hospital to register personal information and then undergo a series of physical examinations. Because of the digitization of the hospital, the system will inevitably be attacked maliciously. The information collection attack, which is depicted in Figure 4, is a hybrid attack [118]–[120] that can be affected by two types of vulnerabilities: operating system vulnerability and OpenSSH vulnerability. There are other types of vulnerabilities, for example, eavesdropping an unencrypted communication, manipulating weak passwords, exploiting the OS of the hospital machines, but this survey only focuses on operating system vulnerability and OpenSSH vulnerability. The information collection attack affects medical devices, and Table 1 shows the attacks, vulnerabilities, effects, and solutions.

a: OPERATING SYSTEM VULNERABILITY

Attackers can perform malicious activities on equipment to gain complete control of the equipment. X-ray machines and

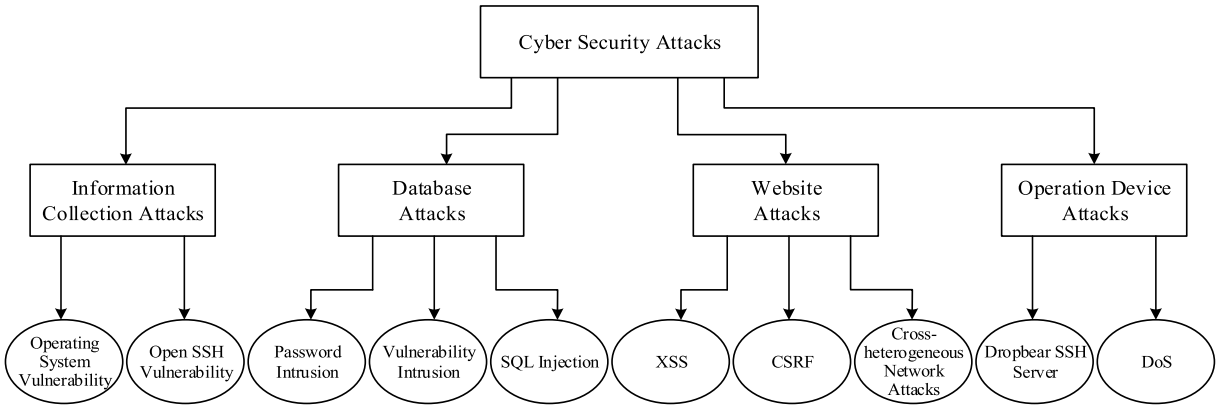

FIGURE 3. Classification of cyber security attacks.

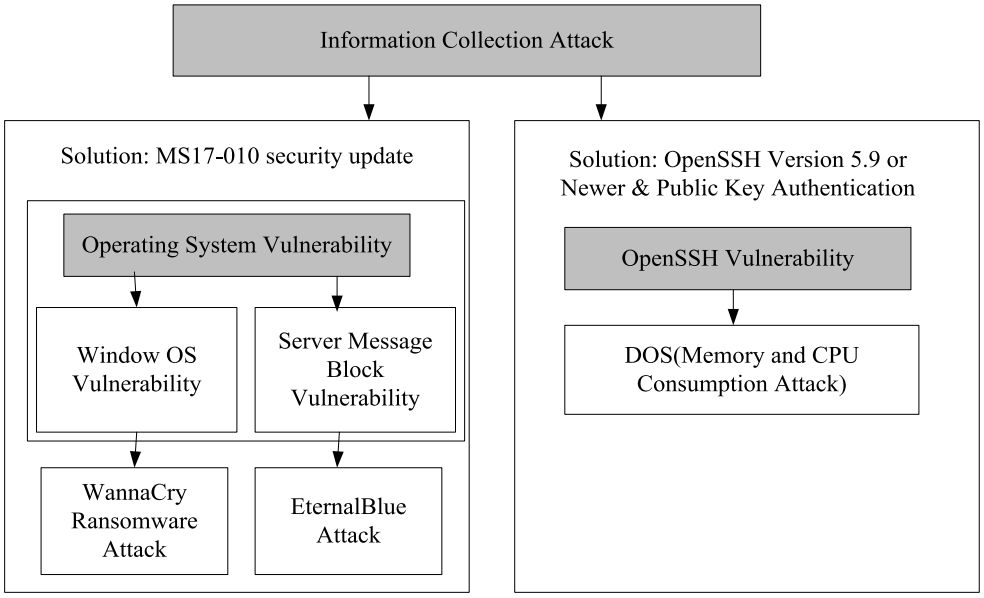

FIGURE 4. Information collection attacks.

TABLE 1. Information collection attack vulnerabilities, effects and solutions.

Attacks	Information Collection Attack		
	Vulnerability Types	Effect on Medical Equipment	Solutions
WannaCry Ransomware	Microsoft Windows OS	MRIs & CT Scans	The MS17-010 security update
EternalBlue	Server Message Block	Implanted Defibrillators	The MS17-010 security update
DOS (Memory & CPU Consumption	OPenSSH	Blood Pressure Monitors, X-ray Machines	-OpenSSH Version 5.9 or Newer -Public Key Authentication

MRI scanners are widely used devices that can be affected by vulnerabilities. For example, radiologists are worried about the results of the CT scans and MRIs due to Windows OS vulnerabilities. An incorrect X-ray report can cause doctors to arrive at an erroneous diagnosis, which may delay treatment. Hence, underlying algorithms working under Windows OS or other unsupported OSs pose a clear security attack risk. These OSs could be vulnerable to WannaCry ransomware attacks. Furthermore, implanted defibrillators (used to monitor the electrical movement of the patient's heart) can be attacked due to server message block vulnerability. In the presence of server message block vulnerability, the attacker launches the EternalBule attack, which executes arbitrary malicious code on the targeted computer. To avoid WannaCry ransomware and EternalBule attacks, these vulnerabilities should be patched. Thus, the MS17-010 security update provides a reasonable solution [121]–[125].

b: OpenSSH VULNERABILITY

The OpenSSH vulnerability is embedded in software applications' multitude and hardware devices. The OpenSSH vulnerability can affect an authentication process because the agent

is running on the client-side system (i.e., computer associated with medical devices) [23]. Hence, the agent running on the client system is connected to blood pressure or X-ray machines. These machines require an authentication process to function and thus require authentication keys. The authentication protocols are vulnerable and could disclose the keys. As a result, the system could be disrupted, which can affect blood pressure monitors, X-ray machines and other equipment; thus, attackers can obtain patient information. We cannot know the exact consequences of attackers obtaining this type of patient information.

2) SOLUTIONS FOR INFORMATION COLLECTION ATTACKS

To safeguard OpenSSH server keys, Ylonen [30] proposed ensuring that the cryptographic key is presented a minimum number of times in the allocated memory. The SSH protocol is expected to handle the authentication process efficiently. OpenSSH vulnerabilities are famous for the Man-in-the-Middle (MITM) attack presented by Chakaravarthi *et al.* [31]. Coonjah *et al.* [32] propose the solution to handle the information collection attack. In this approach, the end-to-end connection is established using a tunneling process based on an OpenSSH and OpenVPN cross-platform. The results demonstrate that OpenSSH utilizes a better link and provides improved transfer speed and time.

It is concluded that OpenSSH is a cost-effective solution. For the problem of an MS17-010 security breach, Qi et al. [33] proposed a homologous analysis approach based on the API sequence of ransomware. The idea involves using Clustalw algorithms to identify unknown software. The experiments in the paper show that this method, when applied for detecting the homology effect, works well, and end-users can distinguish ransomware clearly. However, the problem with this method is that, when using a sequence alignment algorithm, considerable computation time is needed and there is high time complexity. When the medical system is attacked by WannaCry due to the Windows OS vulnerability, a novel method proposed by Guo and Cheng [34] based on API hooking can be used to decrypt and free the damaged data. Thus, when WannaCry infects the host computer through Windows OS, the prototype system records the key information and then decrypts the files. The result in the article shows that the system can decrypt encrypted files. However, the system affects the performance of the operating system and process, which could affect medical system performance.

Zheng *et al.* [35] proposed adopting usable security and a decoupled design to develop a sustainable security solution for implantable medical devices to avoid MS17-010 security update vulnerabilities. The advantage of this design is that three critical trade-offs are presented and analyzed in the security design. However, this design is limited by insufficient experiments, and it has not been applied to real applications.

For OpenSSH vulnerabilities, Alsaadi *et al.* [36] introduced a penetration testing approach to protect the OpenSSH on Raspberry Pi 2. There are particular restrictions that require additional investigation. First, additional work is required to handle the production environment attack. Second, methods of handling the MITM attack on Raspberry Pi with RaspbianJessie using the pixel OS and NOOBS OS and NOOBS OS need to be investigated. A method of identifying and ranking optimal judgement was introduced by Qian & Bridges [37]. In the proposed method, features of malware are automatically extracted from the host logs. The study further demonstrates that the recognition information can be extracted effectively by this method. Future research will be considered in conjunction with other tests. However, this contribution has not led to functioning implementations that accelerate the manual analysis of a log and malware evaluation and provide precise pattern generation from host logs and dynamic analysis tools. Table 2 shows the possible solutions for information collection attacks.

TABLE 2. Possible solutions for information collection attacks.

Approaches	Vulnerabilities	
	Operating Systems	OpenSSH
Ylonen [30]		√
Chakaravarthi & Visuj[31]		√
Coonjah et al. [32]		√
Qi et al.[33]	√	
Guo & Chun-sheng [34]	√	
Guanglou et al. [35]	√	
Hesham et al. [36]		√
Qian & Bridges [37]	√	

B. DATABASE

1) DATABASE ATTACKS

In a digital society, information resource utilization and effective management are prerequisites for decision management and scientific research. In the medical area, databases are used to store electronic medical record information, medical equipment information, relative website data, etc. An attack on a database in the medical area will cause doctors to be unable to retrieve patient information, which may delay treatment.

This survey focuses on five major attacks that greatly affect the database functionality in the medical domain, which include: password intrusion [24], elevation of privilege [25], vulnerability intrusion [26], SQL injection [27] and backup theft, as depicted in Figure 5. The principles of the five main approaches are shown in Table 3:

2) SOLUTION FOR DATABASE ATTACKS

The biggest risk for password security is that the passwords chosen by users are easily guessed. As a result, [38] suggests that the most effective way to improve password security is to develop postfix and prefix password checkers. For the postfix checker, the system would run its password decode program at regular intervals to identify and cancel passwords that are

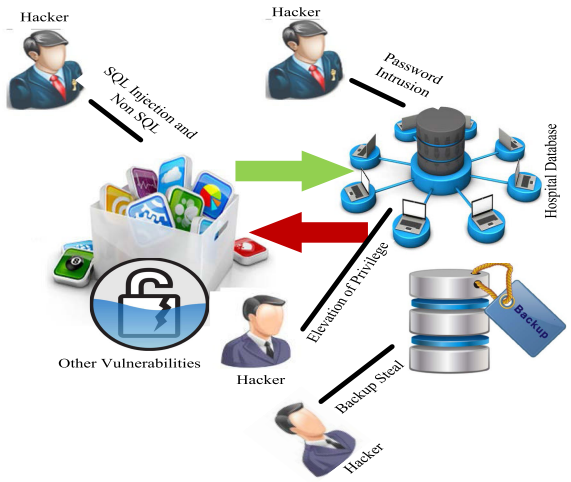

FIGURE 5. Hospital database attacks.

TABLE 3. Five main attack and their principles.

Attacks	Principles
Password intrusion	Hack into the database with the weak passwords of system administrators.
Vulnerability intrusion	Hackers use a number of harmful database security vulnerabilities to do something bad to the database.
Backups Steal	Attackers attack the physical media on which the backups are stored. As a result, backups are deleted and stolen and performed malicious actions not to be made undue.
Elevation of privilege	The attacker tricks Windows 2000 into rational way to demonstrate that the attacker has managerial privileges.
SQL injection	Attackers inject malicious SQL statements to deceive the application server to execute.

easily guessed and then inform the users. The prefix checker is a system program used to reject an inappropriate password after checking whether the user's choice of password is proper. However, these programs cost considerable resources and remain vulnerable for a long time, and a better-distributed intrusion detection system (IDS) is still needed.

