






Review

Security in Wireless Body Sensor Network: A Multivocal Literature Study

Najm Us Sama ¹, Kartinah Zen ¹, Mamoona Humayun ^{2,*}, Noor Zaman Jhanjhi ^{3,*} and Atiq Ur Rahman ⁴

¹ Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan 94300, Malaysia

² Department of Information Systems, College of Computer and Information Sciences, Jouf University, Sakaka 72341, Al Jouf, Saudi Arabia

³ School of Computer Science (SCS), Taylor's University, Subang Jaya 47500, Malaysia

⁴ Faculty of Computer Information Science, Higher Colleges of Technology, Ras Al Khaimah Campus, Ras Al Khaimah 4793, United Arab Emirates

* Correspondence: mahumayun@ju.edu.sa (M.H.); noorzaman.jhanjhi@taylors.edu.my (N.Z.J.)

Abstract: The wireless body sensor network (WBSN) is a wireless communication that might enable 24/7 patient monitoring and health findings through the online platform. Although BSN design is becoming simpler, building a secure BSN seems to be more challenging than designing conventional solutions, and the recent study provides little guidance to designers and developers. The proposed study summarizes the multivocal literature study of security mechanisms for BSN. The investigation found 10,871 academic publications and 697 grey content; duplicates were removed, and selection criteria were employed, resulting in 73 academic papers and 30 grey publications. Various conventional security techniques, scope, and security contexts were used to classify the stated security solutions within each publication. It was crucial to inquire about the frequency of publications, research methods, security mechanisms, and contexts to answer the proposed questions. Our survey concludes that security methods and assessments are categorized into 15 categories, with the most frequently referenced being authentication and authorization; the majority of strategies concentrate on preventing and mitigating security breaches, with a limited number of works focusing on detection and recovery; and the techniques used to conduct the survey vary between the two types of publications. This evaluation might be the first step toward making the BSN platform more consistent by giving professionals and researchers a complete set of security strategies and methods. Experts will apply these solutions to fix security issues while establishing a trustworthy BSN after they have been identified through the process of discovering the most commonly utilized security solutions.

Keywords: body sensor network; security mechanisms; security solutions; multivocal literature review



Citation: Sama, N.U.; Zen, K.; Humayun, M.; Jhanjhi, N.Z.; Rahman, A.U. Security in Wireless Body Sensor Network: A Multivocal Literature Study. *Appl. Syst. Innov.* **2022**, *5*, 79. <https://doi.org/10.3390/asi5040079>

Received: 21 June 2022

Accepted: 4 August 2022

Published: 15 August 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Since individuals worldwide are concerned about their health, the body sensor network assists with collecting essential body details of an individual through sensing devices. Although the wireless body sensor network (WBSN) has elicited great interest in environmental and medical applications, safety and privacy are still significant issues [1]. Due to the fact that it is distant, there are possibilities for various challenges, such as lack of energy, degraded platform's capability, and fake concern. Furthermore, the data shared through the wireless body sensor network (WBSN) are subject to various harmful threats [2].

While the patient's status is transferred between the physician and patients, any intruder can intercept incoming packets between traversing via wireless signals and rebuild the results. This could put the lives of patients in danger. Any patient with a socially unacceptable condition should have their details handled carefully. As a result, we must

ensure that the confidentiality and anonymity of any type of information are protected and transmitted securely. As a result, different intrusion prevention techniques are needed to protect against these assaults. The guarantee of the security and safety of the information obtained has been critical. According to experts, BSN has been the target of numerous assaults in recent decades, ranging from specific functions to the overall network. As a result, experts continually develop new adaptations and combinations of traditional security procedures to defend against these assaults. Security is a significant issue for BSNs, according to surveys. Similarly, several studies [3–5] have revealed a general shortage of studies in BSN protection.

The scholars previously published systematic literature mapping (SLM) of BSN security features, highlighting the immensely unexplored skills and experience of scientific literature experts [6]. Although earlier surveys of security checks research exist for BSN [7,8], we could not find any that included grey literature (GLR). The article addresses this gap by conducting surveys of source papers in academics and GLR as well as discussing multivocal literature review (MLR) of security mechanisms in BSNs. According to the scholars [9], the most commonly used and approved description of GLR is literature obtained in all areas of government, academic institutions, companies, and economy, in both traditional and digital formats, which is not only governed by conventional publishers, i.e., where publications may not be the main activity of the manufacturing body. MLRs are a type of systematic literature review (SLR) that include knowledge from a range of resources, such as scientific research (i.e., academia “papers”) and corporate “grey” literature (i.e., blog posts, white papers, videos, presentations, etc.).

The proposed study is a multivocal literature study that was conducted on security methods for BSN. In total, the assessment discovered 10,871 academic publications and 697 pieces of grey content. Following the exclusion of duplicates and the adoption of selection criteria, the research obtained 73 academic articles and 30 grey articles. When classifying the specified security solutions inside each article, different standard security methodologies, scope, and security scenarios were evaluated. To obtain answers to the posed issues, it was essential to ask questions regarding the number of publications, the techniques of research, the safety procedures, and the contexts. The results of our survey demonstrate that security mechanisms and evaluations are divided into 15 categories, with authentication and authorization being the most commonly mentioned. The mass of strategies focuses on avoiding and alleviating security flaws, while only a small number of works focus on detecting and recovering.

By providing experts and researchers with a comprehensive collection of security tactics and procedures, this review could be the first step toward making the BSN framework more reliable. After researching the most often used security solutions, experts will use these solutions to fix security concerns and build a trusted BSN.

The following sections constitute the rest of this article: Section 2 summarizes the security issues confronting BSN; Section 3 highlights the related research; Section 4 discusses the article’s methodology; Section 5 outlines the findings; Section 6 identifies future research directions; Section 7 identifies application examples for our multivocal literature review; Section 8 discusses validity concerns; and Section 9 summarizes the findings.

2. Security in Wireless Body Sensor Network

A patient’s medical state can be monitored using telemonitoring systems. The rising expense of medical services, the increasing elderly population, and the rise in chronic disease patients worldwide are increasing demands for alternatives in the healthcare sector. Due to these challenges, conventional health care cannot achieve the needed flexibility. As a result, high-performance, low-cost, and appropriate care solutions are required. The wireless body sensor network (WBSN) is a wireless platform that allows sensors attached to a patient’s body to communicate to monitor the body’s essential parameters and surroundings. The use of wireless sensor nodes in public healthcare tracking opens doors for delivering superior patient care. For example, at-risk individuals with a background of

heart problems or aged individuals who live independently can be monitored using various sensors. These sensors allow physicians to diagnose diseases more efficiently by providing ongoing, long-term tracking in an invisible manner [10]. A body sensor network or BSN is a collection of sensors placed on the person's body to gather physiological signals [11].

In recent research and industry, the design and implementation of these WBSN approaches to health monitoring have received increased interest. This focus is primarily driven by the high cost of health care and recent advances in the manufacturing of micro-health applications and new technologies, such as the internet of things (IoT), contributing to the 5G main obstacles. An explicit approach to handling the basic software design and validation should be advantageous for building and maintaining these systems. At various spots, the sensors observe and compare the circumstances. Environmental (e.g., pollution levels, weather, and moisture) and essential human functions are typical examples (e.g., heart and brain signals). A WSN can sense, process, and communicate. To acquire data on the centralized environment, diverse WSN-based monitoring applications have been created in many application sectors. Defense applications [11], global warming tracking applications [12], applications in submarine networking [13], and applications in health monitoring [14] are only a few examples.

Regardless of these applications, security has become a significant challenge. The system must ensure the security and privacy of the collected individual health data. Decomposing activity results in an increase in the platform's flaws and renders it more complex to implement the security architecture. This has resulted in a number of BSN privacy discussions, the most important of which are discussed and taken in context hereinafter [15].

The developers in [16] suggested a secure platform based on heart rate frequency. They used the measurements of the inter-pulse periods to build binary patterns from the beats. In 8 s, they generated a 128-bit sequence using ECG records from the MIT-BIH arrhythmia dataset. As a result, they could minimize the time it took to generate a random sequence of bits. The fundamental issue of employing a heartbeat as a security measure is inconsistent over time. The person's health records should be protected to avoid information misuse, and the patients should be able to reach the practitioner at the appropriate time and without delay. Secure key management in WBAN (SEKBAN) is an innovative approach that addresses security issues at three stages. By constructing keys relying on the ECG signal, this suggested technique protects the data's privacy [17].

Depending on the ECG monitor, the researchers in [17] offer a body sensor network encryption and user authentication (BSN-EUA) approach. The BSN-EUA method provides fingerprint recognition for identity verification, and all of a person's health-related activities are logged on the handset. The descriptive properties of the electrocardiogram (ECG) are employed as a recognized fingerprint feature all through the access control mechanism. When modest alterations are required to modify the cryptography technique on the sensor's side, rapid social security protocols are provided across all approved sensors. The research results reveal that the proposed method meets the required privacy standards. The authors in [18] presented a symmetric security technique for WBAN that uses the ECG wave to produce and deliver the secret key. WBAN nodes should sense the ECG data using a synchronization approach to make the security key. The stability of the suggested method is demonstrated using formal and informal security assessments.

Any breach would not only harm the patients' security, but it might also put their lives at risk. For example, providing physicians with a misleading ECG sensor readout may result in inappropriate actions that are potentially hazardous to patients. When a mechanical insulin pump receives a faulty or corrupted signal, it may deliver an excessive amount of insulin into the patient's veins. WBAN is vulnerable to a wide range of assaults, from interior to exterior, passive to active.

In terms of addressing potential security issues, all of the studies listed above reference security measures that range from conventional security mechanisms, such as encryption and authentication to intrusion detection systems (IDSs) and trust management solutions

(TMSs). For WBANs to be a success and widely adopted, developers must focus on security solutions and authentication mechanisms for data and services.

3. Related Work

Two research projects have investigated the work performed on the security services of BSN. WBSN and its infrastructure were discussed extensively by the researchers in [19]. They discuss the safety and security concerns, provide alternatives to the security threats, and outline the authentication technique employed.

A thorough study of the WBAN technology exists in terms of safety and privacy vulnerabilities, as well as their solutions, followed by suggested research approaches and unresolved questions [20]. The authors review the most recent WBANs signcryption security mechanisms in order that the academic community benefits from the study efforts, which include the identification and comparison of all WBANs sector signcryption mechanisms [21]. These results will be used to compare the various signcryption security methods that are already available on the market and to evaluate the previously suggested solution for WBANs. A few of these major research challenges, in which researchers confront to create the security mechanisms of WBANs, are also highlighted in the survey.

The authors of [22] provide a comprehensive review of conventional routing protocols in WBSN as well as their benefits and drawbacks, thus further providing a framework for improving a more efficient routing protocol in WBSN. The authors only focus on BSN routing protocols and ignore the authentication scheme. The authors of [23] aim to convey the latest advances in various facets of wireless body area sensor networks, including communication structures, WBASN applications, coding frameworks, security concerns, and energy-efficient routing algorithms. They attempted to cover the most recent advances, while also discussing the radio channel technologies for these networks. Moreover, future perspectives and obstacles are mentioned.

A comprehensive analysis of WBSN routing algorithms based on current specifications and articles is proposed [24]. Initially, the authors present an in-depth understanding of WBSN and its associated technology. Following that, the distinguishing features of WBSN and its approaches are demonstrated. Moreover, routing challenges are investigated as a source of motivation for forthcoming WBAN advancement. Traditional routing protocols are temperature aware, QoS aware, security-aware, cluster-based, cross-layered based, and posture-based. In addition, 53 publications that focus on the most significant parameters are examined, such as energy consumption, end-to-end delay, temperature rise, mobility, metrics, and packet delivery, but not latency, path loss, stability or energy efficiency. Moreover, this research is not a multivocal study.

Previous research thoroughly modeled security measures in WBSNs based on ALR. This paper is a substantial extension that covers a broader range of topics (not only techniques) and considers GLR.

4. Research Protocol

Multivocal literature review (MLR) [25] is a SLR survey that accepts data from ALR and GLR. This research aims to act as a bridge between academic papers and industrial/practical expertise. Whereas solely basic research studies cannot provide significant determinations about complex information and a global or state background for distinctions in implementation, MLR stands in the deficit. Not all SLRs would even have to include GL toward becoming MLRs. Still, if the scope is expanded, including GL, and tends to add value and benefits to the studies, scientists might also consider reviewing MLR.

A substantial limited scholarly literature is available on BSNs [26–28]. Since the coverage of BSNs is very diverse and open to interpretation, our findings suggest that GL can provide substantial benefits to experts along with scholarly literature. Several researchers, companies, and internet sources missed GL in previous studies. These sources can include scientific research and publications and a broad range of unpublished non-research literature, including blog posts, white papers, presentation videos, and tools

available online for free. Moreover, the BSN is a research area of both scientific and practical concern, where studies on the topic have been dramatically broadened over the last decade.

