IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 15, 2019, accepted July 22, 2019, date of publication July 25, 2019, date of current version August 9, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2930962*

# A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems

**ABDULLAH ALGARNI**
Information Technology Division, Institute of Public Administration, Riyadh 11141, Saudi Arabia
e-mail: algarniaa@ipa.edu.sa

This work was supported in part by the Institute of Public Administration, Saudi Arabia.

**ABSTRACT** Advances in wireless technology have resulted in the development of smart healthcare systems (SHSs). In SHS, sensors, wearables, and devices monitor a patient's vital parameters. These parameters are transmitted to the designated emergency services or the trusted healthcare professionals for evaluation. The security and privacy of vitals during collection and transmission are the major concerns. Therefore, it is essential to discuss security techniques, concerns, and requirements in SHS. We review the methodologies, objectives, platforms, and techniques used in SHS. First, we present a novel classification scheme for SHS that ranks their methodologies within their applicable domains. Second, we create a classification scheme for the literature concerning SHS. Third, we examine the most important security attacks in SHS and the countermeasures proposed in this paper. Finally, we identify the open-research challenges in security and privacy of SHS and provide directions for future research.

**INDEX TERMS** Internet of Things, smart healthcare system, security, privacy, review.

## I. INTRODUCTION

Advances in technology have led to a new paradigm called the Internet of Things [1], [2]. Smart devices use secure Internet Protocols (IPs) to transfer complex data [3]. These intelligent machines can be used in a wide variety of industries that intersect with healthcare, including education, business, and administration [4]. Smart healthcare systems (SHS) are particularly important because some can give patients increased control over their personal health data. Patients can access these systems from any smart device with enough information processing power [5].

SHS are particularly helpful to the older population, since technological improvements have increased life expectancy. Older adults are more prone to life-threatening diseases, such as heart attack, asthma, diabetes, and cancer. Either directly or indirectly, 68% of deaths in people over 60 years of age are due to these diseases [6]. According to the United Nations, 11.7% of the world's population is currently older than 60, and this number is expected to increase with time [7]. Chronic diseases in older adults require continuous monitoring and early detection if they are to be cured. Older adults tend to spend more time in hospitals than younger patients, which means that countries spend a large amount of money on their care. Current figures project that 19.9% of the Gross Domestic Product (GDP) of the United States will be devoted to care for elders by the end of 2022 [8]. Advances in SHS technology are enabling better care of this population, shifting the focus of healthcare systems from a hospital-based approach to a person-based approach.

A person-based healthcare approach is made possible by using SHS for remote patient monitoring [10]. Connections are made between the physical world and electronic data with the help of sensors, personal devices (PDs), and actuators [11]. These patient monitoring devices continuously monitor a patient's vitals and transmit them to an examiner or trusted healthcare professional. These transmissions use a media access control (MAC) layer and physical (PHY) layer to handle data. The Institute of Electrical and Electronics Engineers (IEEE) and European Telecommunications Standards Institute (ETSI) have developed some standards for these transmissions. These include, but are not limited to, IEEE 802.15.4 low-rate wireless personal area networks, IEEE 802.15.6 wireless body area networks (WBANs), and ETSI smartBAN [12]–[15].

The overall architecture of SHS is generally divided into three different layers, or tiers. The first tier is composed of small, low-power, highly efficient sensors for reading a

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

patient's vitals. These can be placed into, on, or around the body. Some common examples of first-tier devices are pacemakers, motion detectors, and artificial retinas [16]. All these sensors forward health information to a PD. These PDs connect to the second tier, which is the Internet or a cloud server. The third tier is where data are analyzed. Analysis on the third tier helps healthcare professionals decide if action needs to be taken based on sensor readings. Sensors and other intelligent devices in SMS can classify data by taking into account both the patient and the examiner. For example, a doctor needs historical information about a patient's vitals, while a chemist may only need the list of prescriptions the patient currently uses. Similarly, an ambulance crew may need different information than a nurse or specialist. Since communication between sensors and devices is wireless, ensuring that every healthcare provider gets the specific information they need while maintaining the security and privacy of all data involved is a primary concern of SHS. Purposeful data tampering or unintentional data access by the wrong healthcare practitioner could be dangerous to patients.

Smart healthcare system prototypes are on the cutting edge of new security techniques and are poised to pioneer new security technologies in the coming years. Most current internet of things (IoT) literature describes general information about IoT frameworks rather than the application of IoT to specific domains. Therefore, this review examines the current state of data security in SHS and explores the new technologies they use, as well as their future potential. In this paper, we provide the following: 1) a review of the current state of research concerning the security and privacy of SHS, 2) analyses, assessments, and classifications of research on the security and privacy of SHS, and 3) new insights and suggestions for future research directions concerning the security and privacy of SHS.

Section II provides a background on SHS security, followed by section III, which presents the research methodology used for this review. Sections IV and V show the distribution of current work on security and privacy of SHS, categorized by publication venue and publication year. Sections VI through VIII contain classifications of the publications included in this review, sorted by objective, application domain, technique, and security method used. Section IX summarizes the most commonly mentioned security attacks in SHS and the suggested countermeasures against such attacks in literature. Section X discusses how current research handles security and privacy challenges in SHS, identifies the open research challenges in the privacy and security of SHS, and provides directions for future research. Finally, Section XI concludes this work.

## II. BACKGROUND ON SMART HEALTHCARE SYSYEMS' SECURITY

The overall goal of SHS is to deliver optimal patient care by making the most of advanced information and communications technology (ICT). Healthcare is one of today's most attractive applications of IoT. Apart from the advantages of IoT, there are several security and privacy requirements to consider when making a healthcare system smart: the availability of all relevant information when required; effective and reliable surgical and diagnostic processes that facilitate achieving this objective with low error rate, high accuracy, and cost effectiveness; and access to internal and external resources when needed.

IoT devices are producing increasingly large volumes of data that are extremely sensitive. In addition, destroying the security of the medical system may have disastrous consequences. On the other hand, the patient's private information exists at all stages of data collection, data transmission, cloud storage, and data republication. Therefore, the main requirements when developing security and privacy for SHS include: 1) all data values satisfy semantic standards without unauthorized tampering, 2) all medical services and data are continuously available to the user (patient, nurse, practitioner, or provider) when required, 3) all systems are used only by authorized users, 4) data are transmitted securely during all communications between the communicating parties, and 4) all patients' private and sensitive information (including their mental status, sexual orientation, sexual functioning, infectious diseases, fertility status, drug addiction, genetic information, and identity information) must be maintained.

The risks that come with the application of IoT in SHS include possible threats to patient safety or loss of personal health information. These may not only be caused by malicious actions but also by human errors, system or third-party failures, and natural phenomena. As the attack surface increases with the introduction of connected devices, the attack potential can grow exponentially. Furthermore, serious vulnerabilities come with the application of IoT in SHS. The most important sources of these vulnerabilities are [4]: 1) Internet-of-things devices are well interconnected, and some devices can even automatically connect to other devices, such as networked health devices; 2) communication and connection between health systems devices and legacy systems can also increase vulnerability by offering malicious attackers illegal access to systems or data; 3) unauthorized access is crucial in the smart hospital environment, as a lack of authorization policy may lead to allowing unauthorized users to gain access to a critical system through an end device.

As security and privacy are a requirement in healthcare organizations all over the world, there are many different regulations and acts that affect healthcare providers. Nonetheless, though regulations and acts vary greatly from country to country, most are meant to ensure the previously mentioned five requirements. For example, [3] summarizes the American Health Insurance Portability and Accountability Act (HIPAA), which has the following requirements: 1) provide protection against any infringements of security, confidentiality, and integrity, if they occur, 2) provide protection against unauthorized access to or usage of patient health information, 3) establish systems that require user identities (i.e., both internal staff and consumers), 4) limit the access to sensitive data and applications to authorized individuals, and 5) ensure

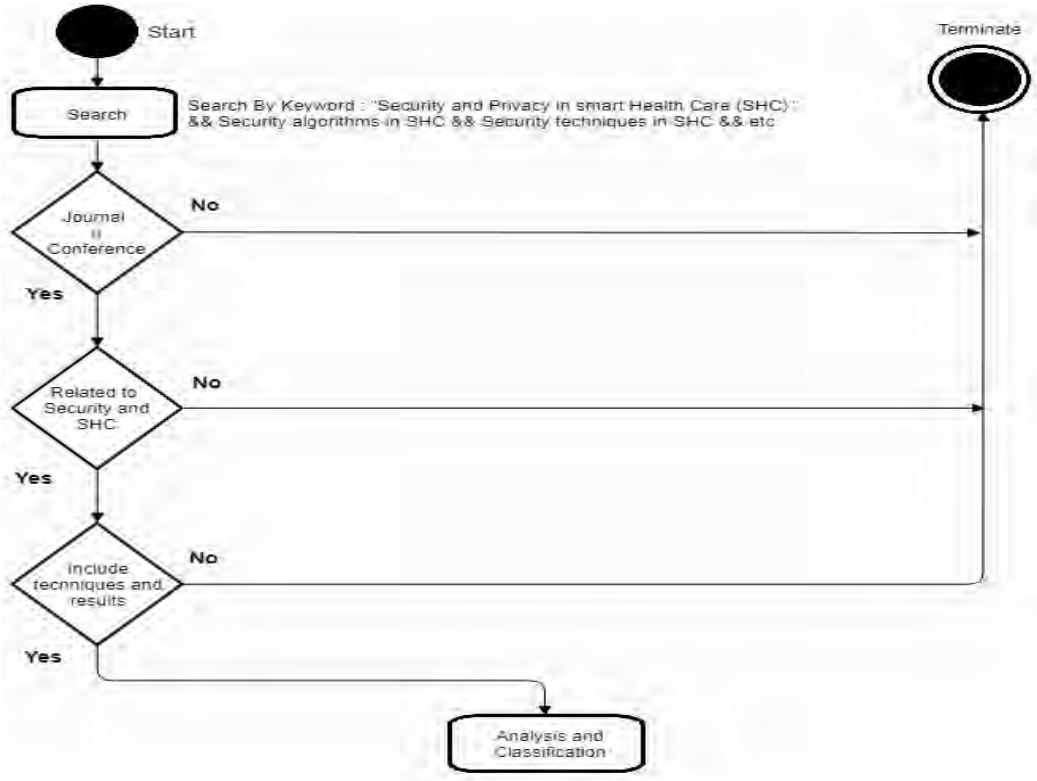


**FIGURE 1.** Research methodology.

the integrity of patient health information throughout its lifecycle within the system.