Gould *et al.* [39] presented a Java Database Connectivity (JDBC) checker tool that checks the queries in Structured Query Language (SQL) statements that are dynamically generated in Java. This approach can detect vulnerabilities of SQL injection that are based on logical errors; however, it does not match the query because it examines only the syntax of the incorrect SQL statement. An SQL injection attack is a leading class of severe web application attack that can be grammatically correct, and it cannot return a database error.

Gould *et al.* [39] introduced a kernel intrusion detection vulnerability scanner that comprehensively evaluates a database kernel. The proposed approach detects the intrusion behaviors of attackers on time. Therefore, it proficiently prevents database intrusions that cause data outflow and malevolent tampering and improves database system security. Xun *et al.* [40] describe that the vulnerability scanner, which ensures database maintenance and automatic backup to a great extent, and it has a powerful network information audit function that monitors, records, and reproduces a comprehensive audit of the operation of network usage. However, the support capabilities of multiservice distributed database vulnerability scanners still need to be improved.

Based on SQL injection attacks injecting strings that are interpreted differently in different databases, Zhang *et al.* [41] proposes an effective solution for TransSQL. TransSQL automatically translates requirements such as SQL requests to a Lightweight Directory Access Protocol (LDAP). After querying the SQL database execution and LDAP, TransSQL examines the differences between the LDAP and SQL database to detect and prevent the response of the SQL injection attack. The experimental results demonstrate that TransSQL is a good solution to the SQL injection attack.

Ramesh *et al.* [42] suggested an approach for checking the value of each field input by examining the SQL injection syntax parsing the SQL injection attack. If effectively analyzed, then SQL injection was probably deliberate. If not, then the access was considered to be authentic and can be coordinated with the database. The authors documented an algorithm that is easy to comprehend and does not require any amendment of the source code. The approach used in this article prevents most kinds of SQL injections and helps safeguard websites from external attacks. However, the complexity of the algorithm is relatively high and thus it is time consuming to identify attacks.

A novel approach was proposed by Temeiza *et al.* [43]. Based on the hash function using the syntax-awareness and SHA-1 algorithm, a new practice for averting SQL injection in entrenched SQL queries is produced and syntax-awareness is applied to protect the stored processes from SQL injection to address several kinds of SQL injections. The approach was able to prevent SQL injection attacks in 209 attack experiments with 100% success. However, it is still in the experimental phase and needs to be enhanced.

Ping *et al.* [44] presented a prototype based on randomized instruction to prevent SQL injection attacks. SQL keywords are generated to add a random integer, and then random SQL statements are sent to the database proxy. The proxy passes the syntax and averts SQL injection attacks. Finally, the database agent sends random standard SQL statements to the database. Experimental results demonstrate that the proposed approach can effectively avert SQL injection attacks, and the processing cost is low. The protection system has a good impact and shows practical value for defending against SQL injection attacks. Nevertheless, the random secret key is defined by users and is easily forgotten or lost.

Wang *et al.* [45] proposed an intrusion-tolerant password-driven authentication method for multiple servers to share password verification data and never reconstruct them on user authentication. Conceding up to (t−1), these servers do

not permit a hacker to launch the offline dictionary attack. However, the system can still work despite the failure of some servers. The experimental results demonstrate that the proposed approach attains high-level security performance at a reasonable expense. However, it cannot prevent all online dictionary attacks and other attacks on passwords.

Desai and Gaikwad [46] implemented a hybrid intrusion detection structure for the identification of both external attacks and SQL injection on passwords. A signature-matching algorithm has also been introduced to detect internal attacks. Furthermore, a fuzzy genetic algorithm is used for external attack detection. This hybrid system is well-matched for offline and online environments. Experimental results prove that this method has better accuracy than some other systems. Furthermore, to enhance the system, the hybrid algorithm needs to be able to identify intrusions in a single system.

Mishra *et al.* [47] proposed an approach for the secure cloud environment by integrating efficient intrusion detection methods by focusing on two major problems in IDS: detection speed and an efficient detection mechanism. The approach aims to create parallelization and machine learning features with support of IDS to address security factors and provide security frameworks to validate how these methods can be used in the cloud computing environment. An initial analysis was conducted for the given approach, and the results were encouraging. However, this technique is at its starting point, and it is not entirely effective.

Appiah *et al.* [48] proposed a signature-based detection framework for SQL injection attack. In this proposed framework, pattern matching and the fingerprint method are integrated to differentiate valid SQL queries from malevolent queries. Furthermore, the proposed framework monitors SQL queries and compares them against a signature dataset of SQL injection attacks. The experimental results prove that the proposed approach is better for all sorts of SQLIA detection tasks, achieving lower false-positive rates. However, due to the difficulty identifying unknown attacks using detection systems, this system still needs to solve the issues of an anomaly-based system.

Ping [49] proposed an approach for second-order SQL injection detection attack based on instruction set randomization (ISR). Reliable SQL keywords, which are confined in the web applications, are randomized to create a new SQL ISR, and a proxy is added to detect whether the conventional SQL instruction consists of SQL keywords to identify the behavior of the attack. The results of experiments demonstrate that the system effectively detects SQL injection attacks. Meanwhile, it has a low processing cost. However, the system still needs to be improved in terms of resource consumption. Table 4 shows possible solutions for database attacks.

TABLE 4. Possible solutions for database attacks.

Solutions	Attacks		
	Password intrusion	Vulnerability intrusion	SQL injection
Chen et al.[38]	√		
Zhang et al.[39]		√	
Gould et al. [40]			√
Zhang et al.[41]			√
Ramesh et al. [42]			√
Temeiza et al. [43]			√
Chen et al.[44]			√
Wang et al.[45]	√		
Desai & Gaikwad[46]			√
Mishra et al.[47]		√	
Appiah et al. [48]			√
Chen[49]			√

C. WEBSITE

1) WEBSITE ATTACKS

Doctors log onto a website that is connected to the hospital database to obtain access to patient information and give prescriptions. Then, patients take medicine. If the website is attacked, doctors may obtain incorrect information sent by malicious attackers instead of the correct patient information. In another case, the website may crash, and the treatment will be delayed if the website is not accessible. There are several attacks on the websites e.g. injection, sensitive data exposure, broken authentication, broken access Control, XML external-entities, security misconfiguration insecure deserialization, insufficient logging & monitoring, components with Known attack, etc. As, most of these attacks are inherited from the two main attacks: cross-site request forgery (CSRF) and cross-site scripting (XSS). The main principles for those both attacks are shown in Table 5.

TABLE 5. Two main attack approaches and their principles.

Attacks	Principles
XSS	It is a kind of vulnerability especially available in the web applications. The XSS permits the malicious attackers to introduce the client-side scripts inserted into web pages that are observed by the users.
CSRF	CSRF is a kind of malevolent misuse of the websites where illegal commands are communicated from the client who is trusted by the web application. The attackers can use a reproducible links to execute the particular act on a targeted page. When a victim user is logged in embedded link on the page they can handle and contrivance the victim when opening the links.
Cross-heterogeneous Network Attacks	Heterogeneous networks are vulnerable to connection attacks because of the lack of improvement and protection of devices and protocols when interconnecting.

2) SOLUTIONS FOR WEBSITE ATTACKS IN THE MEDICAL DOMAIN

Several state-of-the-art solutions are provided to handle website attacks in the medical domain presented in Table 6.

TABLE 6. Possible solutions for website attacks.

Solutions	Attacks		
	XSS	CSRF	Cross-heterogeneous Network Attacks
Shar & Tan[50]	√		
Gundy & Chen[51]	√		
Shahriar & Zulkernine[52]	√		
Barhoom & Kohail[53]	√		
Parameshwaran et al.[54]	√		
Kombade & Meshram[55]		√	
Tatiana et al.[56]		√	
Xu et al.[57]	√		
Gupta & Gupta[58]	√		
Gupta & Gupta[59]	√		
Batarfi et al.[60]		√	
Yao & Wang [61]			√

Shar and Tan [50] developed a tool called safer XSS to detect and prevent server-side and client-side XSS attacks in real time. It uses five specific experiments to ensure the tool's effectiveness for detecting and addressing XSS attacks in real time. However, it cannot detect and prevent Document Object Model-based XSS, and it analyzes the server side. In addition, the tool targets only Java-based web applications.

Van Gundy and Chen [51] developed a web application framework to automatically use Noncespaces managed through a PHP template engine for static content. The article explains how to prevent the misuse of XSS vulnerabilities and helps clients distinguish between legitimate content formed by untrusted content and illegitimate web applications created by attackers. However, the framework does not have a self-protective architecture for JavaScript code when downloading content from remotely available websites.

Shahriar and Zulkernine [52] developed a prototype to automatically add boundaries and produce policies for Java Server Page (JSP) programs. The article evaluates the method with four JSP programs, and the approach can detect XSS attacks without amending client-driven entities. However, the proposed approach consumes considerable time in the policy examinations, and thus the attack detection capability is low.

A novel server-side approach was introduced for XSS attack detection by Barhoom and Kohail [53]. The proposed approach uses Extensible Markup Language (XML) schema definition (XSD) and XML to enforce persuasion. The proposed solution detects injected malicious JavaScript code that breaks the rules of an input schema. However, many requirements are needed from the server side, which reduces open network performance.

Parameshwaran *et al.* [54] introduced the DEXTERJS testing platform for the detection and validation of DOM-based XSS web vulnerabilities. DEXTERJS can identify vulnerabilities in an information web page. It identifies zero-day DOM XSS activities in its benchmark and tests them in the real world. However, the proposed approach cannot determine the client side's original functionality, which may contain malicious code.

Cross-Site Request Forgery (CSRF) vulnerabilities and protection mechanisms were introduced by Kombade and Meshram [55]. The approach compares several protection mechanisms to analyze the protection mechanism. This review helps create a strong and vigorous CSRF protection mechanism. However, it does not apply specific experiments to verify the effectiveness of defensive approaches. Therefore, full protection is not available for CSRF, and these approaches should be improved. Malicious websites force the browser of the user to direct unauthorized requests to legitimate sites due to the HTTP protocol's stateless nature. Therefore, [56] shows some technology that can detect CSRF in some web applications. It proposes an approach in which users can install a simple extension to obtain notifications about probable CSRF vulnerabilities. However, the extension does not have a method for defending against CSRF because it only notifies users of the existence of CSRF. Scripting language (mostly JavaScript) applications are widely used to enhance user experience, but they make XSS a serious problem. Xu *et al.* [57] proposed an XSS defensive schema on behavior certification that actively fortifies the user against XSS attacks. In addition, it can support different technologies on the website such as PHP and ASP. However, its capability is limited because it is based on the expected behavior of the website or browser and produces false negative alerts.

Gupta and Gupta [58] proposed context-sensitive purification based on an XSS protection structure in the cloud computing environment. This method can be used to detect every possible web application so that it can accelerate the use of purifiers on the illegitimated variables on web applications. The method, which has been tested in the real world, has a high degree of true positives and a low degree of false negatives. It is limited in that the method does not provide support to the web application's online social network (OSN). To prevent the virtual machine from XSS attack in the cloud environment, Gupta and Gupta [59] proposed an improved XSS protection procedure for cloud platforms. The approach does not need the web application's browser source code and does not modify the web browser. Additionally, it has a low false-positive rate and false negative rate. However, it does not support the OSN.

Batarfi *et al.* [60] introduced an approach for preventing and detecting the reflected CSRF.

The approach further demonstrates that the solution is effective for attack prevention. The approach can prevent invalid sessions and end them quickly. However, the method can detect only the reflected CSRF, and it does not protect a login CSRF attack. Yao *et al.* [61] introduced the across heterogeneous authentication model and designed the authentication process details in different circumstances.