Furthermore, to my knowledge, very few MLR studies have been conducted on this problem to date. As a result, we decided to perform research using Garousi's MLR recommendations. The following six steps are considered during the MLR process:

- Define the main study question, search process, and search query;
- Describe inclusion/exclusion standards;
- Search the relevant databases;
- Filtration techniques among the established publications;
- Review of articles that passed the filtration process;
- Summarize the results and conclusions.

The following subsections cover the article's design and the results of its implementation.

4.1. Objective and Research Questions

The whole MLR aims to gather and categorize security mechanisms and assessments for BSNs that have been suggested in academia and GLR. Herein, we offer a variety of research questions (RQs) to assist us in accomplishing the objectives. Most of the research is devoted to acquiring, evaluating, and categorizing security mechanisms (RQ1 to RQ4). Moreover, we developed several RQs concerning the content itself, as this is the initial attempt to thoroughly evaluate academic and grey articles (RQ1 to RQ4). The research questions are as follows:

RQ1: How much has the number of security-related BSN articles changed over the period?

RQ2: Which research approaches are used to investigate BSN safety?

RQ3: In BSN, which security strategies and security scope have been introduced?

RQ4: With what security domains have work been conducted?

4.2. Selection Process

In this research, the essential processes for exploring and evaluating publications in the multivocal analysis process are demonstrated in Figure 1. The procedures are described in the subheadings below.

4.3. Selection Process

We searched seven essential virtual libraries accessed at 20th April 2022 for papers in the scholarly research: Science Direct (Science Direct: <https://www.sciencedirect.com/>), IEEE Xplore (IEEE Xplore: <https://ieeexplore.ieee.org/Xplore/home.jsp>), Wiley (Wiley: <https://onlinelibrary.wiley.com/>), Scopus (Scopus: <https://www.scopus.com>), Springer Link (Springer Link: <https://link.springer.com/>), and ACM Digital Library (ACM Digital Library: <https://dl.acm.org/>). Additionally, we used standard search engines, such as Google, to discover publications in the GLR. Assessments, working studies, official records, fact sheets, films, and reviews are all examples of GLR publications. GLR works have been conducted by examining search queries on search engines, as proposed by [25]. Moreover, we used the instructions in [29] to create an organized search query, which was driven by the research goals to investigate digital libraries and search engine results, as follows:

Search Query: (("body sensor network") OR ("Body Area Network")) AND (("privacy") OR ("security") OR ("safety") OR ("integrity")) AND (("challenges") OR ("Issues") OR ("Problems")).

4.3.1. Source Selection

To ensure that only relevant sources are selected for further review, we established the following factors for inclusion and exclusion.

Inclusion Factors

- Sources that are relevant to secure body sensor network;
- Sources that focus on secure body sensor network;
- Studies that find alternatives, approaches, prevention systems or other security-related activities;
- English-language studies;
- Journal and conference papers, standards and white papers, and reports published by reputable organizations.

Exclusion Factors

- Intermediate or tertiary research (literature reviews, surveys, and other types of research);
- Articles in which the entire text is not accessible;
- Tutorials, opinions, and different types of research (only for scholarly papers);
- Studies that do not provide detailed information about BSN security;
- Textbooks and duplicate sources.

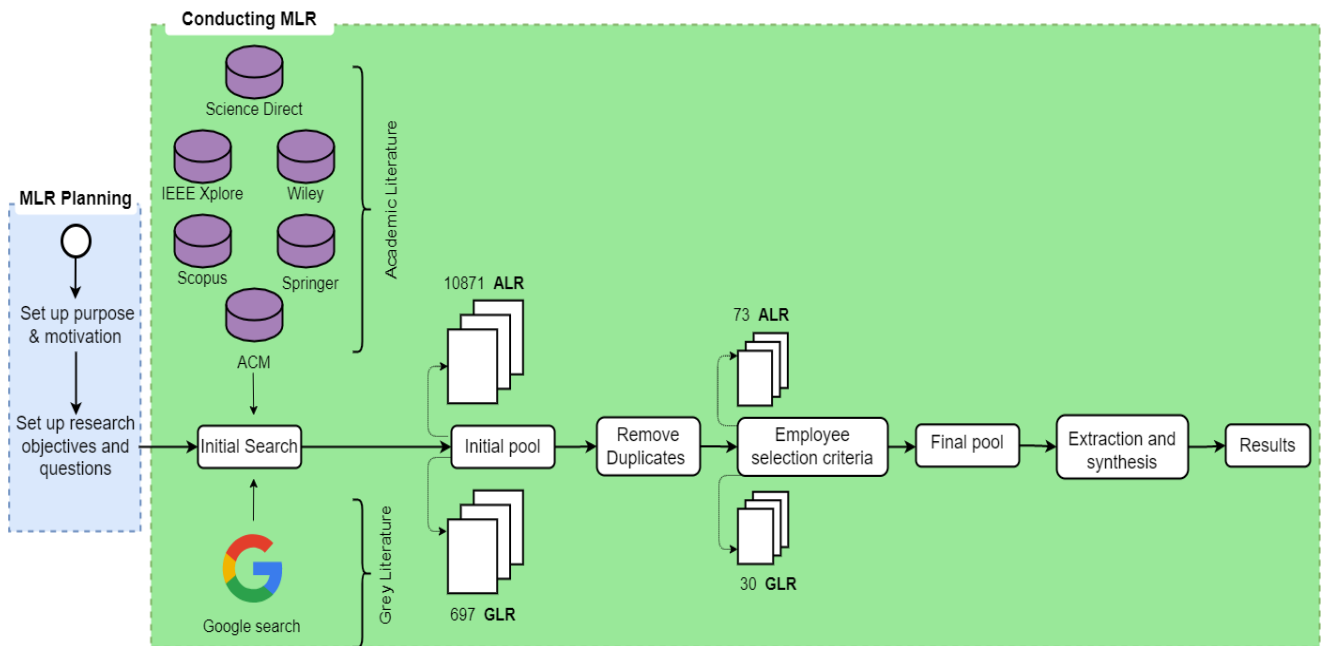


Figure 1. MLR process.

4.3.2. Articles Selection

In this investigation, four phases guided the selection of literature. The first step is to review the titles and abstracts in the query results to compile a list of potential sites. Duplicates are eliminated in stage 2, and in stage 3, appropriate sources are identified by analyzing the entire content of the previously selected sources. Finally, in stage 4, the materials that match the inclusion requirements and satisfy the quality evaluation are reviewed.

4.3.3. Acquisition and Compilation of Data

We retrieved and recorded the essential data from the primary publications of GLR scholarly papers and articles upon selection from the academic papers. Initially, we extracted metadata, which included the name, year of issue, destination type for scholarly articles, and source category for GLR, among other areas.

5. Findings

Using MLR, we determined the best techniques for securing BSN. After presenting the findings of the MLR scan, we provided a brief description of the materials that were selected. Then, we provided a list of techniques that have been found following MLR data analysis. In February 2022, the investigation was finally concluded. The most recent publications discovered between December 2017 and 2021 were covered in the research.

In this study, the selection process included four stages. During the initial screening procedure, 10,871 sources were retrieved from all digital libraries. In the first selection stage 548 sources were selected and in the second stage 433 articles were chosen. Then, in the third selection stage 321 articles and in the fourth selection stage 73 articles were selected. A summary of these findings can be seen in Table 1.

Table 1. MLR search results.

Database Resource	Initial Search	First Stage	Second Stage	Third Stage	Fourth Stage
Science Direct	1662	57	57	49	18
IEEE Xplore	717	62	58	58	16
Wiley	488	39	14	8	5
Scopus	4425	177	158	136	18
Springer	3245	194	129	48	8
ACM Digital Library	334	19	17	17	8
Total	10,871	548	433	321	73

Table 2 lists the excellency criteria used to evaluate each research. With the following question: “Is this excellency factor accomplished?”, we used a five-point scale to rate each article (strongly agree, agree, neither agree nor disagree, disagree, and strongly disagree). Some perspectives were provided on the distinctions between scholarly (white) and industrial (grey) literature from the excellency evaluation of the data source. Figure 2 contains the findings of the excellency evaluation for academic and GLR for each standard as a proportion of the relevant overall review of papers. The majority of all ALR articles (91%) explicitly explained their study objective; each one of them categorized the addressed security breaches openly. Additionally, the majority of them (93%) described quite explicitly the security feature offered. Sixty-seven percent of GLR articles are compiled on trusted web pages, but only a portion of the remainder (17%) are not dated. Moreover, around half of the articles (49%) offer background, and 2/3 (67%) analyze the problem discussed by their security mechanism.

Table 2. Excellence criteria for publications.

EC #	Criteria
	For Academic Literature: conduct the research
EC1	have well-defined research objectives?
EC2	describe the problem considered by the security solution?
EC3	illustrate the security solution?
	For Grey Literature: conduct the study
EC4	obtained from a trustworthy publishing institution?
EC5	have a clearly stated date?
EC6	present the background where the security solution is used?
EC7	provide the problem addressed by the security solution?

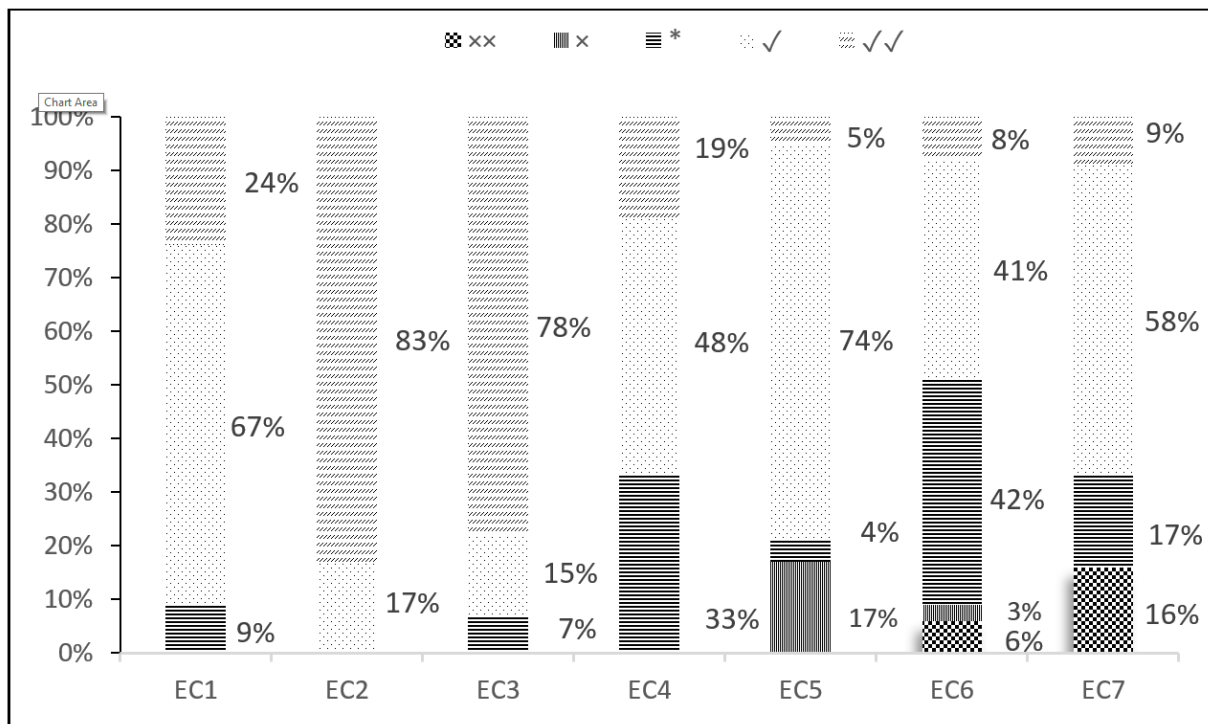


Figure 2. Excellency scores as a percent of articles that meet each of them (academic literature: EC1 through EC3; grey literature: EC4 through EC7).

According to the report’s results, it can be beneficial and challenging to incorporate GLR into the systematic review since the evidence is based on personal views and experiences. For instance, when describing the research methodology, we may come across lower-quality reports. This must be considered at each stage of the study. Table 3 outlines the information extraction strategy used in this analysis and illustrates the metadata generated for each publication type. A peer review is conducted to ensure accurate results.

Table 3. Metadata for extracting article details (GLR: Grey literature; ALR: Academic literature).