Finally, while this section provides the general background of the issues and requirements of SHS, the next sections will delve more deeply, focusing on the relevant research.

## III. METHODOLOGY

This research analyzes publications related to security and privacy in SHS. It identifies key objectives, application domains, techniques, methods, and challenges. To collect the relevant data, many publishers of primary research literature were considered, including IEEE, SAGE, Elsevier, Springer, and ACM. The following methodology was used for paper selection: 1) search each electronic database, 2) use specific keywords to find papers potentially written about SHS security, 3) gather a pool of papers from steps 1 and 2, 4) remove any sources that are not peer-reviewed journals or conferences of high repute, 5) remove any sources that are not relevant to SHS security and privacy, 6) remove any sources that are not research studies, and 7) classify papers with the input of an expert panel.

Using databases in English and an initial search query of ''smart healthcare system security,'' without quotation marks, yielded more than 127,000 literature results. This initial dataset was pruned to include only peer-reviewed articles published in or after the year 2000. This second pruning narrowed the dataset to approximately 2,900 results. The dataset was refined a third time to include only subject terms relevant to smart healthcare: ''access control,'' ''authentication,'' ''computer information security,'' ''cryptography,'' ''data management,'' ''encryption,'' ''health care,'' ''health informatics,'' ''Internet of things,'' ''iot,'' ''medical informatics,'' ''privacy,'' and ''security.'' This resulted in a pruned dataset of 942 articles. Since this research focuses on primary literature, any reviews were excluded. A final pruning removed any articles that did not directly address SHS security and privacy, as were any articles that did not contain adequate information on these topics. The final dataset contained 98 articles. This methodology is summarized in Fig. 1.

## IV. DISTRIBUTION BY PUBLICATION AVENUE

In this section, the papers selected for review are classified based on publication venue. Fig. 2 highlights the distribution of the papers based on their general type: 71% are primary research from well-reputed journals, and 29% originate from conferences.

The reviewed papers were published in 39 different venues. Fig. 3 classifies the publishers on security and privacy of SHS. IEEE and Elsevier comprise approximately 70% of the total publications, at approximately 38% and 33%, respectively. The rest of the represented publishers make up less than 10% of the reviewed papers. Four publishers are represented by one paper each, so they are categorized together as ''Others.'' The total share of these four publishers, relative to the total number of publishers, is 8%. The most notable publication venues are the IEEE *Internet of Things Journal*, Elsevier's

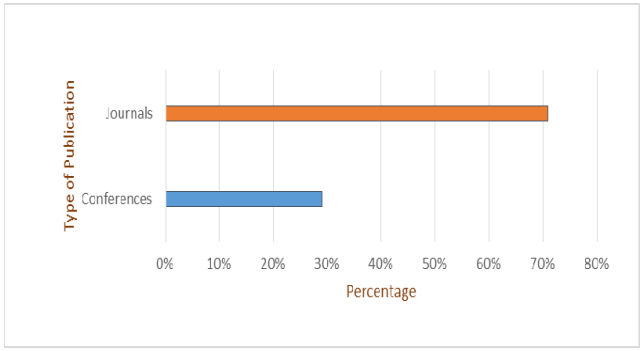


**FIGURE 2.** Distribution by type.

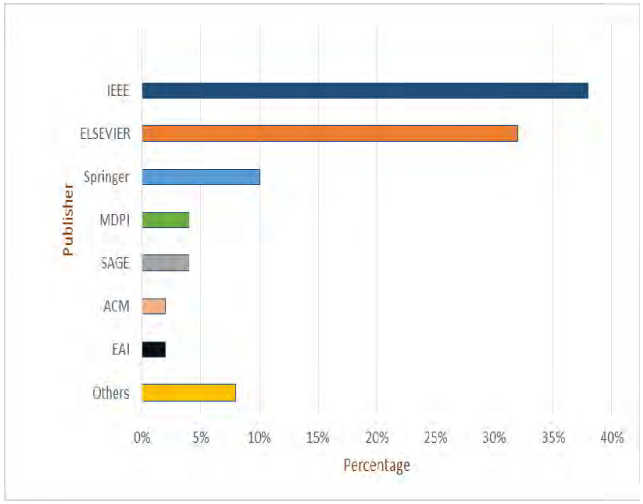


**FIGURE 3.** Classification by publisher.

*Computer and Electrical Engineering Journal*, and Elsevier's *Future Generation Computer Systems*.

## V. DISTRIBUTION BY PUBLICATION YEAR

The frequency of papers concerning security and privacy of SHS is presented in Figure 4. Before 2011, there was minimal interest in SHS, and published papers on the topic from that time account for only 7% of the reviewed papers. After 2013, however, there has been substantial growth in the number of publications each year. Indeed, 2018, the last full year for which data were available, contained the largest number of research papers on security and privacy in SHS, making up 18% of the reviewed papers. It is reasonable to expect that the number of papers about SHS will continue to grow, especially with new types of wearable technology and 5G networks becoming available.

## VI. CLASSIFICATION BY OBJECTIVE

While reviewing the work on the security and privacy of SHS, we found that researchers used different essential aspects for building cyber-security defenses. Table 1 presents the classification scheme for different security defenses. We found that most papers addressed one or more of three main objectives or defenses: authentication, authorization, and access control.

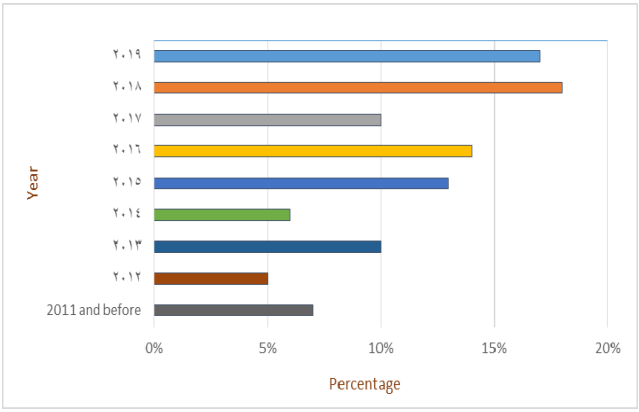


**FIGURE 4.** Publication frequency by year.

**TABLE 1.** Classification by objective/defense.

| Main Objective | Reference | Percentage |
|---|---|---|
| Authentication | [17]; [18]; [19]; [22]; [23]; [24]; [25]; [26]; [27]; [28]; [29]; [30]; [33]; [34]; [35]; [36]; [37]; [38]; [39]; [40]; [41]; [42]; [43]; [44]; [45]; [46]; [50]; [51]; [53]; [55]; [57]; [60]; [62]; [63]; [67]; [68]; [93]; [95]; [97]; [98] | 40% |
| Authorization | [18]; [19]; [29]; [30]; [34]; [36]; [38]; [41]; [45]; [46]; [49]; [50]; [51]; [61]; [63]; [92] | 24% |
| Access Control | [19]; [20]; [21]; [31]; [32]; [41]; [43]; [49]; [50]; [54]; [55]; [61]; [67]; [93] | 19% |
| Others | [47]; [48]; [52]; [54]; [56]; [58]; [59]; [62]; [64]; [65]; [66]; [91] | 17% |

Authentication is the process or action of verifying the identity of a user or process. It is an important step in SHS data security because it is the first line of defense against attacks by those who should not have access to data. Single sign-on utilities or token handling are common ways to implement authentication protocols in SHS. Authorization verifies that an identified user or process possesses the right credentials to view data. This is the second step in SHS data security, often implemented with privilege levels or duty separation. Access control is a broader security technique that regulates how resources in SHS are used. This technique doesn't rely on a user's identity, but rather uses other customizable characteristics, such as laboratory groups, to handle access.

Of the reviewed papers, 40% focused on authentication as a main objective, followed by authorization, at 24%. Access control was the focus in approximately 19% of the papers, and the rest of the papers focused on other objectives. As presented in Table 1, there is some overlap in these categories, and it is common for authentication, authorization, and access control to be addressed together.

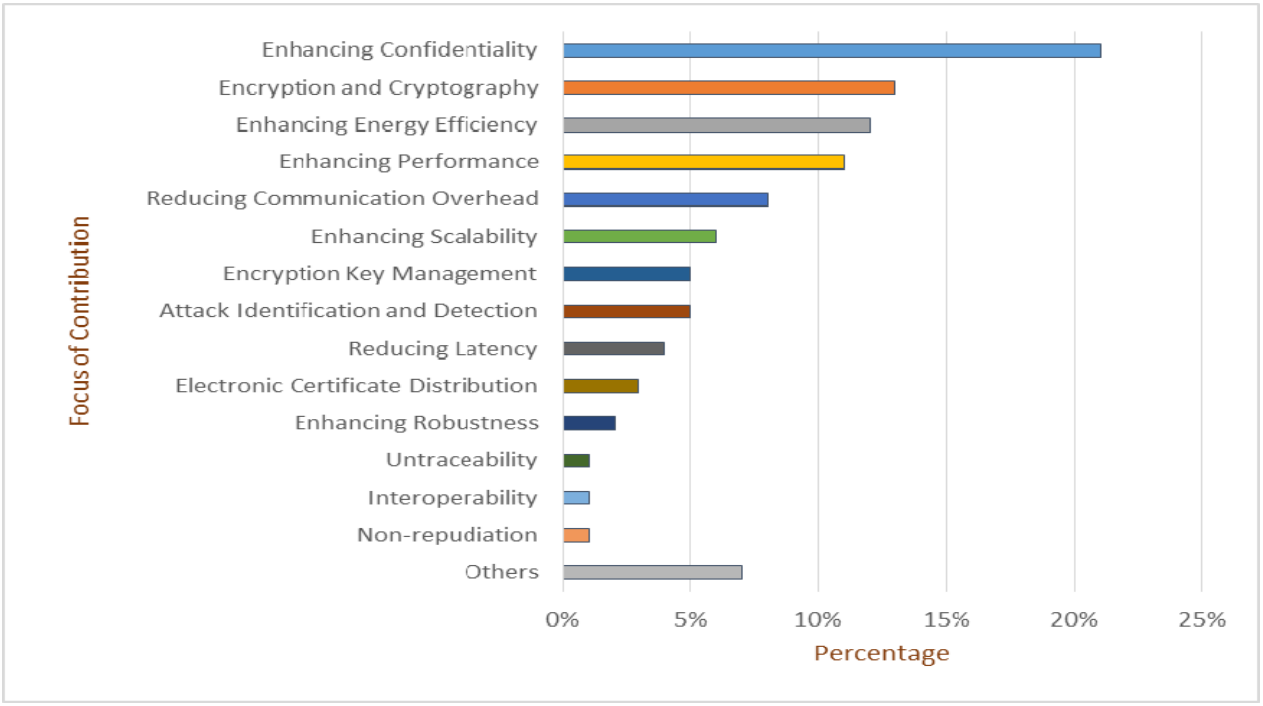


**FIGURE 5.** Classification by focus of contribution.

The studies represented in Table 1 also focused on one or more subtopics. The percentage of papers that dealt with each subtopic is shown in Figure 5. The subtopic with the most coverage was enhancements in data confidentiality, which was present in approximately 21% of the reviewed papers. Encryption and cryptography were also commonly represented, with each topic found in 13% of the papers. Enhancing energy efficiency, performance, and reducing communication overhead also were found at significant percentages: 12%, 11%, and 8% of the reviewed papers, respectively. Two other subtopics, scalability and encryption key management, were found in 5-6% of papers. All other subtopics were found in less than 5% of papers. These included latency, electronic certificate distribution, robustness, interoperability, and non-repudiation.