D. OPERATION DEVICES

1) OPERATION DEVICE ATTACKS

The development of technology will inevitably lead to more accurate treatment, i.e., the patient's treatment will depend more on the medical equipment. Additionally, because most equipment is connected to the Internet, doctors can monitor patients promptly. Accordingly, it is unavoidable that these operation devices will be attacked through the Internet, which threatens the safety of patients. For example, the American Hospital Association (AHA) found that interrupted communication between pacemakers could be fatal [29]. The vulnerability of the Dropbear SSH server and the remote code execution and DOS are reasons for the operation device attacks depicted in Figure 6.

FIGURE 6. DoS and Dropbear SSH server attacks on operation devices.

a: DROPBEAR SSH SERVER

The Dropbear SSH server is the most common vulnerability that contributes to operation device attacks. Sensitive information can be leaked so that attackers can activate malevolent code on the database, which will harm people. For example, AF24 is a radio that communicates with medical equipment that can be easily attacked such as pacemakers. Heart pacemakers are essential for people who have suffered heart attacks. If pacemakers are maliciously operated by attackers, the patients are likely to die.

b: DoS AND REMOTE CODE EXECUTION

Second, the vulnerability of DoS and remote code execution can allow attackers to change information in the system, such as the medication dosages of patients. For example, there is a security vulnerability that hackers can use to send false messages to users of insulin pumps, which may cause people with diabetes to inject a potentially fatal dose of insulin. Table 7 shows main attack approaches and their principles.

TABLE 7. Main attack approaches and their principles.

Attacks	Principles
Dropbear SSH Server	The attackers execute malicious code to leak sensitive information.
DOS and remote code execution	It can change the dosage of the medicine to the patients.
Image Processing Equipment	This equipment analyzes, enhances and displays of images captured via ultrasound, x-ray, nuclear medicine, MRI and optical imaging technologies.

2) SOLUTIONS FOR OPERATION DEVICE ATTACKS

Operation devices are greatly affected due to DoS attacks and Dropbear SSH server vulnerabilities shown in Table 8.

TABLE 8. Possible solutions for operation device attacks.

Solutions	Attacks	
	Dropbear SSH Server	DOS and remote code execution
Schuster & Holz [62]	√	
Mando [63]	√	
Gen & Ma[64]		√
Toyoda et al.[65]		√
Aiello et al.[66]		√
Agarwal et al.[67]		√
Naik et al.[68]		√
Li & Dey[69]		√
Aleroud & Alsmadi [70]		√
Zhu[71]		√

Schuster and Holz [62] defined backdoors in software systems. To reduce this kind of security problem, approaches are proposed to eliminate backdoors. Among them, Dropbear SSH is analyzed. Through the experiment, it is determined that deciders and handlers in the SSH server can be identified.

Alberca [63] analyzed software that can be seen as an external attacker; Dropbear SSH is one such software. The attacks are divided into three types. The first one denies the server by running a DoS, the second one causes a timing error that prevents user commands from running, and the third, when run on concurrency channels, can be used to execute remote code that contributes to the attack.

Li and Ma [64] suggested that DoS attacks can damage the 4-way handshake method and proposed a solution that can defend against DoS attacks. An encryption algorithm is used to change the 4-way handshake method and minimize the standard requirements. The proposed improvements are much better than the existing solutions in terms of compatibility and efficiency. Toyoda et al. [65] found that a DoS attack occurs if the correspondent node must verify all binding update requests. A solution is proposed that results in two challenges in a transaction to reduce the effect. The two

challenges eliminate the malicious node; however, the second challenge is harder than the first challenge. Through these challenges, the impersonation probability is decreased. Moreover, excluding the malicious nodes efficiently decreases the risk of DoS attack. Aiello *et al.* [66] proposed an algorithm that can categorize traffic to detect DoS attacks. It should find the equation that describes the parameters of network traffic, and then it can solve the problem of detecting malicious attacks.

Agarwal *et al.* [67] introduced an intrusion detection system based on machine learning (ML) to detect a DoS attack using a Wi-Fi network. This paper proposed many ML algorithms for detection. Additionally, machine learning based on IDS does not need protocol modifications and has high precision and recall. To improve the firewall, which is included in the Windows OS to avoid DoS attacks, Naik *et al.* [68] proposed an intelligent Windows fuzzy firewall called FR-Win Firewall. The design, implementation and testing are successful because of fuzzy reasoning components that are related to DoS attacks. The firewall with fuzzy intelligence is a good choice for avoiding the control of DoS attacks.

Li *et al.* [69] addressed a DoS attack based on SINR by designing a Markov game framework to solve the Bellman equations. A modified Nash Q-learning (MNQ) algorithm is used to obtain the solutions. However, while this method can solve the problem, there is still a long way to go to ensure the security of wireless networks. Aleroud and Alsmadi [70] proposed a technology that can control a DoS attack by using software-defined networking (SDN). SDN takes advantage of the similarities in the context of prevailing attack patterns to detect DoS attacks in OpenFlow infrastructures. The paper's solution can avoid attacks on SDN; however, it may introduce new attacks such as DOS attacks. Thilak and Amuthan [71] introduced a solution that can prevent a DoS attack under the VANET environment. Additionally, it summarizes the advantages and disadvantages of methods for preventing DoS attacks. Among these methods, although it can ensure the safety of delivering messages, the processor in OBU is over headed. The complete detail of vulnerabilities and their effects that lead to different types of attacks and possible solutions are shown in Table 16. The possible solutions also are evaluated based on several features such as attack reduction, high ransomware detection, low test error, reasonable expense and stability improvement. Furthermore, the limitation of those solutions for each attack are shown in Table 17.

VII. MEDICAL ARCHITECTURES OF CYBERSECURITY

A. INTELLIGENT MEDICAL SYSTEM

This system involves medical information and the knowledge-based and hybrid components depicted in Figure 7. The system is discussed from an IoT perspective.

The construction of an Intelligent Medical System (IMS) architecture with support of ML is designed in Figure 8. This architecture can help with medical activities and consists of following components.

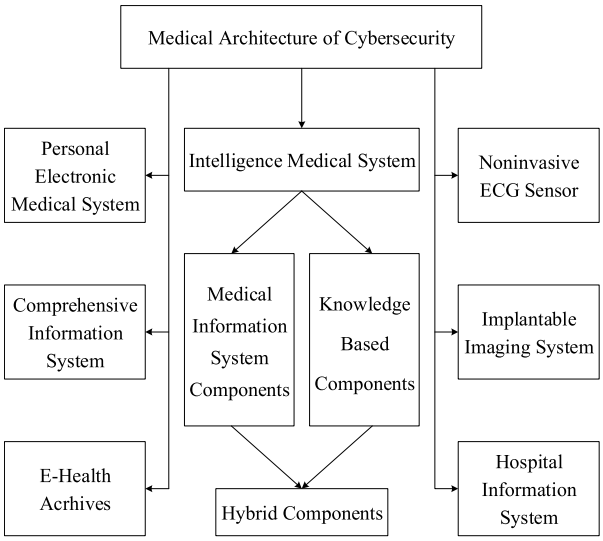

FIGURE 7. Categorization of intelligent medical system.

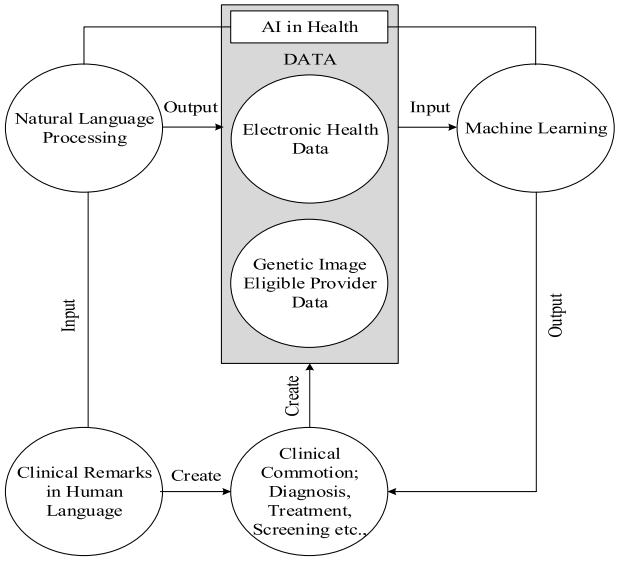

FIGURE 8. Intelligent medical system.

- **Natural Language Processing (NLP):** It is a subfield of several domains such as computer science, linguistics, artificial intelligence and information engineering. It provides the interactions between human and computers particularly how to write the codes for the computers to analyze and process large amounts of data. It sends data as input to clinical remarks for human language component. Similarly, it receives data from AI and forwards to storage repository.
- **Clinical Remarks in Human Language:** It describes and analyzes the data based on received information from NLP. Subsequently it generates the remarks for prescription to next component.
- **Clinical Commotion, Diagnosis, Treatment, screening etc.:**Based on the received remarks, prescription for the patient is suggested and data is sent and stored to genetic image eligible provider.

- **Machine Learning:** It provides the capability to automatically get the electronic health data and infers the results from the data and forwards for different actions (e.g., clinical tumult, diagnosis, treatment, screening etc.).
- **Electronic Health Data**: This data can be used as input raw data and forwarded for action to be performed by machine learning.
- **Genetic Image Eligible Provider Data**: This kind of data is returned to the physician, doctor and clinical staff who have capability to take clinical decision based on the **genetic** findings.

The IMS IoT framework presented by Hu [72] provides services to the public for storing and sharing data, and it has the ability to analyze data for deep understanding. Meanwhile, to address the barrier between doctors and patients, the cooperation between hospitals and the match of patients and equipment, IMSs must improve the ability of remote information interaction using advanced information technology. Hybrid and knowledge-based components help improve the efficiency of the system, while medical components perform the task intelligently. Zang and Yu [73] define the process of International Automotive Task Force (IATF), including the construction of an information security system and its software and hardware components. At the same time, the Defense-in-Depth approach provides multi-level and deep security processes to protect user information and the information system. IATF gives a detailed description of the technical measures for its safety requirements and the corresponding control selection. The objective of these four focal areas—enclave boundaries, the local computing environment, supporting infrastructures and network infrastructures— is to empower individuals to comprehend different characteristics of network security, to systematically evaluate the security information system needs and to consider proper security protection mechanisms. However, this kind of architecture also has weaknesses. It reveals a shortage of connections, which means that IATF focuses on reducing the complexity of technology but ignores the connection between users and systems.

Under the M2M architecture, Sang [74] divided the ''things'' of the Internet into three parts: a perceptual layer, a transportation layer and an application layer. Then, two architectures are combined to include the intelligent perceptual layer, the transportation layer, the data integration layer, the cloud computing layer and the application layer. M2M provides sufficient data assurance and convenient service; however, there are no standard connection equipment platforms for all users in different areas due to the immaturity of the technology.

Xu [75] introduced the National Health Information Framework (NHIF) architecture at the country level to collect, store and release health information. This architecture benefits users by simplifying and systemizing complex information and optimizing the management and operating system to improve information quality and use efficiency. However, the connection between various departments and areas is too hard to control and manage. Pi and Huang [76] proposed processing information in a Hadoop cluster that implements a cloud computing function and storing the analysis results in the database. The relevant medical staff can access the patient's information at any time and place and adjust and update the patient's medical plan.

Patients can also log into the system to access their health status information. Hadoop builds a remote but convenient network between hospitals and patients. However, due to the specific authority in different departments, doctors cannot obtain immediate and comprehensive information when an emergency occurs. The possible proposed solutions for intelligent medical system are shown in Table 9.

TABLE 9. Intelligent medical system.

Parameters	Approaches			
	Zang & Yu [73]	Sang [74]	Xu [75]	Pi & Huang[76]
Large Scale	√		√	
Informational Confidentiality		√		√
Low cost		√		
System generality				√
Transmission Efficiency			√	√

B. COMPREHENSIVE INFORMATION SYSTEM

In hospitals, the process of addressing the patients' problems is related to the lives of the patients, especially when emergencies arise. Wang and Zhang [77] analyze a convenient and open online environment that is the foundation of the construction of hospitals. To ensure the smooth operation of hospitals and the following dynamic improvements in medical information, hospitals can take the responsibility to guarantee the protection of patient information and the transmission of big data.