RQ	Data Field	Definition	Origin
	ID	Code (“A” for academic literature and “G” for grey literature), along with serial numbers starting at 1	ALR/GLR
	Title	Title of study	ALR/GLR
	Type	Publication type (journal, conference)	ALR
	Date	Year of article publication	ALR/GLR
	URL	URL of publication	GLR
	Publisher	Source of publication (company, communication, community, blog, thesis/dissertation)	GLR
	Contribution type	The report, blog post, presentation, white paper, video, audio	GLR
RQ1	Articles frequency	number of publications per year	ALR/GLR
RQ2	Methodology	Literature type (evaluation, validation, novel solution, opinion paper, personal experience) Verification type (case study, simulation, performance analysis, descriptive examples, not mentioned) Methodological approach (block structure, logic, sequence diagram, class diagram, formation diagram, use case model, text only, code, proper analysis)	ALR/GLR

Table 3. *Cont.*

RQ	Data Field	Definition	Origin
RQ3	Categories of Security solutions	Security mechanism reported in the studies analyzed Security scope: Focus of an analysis study	ALR/GLR
RQ4	Security domains	Prevention, mitigation, detection, recovery	ALR/GLR

5.1. RQ1: Articles Frequency

The definitive collection of publications contains 73 ALR articles, numbered from A1 to A73, and 30 GLR articles, numbered from G1 to G30 (see Tables 4 and 5). In Figure 3, a straightforward upswing growth can be observed in the number of publications from both types of content. The rise in involvement and competence in the issue can be related to the interests and mastery of both communities. Each year in the survey, journal writings and conference papers are statistically tied to scholarly papers (see Figure 4). The number of articles presented at conferences has increased steadily; however, the amount of literature published in journals has grown considerably more rapidly. In the timespan investigated, there were 73% journal articles and 22% conference presentations. Each year, articles on professional communities have ranked first in the GLR dataset (see Figure 5), with a blog post in second place. G1 and G2 are the first community articles on protected BSN (2017). The number of articles published in professional communities reached its peak in 2019 and fell in 2020, but the slack was most rewarded by the articles published in companies' blogs.

Table 4. Primary studies in GLR were accessed on 25 April 2022.

ID	Year	Title	Type	URL
G1	2017	IoT Technology Innovations in Healthcare	COMMUNITY	https://bit.ly/3srScKF
G2	2017	Addressing Security Issues in Connected Healthcare	COMMUNITY	https://bit.ly/3GAtLQ7
G3	2018	Telemedicine privacy risks and security considerations	COMPANY	https://bit.ly/3ozCtly
G4	2018	Telehealth Security: Protect Patient Information and Your Practice	BLOG	https://bit.ly/3Ba0WJp
G5	2018	Securing Telehealth Remote Patient Monitoring Ecosystem	COMMUNITY	https://bit.ly/3rAYOqK
G6	2019	Enabling covert body-area network using electro-quasistatic human body communication	COMMUNITY	https://bit.ly/3BfRWCv
G7	2019	Scientists Design a Network That Lives Inside Your Body	COMPANY	https://bit.ly/33difgc
G8	2019	Standardizing Smart Body Area Networks	COMPANY	https://bit.ly/3LdK5tI
G9	2019	Making the 'human-body Internet' more effective	BLOG	https://bit.ly/3379gNo
G10	2019	Low Power Network for Wireless Body Sensors	COMMUNITY	https://bit.ly/3HKFugI
G11	2019	Securing Telehealth Remote Patient Monitoring Ecosystem	COMPANY	https://bit.ly/3uJrD6i
G12	2020	Coronavirus challenges remote networking	COMMUNICATION	https://bit.ly/3Bc0zOn
G13	2020	TURNING THE BODY INTO A WIRE	BLOG	https://bit.ly/3uBZVII
G14	2020	Data Security: Telehealth's Achilles Heel?	COMPANY	https://bit.ly/3GAgJlN
G15	2020	The Privacy and security issues of expanding Telehealth	BLOG	https://bit.ly/3sveriG
G16	2020	The Future of Care Is Telehealth, But Security Risks Could Slow Service Adoption	BLOG	https://bit.ly/3rBdrdN
G17	2020	Monthly Healthcare News Roundup: The State of Healthcare Data Breaches in 2020	BLOG	https://bit.ly/3HFfmUn
G18	2020	Telehealth Privacy and Security	COMMUNITY	https://bit.ly/3sl8QeM
G19	2020	Telehealth data breaches to worsen as adoption skyrockets	COMMUNICATION	https://zd.net/3oCiLvs
G20	2021	Beyond Wearable Devices: Internet of Bodies (IoB)	BLOG	https://bit.ly/3uxGPDH
G21	2021	Next-Generation Cardiac Wearables and Implantable Will Integrate into WBSN	COMMUNICATION	https://bit.ly/3uCovtc

Table 4. Cont.

ID	Year	Title	Type	URL
G22	2021	Wearable patch could predict the risk of stroke and heart attacks	COMMUNICATION	https://bit.ly/3Je3skF
G23	2021	Apple watch series seven might come with body temperature monitor, Glucose sensors	COMMUNICATION	https://bit.ly/35PimPM
G24	2021	Wearables, Body Sensor Networks, Smart Portable Devices	BLOG	https://bit.ly/3LifECJ
G25	2021	Global Body Area Network Market (2021 to 2030)	BLOG	https://bit.ly/361bPSk
G26	2021	Researchers discover how to stick sensors to skin without adhesive	COMMUNITY	https://bit.ly/3JiM4LH
G27	2021	This Implant Could One Day Control Your Sleep and Wake Cycles	COMMUNICATION	https://bit.ly/3JiM5ij
G28	2021	Securing Telehealth Remote Patient Monitoring Ecosystem	COMPANY	https://bit.ly/3GBLx5J
G29	2021	Blockchain in Telemedicine	COMMUNITY	https://bit.ly/3gAn99T
G30	2021	ENSURING THE CYBER SECURITY OF TELEHEALTH	BLOG	https://bit.ly/3HCh7BK

Table 5. Studies in ALR.

Year	ID	References
2017	A1, A2, A3, A4, A5, A6, A7, A8	[30–37]
2018	A9, A10, A11, A12, A13, A14, A15, A16, A17, A18, A19, A20, A21, A22, A23, A24	[38–52]
2019	A25, A26, A27, A28, A29, A30, A31, A32	[53–61]
2020	A33, A34, A35, A36, A37, A38, A39, A40, A41, A42, A43, A44, A45, A46, A47, A48, A49, A50, A51, A52, A53, A54	[62–82]
2021	A55, A56, A57, A58, A59, A60, A61, A62, A63, A64, A65, A67, A68, A69, A70, A71, A72, A73	[83–104]

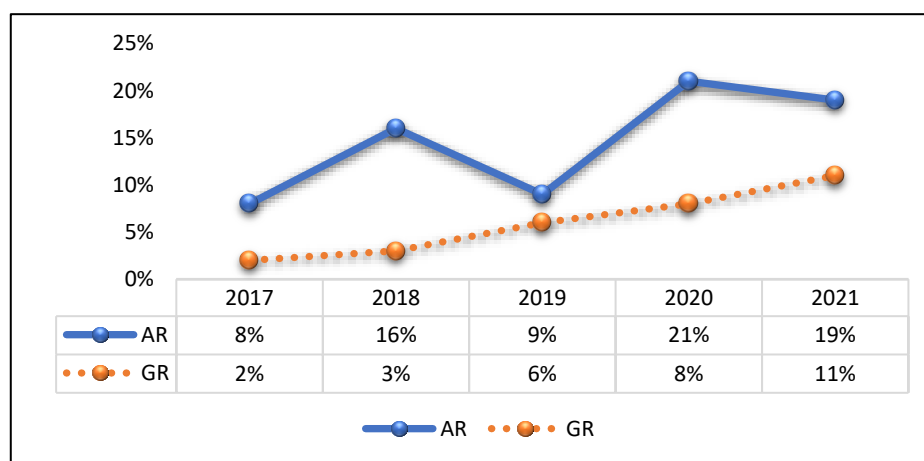


Figure 3. Relevant publications per year for academic (ALR) and grey (GLR) literature, from 2017 to 2021.

In the final score, 33% of articles appeared in blog posts, 27% were on professional communities, 20% were on the company’s website, and the remaining 20% were published on communications channels. Blog posts are still an excellent place to keep up with current advances from experts, but with rigorous viewpoints.

5.2. RQ2: Methodological Approaches

The studies from academic and GLR were classified as research type, validation type or methodologies used.

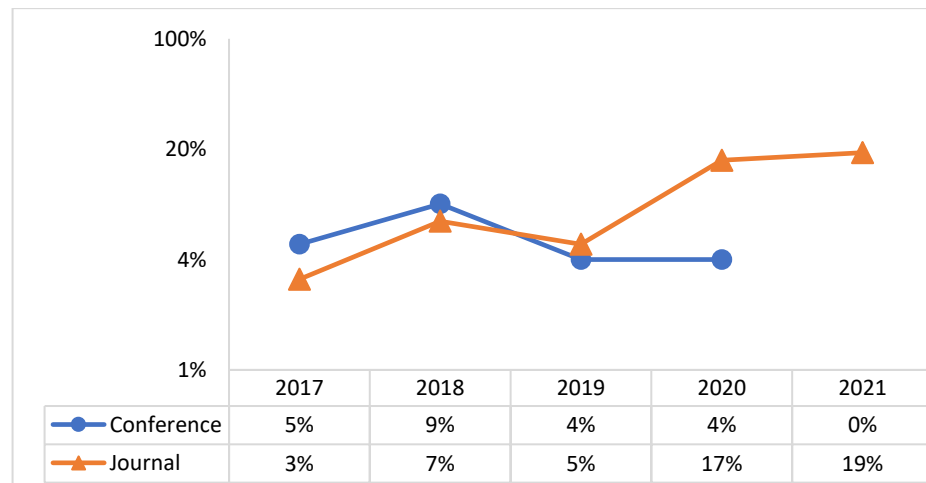


Figure 4. Publication types for ALR.

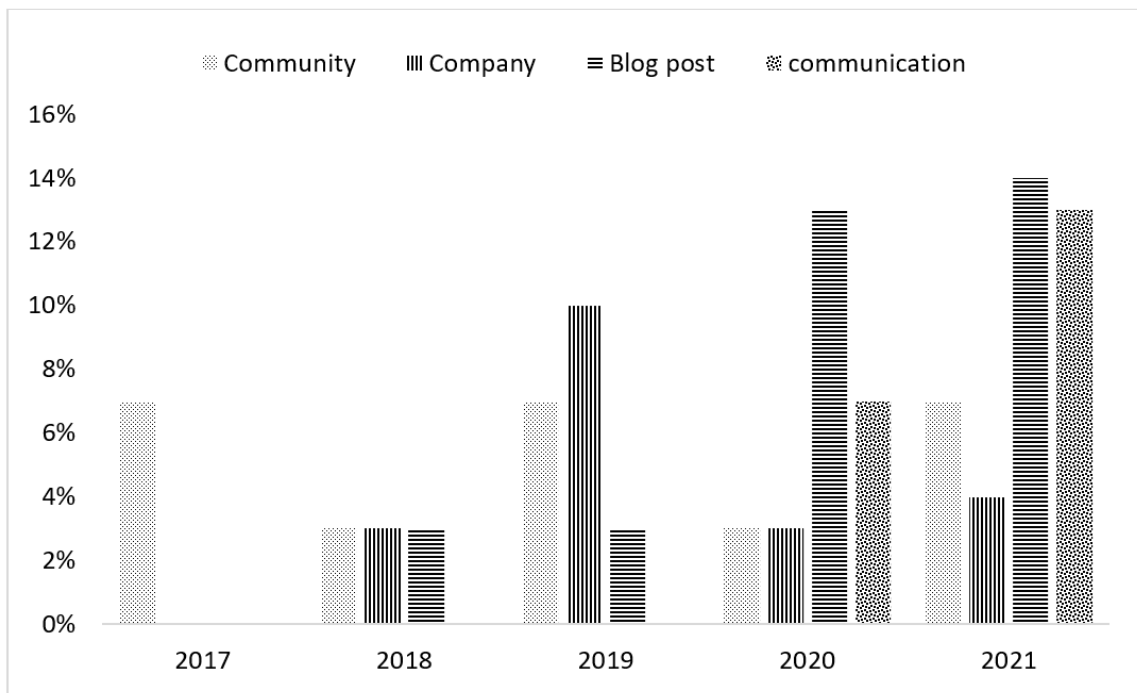


Figure 5. Publication types for GLR.

5.2.1. Research Types

Evaluation, validation, novel research, opinion papers, and individual experience are considered for inclusion in the final selections from academia and the GLR. The evaluative study focuses on analyzing an issue in practice or the adoption of an approach in practice. When a solution proposal has not yet been implemented, validation research examines its properties. A complete validation of the novel solution is not required, which suggests an alternative approach and argues for its validity. An opinion paper is a piece of writing that expresses the writer’s thoughts on a particular topic. Personal experience articles focus on “what” rather than “why”.

The targets and issues of each paper were accumulated and then categorized in the above list of categories. Figure 6 depicts the distribution of academic and grey studies from 2017 to 2021 by categorization. Additionally, over two-thirds (66%) of academia address BSN security issues (see Figure 7). Thirty-three percent of academic research focused on security features that have yet to be applied (see Figure 7). The goal of this research team

is to generate new ideas for BSN security measures. Security mechanisms that have been incorporated are evaluated in primary analyses of academic papers (38%) by the third team. These primary studies used empirical research to better understand the benefits and drawbacks of various BSN security measures.