The most common platforms used in the studies represented by the reviewed papers are: 1) NS-2 Simulator, 2) Virtual Machine, 3) Java Simulator, 4) localhost web service with SQL, 5) MATLAB, 6) NIST Suite, 7) Sim card (smart phone), 8) Visual Basic, 9) smart gateways-based IoT, 10) multi-cloud proxy, and 11) Eclipse Simulator.

## VII. CLASSIFICATION BY APPLICATION DOMAIN

SHS handle three main health modules, or application domains: self-care, home care, and acute care. Self-care has to do with the prevention of disease at the individual patient level. It allows patients to monitor and access their own personal health data so they can react accordingly. Smart devices can help patients monitor their diets, track potential disease, and handle their own fitness [69]. Home care allows healthcare providers to monitor patients' health remotely. If a problem is detected, an alarm alerts the doctor and patient, who can then collaborate to determine what steps should be taken. Acute care refers to with emergency situations and chronic disease management that may require urgent responses [70]. Ambulances receive signals directly from the PD, which gives first responders information that patients may not be able to relay themselves.

Every reviewed paper addressed a security or privacy issue connected to one or more of these domains. Fig. 6 presents the percentage of papers that address issues related to each domain: 45% addressed issues related to self-care, 35% handled home care, and 20% addressed acute care.

Each of these domains can use a combination of sensors, be they inside the body, on the body, an implanted PD, or smart devices. Remote health monitoring is the primary objective of SHS. This is possible due to the wide variety of sensors that can be integrated into the systems. SHS have found success in preventing cardiovascular disease with sensors that can detect high blood pressure [71] and sensors for ECG monitoring [72]. Blood pressure management through SHS can help prevent life-threatening events such as strokes [73].

SHS can also monitor a person's fitness level, whether or not that person has chronic health conditions. The amount of activity people engage in is closely linked with any health conditions they develop, and SHS can serve as an early warning system [74]. Monitoring the body with SHS can directly prevent musculoskeletal disease [75]. Abnormal body movement can lead to nervous system, muscle, and bone injuries, so SHS are also helpful in keeping people safe from injury. Healthcare providers can monitor patients' progress

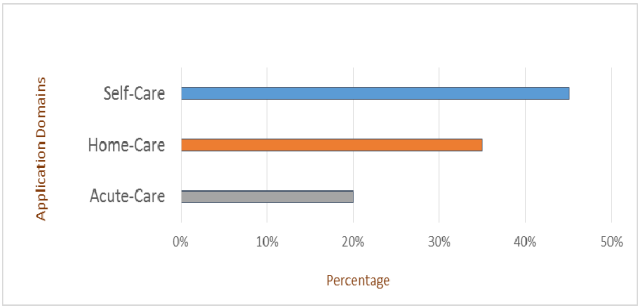


**FIGURE 6.** Classification by application domain.

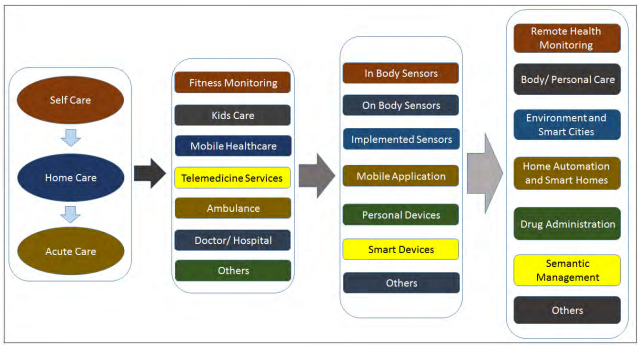


**FIGURE 7.** Health domains and applications.

**TABLE 2.** Classification by health application.

| Application | Reference | Percentage |
|---|---|---|
| Remote health monitoring | [17]; [18]; [19]; [20]; [21]; [22]; [23]; [24]; [25]; [26]; [27]; [28]; [30]; [31]; [32]; [33]; [34]; [35]; [36]; [37]; [38]; [39]; [40]; [41]; [42]; [43]; [45]; [46]; [47]; [48]; [49]; [50]; [51]; [53]; [54]; [55]; [56]; [58]; [60]; [61]; [62]; [63]; [64]; [65]; [66]; [67]; [68] | 85% |
| Body and personal care | [12]; [13]; [14]; [15]; [19]; [26]; [42]; [43]; [45]; [47]; [76]; [83]; [84]; [85]; [86]; [87] | 20% |
| Environment and smart cities | [22]; [53]; [60]; [64]; [4]; [34]; [41]; [53]; [65]; [78]; [90]; [92]; [93]; [97]; [98] | 17% |
| Home automation and smart homes | [27]; [27]; [33]; [36]; [37]; [41]; [42]; [43]; [48]; [50]; [62]; [76]; | 14% |
| Drug administration | [21]; [22]; [26]; [33]; [40] | 7% |
| SMA | [21]; [26]; [40]; [46]; [52] | 7% |
| Others | [44]; [91]; [94] | 6% |

as they recover from injuries, and SHS can help doctors determine if someone is at risk of poor balance or falling. Gyroscopes, accelerometers, and fitness watches are among the SHS devices that can detect any movement problems a patient may have [76], [77].

Semantic medical access (SMA), also called semantic management, is a special ability some SHS have that can monitor brain activity. People at risk of unusual brain activity can have brain scans uploaded to a cloud in real time. Devices that monitor the brain will alert emergency services if a problem arises, increasing the chance that any abnormalities will not turn into long-term brain injuries [78], [79]. These are only a few of the possible uses available for SHS. Fig. 7 provides an overview of the many other unique roles SHS can play in healthcare, and Table 2 lists the most commonly identified of these applications in the pool of reviewed papers

As shown in Table 2, 85% of the reviewed papers addressed remote health monitoring, 20% were related to body or personal care, while 17% connected SHS to the environment and smart cities. The large proportion looking at remote health monitoring demonstrates how interest in the topic has spiked in recent years. Both drug administration and SMA were mentioned in 7% of papers, and 6% handled other applications.

## VIII. CLASSIFICATION BY SECURITY TECHNIQUE

Since security and privacy have become important in SHS, many techniques have been developed to keep those systems secure. Fig. 8 illustrates which techniques were used in the reviewed papers. It is interesting to note that no one technique is a standout, and there remains a wide variety of techniques used in SHS. This variety can almost be thought of as a secondary security feature for SHS, since not all SHS can be handled in the same way. However, it is also possible see the variety in the opposite way, as a lack of universal techniques in SHS security could mean that some SHS are not as secure as others. The rates of use of different security techniques in the papers fall within a very small range. E-health gateways are the most common, yet only 12% of the reviewed papers referenced these. Most of the other security techniques accounted for less than 6% of the papers, and the top 5 most common techniques made up just under half of the overall total.

## IX. COMMON ATTACKS IN SHS

SHS security breaches can lead to life-threatening incidents, so ensuring security and privacy is extremely important. Healthcare providers are aware of the danger that SHS security breaches could cause, and fear of those breaches is slowing the adoption of SHS in medicine. Fortunately, many common attacks on SHS have been identified, and effective countermeasures to those attacks are recommended in the reviewed papers.

Attacks against SHS can generally be classified into four primary categories based on their targets: 1) attacks against the healthcare physical devices, 2) attacks on communication between healthcare devices, 3) attacks against healthcare providers or equipment manufacturers, and 4) attacks against patients. Table 3 presents the most commonly mentioned SHS attack types in the reviewed papers, as well as their potential countermeasures.