For the policy, protection, detection and response (PPDR) architecture, Saurabh *et al.*[78] described the combination of protection, detection, reaction and restoration. This architecture views the protection of information security as the basis, which is also regarded as the process of the activity. After an invasion, the system takes corresponding methods to restore the system to its normal state, which is easy and convenient for providing a comprehensive information guarantee. However, it cannot be applied in every system. Through the rational choice of emergency response measures explained in Saurabh *et al.* [78], the maximum benefits can be obtained at a minimal cost, thus reducing or even eliminating the negative effects of adverse events, which is helpful for achieving the network security objectives of the information organization. However, the cost and the final benefits are hard to predict.

Ali *et al.* [79] introduced the network firewall architecture, which has an independent management port, a separate business port, a security isolation visual system and accurate

location recognition. However, this architecture cannot address unknown problems or eliminate the origin of threats. Wang and Zha [81] designed a system that uses STM32 as the control core to collect a remote patient's ECG and blood oxygen; the collected data are sent to a mobile Android terminal and a PC via the ZigBee wireless module for dynamic display, and the doctor determines a scientific diagnosis according to the display chart and the data. The most fundamental advantage is that ZigBee is used to send information to the primary computer and mobile terminal so that the corresponding indicators of the patient can be monitored in real time; however, it cannot assure information security during transmission. Table 10 shows the possible solutions for the comprehensive information system.

TABLE 10. Comprehensive information system.

Parameters	Approaches			
	Saurabh [78]	Salman et al.[79]	Pan [79]	Wang & Zha [81]
Large Scale		√		√
Informational Confidentiality	√		√	
Low cost		√		
System Generality				
Transmission Efficiency				√

C. HOSPITAL INFORMATION SYSTEM

The focus of a healthcare information system (HIS) in terms of security protection is the control of access, encryption, and authentication. The main task of access control, which is explained in Zhang *et al.* [82] is to ensure that network resources are not illegally used and illegally occupied. The basic idea of encryption technology is to ensure the security and reliability of the network by encrypting network data. The hospital authentication system can authenticate the username, password, login terminal and login time of the operator. Through the intranet management software, hospitals can realize the use of terminals, reduce the hidden dangers of human errors, and prevent these errors from occurring in a timely manner.

The architecture of PPDR was divided by Han and Wu [83] into four relatively simple parts: policy, protection, detection and response introduced. The main methods are closing the connection port, interrupting the connection and interrupting the service. Studying a variety of intrusion response techniques is one direction of future development. The main benefits of PPDR are to broaden the range of protection and reduce the detection and response time. However, inner changes, such as changes in employers and member quality, are ignored.

In the Web-EMR architecture, the information security platform is the fundamental solution for protecting the safety of Web-EMR sources, which consist of the public security supporting platform and the application security supporting platform. Under this architecture, the system, as described in Zhou [84], can connect every part of the departments and provide remote communication between various hospitals. However, the rates and content of transmission cannot be assured. The main job of disaster recovery architecture is to minimize the cost of cybersecurity disasters; Xu [85] divided the disaster recovery system into two parts, i.e., data protection and application protection, which are helpful for identifying disasters in a timely manner and beginning data migration. However, it is relatively difficult to keep the system operating continuously. Once one part breaks, the system cannot deliver the data immediately. Table 11 shows the possible solutions for the hospital information system.

TABLE 11. Hospital information system.

Parameters	Approaches			
	Han & Wu [83]	Zhou [84]	Xu [85]	Wu & Wang[86]
Large Scale	√			
Informational confidentiality		√	√	√
Low cost				
System generality		√		√
Transmission Efficiency	√	√	√	√

Wu and Wang [86] introduced HL7, which defines the standard format for medical data exchange, the time for data exchange, and the handling of erroneous events. The purpose is to develop standards for various medical information systems such as clinical, insurance, management, administration and inspection systems and to reduce medical care. The cost of health information system interconnection increases the degree of information sharing between systems. However, the requirements of HL7 on the equipment of hospitals are so strict that they prevent some developing countries from progressing.

D. NONINVASIVE ECG SENSORS

Electrocardiography is an objective indicator of the occurrence, spread and recovery of heart excitement. The relationships between ECG waveforms and the myocardial action potentials and patterns of action potentials traced by single cardiomyocytes are significantly different from the electrocardiogram of each cardiac cycle because the cardiomyocyte action potential is the change of the membrane potential of a single cell and the electrocardiogram is the instantaneous change of the potential of the functional syncytium composed of many cardiomyocytes, which changes with the propagation and recovery process of the heart, which is the function of the syncytium. Not only is the action potentially different from that of a single cardiomyocyte but the waveforms of multiple leads are also different. For the cyber-physical med-

ical systems mentioned by Hu [72], the rapid development of embedded computing and sensing technology has led to the emergence of intelligent biomedical devices, such as automatic infusion pumps, implantable imaging systems and noninvasive ECG sensors. These architectures are usually implanted in the human body and interact through induction and drive. These network-physical health systems are increasingly being used for critical tasks such as postoperative care, drug delivery and chemotherapy.

The analog front-end mentioned by Banerjee *et al.* [87] has a large impact on system performance. The enhanced architecture described below uses high-precision, high-speed analog-to-digital converters (ADCs) to provide high fidelity over a wide frequency range. Rather than using capacitive coupling, the AEF is driven by a digital-to-analog converter (DAC), allowing the AFE to recover quickly from defibrillation or RF interference. The digitized pacing signal allows for the analysis of pacing data, reducing false pacing indications and detecting defects in pacemakers or connected parts. However, we must also consider that the enhancement system requires expensive components and consumes considerable power. In contrast, the simplified AFE is inexpensive, the battery life is long, and the other characteristics are very small. These devices can be used immediately during a heart attack, releasing a high-energy electrical pulse to the chest, pacing the heart and returning it to a normal heart rate. If the wrong timing is used, then the pulse shock can be life-threatening. Therefore, the ECG must be able to prevent this accident. The automated external defibrillator mentioned by Barbosa *et al.* generally has only one lead and its electrodes are used to both release high-voltage pulses and to collect ECG signals.

The winding nanotechnology mentioned by Lin and Huang [88], used to make multifunction devices, can be directly integrated into existing fluid structures. The efficiency of the wound magnetic sensor is augmented for high sensitivity to weaken the magnetic fields. The winding tube is effectively applied as a fluid channel, and an embedded magnetic sensor device provides the significant function for detecting and responding to the magnetic field.

The deep sensor architecture mentioned by Mönch *et al.* [90] enables collection of the most relevant data in an environment, i.e., behavioral data about every user, process, and network connection across the infrastructure. The sensor's unique technology runs continuously in the user space, making it impossible to crash the system while providing full visibility to all activities at the kernel level. The highly reliable sensor sends data to the behavioral intelligence engine—even when off-network and offline. Table 10 shows the possible solutions for the Noninvasive ECG sensors.

TABLE 12. Noninvasive ECG sensors.

Parameters	Approaches				
	Banerjee et al. [72]	Lin & Huang [87]	Barbosa et al. [88]	Monch et al. [89]	Karnaushenko et al. [90]
Large Scale		√		√	
Informational confidentiality		√		√	√
Low cost		√			√
System generality	√			√	
Transmission Efficiency	√	√	√	√	√

E. IMPLANTABLE IMAGING SYSTEM

The implantable imaging system involves the technology and procedure of acquiring core tissue images of the human body in a noninvasive way for medical research. Mönch *et al.* [90] examined two relatively autonomous systems: medical image processing and the medical imaging system. Medical image processing refers to the image formation process, including the study of imaging equipment, imaging mechanisms, and imaging system investigation; the medical image system refers to the supplementary image processes that have already been obtained, and the goal is to make images that are not sufficiently clear. Refurbishment either highlights the specific image information features or classifies the pattern of the image. As a key task, cyber-physical medical systems should be verified before deployment [93] to meet the safety requirements of dangerous operations. Yansheng *et al.* [92] introduced a model-based engineering approach to analyze CPMS security. However, the close interaction between CPMS and the human body is specified by propagation delay, nonlinearity, nontrivial interaction, and spatiotemporal effects, which aggravates the complexity of the model and analysis.

The community gold standard framework enables organizations to respond to a variety of challenges in Dongbo et al. [94]. The framework cannot provide the single method, such as prescribing a prescription, for selecting and implementing security measures. Instead, it logically understands the system, its management capabilities and the protection and detection capabilities of the organization's security through collaborative work. In a picture archiving and communication system [95], high-performance server, network and storage devices constitute a hardware support platform, and a large-scale relational database is used as a storage and management tool for data and images. The core of the collection, transmission, storage, and diagnosis of medical images is image acquisition, transmission, and storage management. The integrated application system that integrates image diagnosis queries and report management, comprehensive information management, etc., is the main component that stores the various medical images generated daily by the hospital imaging department. When authorized, it can be used quickly and add auxiliary diagnostic management functions, as discussed by Dai *et al.* [94]. Table 13 shows the possible solutions for the implantable image system.

F. PERSONAL ELECTRONIC MEDICAL SYSTEM

Wenfeng and Fengmin [96] introduced the architecture and technology of personal electronic health care systems based

TABLE 13. Implantable image system.

Parameters	Approaches		
	Shi & Liu [93]	Xiao et al.[94]	Dai et al.[95]
Large Scale			√
Informational Confidentiality	√	√	√
Low cost		√	
System Generality	√	√	
Transmission Efficiency	√	√	√

on a WCDMA network, mobile terminal and wireless sensor system. It divides the system into four parts: the wireless health care sensor system (WHSS), the mobile terminal network, the mobile communication network and HIS.

The 3G cellular network is discussed in Mei and Nature [97]. The proposed approach focuses on code division multiple access (CDMA) multiplexing methods. The three best characteristics of the WCDMA are as follows. First, it supports multiplexed modes including FDD and TDD; thus, it has good compatibility and interoperability with GSM networks. Second, it supports high-speed transmission so that it can support multimedia business. In addition, WCDMA uses an adaptive antenna and small area technology, which greatly improves the capacity of the system. A wireless healthcare sensor system (WHSS) is a wireless sensor system integrated with the Application of Search Engine introduced by Zhirong [98] that spans the entire body and includes various medical sensors, wireless self-organizing networks and SINK nodes. Because the wireless medical sensor devices in the software system are structured based on the memory, CPU capacity, power and other limitations, it must use a dedicated OS, protocol stack and related MESH routing protocols. Therefore, the compatibility is not good, and the cost is high.

Yan [99] introduced a health information system that is a typical enterprise information system. It provides a medical information system with a send and receive agent, it is responsible for processing all kinds of packets, and it has a mobile terminal data processing program for communication to ensure the compatibility and scalability of the system structure. For better compatibility, we can perform further processing on the software architecture: the session bean, entity bean and message-driven beans on the application server interoperability effectively reduce the complexity of the system platform and maintenance costs. Wenhua and Pengpeng [101] introduced an N-tier architecture that adopts a multilayer architecture design and different security strategies for different levels to ensure the multilevel security of the system. Regarding security, this system has taken strict measures in architecture, hardware construction and software design, management, training and other aspects to fully guarantee the system in terms of data storage, access, high-security network transmission, etc. To prevent inevitable threats, it also considers countermeasures in terms of the safety log and safety emergency plan to ensure that the problems can be solved in a timely manner. Table 14 shows the possible solutions for the personal electronic health medical system.

TABLE 14. Personal electronic health medical system.

Parameters	Systems				
	Xie & Zhang[97]	Chang [98]	Ye [99]]	Gao et al.[101]	Xie & Zhang [97]
Large scale			√		√
Informational Confidentiality		√		√	√
Low cost			√		
System generality	√				√
Transmission efficiency					√

G. E-HEALTH ARCHIVES

The building of the public health system is most significant for the national medical improvement. With computer-enabled technology, the regional collaborative medical e-health system has been developed that provides the collection of medical documents. The proposed E-health archives are shown in Table 15.