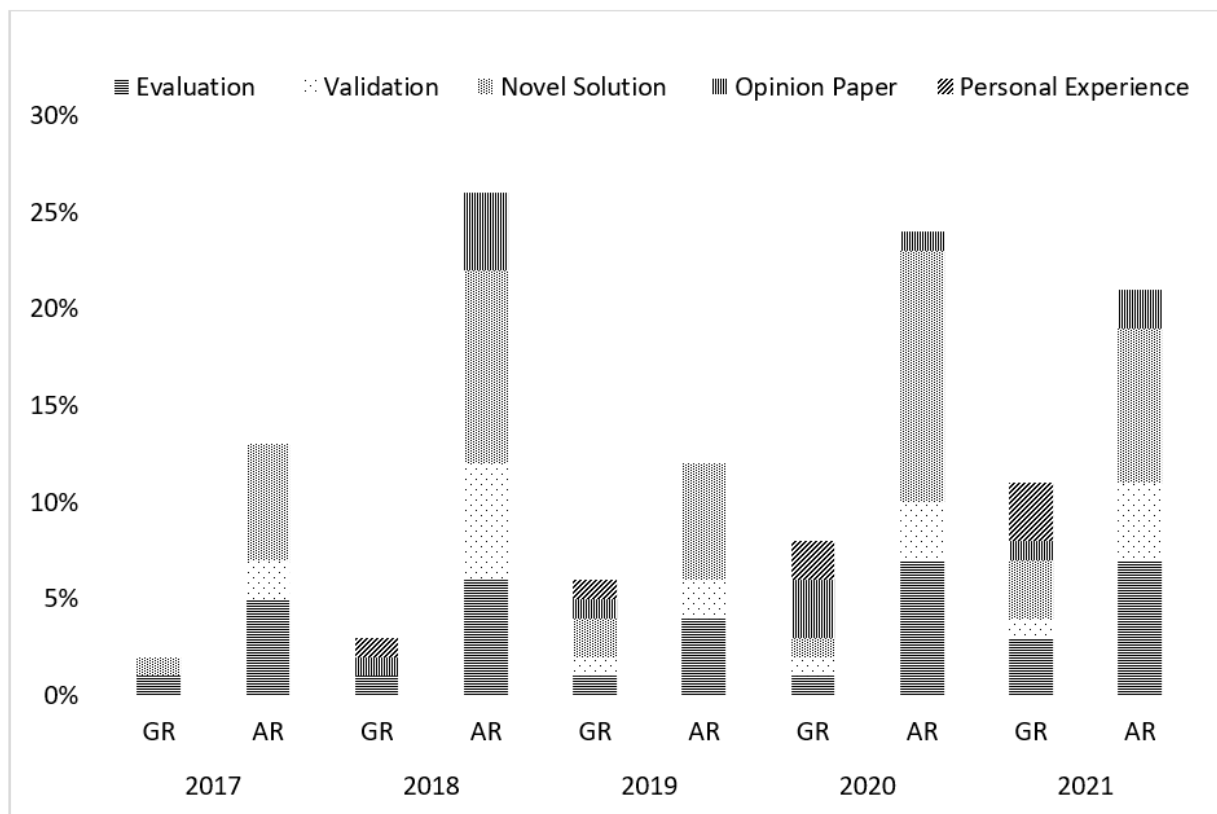


Figure 6. Research type of the academic (ALR) and grey (GLR) literature.

Only 10% of the validation studies shown in Figure 8 can be found in the GLR. From the information published, 20% demonstrated an author’s personal view on how specific security measures should be implemented. Studies based on assessment research, personal opinions, and novel solutions to BSN security problems comprised another group with an increased prevalence (23%).

5.2.2. Validation Types

Case studies, simulations, performance analysis, and descriptive examples are validation types. Primarily, all academic published research provide the type of validation (see Figure 9). Performance assessment (63%) and simulation (53%) are the most commonly used methods for testing and verifying. Numerous types of validation are used in a few cases, such as the A33 case study and simulation and A42 simulation and performance analysis. In 2020, performance analysis was the most popular method, but in 2021, simulation was the most common approach. For each study, Figures 7 and 8 summarize research methodologies, including validation and research types for every academic and GLR study. Only 46% of GLR publications cover this topic, and descriptive examples are used when it comes to validation.

5.2.3. Methodologies

Block structure (67%) is the most common method of describing a solution pictorially (45%) in scholarly articles. Class (16%), sequence (34%), formation (15%), and use case

model (26%) are some of the UML diagrams that the articles use. Only 22% make use of logic, while 20% focus entirely on the text and 18% make use of code.

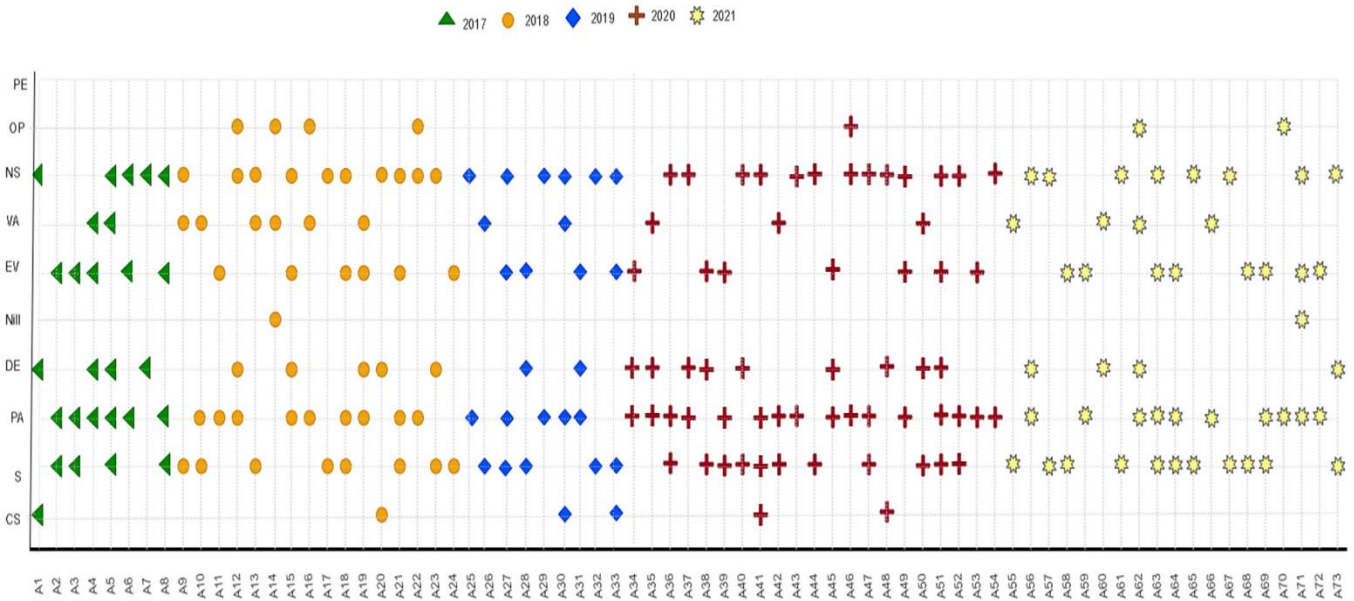


Figure 7. Summary of methodological approaches to ALR. At the Y-axis, abbreviations used for validation types are CS: Case study; S: Simulation; PA: Performance analysis; PC: Proof of concept; Nil: Not mentioned, and for research types abbreviations are EV: Evaluation; VA: Validation; NS: Novel solution; PE: Personal experience.

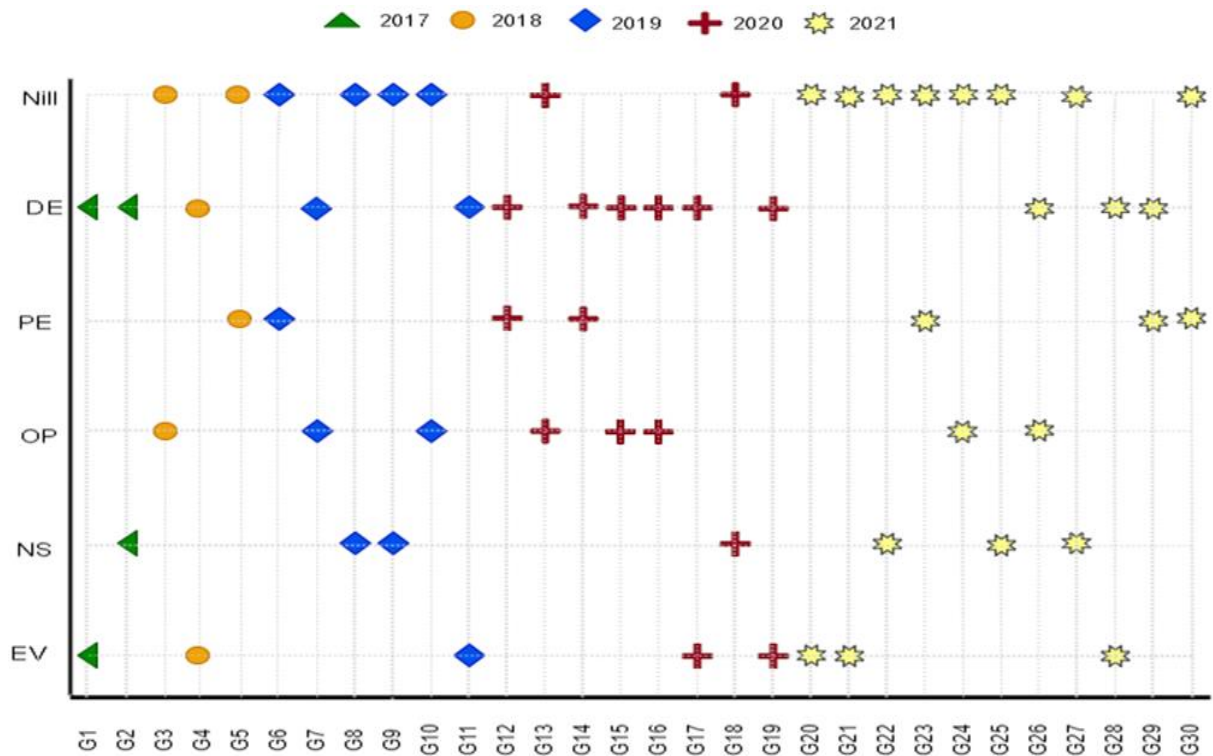


Figure 8. Summary of methodological approaches to GLR. In Y-axis, abbreviations used for research types are EV: Evaluation; NS: Novel solution; OP: Opinion paper; PE: Personal experience, and for validation types abbreviations are EP: Example and NS: Not specified.

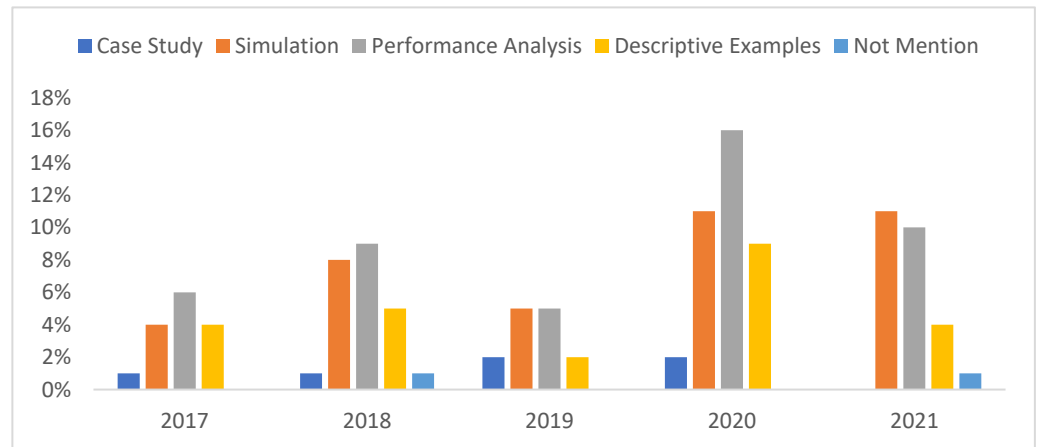


Figure 9. Validation types of research in ALR.

Grey publications strongly rely on text content (32%) and block structure (27%) or even only on sequence diagrams (23%). A code had just been presented by one publication (3%). Methodologies used throughout the grey and academic literature review are shown in Figures 10 and 11, respectively. Figure 12 depicts the methodology used in academic and grey fields along with the year. The sophistication of security mechanisms necessitates a greater depth of understanding, which is why practitioners are underutilizing designs. This flaw could open the door to additional attacks in the future.