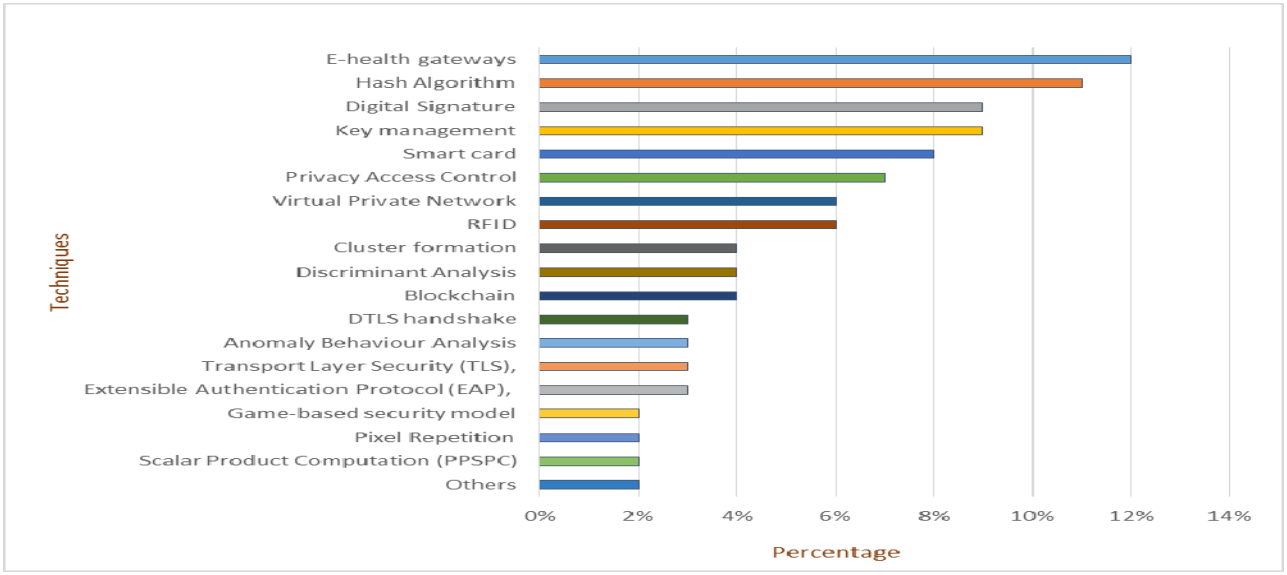


**FIGURE 8.** Classification by security technique.

## X. DISCUSSION

### A. HOW CURRENT RESEARCH HANDLES SHS SECURITY AND PRIVACY CHALLENGES

The three major concerns in smart healthcare are protecting access to data, ensuring the integrity of those data, and moving the data around. Different types of data have different formats and wavelengths, and different types of IoT devices and sensors collect data differently. Although the goal of a smart healthcare system is relatively simple, to centralize and manage protected data, the actual implementation of such a system is difficult. The methods required to handle data properly can change due to advances in technology, pressure from hackers, new discoveries in biology or chemistry, and any number of other variables. Maintaining data integrity in crowdsensing systems is important, and such integrity can be compromised either by attackers or by a breakdown in data storage. Alamri et al. explored mobile crowdsensing, which is an emerging technology that has applications in smart healthcare systems operating with IoT [59]. Sensors in distributed systems can capture many types of information, including personal health information. Two different methods are introduced to ensure data security, one for each potential security weakness. The effectiveness of these methods is shown by a security analysis and extensive simulations.

Traditional public keys aren't useful for IoT devices because of the high computational resources needed to handle them. Chaudhary et al. developed a lattice-based public key cryptosystem for the security of smart healthcare systems [60]. Lattice-based cryptography uses machine learning to solve NP-hard cryptographic problems and can handle multiple different types of encryption. Performance analysis of this technique proves that it is more than one order of magnitude faster than traditional cryptography in some cases. The authors acknowledge that the method is vulnerable to side channel attacks, where hackers infer attack vectors through the system implementation, and this is an open area that needs improvement. Some SHS are already experimenting with this technology, however, because it is more secure than traditional approaches.

Data transfer in the can could be very slow, and any lack of access to the cloud could potentially be life-threatening in hospitals. Kumari et al. use fog computing as an e-health gateway technique to link the cloud and IoT devices [64]. The technique was created to rectify some serious issues when IoT devices relied solely on the cloud. Fog computing is a distributed system like the cloud, but it processes data locally. This is a major advantage over a traditional cloud in terms of security because local processing can filter out confidential parts of medical data before they are sent to the cloud. The most sensitive data are kept on local servers. Wearable biosensors, personalized medical devices, and transmitters can all have data filtered this way.

Hiding patient information is an important part of SHS. Esposito examines a persistent problem when storing healthcare data: the ability to identify people based on those data [61]. Healthcare systems remove personal information that directly identifies patients, but they often also use internal IDs that can identify patients indirectly. Dynamically changing these IDs within a system is an underutilized strategy to prevent patient identification, and this can greatly enhance data security.

Generic IDs have been used to identify patients since the mid-1980s, but the concept of enhancing security with dynamic ID changes is recent. Dynamic IDs are managed by a subsystem of encrypted pseudonyms, providing multiple additional authentication levels based on anonymity.

Hiding patient information and maintaining anonymity can be done in multiple ways, and it is possible to create a reversible system, as described by Ueshima *et al.* [73]. It is possible to encode patient information as images, then add

**TABLE 3.** Common SHS attack types and countermeasures.

| Attack or Threat | Description | Countermeasure |
|---|---|---|
| Unauthorized access | Attacker gains access to a system by using another authorized user's credentials | Encrypt system information, use biometric identification or two-factor authentication |
| Routing attacks | Attacker modifies the route of traffic to a new destination | Implement secure routing algorithms |
| Message disclosure | Attacker targets sensitive information disclosure to access a patient's log file | Encrypt links and the network layer |
| Message modification | Attacker modifies messages between a patient and healthcare provider | Use hashing and digital signatures |
| Eavesdropping | Attacker listens to information through an open SHS communication channel [86] | Use encryption, segmentation, and implement network access control (NAC) |
| Replying attack | Attacker forwards modified information after eavesdropping | Use encryption, segmentation, and implement NAC |
| Compromised node attack | Attacker hacks into openly deployed sensor nodes and injects false information | Use symmetric key security algorithms |
| Denial of service (DoS) attack | Attacker generates so much network traffic that the SHS halts; generally caused by a compromised node [87] | Use encryption and an intrusion detection system, build redundancy in infrastructure, and use region mapping, authentication, and egress filtering |
| Hello flooding | Attacker uses a compromised node with high transmission power to compromise all of its neighbors | Use multi-path, multi-base data forwarding, identity verification protocols, and cryptography |
| Black and gray hole attack | Attacker inserts a malicious node into a network that changes routing tables so that neighboring nodes send the compromised node all their data. Black hole attacks don't reply to the neighboring nodes; gray hole attacks reply with non-critical data. | Use a time-based threshold mechanism, track pending packet tables and node rating tables, and make sure all nodes have different IDs |
| Sybil attack | Attacker uses a malicious sensor that masquerades as multiple sensors to modify the routing table | Validate sensors at a central authority or by using sensor graph connectivity characteristics |
| Social engineering | Attacker influences users to reveal information or perform an action that benefits the attacker. | Raise awareness of security concerns through training, auditing, and adequate security policies |

further encoding by permuting and replacing pixels. This permutation and replacement can then be reversed to restore the original image and data. This technique is useful for medical image data, such as MRI and CT scan results. Most medical data encryption doesn't focus on images, but images can hold sensitive information that is an essential part of patient privacy, so any robust SHS should have some form of image encryption.

There is more than one way to encode medical images reversibly, as demonstrated by Parah *et al.* [65]. Encoded medical images can be attacked and forcibly decoded in several ways, so doing a deep encode that considers these attack vectors results in a coded image that looks very similar, computationally, to the original image. Although the coded image looks like the original image after analysis, a hacker cannot get any useful information from the image itself. This technique relies on precise manipulation of pixels and spreading tiny pieces of encoded data across multiple pixels at once.

Pirbhulal et al. examined how biometric security is finding a place in securing tele-health data and how this security can be integrated into the IoT [66]. Biometric readings from smart devices are converted into unique identifiers that are later processed as data. The technology has been shown to be effective on the small scale but needs more expansive testing to prove its worth on a larger scale. The first version of the system can handle ECG signals, potentially warning patients and doctors of problems before symptoms appear. One lingering issue with this system is that recorded signals from the human body always have some extra noise associated with them, and it can be difficult to remove the noise without changing the important signals and losing data.

Tracking time stamps on healthcare data is another important part of SHS integrated with IoT, according to Fan *et al.* [62]. Since IoT relies by nature on distributed systems, it is essential to synchronize data at every point. Failure to do so could result not only in incorrect timestamps, but also in problems in scheduling or other administrative functions in healthcare. Blockchain-based time synchronization has been put forward as a way to safely synchronize these sensitive data. The model for a secure blockchain contains public and private nodes, identified by unique IDs, and data are verified by multiple nodes before being added permanently into the system. The system overhead is too large to be of use at this time in healthcare, but a reduction in the overhead, relative to the amount of data, will likely make it viable in the future.

SHS also can integrate elements that make the lives of providers and patients easier, not just data strategies. Smart technology can be used to make alarms in hospitals easier to tolerate while still preserving their sense of urgency, a breakthrough discovered by Greer *et al.* [88]. Simple alarms are uninformative because they sound the same regardless of the condition to which they alert medical personnel. People can become desensitized to the sound after they hear it repeatedly at the same volume, as well, so monotonous alarms can lose effectiveness over time. Smart systems can regulate the volume of alarms based on the level of background noise, keeping people sensitized to them. They can also use multiple types of sounds to give physicians more information about what is happening. Smart alarms have already been proven to have a positive impact on the ICU, but they aren't yet common in hospitals.

SHS are also sparking changes in the way hospitals are run, as Ilin et al. describe [89]. With the interconnectivity of the Internet of Things, the ability to offer value-based and personalized medicine is increasing quickly. People can track their own health, and the relative value of medical procedures is becoming more transparent. The amount of data involved is massive, and automation through a smart hospital is becoming a priority. Successful implementation improves existing procedures while leaving room for advancement and reducing costs. The business model must be client-centric, so this particular advance in smart healthcare, if successful, could have a ripple effect throughout the business world.

Another concept gaining prominence in the smart healthcare space is data fusion, which combines multiple types of data to create high-quality information. Jararweh et al. explore this possibility with an experimental framework [90]. Handling data in this way reduces network traffic and makes it easier to parse and organize. Environmental monitoring, which is common in IoT, creates a massive amount of data, and this fusion technique helps to separate sound from noise. There are many potential ways to implement fusion, and the more complex the process, the higher the likelihood that data will be lost. Healthcare sensor data may be handled with multiple types of fusion, depending on how complicated those data are.

Authentication, authorization, and access control have gained a great deal of attention in SHS research. Zhang et al. propose a complete SHS with multiple levels of authentication and access control [55]. The authors focus on strictly controlling access to their healthcare system, rather than on complex encoding or data manipulation within the system. They use a three-step validation process, consisting of a secure sign-in, validation of records, and aggregation of records. Patients remain the owners of their data, and their data are transmitted to a storage center where only their doctors and medical providers can access them. The system uses unique IDs internally to identify data, but the scheme is relatively simple compared to the complex authorization protocols.

Some of the current directions in research in security and privacy of SHS do not directly relate to healthcare systems but cover methods that can be applied to these systems. In fact, a discussion of contributions to healthcare security and privacy, since the field is relatively new, would not be complete without addressing these concepts. There are several other valuable studies in the pool of reviewed articles, but most address similar concepts, techniques, or methods to those presented in this section, so they are not included here. Figure 9 presents common SHS issues and recommended solutions. In addition, Table 4 in the Appendix gives an overview of the papers with the greatest contribution.