TABLE 15. E-Health archives.

Parameters	Systems					
	Gao [101]	Chang [102]	Ren [103]	Zeng et al. [104]	Lu [105]	Li et al. [106]
Large scale			√		√	√
Informational confidentiality		√		√	√	√
Low cost			√		√	
System generality					√	
Transmission efficiency					√	

Wenhua and Pengpeng [101] established an electronic health records system that helps people discover threats to their health and understand their condition. It can decrease the cost of medical care, increase the efficiency and quality of medical services, improve the supply situation of medical sanitation service, and promote the integrated development of medical treatment and public sanitation services.

Chin [102] introduced the idea that an SOA architecture can strengthen the drawbacks of the present system, such as time-lapse information distribution and weak privacy protection. The SOA framework is a service-oriented architecture type of component model. It is based on the object-oriented model. One typical instance of it is common object request broker architecture (CORBA), which can gather all the different parts of the application program through the interfaces and contracts between them. These parts are called 'services', and they can be independent of OS, hardware device, and programming language. This definition of the interface is called 'loose coupling'. Loose coupling has two main characteristics: flexibility and security.

Electronic Health Archive (EHA) is a structure for electronic health records described by chin [102]. Through the unified authentication and authorization of the regional platform with the registration service, the subscriber can complete the sharing and business collaboration of the medical and health machine construction information system. It is an interconnected network of health and health services that uses unified standards to effectively integrate medical and health business application systems.

Wenying *et al.* [104] introduced enterprise service bus (ESB), which is the infrastructure for enterprise-level SOA. Through security, stable messaging, message routing, protocol and data format conversion, it provides a simple, efficient and secure middleware platform for regional collaborative medical services. Its event-driven, highly decentralized and centrally managed features make the regional collaborative medical information platform highly reusable and flexible.

IHE architecture aims to promote the sharing of medical information and to optimize the medical process by defining DICOM, HL7 or other implementation methods of existing standards discussed by Wenying *et al.* [104]. The revs.5 version of the Integration Healthcare Enterprise (IHE) technical framework defines 13 integration models, and each model can allow users to accurately describe the support for IHE without involving roles and transaction details, rather than simply declaring that they are compatible with IHE.

International Classification of Functioning (ICF) is the identification and measurement standard for function and disability, and it is a tool for quantifying the function discussed by Xudong [105]. It provides one or more defined qualifiers that can, for example, indicate the degree of health or the severity of the problem. Therefore, it can ensure the safety of the information, but the efficiency of data transmission still needs to be improved. Evaluation of the cyber security medical systems, and architectures is shown in Table 18. This evaluation is made based on state-of-the-art characteristics such as large scale, information confidentiality, low cost, system generality and transmission efficiency.

VIII. DISCUSSION AND RECOMMENDATION

Cybersecurity can be influenced by information collection attacks, database attacks, website attacks, and operation device attacks. Furthermore, cybersecurity can be used by hackers for nefarious purposes such as forgery, data modification, data breach, etc. [135]. Consequently, patient' privacy is greatly deteriorated, which negatively affect the treatment and medication processes and can hurt the patient's health. An information collection attack is influenced by the MS17-010 security update and OpenSSH vulnerabilities. The MS17-010 security update is the most common vulnerability that allows attackers to take complete control of the equipment. Several methods were identified as addressing this vulnerability [136]. First, the API sequence of ransomware can be used. Second, an alternative solution can be developed to use the decoupled design and usable security. This method can reduce attacks and has a high ransomware detection capability. However, it still has some drawbacks due to inheriting the poor system performance. The second vulnerability, OpenSSH, can allow attackers to completely gain the access to the patients' body. To solve this problem, the cryptographic key is suggested to reduce the attack success rate. Additionally, the RSA algorithm can also be used [137]. However, there is still a long way to go to reduce the need for resources and improve the data transfer rate.

For a healthcare system, the website is important because it is widely used in different areas, and both people and doctors benefit from it. The safety of a website is of vital importance when the patient's information is transmitted on the Internet or transmitted between hospitals. Thus, it is useful to address website attacks. However, medical-driven websites can also easily be attacked. Most of the solutions to website attacks have been identified and can detect correlated attack types promptly. The website attacks are mainly cases of session hijacking. The two main attacks (CSRF and XSS) harm the performance of the websites. To solve the problem of XSS attacks, most mentioned solutions can detect potential attacks and reduce the possibility of being attacked. Some of the proposed solutions use mathematical methods to improve efficiency. Meanwhile, several solutions consume high amounts of system resources, and their performance is low. Also, most of the solutions to XSS attacks are applied to script languages or programming languages; thus, their applicability is not highly acceptable in medical domain. Besides, several solutions have been proposed for CSRF attack, as some of them have limitations and just solve one kind of attack so that it cannot be applied to all cases. As a result, the system remains in danger because it is likely to be attacked by another factor. On the other hand, some of the approaches can cause high resource consumption so that the system's performance is compromised and efficiency is degraded.

The database is used to store all medical information for both patients and hospitals. Making the most of databases in the medical area is of vital importance because it can help ensure that medical treatment is scientific and systematic. Regarding database attacks, there are three main potential attacking threats: password intrusion, vulnerability intrusion, and SQL injection. Among these threats, the most common and dangerous one is SQL injection. Discoveries are required to make databases much safer. It is suggested that people should not rely on existing outcomes and solutions. Operation device attacks are mainly caused by the Dropbear SSH server and DoS. The Dropbear SSH server is the most common vulnerability among them. Attackers execute malicious code to change the message in the operation device to cause harm to a patient's body.

In future research directions, the potential and viable solutions to CSRF attacks should be considered to secure the operation devices. As just awareness of this attack is not enough for people to prevent the medical system from being attacked. Furthermore, the solutions should be focused on improving the performance efficiency because most examinations and operations can highly be depreciated. The

TABLE 16. Attacks, vulnerabilities and possible solutions.

Attacks	Vulnerabilities	Solutions	Attack Reduction	High Ransomware Detection	Low Test Error	Reasonable Expense	Stability Improvement
Information Collection	OpenSSH Vulnerability	Ylonen [30]	√				
		Chakaravarthi & Visuj[31]	√				
		Coonjah et al. [32]	√				
		Hesham et al. [36]	√		√		√
	Operating Systems Vulnerability	Qi et al. [33]		√			
		Guo & Chun-sheng [34]	√				
		Guanglou et al. [35]	√				
		Qian & Bridges [37]		√	√		√
Database	Password Intrusion Vulnerability	Chen et al.[38]	√	√			
	Intrusion Vulnerability	Zhang et al.[39]	√	√			√
		Gould et al. [40]	√				√
		Zhang et al.[41]		√		√	
	SQL Injection Vulnerability	Ramesh et al. [42]		√			
		Temeiza et al. [43]		√			
		Chen et al.[44]	√				
		Wang et al.[45]	√			√	
		Desai & Gaikwad[46]	√		√		
		Mishra et al.[47]		√			
		Appiah et al. [48]		√	√		
		Chen[49]		√		√	
Website	XSS	Shar & Tan[50]	√	√			
		Gundy & Chen[51]	√	√			
		Shahriar & Zulkernine[52]		√	√		
		Barhoom & Kohail[53]		√		√	
		Parameshwaran et al.[54]		√	√		
		Kombade & Meshram[55]		√			√
		Tatiana et al.[56]			√	√	√
		Xu et al.[57]		√	√		√
	CSRF	Gupta & Gupta[58]					√
		Gupta & Gupta[59]		√			
		Batarfi et al.[60]	√	√			√
Operation Devices	Dropbear SSH Server	Schuster & Holz [62]	√		√		
		Mando [63]		√			
	Remote Code Execution	Gen & Ma[64]		√	√		
		Toyoda et al.[65]	√	√			
		Aiello et al.[66]	√				
		Agarwal et al.[67]	√		√		
		Naik et al.[68]	√	√			
		Li & Dey[69]	√				√
		Aleroud & Alsmadi [70]	√				
		Zhu[71]	√				

DoS, backdoor and ransomware attacks negatively impact the partially or entirely data input and data generation processes. As, existing solutions were proposed for achieving different goals, which cannot be compatible with the medical domain. Thus, there is dire need to introduce novel detection methods to address and eliminate backdoors, DoS and ransomware

TABLE 17. Limitation of the solution for each attack.

Attacks	Vulnerabilities	Solutions	High Resource Consumption	Poor System Performance	Poor Applicability	High Attack Probability	Insufficient Experiments
Information Collection	OpenSSH Vulnerability	Ylonen [30]				√	
		Coonjah et al. [32]	√				
		H. Alsaadi et al. [36]		√	√		
	Operating Systems Vulnerability	Qi et al. [33]	√	√			
		Chun-sheng &Guang[34]		√			
		Guanglou et al. [35]			√		
		Qian & A. Bridges[37]			√		
Database	Password Intrusion Vulnerability	Chen et al.[38]	√			√	
	Intrusion Vulnerability	Zhang et al.[39]			√		
		Gould et al. [40]					√
		Zhang et al.[41]		√	√		√
	SQL Injection Vulnerability	Ramesh et al. [42]				√	
		Temeiza et al. [43]	√	√			
		Chen et al.[44]	√			√	
		Wang et al.[45]			√		
		Desai & Gaikwad[46]					√
		Mishra et al.[47]			√		
		Appiah et al. [48]			√		
		Chen[49]	√				
Website	XSS	Shar & Tan[50]			√		√
		Gundy & Chen[51]			√		
		Shahriar & Zulkernine[52]	√	√			
		Barhoom & Kohail[53]	√				
		Parameshwaran et al.[54]			√		
		Kombade & Meshram[55]			√		
		Tatiana et al.[56]			√		
		Xu et al.[57]		√	√		
	CSRF	Gupta & Gupta[58]					√
		Gupta & Gupta[59]					√
		Batarfi et al.[60]			√		√
Operation Devices	Dropbear SSH Server	Schuster & Holz [62]		√			
		Mando [63]			√		
	Remote Code Execution	Gen & Ma[64]	√	√			
		Toyoda et al.[65]	√				
		Aiello et al.[66]		√			
		Agarwal et al.[67]		√			
		Naik et al.[68]			√		
		Li & Dey[69]	√				
		Aleroud & Alsmadi [70]			√		
		Zhu[71]	√				

TABLE 18. Evaluation of the cyber security medical systems, architectures and characteristics.

Medical Systems	Proposed Architectures/Solutions	Large Scale	Information Confidentiality	Low cost	System Generality	Transmission Efficiency
Intelligent Medical System [71]	Zang & Yu[73]	√				
	Sang[74]	√				
	Xu[75]	√		√		√
	Pi & Huang[76]		√		√	√
Comprehensive Information System Wang & Zhang [77]	Wang & Zhang [77]				√	
	Saurabh [78]	√	√			
	Salman et al. [78]	√			√	√
	Pan[79]	√	√			√
	Wang & Zha[81]	√				√
Hospital Information System	Han & Wu[83]	√	√			
	Zhou[84]	√	√			
	Xu[85]		√	√		
	Wu &Wang[86]		√		√	√
Non-invasive ECG sensors	Banerjee et al.[86]	√		√		
	Lin & Huang[87]		√			
	Barbosa et al.[88]		√	√		
	Monch et al.[89]	√	√		√	√
	Karnaushenko et al. [90]		√	√		√
Implantable Imaging System	Shi &Liu [92]	√		√		
	Xiao et al.[93]		√			
	Dai et al.[94]		√	√		
Personal Electronic Health Medical System[96]	Xie&Zhang[97]	√		√		
	Chang[98]		√			
	Ye[99]		√	√		
	Gao et al.[100]	√	√		√	√
E-Health Archives [101]	Chang[102]	√		√		
	Ren[103]		√			
	Zeng et al.[104]		√	√		
	Lu[105]	√	√	√	√	√
	Li et al.[106]	√	√			

attacks. The ransomware attack is highly dangerous, as existing ransomware approaches have poor system performance, which may influence the result. The attackers can change the dosage of a patient's medicine using DoS and remote code execution, which may take the life of the patient. It has been observed that most of the architectures perform better in terms of transmission efficiency and information confidentiality. However, not all architectures lead to low costs. Therefore, the future direction for development is to build architectures that should be less expensive. By lowering cost, future health frameworks can benefit patients and other medical staff by providing less expensive services. To meet the medical demands efficiently, CCS, HIS, and AFE frameworks should be deployed that has edge over other frameworks proved by analyzing various frameworks. However, these frameworks are not perfect solutions, but still, considerable research is required. Future research should also focus on people's awareness of preventing the database from being attacked so that attacks can be discouraged at inception.