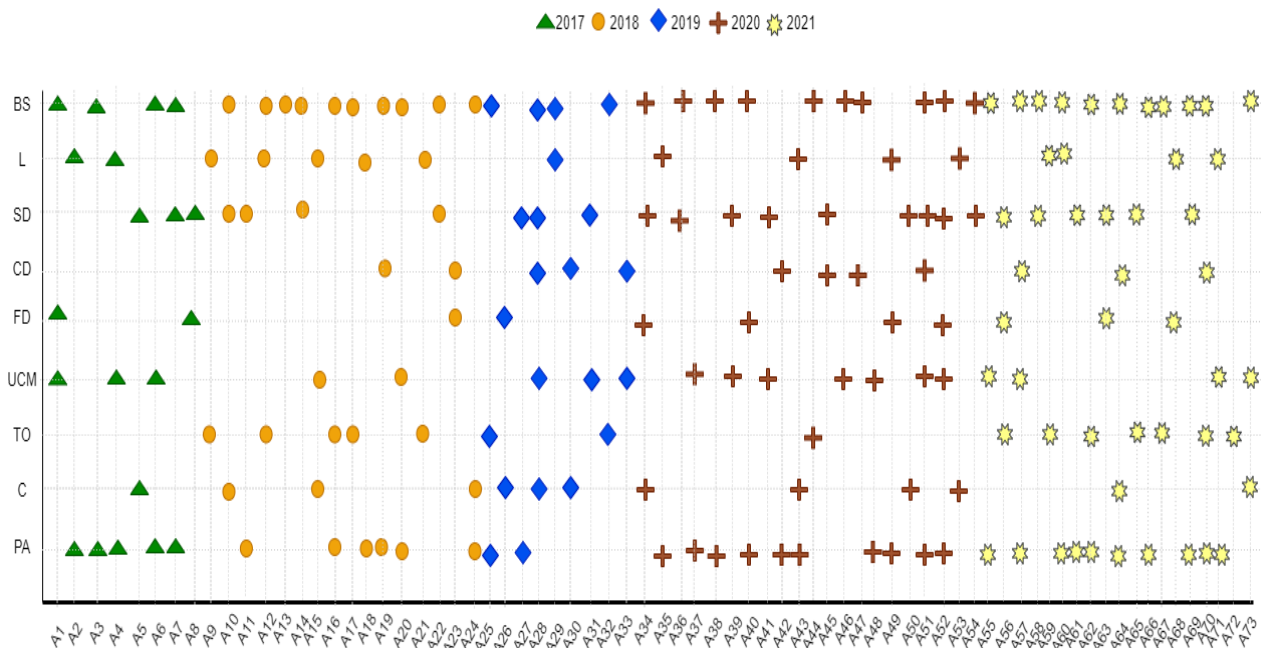


Figure 10. Summary of methodologies used for ALR. In the Y-axis, abbreviations of methodologies are BS: Block structure; L: Logic; SD: Sequence diagram; CD: Class diagram; FD: Formation diagram; UCM: Use case model; TO: Text only; C: Code; PA: Proper analysis.

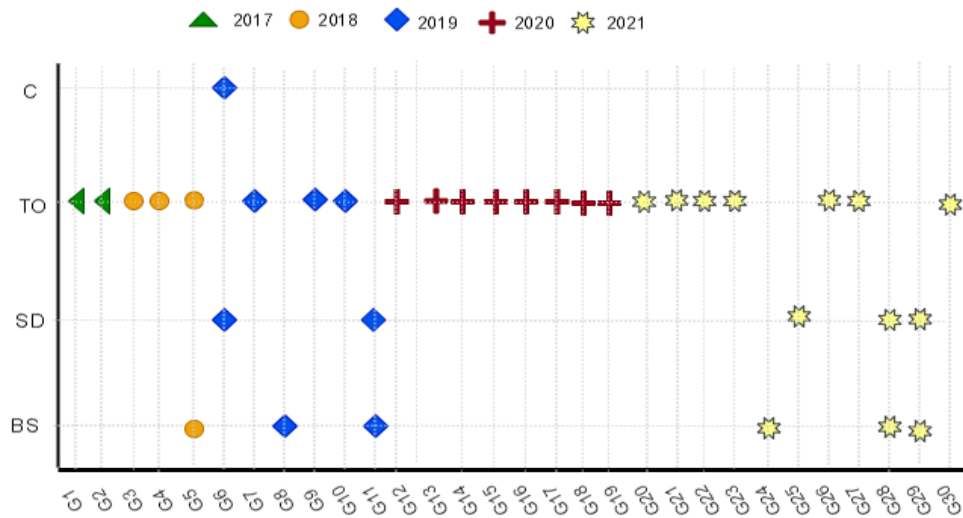


Figure 11. Summary of methodologies used for GLR. In the Y-axis, abbreviations of methodologies are BS: Block structure; SD: Sequence diagram; TO: Text only; C: Code.

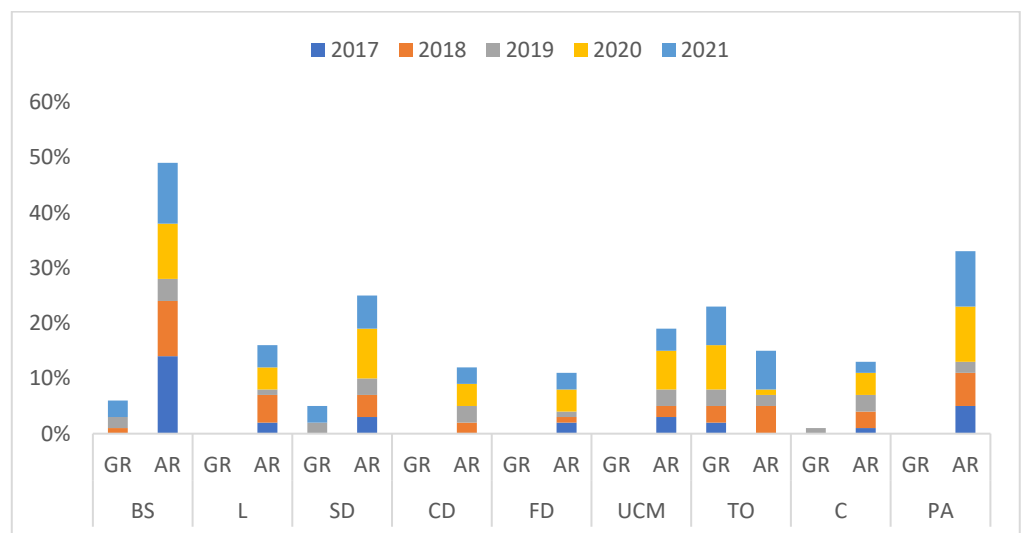


Figure 12. Methodologies used for the academic (ALR) and grey (GLR) literature studies. The abbreviations used are BS: Block structure; L: Logic; SD: Sequence diagram; CD: Class diagram; FD: Formation diagram; UCM: Use case model; TO: Text only; C: Code; PA: Proper analysis.

5.3. RQ3: Categories of Security Solutions

The categorization of security mechanisms included authorization, authentication, access control, secure transmission, filtering, monitoring, execution control, and secure data management. Moreover, categories of security scope have been provided to consider security requirements that do not directly correlate to mechanisms, such as implementation security, security evaluation, threat modeling, generic security architecture, and secure application. The possible strategies for BSN security are demonstrated in Figure 13 regarding the distribution of security measures and the scope of protection. Figure 14 depicts the evolution of academic and GLR reports on security scopes and security mechanisms throughout the years studied. In the subsequent subsections, we will look at the findings for each of the research papers’ chosen security mechanisms and scopes.

5.3.1. Security Mechanisms

Users’ access to system resources is referred to as authorization. Approximately 17% of the grey writings and 32% of the ALR discuss methods for achieving authorization. Identification of participants is the goal of the authentication mechanism. Tracking and monitoring can only take place if a user has an identity. In our data analysis, we discovered that 20% of the publications and 45% of ALR reported alternative solutions that use identity management to improve BSN confidentiality. Access control is the validation of an entity’s legitimation to use resources implicitly in this concept. For a complete access control system to work, authentication and authorization must be in place. Twenty three percent of GLR and 29% of ALR in our dataset included some form of access control in security measures.

Encrypted communications and strong authentication are the most common methods for ensuring secure communications. The encrypted information is sent from the origin and decrypted at the target to retain burglars from having to read them. A safe link is established through authentication and authorization. A few methods to ensure a secure connection are reported in 29% of ALR and 27% in publications. Communication among a webpage is potentially harmful; it can be restricted through filtration. Firewalls of various kinds are typically used in this process. Ultimately, we found a minimum percentage of grey and ALR, i.e., 7% and 9%, respectively, that focus on filtering. In general, this demonstrates that filtering is not adapted for use in the security of BSNs.

The purpose of monitoring is to identify unusual behavior that could indicate an attack. Strategies of this type are found in only 20% (in grey publications) and 16% (in academic publications). Process interruption is prevented by execution control, which limits a process’s execution to a particular execution scope, in which only authorized assets can be used. Only 13% of literature in the grey publications and 23% in ALR confirmed its use. It is necessary to have a system for keeping track of authentication and authorization rules. These key attributes would be at risk if this information was not secured. Twenty seven percent of academic and 23% of grey sources cited in the BSN security studies considered managing security information.

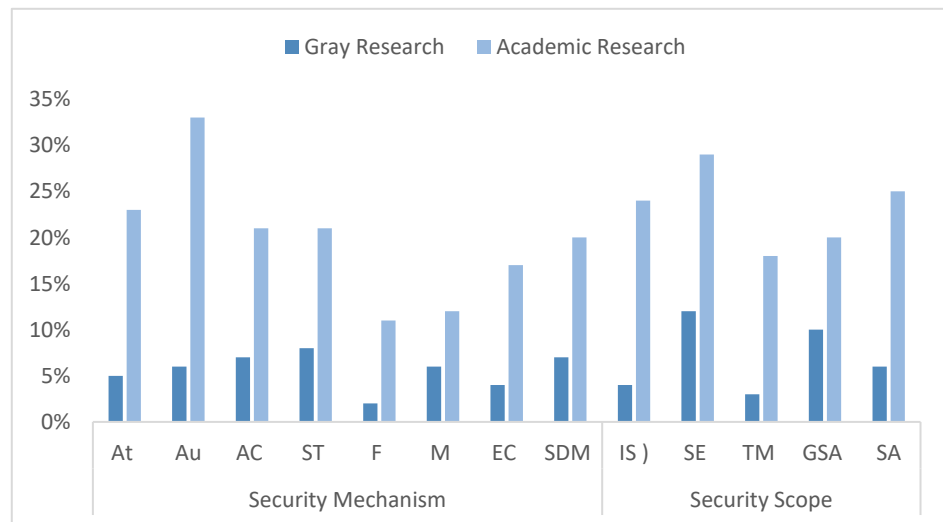


Figure 13. Security mechanisms and security scope identified in studies of academic and GLR. The abbreviations used are At: Authorization; Au: Authentication; AC: Access control; ST: Secure transmission; F: Filtering; M: Monitoring; EC: Execution control; SDM: Security data management; IS: Implementation security; SE: Security evaluation; TM: Threat modeling; GSA: Generic security architecture; SA: Secure application.

5.3.2. Security Scope

Technologies and other design details influenced implementation security. ALR reported 33% of this research. The GLR indicates 13% of research on implementation

security. Security evaluation is used in roughly half of all grey and ALR. Threat modeling indicates defining and enumerating threats for a specific platform. Threats leverage system weaknesses, and some research focus on finding defects. Only 10% of GLR papers consider threat modeling, while 25% of academic studies do not.

The general security architecture of BSN is covered in articles, including security standards, secure advancement cycles, and protection design patterns. General security architecture is described in 33% of grey and 27% of academic papers. Lower-level layers must only enforce limitations defined at a higher-level of application security. Application ambiguity should be kept in mind throughout the application development lifecycle. Application security mechanisms were reported in only 34% of scholarly articles, but in GLR, the number is 20%.

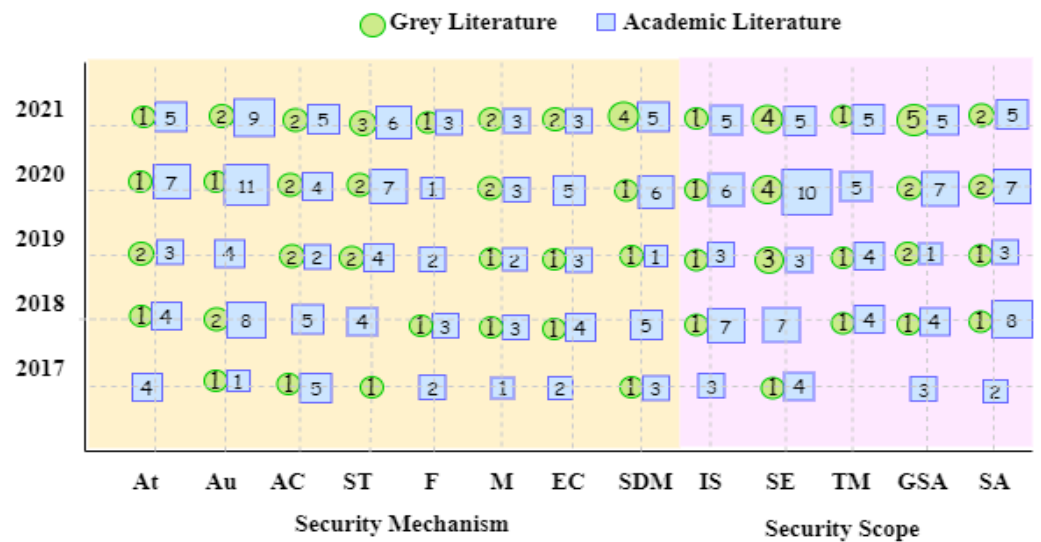


Figure 14. Security mechanisms and security scope identified in studies of academic and GLR throughout the years. The numbers inside are quantities of papers. The abbreviations used are At: Authorization; Au: Authentication; AC: Access control, ST: Secure transmission; F: Filtering; M: Monitoring; EC: Execution control; SDM: Security data management; IS: Implementation security; SE: Security evaluation; TM: Threat modeling; GSA: Generic security architecture; SA: Secure application.