### B. OPEN RESEARCH CHALLENGES IN SHS SECURITY AND PRIVACY

SHS security is emerging as its own integrated area of study, distinct from other types of data and healthcare security. The explosion of interest and research in recent years has inspired a lot of progress in the field, but the general field is still nascent [80], [85]. There are many open challenges that require more research attention, and there will likely be many more as SHS evolve over time. Some important research challenges are listed below.

#### 1) CONFIDENTIALITY

Keeping health information confidential, due to the vulnerabilities of wireless networks and the unique hardware of sensors, remains difficult. There is no single solution that can work for all types of sensors, and even broader solutions, such as those in the upcoming 5G networks, are not foolproof. Maintaining the privacy of patients and their healthcare providers is essential, however, and sometimes their personal safety can be impacted if that confidentiality is breached.

#### 2) DATA FRESHNESS

SHS sensors must always transmit up-to-date data to healthcare providers. It's important to check the status of system nodes periodically, as well as to get information from sensors at regular intervals. Determining how far apart these intervals should be poses a challenge because making calls for new information too frequently could overtax the network. Not making calls frequently enough, however, could put patients in danger if sensors don't transmit a problematic status.

#### 3) AUTHENTICATION

Sensors can be built in a variety of configurations, requiring unique software and hardware, so making sure that the system is getting data from and sending data to an authorized sensor can be difficult. Universal standards of communication or design for sensor types are lacking, so SHS cannot always adapt well to new types of sensors. Loosening authentication rules in response could put patients at risk.

#### 4) RESILIENCY

Sensors and servers must have the ability to recover from errors as quickly as possible to minimize the amount of

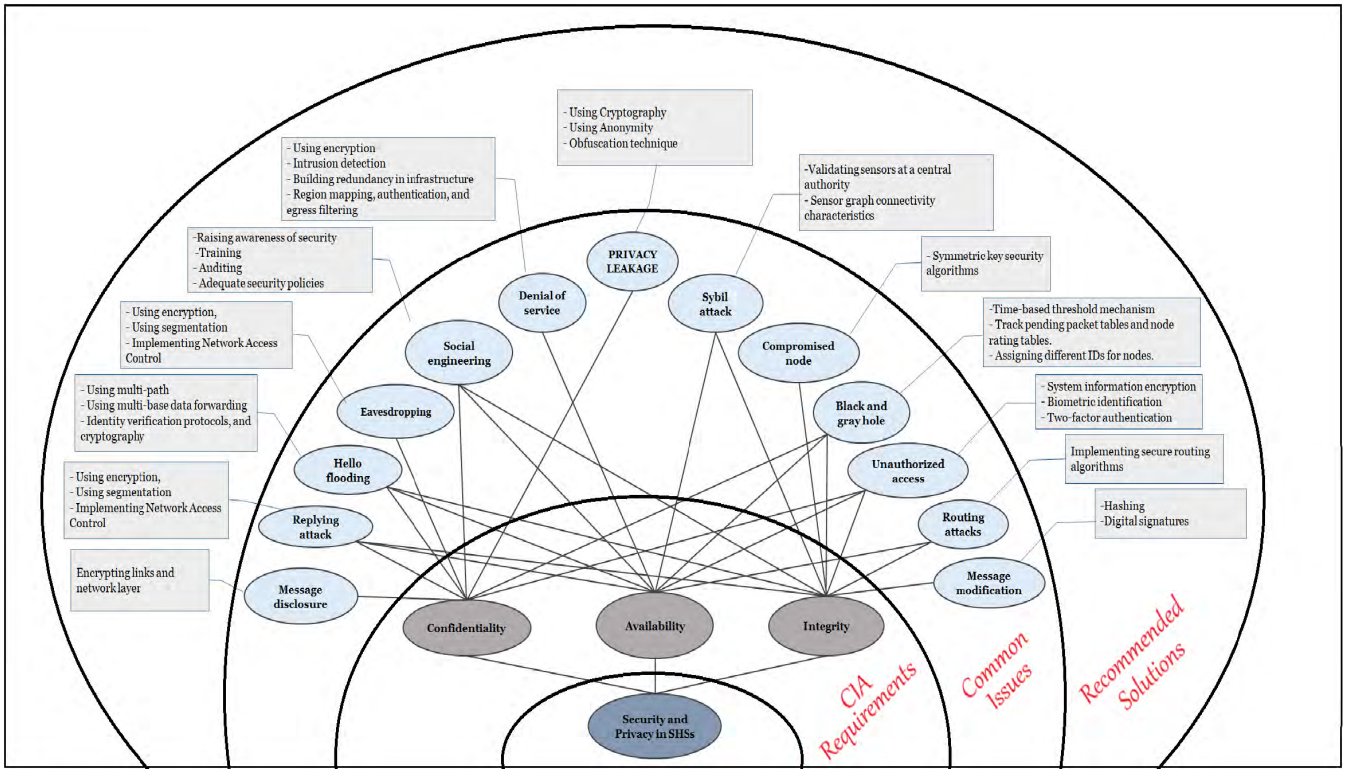


**FIGURE 9.** Common SHS issues and recommended solutions.

time that patients are not monitored. It is possible to test sensors and servers, but some hardware cannot include backups because of how they are built, while others are inherently fragile. Designing servers and sensors that are resilient regardless of their physical form is still challenging.

### 5) SELF-HEALING

SHS sensors should one day have the ability to identify problems such as outages, link failures, and hardware problems. They should also be able to diagnose and heal those problems automatically. The high variation in sensor technology and requirements makes this an open problem. It is one of the most complex research questions concerning SHS because it involves developing new technology for both hardware and software.

### 6) FAULT TOLERANCE

SHS components should be able to continue functioning if part of the system fails or if power is cut off. Backup sensors are one possible solution to this, but this is not always possible, and engineering fault tolerance in life-critical systems can save lives. This challenge is based more on how sensors operate, rather than on how they work internally, although keeping the internal workings robust is also important.

### 7) AUTHORIZATION

Ensuring that only the proper people have access to a patient's information is an important ongoing security concern. This is linked to information confidentiality, but it is slightly different because confidentiality can be broken even if authorized users are the only ones with access to information.

### 8) AVAILABILITY

The historical data and current vitals of patients should always be available to them and to the examiner at any location and time. In addition, the servers and sensors should never go down, and information should always be in the correct format. Based on current technology and scientific understanding, these ideals of operation are likely unattainable, but advances in other fields, such as superconductors or quantum computing, may change that outlook.

### 9) NON-REPUDIATION

Two securely authorized and contracted parties should not have any trouble accessing data or verifying that the data came from each other. Digital signatures are the current process for ensuring information integrity, but some types of sensors do not know how to process signatures or lack enough power to do so.

### 10) ENERGY LIMITATION

Although sensors rely on a certain amount of processing power, there are instances in which using less energy is preferable, such as when sensors are implanted in the body. Implanted sensors also need to have enough power to remain active for a long time, preferably the average duration of a diagnosis, because replacing them is painful and expensive. Finding a balance between the energy needed to run and

the energy that a patient can tolerate is difficult and likely different for every type of sensor.

#### 11) MEMORY AND COMPUTATIONAL LIMITATIONS

SHS sensors usually have a small physical size, which means that their memory capacity and computational power are also small. Security algorithms for these sensors must be able to function with very little memory without interrupting the functioning of the sensor. Most current security algorithms are far too large to work well with such limited resources, so new computational approaches are needed.

#### 12) MOBILITY

SHS sensors are generally quite mobile, since many are designed to be attached to the body in some way. This means that the sensors can routinely move in and out of wireless networks through areas that could interfere with transmissions, have trouble transmitting if they are moved a certain way, or become detached from a patient. All these possibilities need to be addressed when designing hardware or software for sensors.

#### 13) SCALABILITY

SHS networks must be able to grow bigger or smaller depending on patients' needs. Modifying the system should not compromise the existing system, and new sensors should integrate into an existing system. Once again, variations in sensor technology can make this difficult, and limitations on network traffic can also pose problems.

#### 14) ALGORITHMS

Perhaps the biggest open challenge is the design of security algorithms for sensors and servers that are lightweight enough to work with very limited processing power but robust enough to ensure data security. Some security algorithms require a lot of memory, and adding encryption to the algorithm, which is a requirement in SHS, further increases the memory footprint. New security concepts are needed in algorithms, because they are the most common area of attack.

### C. SUGGESTIONS FOR FUTURE RESEARCH

Analysis of the reviewed papers has shown that there are some useful directions for further SHS research. While all these suggestions would be useful for SHS privacy and security, they may also be useful in other emerging healthcare-related fields.

#### 1) FOG COMPUTING

Cloud computing is useful to SHS because it allows for distributed networks, but fog computing may be better suited to the demands of SHS. Fog computing systems have better privacy controls and are more cost effective than traditional cloud computing. They are also more resilient in the case of failures and have lower latency. The decentralized nature of fog computing makes processing more efficient and allows divisions between remote and local processing.

#### 2) PROTOCOL STANDARDIZATION

Communication in SHS is critical, so finding a balance between speed and content is important. This is complicated by the many protocols available through the many different types of sensors. Standardizing the protocols used to communicate between different sensor types would allow many different sensors to work together seamlessly on the same network. Standardized protocols could also be optimized to transmit data at appropriate times without clogging the network with unnecessary requests.

#### 3) MACHINE LEARNING

Data produced by SHS sensors are often noisy, redundant, and unstructured. Sensors also produce a lot of data in a short amount of time, so parsing the signal from the noise is a crucial step in deciphering the data. Machine learning algorithms could potentially be trained to understand sensor data and pick out the important information from everything else the sensor transmits. As these algorithms learn, they may also be able to reduce the number of necessary sensors for gathering data and the amount of data that healthcare practitioners must go through manually.

#### 4) OPTIMIZING ENERGY

Since there is a limit to how much processing power sensors have, there is also a limit to how long they can last and how much energy they can use. Energy usage and consumption in SHS sensors is far from optimized, so designing lightweight algorithms and efficient hardware should be a priority. One way that future SHS could reduce the energy load on sensors would be to place algorithms that require a lot of computational power on PD.

#### 5) BLOCKCHAIN

The ability of blockchain to link record lists through cryptography could revolutionize security and privacy in SHS. The problem currently holding back an SHS from implementing blockchain is its high computational requirements. If it were possible to make blockchain functionality more lightweight, a new level of encryption could be added to SHS that would be very difficult to break. Blockchain records contain timestamps and hash functions along with their data, so attackers would need to break through the SHS and the blockchain before getting to important information.