IX. CONCLUSION

This paper surveys the vulnerabilities, attacks, solutions, and architectures of cybersecurity from a medical domain perspective. It provides an extensive overview of dataflow in the medical field, offers comprehensive data about potential cyber-attacks and presents medical cybersecurity architectures that can be used to support medical industries for safety enhancement.

The paper introduces four attacks that are easily implemented and influences people's health: (i) information collection attacks, (ii) database attacks, (iii) website attacks and (iv) operation device attacks. In particular, to solve these problems, this paper collects and analyzes several articles, summarizes the solutions of different attacks and lists both advantages and disadvantages. For example, mathematical methods can solve XSS attacks, which reduces the possibility of attack; however, the resolution consumes many system resources and has poor performance. This survey also explores some of the cybersecurity architectures used

in the medical domain: IMSs, comprehensive information systems, hospital information systems, noninvasive ECG sensors, implantable imaging systems, personal electronic health medical systems, and E-health archives. This paper classifies and studies the architectures of different applications. It also analyzes the benefits and deficiencies in terms of several factors, i.e., large scale, information confidentiality, low cost, system generality, and transmission efficiency, to perform a deep analysis of different security architectures and recommend the best architecture. At the same time, it summarizes all the medical systems and provides personal but comprehensive thoughts regarding the combination of present medical systems and advanced technologies. In this article, the best architectures for CCS, HIS, and AFE are presented, and they show better performance in all aspects. However, we cannot deny that other architectures have advantages. In the future, better ways to modify these weaknesses will be identified to prevent attacks and protect human health. Moreover, as the frameworks are not inexpensive, future research should explore the topic of cost reduction. Currently, due to a lack of knowledge and some unknown points, the paper includes some drawbacks and will require additional research; the gradual increased knowledge and advanced technology can be combined to provide convenient services to the public, especially in the healthcare field. New attacks and challenges may arise over time, and other innovations may be applied in different areas. This paper focuses on architectures and corresponding systems that can improve the inner quality of service and data transmission speed.

APPENDIX

See Tables 16–18.

REFERENCES

[1] [Online]. Available: http://www.lgcnsblog.com/features/how-well-is-your-medical-data-secured/#sthash.eDLoB3Tw.8Vjfnb4r.dpbs
[2] P. Ambrose and C. Basu, "Interpreting the impact of perceived privacy and security concerns in patients' use of online health information systems," *J. Inf. Privacy Secur.*, vol. 8, no. 1, pp. 38–50, Feb. 2015.
[3] D. Birnbaum, E. Borycki, B. T. Karras, E. Denham, and P. Lacroix, "Addressing public health informatics patient privacy concerns," *Clin. Governance Int. J.*, vol. 20, no. 2, pp. 91–100, 2015.
[4] W. Chung and L. Hershey, "Enhancing information privacy and data sharing in a healthcare IT firm: The case of Ricerro communications," *J. Inf. Privacy Secur.*, vol. 8, no. 4, pp. 56–78, 2014.
[5] F. A. Rahim, Z. Ismail, and G. N. Samy, "Healthcare employees' perception on information privacy concerns," in *Proc. Int. Conf. Res. Innov. Inf. Syst. (ICRIIS)*, Jul. 2017, pp. 1–6.
[6] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: Current state of research," *Int. J. Internet Enterprise Manag.*, vol. 6, no. 4, pp. 279–314, 2010.
[7] Q. W. Cao, "Description of SA weak password's harm and solution in the SQL server system," *J. Xingtai Polytech. College*, vol. 29, no. 1, Feb. 2012.
[8] F. Yang, J. Yan, S. Li, and C. Yang, "Risk analysis and safety design of mobile smart medical system," in *Proc. 3rd Inf. Technol. Mechatronics Eng. Conf. (ITOEC)*, Oct. 2017, pp. 3–5.
[9] S. A. Hareland, "Medical system design in a dynamic, regulated, multi-product, multi-life cycle environment," in *Proc. Annu. Syst. Conf. (SysCon)*, Apr. 2016, pp. 1–7.
[10] G. Sun, F. Yu, X. Lei, Y. Wang, and H. Hu, "Research on mobile intelligent medical information system based on the Internet of Things technology," in *Proc. 8th Int. Conf. Inf. Technol. Med. Educ. (ITME)*, Dec. 2016, pp. 260–266.
[11] S. A. Hareland, M. Kramer, S. Siddiqui, F. Navers, and B. Kastanek, "A see-saw commander/follower architecture for optimal control, safety, and extensibility in a medical system," in *Proc. IEEE Int. Syst. Eng. Symp. (ISSE)*, Oct. 2017, pp. 1–6.
[12] M. Hiltzik, "Anthem is warning consumers about its huge data breach. Here'sa translation," Los Angeles, CA, USA, Tech. Rep., Feb. 2017.
[13] J. Sametinger, J. Rozenblit, R. Lysecky, and P. Ott, "Security challenges for medical devices," *Commun. ACM*, vol. 58, no. 4, pp. 74–82, Mar. 2015.
[14] H. Lin, Z. Yan, and Y. Fu, "Adaptive security-related data collection with context awareness," *J. Netw. Comput. Appl.*, vol. 126, pp. 88–103, Jan. 2019.
[15] H. Lin, Z. Yan, and Y. Fu, "Adaptive security-related data collection with context awareness," *J. Netw. Comput. Appl.*, vol. 126, pp. 88–103, Jan. 2019.
[16] M. A. Malik, "Internet of Things (IoT) healthcare market by component (implantable sensor devices, wearable sensor devices, system and software), application (patient monitoring, clinical operation and workflow optimization, clinical imaging, fitness and wellness measurement)—Global opportunity analysis and industry forecast, 2014–2021," Allied Market Res., Pune, Maharashtra, Tech. Rep., 2016, p. 124.
[17] N. Pollard, J. Healey, and B. Woods, *The Healthcare Internet of Things: Rewards and Risks*. Washington, DC, USA: Atlantic Council, 2015, p. 17.
[18] A. Mohan, "Cyber security for personal medical devices Internet of Things," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, May 2014, pp. 372–374.
[19] U.S. Food and Drug Adminstration. *Classify Your Device*. [Online]. Available: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm2005371.htm
[20] A. Strielkina, D. Uzun, and V. Kharchenko, "Modelling of healthcare IoT using the queueing theory," in *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl.*, Bucharest, Romania, Sep. 2017, pp. 849–852.
[21] W. Hui and Z. Shaoping, "Risk analysis and security protection technology of Internet of Things attacks," *China Acad. J. Electron. Publishing House*, 2015.
[22] Z. Shunhua and Y. Kangmin, "Information security countermeasures of hospital information system," *Chin. J. Current Hospital Admin.*, Aug. 2006.
[23] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Jul. 2017, pp. 176–178.
[24] Q. W. Cao, "Description of SA weak password's harm and solution in the SQL server system," *J. Xingtai Polytech. College*, vol. 29, no. 1, Feb. 2012.
[25] Y. Z. Zhang, X. C. Yun, and M. Z. Hu, "Research on privilege-escalating based vulnerability taxonomy with multidimensional quantitative attribute," *J. China Inst. Commun.*, vol. 25, no. 7, pp. 107–114, Jul. 2004.
[26] B. Zhang, Y. C. Lei, and X. W. Lian, "The analysis to database security vulnerabilities," Technology World, Tech. Rep., 2012.
[27] A. Patil, A. Laturkar, S. V. Athawale, R. Takale, and P. Tathawade, "A multilevel system to mitigate DDoS, brute force and SQL injection attack for cloud security," in *Proc. Int. Conf. Inf., Commun., Instrum. Control (ICICIC)*, Aug. 2017, pp. 1–7.
[28] [Online]. Available: https://www.rapid7.com/fundamentals/cross-site-scripting/
[29] A. Peterson, "Connected medical devices: The Internet of Things-that-could-kill-you," Washington Post. WP Company, Tech. Rep., Feb. 2017.
[30] T. J. Ylonen, "User key management for the secure shell (SSH)," U.S. Patent 10 003 458, Jun. 19, 2018.
[31] S. Chakaravarthi, P. Visu, B. Balu, V. Vineshwaran, and M. Yakeshraj, "Web service registration and routing system and inter Web proxy service model prevents the message alteration attacks, man-in-the middle attacks," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2017, pp. 1–10.
[32] I. Coonjah, P. C. Catherine, and K. M. S. Soyjaudah, "Performance evaluation and analysis of layer 3 tunneling between OpenSSH and OpenVPN in a wide area network environment," in *Proc. Int. Conf. Comput., Commun. Secur. (ICCCS)*, Dec. 2015, pp. 1–4.
[33] G. Qi, C. Jinxuan, and L. Tianliang, "Homology analysis of ransomware based on sequence alignment," Tech. Rep., doi: 10.3969/j.issn.1006-2475.2018.02.001.

[34] G. Chun-Sheng and C. Guang, "An approach to decrypting ransomware wannacry based on API hooking," Tech. Rep., Jan. 2018, vol. 9, no. 1.

[35] G. Zheng, G. Zheng, W. Yang, C. Valli, R. Shankaran, and M. A. Orgun, "From WannaCry to WannaDie: Security trade-offs and design for implantable medical devices," in *Proc. 17th Int. Symp. Commun. Inf. Technol. (ISCIT)*, Sep. 2017, pp. 1–5.

[36] H. H. Alsaadi, M. Aldwairi, M. A. Taei, M. AlBuainain, and M. AlKubaisi, "Penetration and security of OpenSSH remote secure shell service on Raspberry Pi 2," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–5.

[37] Q. Chen and R. A. Bridges, "Automated behavioral analysis of malware: A case study of wannacry ransomware," in *Proc. 16th IEEE Int. Conf. Mach. Learn. Appl.*, Dec. 2017, pp. 454–460.

[38] C. Bo, Y. Ling, and S. Rushun, "Approach to paralleling password cracking intrusion andcountermeasures to defending," *Comput. Eng. Appl.*, vol. 2001, no. 23, p. 27, 2001.

[39] C. Gould, Z. Su, and P. Devanbu, "JDBC checker: A static analysis tool for SQL/JDBC applications," in *Proc. 26th Int. Conf. Softw. Eng.*, May 2004, pp. 697–698.

[40] Z. Xun, M. Zhi-Li, Z. Yong, Z. Xiao-Qin, G. Bo, and L. Zhi-Ru, "Design and implementation of kernel detecting based database vulnerability scanner," *China Acad. J. Electron. Publishing House*, 2016.

[41] K.-X. Zhang, C.-J. Lin, S.-J. Chen, Y. Hwang, H.-L. Huang, and F.-H. Hsu, "TransSQL: A translation and validation-based solution for SQL-injection attacks," in *Proc. 1st Int. Conf. Robot, Vis. Signal Process.*, Nov. 2011, pp. 248–251.

[42] A. Ramesh, A. Bhowmick, and A. V. Lal, "An authentication mechanism to prevent SQL injection by syntactic analysis," in *Proc. Int. Conf. Trends Automat., Commun. Comput. Technol. (I-TACT)*, Dec. 2015, pp. 1–6.