5.4. RQ4: Security Contexts

According to their security contexts, academic and GLR security solutions are classified in Figure 15. Sixty-seven percent of the strategies in the GLR and 49% of the ALR describe security mechanisms that seek to avoid threats and mitigate (30% and 60%, respectively). Only 15% of the ALR and 6% of the grey publications describe frameworks other than those focusing on detection and recovery of breaches (8% in the ALR, while 6% in the GLR). Figures 16 and 17 illustrate a summary of each of the findings in ALR and GLR.

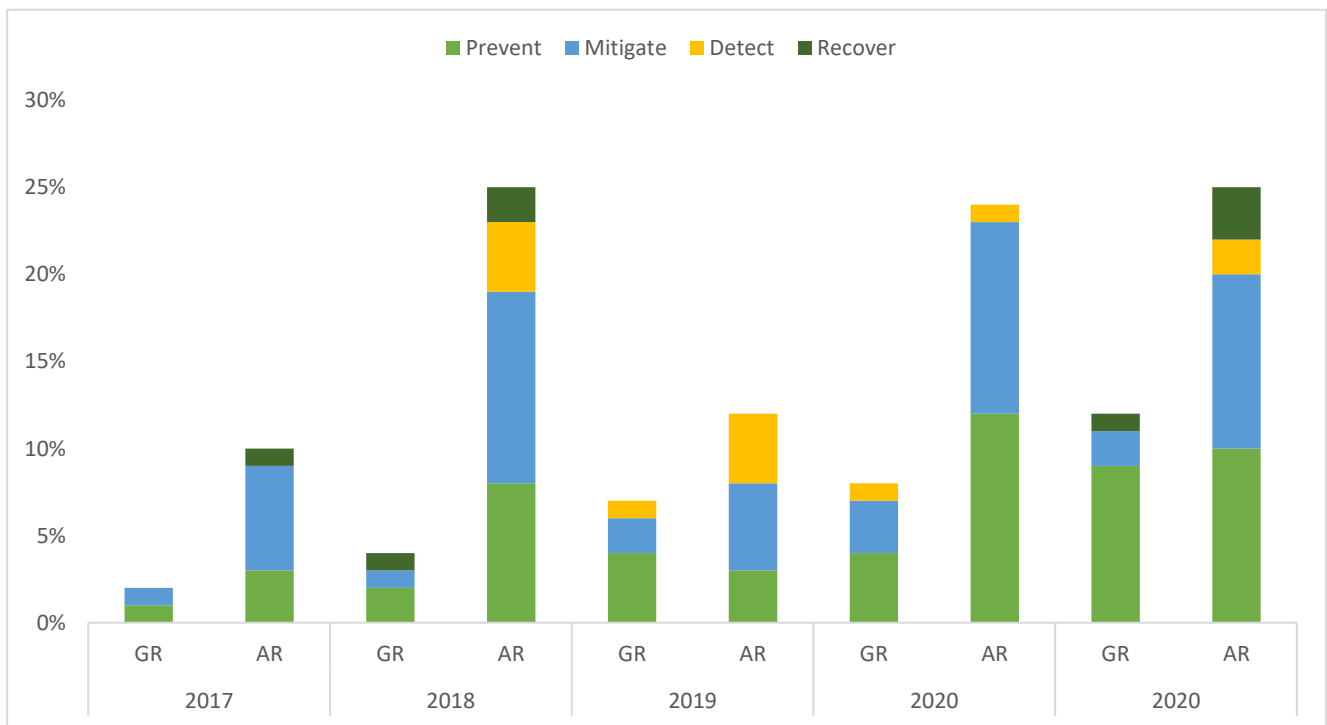


Figure 15. Security contexts addressed by the security solutions. ALR: Academic literature; GLR: Grey literature.

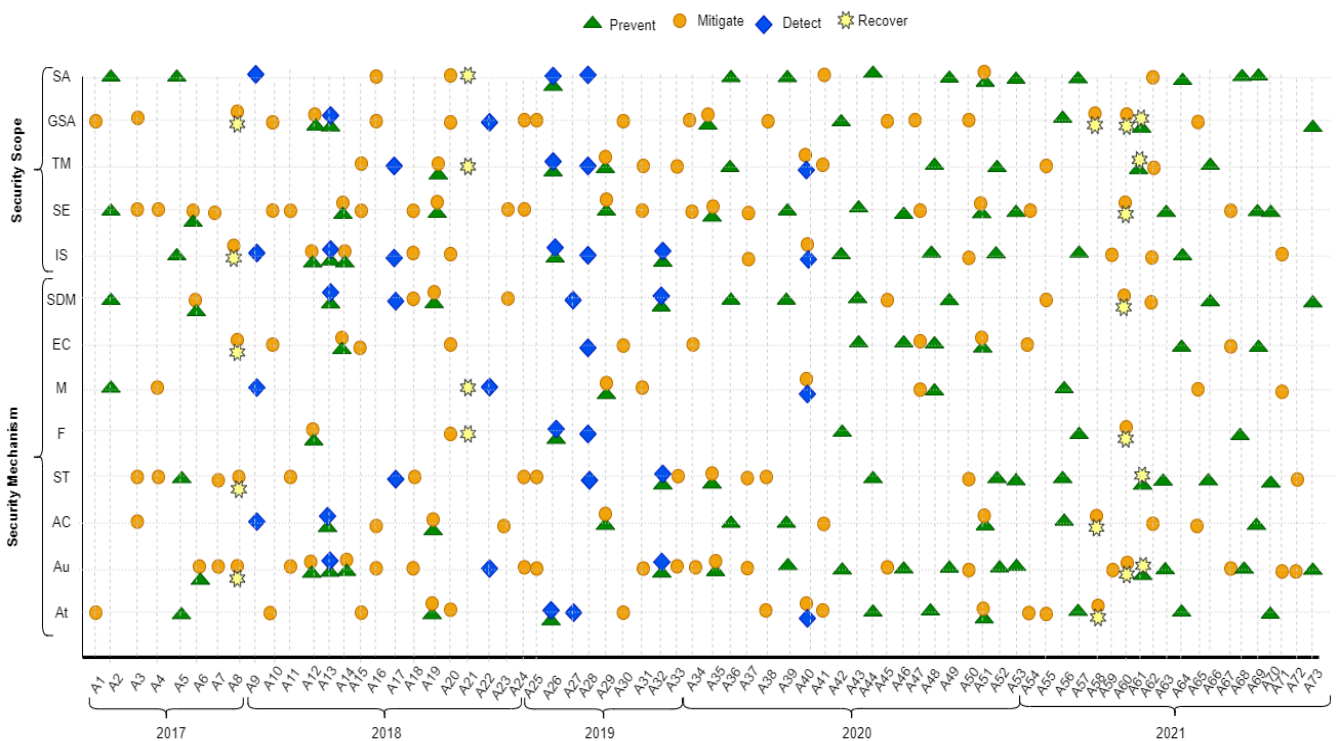


Figure 16. Summary of the security scope and security mechanisms reported by each study in the ALR. The abbreviations are At: Authorization; Au: Authentication; AC: Access control; ST: Secure transmission; F: Filtering; M: Monitoring; EC: Execution control; SDM: Security data management; IS: Implementation security; SE: Security evaluation; TM: Threat modeling; GSA: Generic security architecture; SA: Secure application.



Figure 17. Review of the security scope and security mechanisms reported by each study in the GLR. The abbreviations are At: Authorization; Au: Authentication; AC: Access control; ST: Secure transmission; F: Filtering; M: Monitoring; EC: Execution control; IS: Implementation security; GSA: Generic security architecture.

6. Proposed Research Implications

From our findings, we can conclude that there are several potential directions for the upcoming research.

6.1. Few Works on Attack Detection

Very little progress has been made in the field of attack detection. In general, threat detection systems are used to analyze data traffic to diagnose the behavior of breaches. For instance, articles A9 and A17 are monitoring systems explicitly designed to identify anomalies in BSN implementation. However, more effort is necessary. Comprehensively scanning incidents on BSN to assess their behaviors in a specific monitoring system might be an exciting approach.

6.2. Secure BSN Application Development

Reliable applications are crucial from a functional standpoint. A comprehensive technique of developing secure applications is lacking, despite the numerous studies on safeguarding specific components of a system. Therefore, we need a general and complete development methodology for secured application.

6.3. Lack of Attention on Attack Recovery

There is a deficit of assault recovery approaches in academic and commercial literature. This can be reflected in the fact that current ways to restore network threats do not focus on the particular strategy used to design the systems. In the case of running a system partitioned into several BSN areas, it is necessary to have a backup that can be restored in the event of a significant disruption. This is primarily concerned with assuring that the software is always available. According to the findings, the regular operation will have to be suspended, but only reading activities are allowed to verify that the entire content of every BSN section is stable. This seems to be an issue that should be given more significant consideration.

6.4. Adaptation of Reliable Technology

Prior to use, the devices should guarantee genuineness and trustworthiness. Additionally, the equipment should use authorized domains to guarantee smooth implementation of programs and the secure storing of digital certificates. When it comes to sensitive material, such as those received by BSN, this seems to be a vital implication to focus on hardware privacy.

7. Potential Applications of Proposed MLR

The results of our MLR should be helpful to guide practitioners and researchers in the following possible applications:

7.1. To Publish New Security Mechanisms of BSN

Scholars can minimize replicating previous research while writing and publishing “innovative” algorithms or privacy evaluations if they become familiar with relevant early studies. Problems with existing approaches, such as their inefficiencies, might encourage innovation. Furthermore, this collection of study directions can point to places where a large amount of work has not been conducted, which might give rise to novel work. These strategies can serve as a starting point for identifying acceptable dimensions, methodologies, and areas of expertise for new studies. The categorization of the validation techniques utilized by other scholars might provide a portfolio of choices for validating the latest findings.

7.2. To Solve BSN Security Design Problems

The insights of our assessment can be used to evaluate advanced techniques, and then choose and reapply the most relevant one for addressing development difficulties in BSN solutions. Designers can use our categorization system and its findings at any stage of development: The structures of the evaluation stage and the initial designing and implementing phase should be examined for adequate safety restrictions. Secondly, designers can look at existing models for motivation.

7.3. To Communicate and Search for New Ideas

BSN professionals and academics can use our classification results as a guideline. Using these findings as a starting point, other researchers can expand even more on this work and contribute to the existence of data on the issue. In future experiments, simplifying this information into a standard database would be helpful.

8. Conclusions

E-Health is becoming increasingly popular not only in the science community but also in the manufacturing and commercial worlds. Information and communication technologies, which are both new, have a large amount of capability in making the public healthcare platform more efficient. There are few problems with a digitalized healthcare system, such as security worries, system unscheduled downtime, and loss of security for patient information. With the aid of technology, WBSN clients can access their body sensor data and other resources from all over the world. This will assist in reducing the cost of diagnosis, improving services, providing better analytical reports, and accelerating the process of receiving care. However, although there are numerous advantages, data security and privacy are still major concerns. Therefore, in this article, we discussed security and privacy issues and proposed solutions.

As part of our research, we considered 73 ALR and 30 GLR studies to understand the different privacy aspects that have already been employed to secure BSN. The findings of this study demonstrate that authorization, access control, and authentication protocols are the most popular protection techniques in BSN research and practice. Furthermore, the review reveals that avoiding and mitigating threats are possibly the most common security approaches, and a large number of security measures are validated via case studies and

simulations. Moreover, according to a proposed analysis, the most common research type is possibly evaluation research. These findings led us to propose a wide range of research recommendations. In the proposed study, different methods are considered to view how the security of patients' health data can be improved. We assume this will be the first multivocal survey of BSN safety. Therefore, it will be helpful for practitioners and scholars.

However, there is still a big necessity to find better and more creative ways to deal with the growing sophistication, which is due to the rapid development and advancement of wireless sensor networks used in vital applications now and in the coming decades.

9. Patents

None.