#### 6) SMART GATEWAYS

Smart gateways create a secure entry point to improve authentication and authorization of data. These gateways are also resistant to denial of service attacks and any other attack that relies on unauthorized users sending data, such as a routing attack. Smart gateways could potentially consolidate data from many devices, handle some parts of network routing, and increase security all at once.

#### 7) TRUST MANAGEMENT

Although nodes on a network should be able to trust other nodes on that network, this is not always advisable since

attackers can mimic trusted nodes to gain access to data. Trust management refers to the degree to which one node can trust another. All nodes in a network are dependent on each other to process and transmit data properly, so it is important that nodes know how to recognize each other and can react if one or more are compromised.

## XI. CONCLUSION

Data security and privacy has been a concern since the beginning of the digital age. As technology evolves, the precise nature of these concerns changes. Nowhere is this more obvious than in the Internet of Things, as the number of smart devices has increased exponentially in recent years. The advent of wearable technology, as well as advances in smart technology, has spawned the concept of smart healthcare systems. These systems, in theory, can store and analyze private healthcare information and keep people better informed of their own health in real time. The privacy and security of healthcare information is a particularly delicate subject, however, so keeping people's data safe is a primary concern of any potential smart healthcare system. At the same time, it is important to make these systems maintainable, since they must change as technology does if they are to remain relevant.

The direct application of IoT principles to smart healthcare is still in its infancy, and there are very few examples of SHS fully integrated with the IoT. The few trailblazers currently available will likely start a revolution in how healthcare data are managed. Perhaps most importantly, it will change how people are able to access information about their health, since the Internet of Things connects many diverse applications and technologies. Healthcare integration with the Internet of Things relies on both old and new technology. Since there will undoubtedly be improvements in both hardware and software in the coming years, the future of healthcare will likely look very different. The foundational concepts being pioneered right now will continue to bolster new developments, and although there are some significant questions that must be answered right now, there is no reason to think they will not be solved in the future. This is not to say, of course, that the prospect of a smart healthcare system is a pipe dream. Constant innovation in the field is, and will continue to be, critical for the systems to remain relevant. While the responsibility for the first generations of smart healthcare systems will likely be on software developers and medical professionals, some of that burden will likely shift to patients over time, and partaking in new systems may confer significant advantages. Ideally, data security and adoption of secure privacy measures will evolve along with smart healthcare systems, but no matter how complex and secure a system is, the patients who rely on them will always have a direct impact on security.

This paper critically reviewed research articles that addressed security and privacy in SHS. Doing so has shown the distribution of work on security and privacy. Distributions and categorizations were provided based on publication venue, publication year, objective, application domain, and security technique. In addition, the most common security attacks in SHS are summarized, along with their suggested countermeasures. Furthermore, an analysis of the ways current research handles SHS security and privacy is provided. Open research challenges are discussed, as well as directions for future research.

## APPENDIX

**TABLE 4.** Overview of the top contributed papers.

| Purpose | Reference |
|---|---|
| Use of smart card for secure identification and transmission of health information. | 17 |
| Medical data authorization and recovery in case of lost token. | 18 |
| Secure communication of medical data through protocol encapsulation and pre-shared keys. | 19 |
| A lightweight encryption scheme for secure cloud-based medical communication. | 20 |
| Minimum privacy disclosure in case of an emergency scenario. This is achieved by implementing user-centric privacy access control so the medical user can define who can participate in the computation to process user's data. | 21 |
| Three-phase authentication of telemedicine system by utilization of a smartphone over a dynamic cloud computing. | 22 |
| A hybrid technique that aims to enhance the security, integration, and robustness of Electronic Medical Records (EMRs). | 23 |
| Energy-efficient and secure key management hybrid scheme using sensor energy. | 24 |
| A hybrid technique for secure intra- and inter-WBAN communications. It also aims to provide energy efficiency to different sensor nodes. | 25 |
| Remove overhead with server key distribution and provide securely encrypted communication. | 26 |
| A three-phase encryption scheme for secure, efficient key management. | 27 |
| Implementation of a model for SHS depending on the available resources, balancing energy and algorithm processing. | 28 |
| Secure, efficient authentication and authorization of medical IoT through distributed e-health gateways. | 29 |

| | |
|---|---|
| A lightweight homomorphic encryption algorithm based on a scrambling matrix. | 30 |
| Implementation of smart e-health gateways has improved the security, efficiency, scalability, and reliability of SHS. | 31 |
| Hybrid sensing network, on zero power RFID-based transmission, is implanted to collect real-time vitals. The security is enhanced by implementation of a VPN between the mobile devices and gateways. | 32 |
| A low-cost, secure communication system for medical healthcare. In addition to various security protocols, it allows dynamic assignment of doctors to patients. | 33 |
| Secure end-to-end communication between the sensing nodes and remote healthcare centers through gateways. | 34 |
| A lightweight security management protocol that establishes a secure end-to-end communication channel between a resource-constrained node and a remote entity. | 35 |
| Provide a high level of privacy and security for patient data in semi-trusted cloud using encryption and cryptography. | 36 |
| Lightweight Elliptic Curve Cryptography (ECC) is implemented for secured transmission and authentication in SHS. | 37 |
| Reduce latency and energy consumption while improving the performance and security of medical communications. | 38 |
| An infrastructure for a biometrics-based end-to-end security solution for medical IoT. | 39 |
| The blockchain allows nodes to share information securely using advanced IEEE 802.15.6 protocol for authentication. | 40 |
| A threat model and IoT framework consisting of four layers that can defend against known and unknown attacks. | 41 |
| Two communication channels to address authentication and confidentiality. | 42 |
| A secure cryptosystem as a scheme for secure transmission using a password and smart card. | 43 |
| Distributing shared secret keys to less resource-constrained nodes in a secure and efficient way. | 44 |
| Hash-based message transmission for secure authentication and integrity management. | 45 |
| A lightweight cipher based on chaos-based scrambling for security in emergency events. | 46 |
| Double authentication for Human Body Communication (HBC) using biometric keys and the keys of wearable devices. | 47 |
| Grouping and Choosing algorithm along with key management. | 48 |
| Provide secure authentication on the cloud using encryption. | 49 |
| A lightweight and energy-efficient encryption algorithm provides secure communication among sensor nodes. | 50 |
| Smart gateways and an enhanced DTLS scheme provide security. | 51 |
| Apache Ranger with data encryption provides confidentiality of data. | 52 |
| A lightweight hash-based RFID authentication. | 53 |
| Fine-grained access control improves security, authentication, and confidentiality. | 54 |
| A parallel ECG provides accurate, effective biometrics. | 55 |
| Predefined location-based authentication for security. | 56 |
| Hybrid swarm optimization selects secure keys for encryption. | 57 |
| A four-layer cipher enhances the security of medical data. | 58 |
| Collaborative Path Hiding (CPH) as a basis for a patient privacy system. | 59 |
| Lattice-based cryptography provides data protection. | 60 |
| Ontology-based solution for increasing privacy. | 61 |
| The blockchain improves system security. | 62 |
| Reverse data hiding keeps patient data secure. | 63 |
| Three-layer healthcare architecture dependent on fog computing. | 64 |
| A lightweight algorithm avoids hacking with coded images. | 65 |

| | |
|---|---|
| A resource-efficient biometric security scheme based on key and entity identification. | 66 |
| Privacy-aware authentication and access control for security. | 67 |
| Modified blockchain based scheme that improves security. | 68 |
| Encode patient information as images, then add further encoding by permuting and replacing pixels. | 73 |
| Smart technology is used for alarms in hospitals that are easier to tolerate while still preserving their sense of urgency. | 88 |
| Data fusion, which combines multiple different types of data to create high-quality information. | 90 |
| Smart ambulance system using the concepts of big data and internet of things. | 92 |
| A lightweight authentication scheme for cloud-based RFID healthcare systems. | 95 |
| A joint resource-aware and medical data security framework for wearable healthcare systems. | 96 |
| A lightweight three-factor authentication, access control, and ownership transfer scheme for e-health systems in IoT. | 98 |

## REFERENCES

[1] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015. doi: 10.1109/ACCESS.2015.2437951.

[2] K. K. Goyal, A. Garg, A. Rastogi, and S. Singhal, "A literature survey on Internet of Things (IoT)," *Int. J. Adv. Netw. Appl.*, vol. 9, no. 6, pp. 3663–3668, 2018.

[3] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[4] ENISA. (2016). *Cyber Security and Resilience for Smart Hospitals [Report]*. Accessed: Jul. 12, 2019. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

[5] S. Agrawal and D. Vieira, "A survey on Internet of Things," *Abakós*, vol. 1, no. 2, pp. 78–95, 2018. doi: 10.5752/10.5752/p.2316-9451.2013v1n2p78.

[6] *Noncommunicable Diseases Country Profiles 2014*, World Health Org., Geneva, Switzerland, 2014.

[7] *World Population Ageing 2013*, Dept. Int. Econ. Social Affairs, Population Division, Austin, TX, USA, 2013.

[8] A. Chatterjee, *Chronic Disease and Wellness in America: Measuring the Economic Burden in a Changing Nation*. Santa Monica, CA, USA: Milken Institute, 2014.

[9] A.-M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen, "Smart e-health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2015, pp. 826–834. doi: 10.1109/CCNC.2015.7158084.

[10] K. Ullah, M. A. Shah, and S. Zhang, "Effective ways to use Internet of Things in the field of medical and smart health care," in *Proc. Int. Conf. Intell. Syst. Eng. (ICISE)*, Jan. 2016, pp. 372–379. doi: 10.1109/INTELSE.2016.7475151.

[11] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5, Aug. 2010, pp. 484–487. doi: 10.1109/ICACTE.2010.5579493.

[12] *IEEE Standard for Local and Metropolitan Area Networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, IEEE Standard 802.15.4-2011, IEEE Computer Society, 2011. doi: 10.1109/IEEESTD.2011.6012487.

[13] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, IEEE Standard 802.15.6-2012, 2012. doi: 10.1109/ieeestd.2012.6161600.

[14] *Smart Body Area Network (SmartBan); Low Complexity Medium Access Control (MAC) for SmartBAN 1*, document ETSI TS 103 325 (V1.1.1), ETSI, 2015, pp. 1–36.