[43] Q. Temeiza, M. Temeiza, and J. Itmazi, "A novel method for preventing SQL injection using SHA-1 algorithm and syntax-awareness," in *Proc. Joint Int. Conf. Inf. Commun. Technol. Educ. Training Int. Conf. Comput. Arabic*, Aug. 2017, pp. 1–4.

[44] C. Ping, W. Jinshuang, P. Lin, and Y. Han, "Research and implementation of SQL injection prevention method based on ISR," in *Proc. 2nd IEEE Int. Conf. Comput. Commun.*, Oct. 2016, pp. 1153–1156.

[45] X. Wang, M. H. Heydari, and H. Lin, "An intrusion-tolerant password authentication system," in *Proc. 19th Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 2013, pp. 110–118.

[46] A. S. Desai and D. P. Gaikwad, "Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA," in *Proc. IEEE Int. Conf. Adv. Electron., Commun. Comput. Technol. (ICAECCT)*. Pune, India: Rajarshi Shahu College of Engineering, Dec. 2016, pp. 291–294.

[47] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, "Efficient approaches for intrusion detection in cloud environment," in *Proc. Int. Conf. Comput., Commun. Automat. (ICCCA)*, Apr. 2016, pp. 1211–1216.

[48] B. Appiah, E. Opoku-Mensah, and Z. Qin, "SQL injection attack detection using fingerprints and pattern matching technique," in *Proc. 8th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Nov. 2017, pp. 583–587.

[49] C. Ping, "A second-order SQL injection detection method," in *Proc. IEEE 2nd Inf. Technol., Netw., Electron. Automat. Control Conf. (ITNEC)*, Dec. 2017, pp. 1792–1796.

[50] L. K. Shar and H. B. K. Tan, "Automated removal of Cross Site Scripting vulnerabilities in Web applications," *Inf. Softw. Technol.*, vol. 54, no. 5, pp. 467–478, 2012.

[51] M. Van Gundy and H. Chen, "Noncespaces: Using randomization to defeat cross-site scripting attacks," *Comput. Secur.*, vol. 31, pp. 612–628, Jun. 2012.

[52] H. Shahriar and M. Zulkernine, "$S^2 \times S^2$: A server side approach to automatically detect XSS attacks," in *Proc. 9th Int. Conf. Dependable, Autom. Secure Comput.*, Dec. 2011, pp. 7–17.

[53] T. S. Barhoom and S. N. Kohail, "A new server-side solution for detecting cross site scripting attack," *Int. J. Comput. Inf. Syst.*, vol. 3, no. 2, pp. 19–23, 2011.

[54] I. Parameshwaran, E. Budianto, S. Shinde, H. Dang, A. Sadhu, and P. Saxena, "DexterJS: Robust testing platform for DOM-based XSS vulnerabilities," in *Proc. 10th Joint Meeting Found. Softw. Eng.*, Bergamo, Italy, 2015, pp. 946–949.

[55] R. D. Kombade and B. B. Meshram, "CSRF vulnerabilities and defensive techniques," *J. Comput. Netw. Inf. Secur.*, vol. 4, no. 1, p. 31, 2012.

[56] A. Tatiana, J. Mark, D. R. Suman, and W. J. Zeng, "Cross-site request forgery: Attack and defense," Tech. Rep., 2010.

[57] H. J. Xu, X. M. Hu, and D. D. Zhang, "A XSS defensive scheme based on behavior certification," *Appl. Mech. Mater.*, vols. 241–244, pp. 2365–2369, Dec. 2013.

[58] S. Gupta and B. B. Gupta, "CSSXC: Context-sensitive sanitization framework for Web applications against XSS vulnerabilities in cloud environments," *Procedia Comput. Sci.*, vol. 85, pp. 198–205, 2016.

[59] S. Gupta and B. B. Gupta, "Enhanced XSS defensive framework for Web applications deployed in the virtual machines of cloud computing environment," *Procedia Technol.*, vol. 24, pp. 1595–1602, 2016.

[60] O. A. Batarfi, A. M. Alshiky, A. A. Almarzuki, and N. A. Farraj, "Csrfdtool: Automated detection and prevention of a reflected cross-site request forgery," *J. Inf. Eng. Electron. Bus.*, vol. 6, no. 5, p. 10, 2014.

[61] Y. Yao, W. Xingwei, and S. Xiaoguang, "A cross heterogeneous domain authentication model based on PKI," in *Proc. 4th Int. Symp. Parallel Archit., Algorithms Program.*, Dec. 2011, pp. 325–329.

[62] F. Schuster and T. Holz, "Towards reducing the attack surface of software backdoors," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Berlin, Germany, Nov. 2013, pp. 851–862.

[63] C. Alberca, S. Pastrana, G. Suarez-Tangil, and P. Palmieri, "Security analysis and exploitation of arduino devices in the Internet of Things," in *Proc. ACM Int. Conf. Comput. Frontiers*, Como, Italy, May 2016, pp. 437–442.

[64] G. Li and M. Ma, "A KRC encryption solution protecting IEEE 802.11I 4-way handshake from DoS attacks," in *Proc. 4th IEEE Int. Conf. Broadband Netw. Multimedia Technol.*, Oct. 2011, pp. 586–591.

[65] K. Toyoda, Y. Kamiguchi, S. Inoue, and I. Sasase, "Efficient solution to decrease the effect of DoS attack against IP address ownership proof in mobile IPv6," in *Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun.*, Sep. 2011, pp. 1223–1227.

[66] M. Aiello, E. Cambiaso, S. Scaglione, and G. Papaleo, "A similarity based approach for application DoS attacks detection," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2013, pp. 000430–000435.

[67] M. Agarwal, S. Biswas, and S. Nandi, "Detection of De-authentication DoS attacks in Wi-Fi networks: A machine learning approach," in *Proc. IEEE Int. Conf. Syst., Man, Cybern.*, Oct. 2015, pp. 246–251.

[68] N. Naik, P. Jenkins, R. Cooke, D. Ball, A. Foster, and Y. Jin, "Augmented windows fuzzy firewall for preventing denial of service attack," in *Proc. IEEE Int. Conf. Fuzzy Syst.*, Jul. 2017, pp. 1–6.

[69] Y. Li, D. E. Quevedo, S. Dey, and L. Shi, "SINR-based DoS attack on remote state estimation: A game-theoretic approach," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 3, pp. 632–642, Sep. 2017.

[70] A. Aleroud and I. Alsmadi, "Identifying DoS attacks on software defined networks: A relation context approach," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2016, pp. 853–857.

[71] K. D. Thilak and A. Amuthan, "DoS attack on VANET routing and possible defending solutions—A survey," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2016, pp. 1–7.

[72] X. Hu, "The construction of intelligent medical system model under the Internet of Things framework," E-Government, Tech. Rep., 2013.

[73] C. Zang and W. Yu, "Construction of E-government cloud computing security system based on IATF model," Tech. Rep., doi: 10.16661/j.cnki 1672-3791.2015.34.046.

[74] L. Sang, "Research and application of intelligent medical system based on Internet of Things Jilin," Inst. Bus. Technol., Tech. Rep., doi: 10.13751/j.cnki.kjyqy.2011.13.124.

[75] J. Xu, "Research on hospital data disaster recovery system," Univ. Electron. Sci. Technol., Chengdu, China, Tech. Rep., 2006.

[76] J. Pi and C. Huang, "Design and research of smart medical analysis system based on Hadoop," Hubei Univ., Hubei, China, Tech. Rep.

[77] H. Wang and K. Zhang, "Analysis of hospital integrated information system architecture," *Silicon Valley*, vol. 5, no. 19, pp. 176–181, 2012.

[78] S. T. P. Saurabh, "A PDRR based detection technique for blackhole attack in MANET," *Int. J. Comput. Sci. Inf. Technol.*, vol. 2, no. 4, pp. 1513–1516, 2011.

[79] S. Ali, S. Qaisar, H. Saeed, M. Khan, M. Naeem, and A. Anpalagan, "Network challenges for cyber physical systems with tiny wireless devices: A case study on reliable pipeline condition monitoring," *Sensors*, vol. 15, no. 12, pp. 7172–7205, Mar. 2015.

[80] X. Pan, "Application of database firewall in hospital information system," *China Digit. Med.*, vol. 10, no. 4, pp. 91–93, 2015.

[81] L. Wang and M. Zha, "The design of intelligent medical system based on Zigbee," School Commun. Eng., Nanjing Inst. Technol., Nanjing, China, Tech. Rep.