Author Contributions: Conceptualization, N.U.S. and K.Z.; methodology, N.U.S., K.Z. and M.H.; software, N.U.S., K.Z. and M.H.; validation, N.U.S., N.Z.J. and A.U.R.; formal analysis, N.U.S. and A.U.R.; resources, K.Z., M.H. and A.U.R.; data curation, N.U.S. and K.Z.; writing—original draft preparation, N.U.S., K.Z. and Humayun, H.; writing—review and editing, N.U.S., K.Z., M.H., N.Z.J. and A.U.R.; visualization, N.U.S.; supervision, N.U.S., K.Z. and M.H.; project administration, N.U.S., K.Z., M.H. and N.Z.J.; funding acquisition, N.U.S. and K.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Universiti Malaysia Sarawak.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors thank Universiti Malaysia Sarawak and the anonymous reviewers for their insightful suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Olewi, S.S.; Mohammed, G.N.; Albarazanchi, I. Mitigation of packet loss with end-to-end delay in wireless body area network applications. *Int. J. Electr. Comput. Eng.* **2022**, *12*, 460. [\[CrossRef\]](#)
- Liu, Q.; Mkongwa, K.G.; Zhang, C. Performance issues in wireless body area networks for the healthcare application: A survey and future prospects. *SN Appl. Sci.* **2021**, *3*, 1–19. [\[CrossRef\]](#)
- Karchowdhury, S.; Sen, M. Survey on attacks on wireless body area network. In *International Journal of Computational Intelligence & IoT, Forthcoming*; SSRN: Rochester, NY, USA, 2019.
- Roy, M.; Chowdhury, C.; Aslam, N. Security and privacy issues in wireless sensor and body area networks. In *Handbook of Computer Networks and Cyber Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 173–200.
- Asam, M.; Ajaz, A.; Jamal, T.; Adeel, M.; Hassan, A.; Butt, S.A.; Gulzar, M. Challenges in wireless body area network. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [\[CrossRef\]](#)
- Narwal, B.; Mohapatra, A.K. A survey on security and authentication in wireless body area networks. *J. Syst. Archit.* **2021**, *113*, 101883. [\[CrossRef\]](#)
- Maheswar, R.; Kanagachidambaresan, G.; Jayaparvathy, R.; Thampi, S.M. *Body Area Network Challenges and Solutions*; Springer: Berlin/Heidelberg, Germany, 2019.
- Abdulhameed, I.S. The Security and Privacy of Electronic Health Records in Healthcare Systems: A Systematic Review. *Turk. J. Comput. Math. Educ.* **2021**, *12*, 1979–1992.
- Garousi, V.; Rainer, A.; Felderer, M.; Mäntylä, M.V. Introduction to the Special Issue on: Grey Literature and Multivocal Literature Reviews (MLRs) in Software Engineering. *Inf. Softw. Technol.* **2022**, *141*, 106697.
- Yoo, J.; Cho, N.; Yoo, H.-J. Analysis of body sensor network using human body as the channel. In Proceedings of the ICST 3rd International Conference on Body Area Networks, Princeton, NJ, USA, 13–15 March 2008; CiteseerX: Princeton, NJ, USA, 2008.
- Tan, C.C.; Wang, H.; Zhong, S.; Li, Q. Body sensor network security: An identity-based cryptography approach. In Proceedings of the First ACM Conference on Wireless Network Security, Alexandria, VA, USA, 31 March–2 April 2008.
- Pahuja, R.; Verma, H.; Uddin, M. A wireless sensor network for greenhouse climate control. *IEEE Pervasive Comput.* **2013**, *12*, 49–58. [\[CrossRef\]](#)
- Mansour, A.; Leblond, I. Ecosystem monitoring and port surveillance systems. *AIAAS Adv. Appl. Acoust.* **2013**, *2*, 91–111.
- Reyer, M.; Hurlebaus, S.; Mander, J.; Ozbulut, O.E. Design of a wireless sensor network for structural health monitoring of bridges. In *Wireless Sensor Networks and Ecological Monitoring*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 195–216.

15. Oh, S.-R.; Seo, Y.-D.; Lee, E.; Kim, Y.-G. A comprehensive survey on security and privacy for electronic health data. *Int. J. Environ. Res. Public Health* **2021**, *18*, 9668. [[CrossRef](#)]
16. Pirbhulal, S.; Zhang, H.; Wu, W.; Mukhopadhyay, S.C.; Zhang, Y.-T. Heartbeats based biometric random binary sequences generation to secure wireless body sensor networks. *IEEE Trans. Biomed. Eng.* **2018**, *65*, 2751–2759. [[CrossRef](#)]
17. Sivasangari, A.; Ajitha, P.; Gomathi, R. Light weight security scheme in wireless body area sensor network using logistic chaotic scheme. *Int. J. Netw. Virtual Organ.* **2020**, *22*, 433–444. [[CrossRef](#)]
18. Sammoud, A.; Chalouf, M.A.; Hamdi, O.; Montavont, N.; Bouallegue, A. A new biometrics-based key establishment protocol in WBAN: Energy efficiency and security robustness analysis. *Comput. Secur.* **2020**, *96*, 101838. [[CrossRef](#)]
19. Chaudhary, S.; Singh, A.; Chatterjee, K. Wireless body sensor network (WBSN) security and privacy issues: A survey. In *International Journal of Computational Intelligence & IoT*; SSRN: Rochester, NY, USA, 2019; Volume 2.
20. Hajar, M.S.; Al-Kadri, M.O.; Kalutarage, H.K. A survey on wireless body area networks: Architecture, security challenges and research opportunities. *Comput. Secur.* **2021**, *104*, 102211. [[CrossRef](#)]
21. Hussain, S.; Ullah, S.S.; Uddin, M.; Iqbal, J.; Chen, C.-L. A comprehensive survey on signcryption security mechanisms in wireless body area networks. *Sensors* **2022**, *22*, 1072. [[CrossRef](#)]
22. Jijesh, J. A survey on Wireless Body Sensor Network routing protocol classification. In Proceedings of the 2017 11th International Conference on Intelligent Systems and Control (ISCO), Coimbatore, India, 5–6 January 2017.
23. Hamza, M.; Khan, A.A.; Akbar, M.A. Toward a secure global contact tracing app for COVID-19. In Proceedings of the International Conference on Evaluation and Assessment in Software Engineering 2022, Gothenburg, Sweden, 12–15 June 2022.
24. Zuhra, F.T.; Bakar, K.A.; Ahmed, A.; Tunio, A.M. Routing protocols in wireless body sensor networks: A comprehensive survey. *J. Netw. Comput. Appl.* **2017**, *99*, 73–97. [[CrossRef](#)]
25. Garousi, V.; Felderer, M.; Mäntylä, M.V. Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Inf. Softw. Technol.* **2019**, *106*, 101–121. [[CrossRef](#)]
26. SunilKumar, K. A review on security and privacy issues in wireless sensor networks. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017.
27. Mohsin, A.; Zaidan, A.; Zaidan, B.; Albahri, A.S.; Albahri, O.S.; Alsalem, M.; Mohammed, K. Real-time remote health monitoring systems using body sensor information and finger vein biometric verification: A multi-layer systematic review. *J. Med. Syst.* **2018**, *42*, 1–36. [[CrossRef](#)]
28. Itani, W.; Kayssi, A.; Chehab, A. Wireless body sensor networks: Security, privacy, and energy efficiency in the era of cloud computing. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2019; pp. 731–763.
29. Petersen, K.; Feldt, R.; Mujtaba, S.; Mattsson, M. Systematic mapping studies in software engineering. In Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), Bari, Italy, 26–27 June 2008.
30. Gebrie, M.T.; Abie, H. Risk-based adaptive authentication for internet of things in smart home eHealth. In Proceedings of the 11th European Conference on Software Architecture: Companion Proceedings, Canterbury, UK, 11–15 September 2017; pp. 102–108.
31. Hashemi, S.M. Secure Routing of WBAN with Monarchy Butterfly Optimization. In Proceedings of the 2017 2nd International Conference on Communication and Information Systems, Wuhan, China, 7–9 November 2017; pp. 155–158.
32. Hassan, M.; Katangur, A.; Kar, D. A Secure Body Sensor Network Architecture with CP-ABE Based Fine-Grained Data Access Control. In Proceedings of the Second International Conference on Advanced Wireless Information, Data, and Communication Technologies, Paris, France, 13–14 November 2017.
33. Altop, D.K.; Levi, A.; Tuzcu, V. SU-PhysioDB: A physiological signals database for body area network security. In Proceedings of the 2017 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), Istanbul, Turkey, 5–8 June 2017.
34. Gowtham, M.; Ahila, S.S. Privacy enhanced data communication protocol for wireless body area network. In Proceedings of the 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 6–7 January 2017.
35. He, D.; Zeadally, S.; Kumar, N.; Lee, J.H. Anonymous Authentication for Wireless Body Area Networks With Provable Security. *IEEE Syst. J.* **2017**, *11*, 2590–2601. [[CrossRef](#)]
36. Li, X.; Peng, J.; Kumari, S.; Wu, F.; Karuppiyah, M.; Choo, K.-K.R. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. *Comput. Electr. Eng.* **2017**, *61*, 238–249. [[CrossRef](#)]
37. Deng, Y.Y.; Chen, C.L.; Tsaur, W.J.; Tang, Y.W.; Chen, J.H. Internet of things (IoT) based design of a secure and lightweight body area network (BAN) healthcare system. *Sensors* **2017**, *17*, 2919. [[CrossRef](#)]
38. AlHamouz, S.; Naimat, A.M.A.; Fraihat, A. An Energy Preserving Practical Security Assessment on Wireless Body Area Networks. In Proceedings of the 2018 11th International Conference on Developments in eSystems Engineering (DeSE), Cambridge, UK, 2–5 September 2018.
39. Arfaoui, A.; Letaifa, A.b.; Kribeche, A.; Senouci, S.M.; Hamdi, M. A stochastic game for adaptive security in constrained wireless body area networks. In Proceedings of the 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 12–15 January 2018.

40. Izza, S.; Benssalah, M.; Ouchikh, R. Security Improvement of the Enhanced 1-round Authentication Protocol for Wireless Body Area Networks. In Proceedings of the 2018 International Conference on Applied Smart Systems (ICASS), Medea, Algeria, 24–25 November 2018.
41. Ji, S.; Gui, Z.; Zhou, T.; Yan, H.; Shen, J. An Efficient and Certificateless Conditional Privacy-Preserving Authentication Scheme for Wireless Body Area Networks Big Data Services. *IEEE Access* **2018**, *6*, 69603–69611. [[CrossRef](#)]
42. Mekki, N.; Hamdi, M.; Aguli, T. A Privacy-Preserving Scheme Using Chaos Theory for Wireless Body Area Network. In Proceedings of the 2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC), Limassol, Cyprus, 25–29 June 2018.
43. Wang, J.; Han, K.; Alexandridis, A.; Zilic, Z.; Pang, Y.; Lin, J. An ASIC Implementation of Security Scheme for Body Area Networks. In Proceedings of the 2018 IEEE International Symposium on Circuits and Systems (ISCAS), Florence, Italy, 27–30 May 2018.
44. Koya, A.M.; Deepthi, P.P. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. *Comput. Netw.* **2018**, *140*, 138–151. [[CrossRef](#)]
45. Shen, J.; Chang, S.; Shen, J.; Liu, Q.; Sun, X. A lightweight multi-layer authentication protocol for wireless body area networks. *Future Gener. Comput. Syst.* **2018**, *78*, 956–963. [[CrossRef](#)]
46. Ahlawat, R.K.; Malik, A.; Sadhu, A. Sybil attack prevention algorithm for body area networks. In *Nature Inspired Computing*; Springer: Singapore, 2018; pp. 125–134.
47. Anusya, G.; Sharmada, M.A.; Anitha, G.; Akilandeswari, G.; Azees, M. An Efficient and Secure Authentication Scheme for Wireless Body Area Networks. In Proceedings of the 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 20–21 April 2018.
48. Arfaoui, A.; Kribeche, A.; Boudia, O.R.M.; Letaifa, A.B.; Senouci, S.M.; Hamdi, M. Context-aware authorization and anonymous authentication in wireless body area networks. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018.
49. He, D.; Zeadally, S.; Wu, L. Certificateless Public Auditing Scheme for Cloud-Assisted Wireless Body Area Networks. *IEEE Syst. J.* **2018**, *12*, 64–73. [[CrossRef](#)]
50. Odesile, A.; Thamilarasu, G. Distributed intrusion detection using mobile agents in wireless body area networks. In Proceedings of the 2017 Seventh International Conference on Emerging Security Technologies (EST), Canterbury, UK, 6–8 September 2017.
51. Omala, A.A.; Mbandu, A.S.; Mutiria, K.D.; Jin, C.; Li, F. Provably Secure Heterogeneous Access Control Scheme for Wireless Body Area Network. *J. Med. Syst.* **2018**, *42*, 108. [[CrossRef](#)]
52. Omala, A.A.; Ali, I.; Li, F. Heterogeneous signcryption with keyword search for wireless body area network. *Secur. Priv.* **2018**, *1*, e25. [[CrossRef](#)]
53. Parvez, K.; Zohra, F.T.; Jahan, M. A secure and lightweight user authentication mechanism for wireless body area network. In Proceedings of the 6th International Conference on Networking, Systems and Security, Dhaka, Bangladesh, 17–19 December 2019; pp. 139–143.
54. Remu, S.R.H.; Faruque, M.O.; Ferdous, R.; Arifeen, M.M.; Sakib, S.; Reza, S.M.S. Naive Bayes based Trust Management Model for Wireless Body Area Networks. In Proceedings of the International Conference on Computing Advancements, Dhaka, Bangladesh, 10–12 January 2020.
55. Razaque, A.; Amsaad, F.; Khan, M.J.; Toksanovna, A.S.; Oun, A.; Almiani, M. Privacy Preserving Medium Access Control Protocol for wireless Body Area Sensor Networks. In Proceedings of the 2019 IEEE National Aerospace and Electronics Conference (NAECON), Dayton, OH, USA, 15–19 July 2019.
56. Hale, M.L.; Lotfy, K.; Gamble, R.F.; Walter, C.; Lin, J. Developing a platform to evaluate and assess the security of wearable devices. *Digit. Commun. Netw.* **2019**, *5*, 147–159. [[CrossRef](#)]
57. Karaođlan Altop, D.; Seymen, B.; Levi, A. SKA-PS: Secure key agreement protocol using physiological signals. *Ad Hoc Netw.* **2019**, *83*, 111–124. [[CrossRef](#)]
58. Konan, M.; Wang, W. A secure mutual batch authentication scheme for patient data privacy preserving in WBAN. *Sensors* **2019**, *19*, 1608. [[CrossRef](#)]
59. Yao, X.; Liao, W.; Du, X.; Cheng, X.; Guizani, M. Using Bloom Filter to Generate a Physiological Signal-Based Key for Wireless Body Area Networks. *IEEE Internet Things J.* **2019**, *6*, 10396–10407. [[CrossRef](#)]
60. Saif, S.; Biswas, S. Secure Data Transmission Beyond Tier 1 of Medical Body Sensor Network. In Proceedings of the International Ethical Hacking Conference 2018; Springer: Singapore, 2019; p. 811.
61. Xu, Z.; Xu, C.; Chen, H.; Yang, F. A lightweight anonymous mutual authentication and key agreement scheme for WBAN. *Concurr. Comput. Pract. Exp.* **2019**, *31*, e5295. [[CrossRef](#)]
62. Choi, S.; Shin, S.; Jin, X.; Shin, S. Secure and low computation authentication protocol for Wireless Body Area Network with ECC and 2D hash chain. In Proceedings of the International Conference on Research in Adaptive and Convergent Systems, Gwangju, Korea, 13–16 October 2020; pp. 130–135.
63. Voigt, T.; Yan, W.; Joseph, L.; Hylamia, S.; Asan, N.B.; Mani, M.; Mandal, B.; Perez, M.; Augustine, R. Jamming to Support Privacy-preserving Continuous Tumour Relapse Monitoring Using In-body Radio Signals. In Proceedings of the 1st International Workshop on Physical-Layer Augmented Security for Sensor Systems, Virtual Event, Japan, 16–19 November 2020; pp. 1–2.