[15] *Smart Body Area Network (SmartBan); Enhanced Ultra-Low Power Physical Layer. 1*, document ETSI TS 103 325 (V1.1.1), ETSI, 2015, pp. 1–13.

[16] A. Saboor, R. Ahmad, W. Ahmed, A. K. Kiani, Y. Le Moullec, and M. M. Alam, "On research challenges in hybrid medium access control protocols for IEEE 802.15.6 WBANs," *IEEE Sensors J.*, to be published. doi: 10.1109/JSEN.2018.2883786.

[17] G. Kardas and E. T. Tunali, "Design and implementation of a smart card based healthcare information system," *Comput. Methods Programs Biomed.*, vol. 81, no. 1, pp. 66–78, Jan. 2006. doi: 10.1016/j.cmpb.2005.10.006.

[18] B. Riedl, V. Grascher, and T. Neubauer, "A secure e-health architecture based on the appliance of pseudonymization," *J. Softw.*, vol. 3, no. 2, pp. 23–32, 2008. doi: 10.4304/jsw.3.2.23-32.

[19] F. Bagci, T. Ungerer, and N. Bagherzadeh, "SecSens—Security architecture for wireless sensor networks," in *Proc. 3rd Int. Conf. Sensor Technol. Appl. (SENSORCOMM)*, Jun. 2009, pp. 449–454. doi: 10.1109/SENSORCOMM.2009.74.

[20] S. Alshehri, S. P. Radziszowski, and R. K. Raj, "Secure access for healthcare data in the cloud using ciphertext-policy attribute-based encryption," in *Proc. IEEE 28th Int. Conf. Data Eng. Workshops (ICDEW)*, Apr. 2012, pp. 143–146. doi: 10.1109/ICDEW.2012.68.

[21] R. Lu, X. Lin, and X. Shen, "SPOC: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 3, pp. 614–624, Mar. 2013. doi: 10.1109/TPDS.2012.146.

[22] Z. Siddiqui, A. H. Abdullah, M. K. Khan, and A. S. Alghamdi, "Smart environment as a service: Three factor cloud based user authentication for telecare medical information system," *J. Med. Syst.*, vol. 38, no. 1, p. 9997, 2014. doi: 10.1007/s10916-013-9997-5.

[23] M. L. M. Kiah, M. S. Nabi, B. B. Zaidan, and A. A. Zaidan, "An enhanced security solution for electronic medical records based on AES hybrid technique with SOAP/XML and SHA-1," *J. Med. Syst.*, vol. 37, no. 5, p. 9971, 2013. doi: 10.1007/s10916-013-9971-2.

[24] A. Ali and F. A. Khan, "Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, pp. 1–19, 2013. doi: 10.1186/1687-1499-2013-216.

[25] S. Irum, A. Ali, F. A. Khan, and H. Abbas, "A hybrid security mechanism for intra-WBAN and inter-WBAN communications," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 8, Aug. 2013, Art. no. 842608. doi: 10.1155/2013/842608.

[26] A. Alsadhan and N. Khan, "An LBP based key management for secure wireless body area network (WBAN)," in *Proc. 14th ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. (SNPD)*, Jul. 2013, pp. 85–88. doi: 10.1109/SNPD.2013.32.

[27] Y. S. Lee, E. Alasaarela, and H. Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," in *Proc. Int. Conf. Inf. Netw.*, Feb. 2014, pp. 453–457. doi: 10.1109/ICOIN.2014.6799723.

[28] M. Hamdi and H. Abie, "Game-based adaptive security in the Internet of Things for eHealth," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 920–925. doi: 10.1109/ICC.2014.6883437.

[29] S. R. Moosavi, T. N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, and H. Tenhunen, "SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways," *Procedia Comput. Sci.*, vol. 52, no. 1, pp. 452–459, 2015. doi: 10.1016/j.procs.2015.05.013.

[30] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proc. Int. Symp. Parallel Architectures, Algorithms Program. (PAAP)*, Dec. 2015, pp. 217–222. doi: 10.1109/PAAP.2015.48.

[31] A.-M. Rahmani, N. K. Thanigaivelan, T. N. Gia, J. Granados, B. Negash, P. Liljeberg, and H. Tenhunen, "Smart e-health gateway: Bringing intelligence to Internet-of-Things based ubiquitous healthcare systems," in *Proc. 12th Annu. IEEE Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2015, pp. 826–834. doi: 10.1109/CCNC.2015.7158084.

[32] L. Catarinucci, D. de Donno, L. Mainetti, L. Palano, L. Patrono, M. L. Stefanizzi, and L. Tarricone, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015. doi: 10.1109/JIOT.2015.2417684.

[33] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, "Human-oriented design of secure machine-to-machine communication system for e-healthcare society," *Comput. Hum. Behav.*, vol. 51, pp. 977–985, Oct. 2015. doi: 10.1016/j.chb.2014.10.010.

[34] S. R. Moosavi, T. N. Gia, E. Nigussie, A.-M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "Session resumption-based end-to-end security for healthcare Internet-of-Things," in *Proc. 15th IEEE Int. Conf. Comput. Inf. Technol.*, Oct. 2015, pp. 581–588. doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.83.

[35] M. R. Abdmeziem and D. Tandjaoui, "An end-to-end secure key management protocol for e-health applications," *Comput. Elect. Eng.*, vol. 44, pp. 184–197, May 2015. doi: 10.1016/j.compeleceng.2015.03.030.

[36] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015. doi: 10.1016/j.is.2014.05.004.

[37] S. K. Shankar, A. S. Tomar, and G. K. Tak, "Secure medical data transmission by using ECC with mutual authentication in WSNs," *Procedia Comput. Sci.*, vol. 70, pp. 455–461, Dec. 2015. doi: 10.1016/j.procs.2015.10.078.

[38] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, Nov. 2016. doi: 10.1016/j.future.2016.02.020.

[39] M. S. Hossain, G. Muhammad, S. M. M. Rahman, W. Abdul, A. Alelaiwi, and A. Alamri, "Toward end-to-end biomet rics-based security for IoT infrastructure," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 44–51, Oct. 2016. doi: 10.1109/MWC.2016.7721741.

[40] J. Zhang, N. Xue, and X. Huang, "A secure system for pervasive social network-based healthcare," *IEEE Access*, vol. 4, pp. 9239–9250, 2016. doi: 10.1109/ACCESS.2016.2645904.

[41] J. Pacheco and S. Hariri, "IoT security framework for smart cyber infrastructures," in *Proc. IEEE 1st Int. Workshops Found. Appl. Self-Syst. (FAS-W)*, Sep. 2016, pp. 242–247. doi: 10.1109/FAS-W.2016.58.

[42] K.-H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016. doi: 10.1109/ACCESS.2016.2638038.

[43] C.-H. Liu and Y.-F. Chung, "Secure user authentication scheme for wireless healthcare sensor networks," *Comput. Elect. Eng.*, vol. 59, pp. 250–261, Aug. 2017. doi: 10.1016/j.compeleceng.2016.01.002.

[44] M. A. Iqbal and M. Bayoumi, "Secure end-to-end key establishment protocol for resource-constrained healthcare sensors in the context of IoT," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Innsbruck, Austria, Jul. 2016, pp. 523–530. doi: 10.1109/HPCSim.2016.7568379.

[45] A. Alzubi and A. Sari, "Deployment of hash function to enhance message integrity in wireless body area network (WBAN)," *Int. J. Commun., Netw. Syst. Sci.*, vol. 9, no. 12, pp. 613–621, 2016. doi: 10.4236/ijcns.2016.912047.

[46] S. F. Raza, C. Naveen, V. R. Satpute, and A. G. Keskar, "A proficient chaos based security algorithm for emergency response in WBAN system," *Proc. IEEE Students' Technol. Symp. (TechSym)*, Sep./Oct. 2016, pp. 18–23. doi: 10.1109/TechSym.2016.7872648.

[47] S. Sen, "SocialHBC: Social networking and secure authentication using interference-robust human body communication," in *Proc. Int. Symp. Low Power Electron. Design*, 2016, pp. 34–39. doi: 10.1145/2934583.2934609.

[48] G. Manogaran, R. Varatharajan, D. Lopez, P. M. Kumar, R. Sundarasekar, and C. Thota, "A new architecture of Internet of Things and big data ecosystem for secured smart healthcare monitoring and alerting system," *Future Gener. Comput. Syst.*, vol. 82, pp. 375–387, May 2018. doi: 10.1016/j.future.2017.10.045.

[49] S. Patel, N. Singh, and S. Pandya, "IoT based smart hospital for secure healthcare system," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 5, no. 5, pp. 404–408, 2017. [Online]. Available: http://www.ijritcc.org, 2017.

[50] S. Pirbhulal, H. Zhang, E. Alahi, H. Ghayvat, S. C. Mukhopadhyay, Y.-T. Zhang, and W. Wu, "A novel secure IoT-based smart home automation system using a wireless sensor network," *Sensors*, vol. 17, no. 1, p. 606, 2017. doi: 10.3390/s17010069.

[51] P. M. Kumar and U. D. Gandhi, "Enhanced DTLS with CoAP-based authentication scheme for the Internet of Things in healthcare application," *J. Supercomput.*, pp. 1–21, Oct. 2017. doi: 10.1007/s11227-017-2169-5.

[52] P. K. Binu, V. Akhil, and V. Mohan, "Smart and secure IOT based child behaviour and health monitoring system using hadoop," in *Proc. Int. Conf. Adv. Comput., Commun. Inform. (ICACCI)*, Sep. 2017, pp. 418–423.

[53] P. Gope, R. Amin, S. K. H. Islam, N. Kumar, and V. K. Bhalla, "Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment," *Future Gener. Comput. Syst.*, vol. 83, pp. 629–637, Jun. 2018. doi: 10.1016/j.future.2017.06.023.

[54] S. Pal, M. Hitchens, V. Varadharajan, and T. Rabehaja, "Fine-grained access control for smart healthcare systems in the Internet of Things," *EAI Endorsed Trans. Ind. Netw. Intell. Syst.*, vol. 4, no. 13, 2018, Art. no. 154370. doi: 10.4108/eai.20-3-2018.154370.

[55] Y. Zhang, R. Gravina, H. Lu, M. Villari, and G. Fortino, "Pea: Parallel electrocardiogram-based authentication for smart healthcare systems," *J. Netw. Comput. Appl.*, vol. 117, pp. 10–16, Sep. 2018. doi: 10.1016/j.jnca.2018.05.007.