[82] L. Zhang, Z. Hu, Z. Du, and S. Zhang, "The purpose and effect of hospital information system integration platform construction," *Chin. J. Health Inf. Manage.*, vol. 9, no. 2, pp. 47–49, 2012.
[83] R. Han and J. Wu, "Application of P2DR model in security of HIS," *Sci. Manage.*, vol. 1674, pp. 0081-3–0081-7, 2013.
[84] K. Zhou, "Research on electronic medical record system and access control strategy based on cloud storage," Shanghai Jiaotong Univ., Tech. Rep., 2011.
[85] J. Xu, "Research on hospital data disaster recovery system," Univ. Electron. Sci. Technol., Chengdu, China, Tech. Rep., 2006.
[86] S. Wu and X. Wang, "Application of medical information system integration based on HL7," *Chin. J. Med. Library Inf. Sci.*, vol. 23, no. 1, pp. 60–64, 2014.
[87] A. Banerjee, S. K. S. Gupta, G. Fainekos, and G. Varsamopoulos, "Towards modeling and analysis of cyber-physical medical system," Arizona State Univ., Tempe, AZ, USA, Tech. Rep.
[88] Y.-Q. Lin and C.-H. Huang, "Research on ESB framework for enterprise application integration," *Jisuanji Yingyong/J. Comput. Appl.*, vol. 30, no. 6, pp. 1658–1660, 2010.
[89] D. Barbosa, A. O. Mendelzon, L. Libkin, L. Mignet, and M. Arenas, "Efficient incremental validation of XML documents," in *Proc. 20th Int. Conf. Data Eng.*, Apr. 2004, pp. 671–682.
[90] I. Mönch, D. Makarov, R. Koseva, L. Baraban, D. Karnaushenko, C. Kaiser, K.-F. Arndt, and O. G. Schmidt, "Rolled-up magnetic sensor: Nanomembrane architecture for in-flow detection of magnetic objects," *ACS nano*, vol. 5, no. 9, pp. 7436–7442, 2011.
[91] R. Streubel, D. J. Thurmer, D. Makarov, F. Kronast, T. Kosub, V. Kravchuk, D. D. Sheka, Y. Gaididei, R. Schäfer, and O. G. Schmidt, "Magnetically capped rolled-up nanomembranes," *Nano Lett.*, vol. 12, no. 8, pp. 3961–3966, 2012.
[92] S. Yansheng, L. Liqiang, and Y. Quanfeng, "Application of data mining technology in regional health information platform," *Electron. Technol.*, vol. 38, no. 12, pp. 41–42, 2011.
[93] X. Jing, H. Tuxing, and Z. Ruoyun, "Improved algorithm for fast similarity search of time series," *Comput. Sci.*, vol. 30, no. 9, pp. 97–99, 2003.
[94] D. Dongbo, X. Zan, and Z. Yangyong, "Efficient sequence similarity search algorithm based on reference set index," *J. Softw.*, vol. 21, no. 4, pp. 718–731, 2010.
[95] H. Jin, "Design and implementation of symbol execution tool based on PAT tree," Huazhong Univ. Sci. Technol., Wuhan, China, Tech. Rep., 2007.
[96] J. Wenfeng and Y. Fengmin, "Personal electronic health medical system architecture based on WCDMA," CNKI China Nat. Knowl. Infrastruct., Tech. Rep., 2009.
[97] X. Mei and Z. Nature, "WCDMA system power control research," *J. Univ. Electron. Sci. Technol. China*, 2003.
[98] C. Zhirong, "Research and implementation of the integrated application of search engine Nutch in digital library," Beijing Univ. Posts Telecommun., CNKI China Nat. Knowl. Infrastruct., Tech. Rep., 2010.
[99] Y. Yan, "Design and implementation of data exchange platform of HIS system and healthcare system," CNKI China Nat. Knowl. Infrastruct., Lanzhou Univ., Lanzhou, China, Tech. Rep., 2014.
[100] G. Weifeng, R. Zhenbang, and L. Zihui, "Application of multi-layer architecture technology in information management system," Fujian Computer, CNKI China Nat. Knowl. Infrastruct., Tech. Rep., 2007.
[101] Z. Wenhua and Z. Pengpeng, "Research on information dissemination and privacy protection of residents health records based on SOA," CNKI China Nat. Knowl. Infrastruct., Tech. Rep., 2013.
[102] C. Chin, "Application framework design and application prospect of enterprise information system based on cloud computing and SOA," China Offshore Oil Gas, CNKI China Nat. Knowl. Infrastruct., Tech. Rep., 2013.
[103] R. Guanhua, "Analysis of concept analysis and standardization of electronic health archive," *J. Med. Informat.*, 2015.
[104] Z. Wenying, Z. Yulong, and Q. Deyu, "ESB principle, architecture, implementation and application, computer engineering and applications," CNKI China Nat. Knowl. Infrastruct., Tech. Rep., 2008.
[105] L. Xudong, "IHE technical framework and medical workflow integration," *China Med. Device Inf.*, 2004.
[106] L. Qinyan, Q. Zhuoying, C. Di, L. Xin, and Y. Jian, "Chinese journal of rehabilitation theory and practice, based on ICF's information architecture and data system of national function, disability and health," CNKI China Nat. Knowl. Infrastruct., Tech. Rep.
[107] C. Camara, P. Peris-Lopez, and J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *J. Biomed. Inform.*, vol. 55, pp. 272–289, Jun. 2015.
[108] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015.
[109] S. Al-Janabi, I. Al-Shourbaji, M. Shojafar, and S. Shamshirband, "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications," *Egyptian Inform. J.*, vol. 18, no. 2, pp. 113–122, 2017.
[110] K. Malasri and L. Wang, "Securing wireless implantable devices for healthcare: Ideas and challenges," *IEEE Commun. Mag.*, vol. 47, no. 7, pp. 74–80, Jul. 2009.
[111] I. B. Ida, A. Jemai, and A. Loukil, "A survey on security of IoT in the context of eHealth and clouds," in *Proc. 11th Int. Design Test Symp. (IDT)*, Dec. 2016, pp. 25–30.
[112] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Jul. 2017, pp. 176–178.
[113] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in telecare medicine information systems," *J. Netw. Comput. Appl.*, vol. 87, pp. 1–19, 2017.
[114] A. Strielkina, V. Kharchenko, and D. Uzun, "Availability models for healthcare IoT systems: Classification and research considering attacks on vulnerabilities," in *Proc. IEEE 9th Int. Conf. Dependable Syst., Services Technol. (DESSERT)*, May 2018, pp. 58–62.
[115] A. Alzahrani, A. Alqhtani, H. Elmiligi, F. Gebali, and M. S. Yasein, "NFC security analysis and vulnerabilities in healthcare applications," in *Proc. IEEE Pacific Rim Conf. Commun., Comput. Signal Process. (PACRIM)*, Aug. 2013, pp. 302–305.
[116] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017.
[117] C. S. Kruse, B. Frederick, T. Jacobson, and D. K. Monticone, "Cybersecurity in healthcare: A systematic review of modern threats and trends," *Technol. Health Care*, vol. 25, no. 1, pp. 1–10, 2017.
[118] H.-S. Yang, "A study on attack information collection using virtualization technology," *Multimedia Tools Appl.*, vol. 74, no. 20, pp. 8791–8799, 2015.
[119] S. Rahimi and M. Zargham, "Vulnerability scrying method for software vulnerability discovery prediction without a vulnerability database," *IEEE Trans. Rel.*, vol. 62, no. 2, pp. 395–407, Jun. 2013.
[120] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Jul. 2017, pp. 176–178.
[121] T. Farral, "Nation-state attacks: Practical defences against advanced adversaries," *Netw. Secur.*, vol. 2017, no. 9, pp. 5–7, Sep. 2017.
[122] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, "Ransomware detection and mitigation using software-defined networking: The case of WannaCry," *Comput. Electr. Eng.*, vol. 76, pp. 111–121, Jun. 2019.
[123] E. McMahon, R. Williams, M. El, S. Samtani, M. Patton, and H. Chen, "Assessing medical device vulnerabilities on the Internet of Things," in *Proc. IEEE Int. Conf. Intell. Secur. Inform. (ISI)*, Jul. 2017, pp. 176–178.
[124] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry ransomware," in *Proc. 20th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2018, pp. 159–166.
[125] K. Ganame, M. A. Allaire, G. Zagdene, and O. Boudar, "Network behavioral analysis for zero-day malware detection-A case study," in *Proc. Int. Conf. Intell., Secure, Dependable Syst. Distrib. Cloud Environ.* Cham, Switzerland: Springer, 2017, pp. 169–181.
[126] A. E. Widjaja and J. V. Chen, B. M. Sukoco, Q.-A. Ha, and Q.-A. Ha, "Understanding users' willingness to put their personal information on the personal cloud-based storage applications: An empirical study," *Comput. Hum. Behav.*, vol. 91, pp. 167–185, Feb. 2019.
[127] A. Arfaoui, A. Kribeche, and S.-M. Senouci, "Context-aware anonymous authentication protocols in the Internet of Things dedicated to e-health applications," *Comput. Netw.*, vol. 159, pp. 23–36, Aug. 2019.
[128] M. Masdari and S. Ahmadzadeh, "A survey and taxonomy of the authentication schemes in telecare medicine information systems," *J. Netw. Comput. Appl.*, vol. 87, pp. 1–19, Jun. 2017.
[129] B. Nour, K. Sharif, F. Li, S. Biswas, H. Moungla, M. Guizani, and Y. Wang, "A survey of Internet of Things communication using ICN: A use case perspective," *Comput. Commun.*, vols. 142–143, pp. 95–123, Jun. 2019.
[130] A. Yeole, D. R. Kalbande, and A. Sharma, "Security of 6LoWPAN IoT networks in hospitals for medical data exchange," *Procedia Comput. Sci.*, vol. 152, pp. 212–221, Jan. 2019.

[131] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Comput. Netw.*, vol. 148, pp. 283–294, Jan. 2019.
[132] N. A. Azeez and C. Van der Vyver, "Security and privacy issues in e-health cloud-based system: A comprehensive content analysis," *Egyptian Inform. J.*, vol. 20, no. 2, pp. 97–108, Jul. 2018.
[133] [Online]. Available: https://info.varonis.com/hubfs/2018%20Varonis%20Global%20Data%20Risk%20Report.pdf
[134] S. Morgan. *Cybersecurity Business Report*. Accessed: Nov. 20, 2017. [Online]. Available: https://www.csoonline.com/article/3237674/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html
[135] S. Parasuraman and A. K. Sangaiah, "Fog—Driven healthcare framework for security analysis," in *Computational Intelligence for Multimedia Big Data on the Cloud With Engineering Applications*. New York, NY, USA: Academic, 2018, pp. 253–270.
[136] SSH OpenSSH, 2011, pp. 54–56, vol. 6.
[137] J. Harris and R. L. Hill, "Statictrust: A practical framework for trusted networked devices," in *Proc. 44th Hawaii Int. Conf. Syst. Sci.*, Jan. 2011, pp. 1–10.
[138] M. S. Jalali, S. Razak, W. Gordon, E. Perakslis, and S. Madnick, "Health care and cybersecurity: Bibliometric analysis of the literature," *J. Med. Internet Res.*, vol. 21, no. 2, 2019, Art. no. e12644.
[139] D. S. McDermott and L. T. Jessica Kamerer Andrew Birk, "Electronic health records: A literature review of cyber threats and security measures," *Int. J. Cyber Res. Educ.*, vol. 1, no. 2, pp. 42–49, 2019.
[140] L. Coventry and D. Branley, "Cybersecurity in healthcare: A narrative review of trends, threats and ways forward," *Maturitas*, vol. 113, pp. 48–52, Jul. 2018.
[141] J. L. Fernández-Alemán, I. C. Señor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Inform.*, vol. 46, no. 3, pp. 541–562, 2013.
[142] C. A. Tschider, "Enhancing cybersecurity for the digital health marketplace," *Ann. Health L.*, vol. 26, p. 1, 2017.
[143] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *J. Comput. Syst. Sci.*, vol. 80, no. 5, pp. 973–993, 2013.

ABDUL RAZAQUE received the Ph.D. degree in computer science and engineering from the University of Bridgeport, USA, in 2015. He is currently an Associate Professor with the Department of Computer Engineering and Telecommunication, International Information Technology University, Almaty, Kazakhstan. He has authored over 150 international academic publications, including journals, conferences, book, and book chapters. His current research interests include the wireless sensor networks, cyber security, cloud computing security, design and development of mobile learning environments, and ambient intelligence. He served as an Editor-in-Chief for the *International Journal for Engineering and Technology* (IJET), Singapore, from 2012 to 2015. He is an editor, an associate editor, and a member of Editorial Board of several international journals.

FATHI AMSAAD received the Ph.D. degree in engineering science from the University of Toledo (UToledo), Toledo, OH, USA. He is currently an Assistant Professor with the School of Computing, The University of Southern Mississippi (USM), Hattiesburg, MS, USA, where he is also the Founder and a Director of the Cyber Security Laboratory, and a Co-director of the Advanced Computing Research Laboratory. His current research interests include cyber security and cyber-physical systems with special interests in hardware-oriented security and trust for device and system authentication, secure embedded architectures, VLSI/FPGA systems testing, fault tolerance hardware, detection and prevention of hardware trojans, network and mobile wireless security, and security of the IoT applications and smart systems. He was a recipient of the prestigious IEEE Best Graduate Student Award from IEEE Region four and College of Engineering, UToledo. In addition, he was the 2017 nominee for the best Ph.D. Dissertation Award. He holds MCP, MCSA, MCTS, and MCSE Professional Certificates from Microsoft Company. He is an active member of ACM, and served as a project adviser for several groups of senior undergraduate students and a reviewer for high impact and peer-review conferences/journals.

MEER JARO KHAN is currently pursuing the B.S. degree in business information management with Islamic International University Islamabad, Pakistan. His current research interest includes designing complex mathematical models, including security of cloud computing, wireless sensor networks, and cyber physical systems.

SALIM HARIRI received the Ph.D. degree in computer engineering from the University of Southern California, in 1986. He is currently a Professor and a Site Director of the NSF-funded Center for Cloud and Autonomic Computing, The University of Arizona. He coauthored three books on autonomic computing, parallel and distributed computing, and edited *Active Middleware Services*, a collection of articles from the second annual AMS workshop published by Kluwer, in 2000. Prof. Hariri founded the IEEE/ACM International Symposium on High Performance Distributed Computing, or HPDC, and is the Co-founder of the IEEE/ACM International Conference on Cloud and Autonomic Computing. He serves as an Editor-in-Chief for the scientific journal *Cluster Computing*, which presents research and applications in parallel processing, distributed computing systems, and computer networks.

SHUJING CHEN is currently pursuing the degree in computer science and technology with the Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China. Her current research interests include database management and a series of problems about network security. She has designed software that can detect sensitive words which contributes to protect information security.

CHEN SITING is currently pursuing the B.S. degree in computer science with the New York Institute of Technology, USA. She is doing research in the field of the natural language processing (NLP) part. Her current research interests include multiple document summarization, machine translation, cyber security, data analytics, and cloud security.

XINGCHEN JI is currently pursuing the degree in computer science and technology with the Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, China, where she is focusing on the computer science area. She gets good grades in lessons and she actively takes part in all kinds of activities. She acts as the Leader of the Group in Science and Technology Innovation Training Program. Her current research interests include the Internet-of-things and artificial intelligence. She is trying to make combinations between computer science and other subjects.