64. Jabeen, T.; Ashraf, H.; Khatoon, A.; Band, S.S.; Mosavi, A. A Lightweight Genetic Based Algorithm for Data Security in Wireless Body Area Networks. *IEEE Access* **2020**, *8*, 183460–183469. [[CrossRef](#)]
65. Jegadeesan, S.; Azees, M.; Babu, N.R.; Subramaniam, U.; Almakhlles, J.D. EPAW: Efficient Privacy Preserving Anonymous Mutual Authentication Scheme for Wireless Body Area Networks (WBANs). *IEEE Access* **2020**, *8*, 48576–48586. [[CrossRef](#)]
66. Jouini, O.; Sethom, K. Physical Layer Security Proposal for Wireless Body Area Networks. In Proceedings of the 2020 IEEE 5th Middle East and Africa Conference on Biomedical Engineering (MECBME), Amman, Jordan, 27–29 October 2020.
67. Zhao, K.; Sun, D.; Ren, G.; Zhang, Y. Public Auditing Scheme with Identity Privacy Preserving Based on Certificateless Ring Signature for Wireless Body Area Networks. *IEEE Access* **2020**, *8*, 41975–41984. [[CrossRef](#)]
68. Hameed, M.E.; Ibrahim, M.M.; Manap, N.A.; Mohammed, A.A. A lossless compression and encryption mechanism for remote monitoring of ECG data using Huffman coding and CBC-AES. *Future Gener. Comput. Syst.* **2020**, *111*, 829–840. [[CrossRef](#)]
69. Liu, X.; Wang, Z.; Ye, Y.; Li, F. An efficient and practical certificateless signcryption scheme for wireless body area networks. *Comput. Commun.* **2020**, *162*, 169–178. [[CrossRef](#)]
70. Mahendran, R.K.; Velusamy, P. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Comput. Commun.* **2020**, *153*, 545–552. [[CrossRef](#)]
71. Qiu, H.; Qiu, M.; Lu, Z. Selective encryption on ECG data in body sensor network based on supervised machine learning. *Inf. Fusion* **2020**, *55*, 59–67. [[CrossRef](#)]
72. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J. Infect. Public Health* **2020**, *13*, 1567–1575. [[CrossRef](#)]
73. Shuai, M.; Liu, B.; Yu, N.; Xiong, L.; Wang, C. Efficient and privacy-preserving authentication scheme for wireless body area networks. *J. Inf. Secur. Appl.* **2020**, *52*, 102499. [[CrossRef](#)]
74. Sowjanya, K.; Dasgupta, M. A ciphertext-policy Attribute based encryption scheme for wireless body area networks based on ECC. *J. Inf. Secur. Appl.* **2020**, *54*, 102559. [[CrossRef](#)]
75. Wang, J.; Han, K.; Fan, S.; Zhang, Y.; Tan, H.; Jeon, G.; Pang, Y.; Lin, J. A logistic mapping-based encryption scheme for Wireless Body Area Networks. *Future Gener. Comput. Syst.* **2020**, *110*, 57–67. [[CrossRef](#)]
76. Wang, W.; Qin, T.; Wang, Y. Encryption-free data transmission and hand-over in two-tier body area networks. *Comput. Methods Programs Biomed.* **2020**, *192*, 105411. [[CrossRef](#)]
77. Chatterjee, K. An Improved Authentication Protocol for Wireless Body Sensor Networks Applied in Healthcare Applications. *Wirel. Pers. Commun.* **2020**, *111*, 2605–2623. [[CrossRef](#)]
78. Dakhel, M.; Hassan, S. A Secure Wireless Body Area Network for E-Health Application Using Blockchain. In *International Conference on Applied Computing to Support Industry: Innovation and Technology*; Springer: Cham, Switzerland, 2020; pp. 395–408.
79. Iqbal, J.; Waheed, A.; Zareei, M.; Umar, A.I.; Amin, N.U.; Aldosary, A.; Mohamed, E.M. A lightweight and secure attribute-based multi receiver generalized signcryption scheme for body sensor networks. *IEEE Access* **2020**, *8*, 200283–200304. [[CrossRef](#)]
80. Xiao, L.; Han, D.; Meng, X.; Liang, W.; Li, K.C. A Secure Framework for Data Sharing in Private Blockchain-Based WBANs. *IEEE Access* **2020**, *8*, 153956–153968. [[CrossRef](#)]
81. Ding, Y.; Xu, H.; Wang, Y. Group Authentication for Sensors in Wireless Body Area Network. Security, Privacy, and Anonymity in Computation, Communication, and Storage. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*; Springer: Cham, Switzerland, 2020; Volume 2021, p. 12383.
82. Shuai, M.; Xiong, L.; Wang, C.; Yu, N. Lightweight and privacy-preserving authentication scheme with the resilience of desynchronization attacks for WBANs. *IET Inf. Secur.* **2020**, *14*, 380–390. [[CrossRef](#)]
83. Chen, G.; Liu, X.; Shorfuazzaman, M.; Karime, A.; Wang, Y.; Qi, Y. MEC-Based Jamming-Aided Anti-Eavesdropping with Deep Reinforcement Learning for WBANs. *ACM Trans. Internet Technol.* **2021**, *22*, 1–17. [[CrossRef](#)]
84. Jiang, Z.; Liu, W.; Ma, R.; Shirazi, S.H.; Xie, Y. Lightweight Healthcare Wireless Body Area Network Scheme with Amplified Security. *IEEE Access* **2021**, *9*, 125739–125752. [[CrossRef](#)]
85. Morales-Sandoval, M.; De-La-Parra-Aguirre, R.; Galeana-Zapién, H.; Galaviz-Mosqueda, A. A Three-Tier Approach for Lightweight Data Security of Body Area Networks in E-Health Applications. *IEEE Access* **2021**, *9*, 146350–146365. [[CrossRef](#)]
86. Amudha, S.; Murali, M. DESD-CAT inspired algorithm for establishing trusted connection in energy efficient FoG-BAN networks. *Mater. Today Proc.* **2021**. [[CrossRef](#)]
87. Izza, S.; Benssalah, M.; Drouiche, K. An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *J. Inf. Secur. Appl.* **2021**, *58*, 102705. [[CrossRef](#)]
88. Mohit, P. An efficient mutual authentication and privacy prevention scheme for e-healthcare monitoring. *J. Inf. Secur. Appl.* **2021**, *63*, 102992. [[CrossRef](#)]
89. Sharmila, A.H.; Jaisankar, N. Edge Intelligent Agent Assisted Hybrid Hierarchical Blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT. *Comput. Netw.* **2021**, *200*, 108508.
90. Kumar, A.; Singh, K.; Khan, T. L-RTAM: Logarithm based reliable trust assessment model for WBSNs. *J. Discrete Math. Sci. Cryptogr.* **2021**, *24*, 1701–1716. [[CrossRef](#)]
91. Li, Y.; Zhang, F. An Efficient Certificate-based Data Integrity Auditing protocol for Cloud-Assisted WBANs. *IEEE Internet Things J.* **2021**, *9*, 11513–11523. [[CrossRef](#)]

92. Liu, Q.; Mkongwa, K.G.; Zhang, C.; Wang, S. A simple cross-layer mechanism for congestion control and performance enhancement in a localized multiple wireless body area networks. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–18. [[CrossRef](#)]
93. Noor, F.; Kordy, T.A.; Alkhodre, A.B.; Benrhouma, O.; Nadeem, A.; Alzahrani, A. Securing Wireless Body Area Network with Efficient Secure Channel Free and Anonymous Certificateless Signcryption. *Wirel. Commun. Mob. Comput.* **2021**, 2021, 5986469. [[CrossRef](#)]
94. Zhang, X.; Zhao, J.; Xu, C.; Li, H.; Wang, H.; Zhang, Y. CIPPPA: Conditional Identity Privacy-Preserving Public Auditing for Cloud-Based WBANs against Malicious Auditors. *IEEE Trans. Cloud Comput.* **2021**, 9, 1362–1375. [[CrossRef](#)]
95. Nidhya, R.; Shanthy, S.; Kumar, M. A Novel Encryption Design for Wireless Body Area Network in Remote Healthcare System Using Enhanced RSA Algorithm. In *Intelligent System Design*; Springer: Singapore, 2021.
96. Sudha, R. An Emerging Trust-Based Security on Wireless Body Area Network. In *Sustainable Communication Networks and Application*; Springer: Singapore, 2021.
97. Shanmugavadeivel, G.; Gomathy, B.; Ramesh, S.M. An Enhanced Data Security and Task Flow Scheduling in Cloud-enabled Wireless Body Area Network. *Wirel. Pers. Commun.* **2021**, 120, 849–867. [[CrossRef](#)]
98. Zhang, S.; Zhuang, Y.; Cao, Z. Intelligent Medical Security Framework of Body Area Network Based on Fog Computing. Security, Privacy, and Anonymity in Computation, Communication, and Storage. In *International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage*; Springer: Cham, Switzerland, 2020; Volume 2021, p. 12382.
99. Chunka, C.; Banerjee, S. An Efficient Mutual Authentication and Symmetric Key Agreement Scheme for Wireless Body Area Network. *Arab. J. Sci. Eng.* **2021**, 46, 8457–8473. [[CrossRef](#)]
100. Liu, Y.; Wang, Y.; Peng, Z. A novel and efficient anonymous authentication for WBANs. *Internet Technol. Lett.* **2021**, e304. [[CrossRef](#)]
101. Ramadoss, J. Body sensor network encryption and team user authentication scheme based on electrocardiogram detector. *Int. J. Commun. Syst.* **2021**, 34, e5002. [[CrossRef](#)]
102. Hussain, S.J.; Irfan, M.; Jhanjhi, Z.N.; Hussain, K.; Humayun, M. Performance enhancement in wireless body area networks with secure communication. *Wirel. Pers. Commun.* **2021**, 116, 1–22. [[CrossRef](#)]
103. Aadil, F.; Mehmood, B.; Ul Hasan, N.; Lim, S.; Ejaz, S.; Zaman, N. Remote health monitoring using IoT-based smart wireless body area network. *CMC-Comput. Mater. Contin.* **2021**, 68, 2499–2513. [[CrossRef](#)]
104. Hamid, B.; Jhanjhi, N.; Humayun, M.; Khan, A.; Alsayat, A. Cyber Security Issues and Challenges for Smart Cities: A survey. In *Proceedings of the 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS)*, Karachi, Pakistan, 14–15 December 2019; pp. 1–7. [[CrossRef](#)]