[56] I. Natgunanathan, A. Mehmood, Y. Xiang, L. Gao, and S. Yu, "Location privacy protection in smart health care system," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3055–3069, Apr. 2019. doi: 10.1109/JIOT.2018.2878917.

[57] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," in *Neural Computing and Applications*. Cham, Switzerland: Springer, 2018. doi: 10.1007/s00521-018-3801-x.

[58] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, Feb. 2019. doi: 10.1109/JIOT.2018.2854714.

[59] B. H. Alamri, M. M. Monowar, and S. Alshehri, "A privacy-preserving collaborative reputation system for mobile crowdsensing," *Int. J. Distrib. Sensor Netw.*, vol. 14, no. 9, pp. 1–12, 2018. doi: 10.1177/1550147718802189.

[60] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice based public key cryptosystem for Internet of Things environment: Challenges and solutions," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2018.2878707.

[61] C. Esposito, "Interoperable, dynamic and privacy-preserving access control for cloud data storage when integrating heterogeneous organizations," *J. Netw. Comput. Appl.*, vol. 108, pp. 124–136, Apr. 2018. doi: 10.1016/j.jnca.2018.01.017.

[62] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, "Blockchain-based secure time protection scheme in IoT," *IEEE Internet Things J.*, to be published. doi: 10.1109/JIOT.2018.2874222.

[63] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. M. Bhat, "A reversible and secure patient information hiding system for IoT driven e-health," *Int. J. Inf. Manage.*, vol. 45, pp. 262–275, Sep. 2018. doi: 10.1016/j.ijinfomgt.2018.09.008.

[64] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Comput. Elect. Eng.*, vol. 72, pp. 1–13, Nov. 2018. doi: 10.1016/j.compeleceng.2018.08.015.

[65] S. A. Parah, J. A. Sheikh, J. A. Akhoon, and N. A. Loan, "Electronic health record hiding in images for smart city applications: A computationally efficient and reversible information hiding technique for secure communication," *Future Gener. Comput. Syst.*, to be published. doi: 10.1016/j.future.2018.02.023.

[66] S. Pirbhulal, P. Shang, W. Wu, A. K. Sangaiah, O. W. Samuel, and G. Li, "Fuzzy vault-based biometric security method for tele-health monitoring systems," *Comput. Elect. Eng.*, vol. 71, pp. 546–557, Oct. 2018. doi: 10.1016/j.compeleceng.2018.08.004.

[67] Y. Zhang, R. H. Deng, G. Han, and D. Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things," *J. Netw. Comput. Appl.*, vol. 123, no. 12, pp. 89–100, Dec. 2018. doi: 10.1016/j.jnca.2018.09.005.

[68] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, pp. 1–17, 2019. doi: 10.3390/s19020326.
[69] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 18–28, Jan. 2018.
[70] T. Suzuki, H. Tanaka, S. Minami, H. Yamada, and T. Miyata, "Wearable wireless vital monitoring technology for smart health care," in *Proc. 7th Int. Symp. Med. Inf. Commun. Technol. (ISMICT)*, Mar. 2013, pp. 1–4, doi: 10.1109/ISMICT.2013.6521687.
[71] A. S. Go *et al.*, "Heart disease and stroke statistics–2013 update: A report from the american heart association," *Circulation*, vol. 127, no. 1, pp. e6–e245, 2013. doi: 10.1161/cir.0b013e31828124ad.
[72] A. B. de Luna and A. Genis, *Clinical Electrocardiography*, Chichester, U.K.: Wiley, 2012. doi: 10.1016/b978-1-59749-995-8.09975-0.
[73] H. Ueshima, A. Sekikawa, K. Miura, T. C. Turin, N. Takashima, Y. Kita, M. Watanabe, A. Kadota, N. Okuda, T. Kadowaki, Y. Nakamura, and T. Okamura, "Cardiovascular disease and risk factors in Asia," *Circulation*, vol. 118, no. 25, pp. 2702–2709, 2008. doi: 10.1161/CIRCULATIONAHA.108.790048.
[74] S. Mulroy, J. Gronley, W. Weiss, C. Newsam, and J. Perry, "Use of cluster analysis for gait pattern classification of patients in the early and late recovery phases following stroke," *Gait Posture*, vol. 18, no. 1, pp. 114–125, 2003. doi: 10.1016/S0966-6362(02)00165-0.
[75] S. Majumder, T. Mondal, and M. J. Deen, "Wearable sensors for remote health monitoring," *Sensors*, vol. 17, no. 1, p. 130, 2017. doi: 10.3390/s17010130.
[76] M. J. Deen, "Information and communications technologies for elderly ubiquitous healthcare in a smart home," *Pers. Ubiquitous Comput.*, vol. 19, nos. 3–4, pp. 573–599, 2015. doi: 10.1007/s00779-015-0856-x.
[77] N. Agoulmine, M. J. Deen, J.-S. Lee, and M. Meyyappan, "U-health smart home," *IEEE Nanotechnol. Mag.*, vol. 5, no. 3, pp. 6–11, Sep. 2011.
[78] A. Solanas, C. Patsakis, M. Conti, I. S. Vlachos, V. Ramos, F. Falcone, O. Postolache, P. A. Perez-Martinez, R. Di Pietro, D. N. Perrea, and A. Martinez-Balleste, "Smart health: A context-aware health paradigm within smart cities," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 74–81, Aug. 2014.
[79] B. Xu, L. D. Xu, H. Cai, C. Xie, J. Hu, and F. Bu, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1390–1392, May 2014. doi: 10.1109/TII.2014.2306382.
[80] C. Sharma and D. Sunanda, "Survey on smart healthcare: An application of IoT," *Int. J. Emerg. Technol.*, vol. 8, no. 1, pp. 330–333, 2017. doi: 10.1109/ACCESS.2015.2437951.2017.
[81] S. K. Verma, "Security and privacy issues in wireless ad hoc, mesh, and sensor networks," *Adv. Electron. Elect. Eng.*, vol. 4, no. 4, pp. 381–388, 2014. [Online]. Available: http://www.ripublication.com/aeee_spl/aeeev4n4spl_09.pdf
[82] P. Usha and N. Priya, "Survey on security issuses in WBAN," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 1, pp. 482–485, 2015.
[83] S. F. Qadri, S. A. Awan, M. Amjad, M. Anwar, and S. Shehzad, "Applications, challenges, security of wireless body area networks (WBANs) and functionality of IEEE 802.15.4/ZIGBEE," *Sci. Int.*, vol. 25, no. 4, pp. 697–702, 2013.
[84] S. Pathania and N. Bilandi, "Security issues in wireless body area network," *Int. J. Comput. Sci. Mobile Comput.*, vol. 3, no. 4, pp. 1171–1178, 2014.
[85] 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. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1110866516300482
[86] J. Liu and K. S. Kwak, "Hybrid security mechanisms for wireless body area networks," in *Proc. 2nd Int. Conf. Ubiquitous Future Netw. (ICUFN)*, 2010, pp. 98–103. doi: 10.1109/ICUFN.2010.5547221.
[87] T. V. P. Sundararajan and A. Shanmugam, "A novel intrusion detection system for wireless body area network in health care monitoring," *J. Comput. Sci.*, vol. 6, no. 11, pp. 1355–1361, 2010.
[88] J. M. Greer, K. J. Burdick, A. R. Chowdhury, and J. J. Schlesinger, "Dynamic alarm systems for hospitals (DASH)," *Ergonom. Des.*, vol. 26, no. 4, pp. 14–19, Oct. 2018. doi: 10.1177/1064804618769186.
[89] I. Ilin, O. Iliyaschenko, and A. Konradi, "Business model for smart hospital health organization," in *Proc. SHS Web Conferences*, vol. 44, 2018, p. 41. doi: 10.1051/shsconf/20184400041.
[90] Y. Jararweh, M. Al-Ayyoub, and E. Benkhelifa, "An experimental framework for future smart cities using data fusion and software defined systems: The case of environmental monitoring for smart healthcare," *Future Gener. Comput. Syst.*, to be published. doi: 10.1016/j.future.2018.01.038.
[91] J. Torous, G. Andersson, A. Bertagnoli, H. Christensen, P. Cuijpers, J. Firth, A. Haim, H. Hsin, C. Hollis, S. Lewis, D. C. Mohr, A. Pratap, S. Roux, J. Sherrill, and P. A. Arean, "Towards a consensus around standards for smartphone apps and digital mental health," *World Psychiatry*, vol. 18, no. 1, p. 97, 2019.
[92] A. Dumka and A. Sah, "Smart ambulance system using concept of big data and Internet of Things," in *Healthcare Data Analytics and Management*. New York, NY, USA: Academic, 2019, pp. 155–176.
[93] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Inf. Sci.*, vol. 479, pp. 567–592, Apr. 2019.
[94] A. E. Hassanien, M. Elhoseny, S. H. Ahmed, and A. K. Singh, Eds., *Security in Smart Cities: Models, Applications, and Challenges*. Cham, Switzerland: Springer, 2019.
[95] K. Fan, S. Zhu, K. Zhang, H. Li, and Y. Yang, "A lightweight authentication scheme for cloud-based RFID healthcare systems," *IEEE Netw.*, vol. 33, no. 2, pp. 44–49, Mar. 2019.
[96] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," *Future Gener. Comput. Syst.*, vol. 95, pp. 382–391, Jun. 2019.
[97] S. Ahmed, "Threats to patients' privacy in smart healthcare environment," in *Innovation in Health Informatics: A Smart Healthcare Primer*. Amsterdam, The Netherlands: Elsevier, 2019.
[98] S. F. Aghili, H. Mala, M. Shojafar, and P. Peris-Lopez, "LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT," *Future Gener. Comput. Syst.*, vol. 96, pp. 410–424, Jul. 2019.

**ABDULLAH ALGARNI** received the bachelor's degree from King Abdulaziz University, Saudi Arabia, the master's degree from Western Michigan University, USA, and the Ph.D. degree from the Queensland University of Technology (QUT), Australia, all in computer science. He was with QUT. He is currently an Assistant Professor with the Division of Information Technology and the Director of the Studies Department, Institute of Public Administration (IPA), Saudi Arabia. He has published several papers in top information systems journals and conference proceedings. His current research interests include social engineering, phishing, deception, and information security management.