technologies

MDPI

Review

Advanced Security Framework for Internet of Things (IoT)

Abid Ali [1], Abdul Mateen [1], Abdul Hanan [2] and Farhan Amin [3,*]

[1] Department of Computer Science, Federal Urdu University of Arts, Science & Technology, Islamabad 44000, Pakistan; abid.khawaja11@gmail.com (A.A.); abdul.mateen.cs@gmail.com (A.M.)
[2] Department of Computer Science, CECOS University, Peshawar 25000, Pakistan; hanan@cecos.edu.pk
[3] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Korea
* Correspondence: farhanamin10@hotmail.com

Abstract: The stimulus to carry out this research was to identify and propose a secure framework for the Internet of Things (IoT). Due to the massive accessibility and interconnection of IoT devices, systems are at risk of being exploited by hackers. Therefore, there is a need to find an advanced security framework that covers data security, data confidentiality, and data integrity issues. The study uses a systematic literature review (SLR) technique and complete substantive literature is reviewed to find out the constructs and themes in the existing literature. We performed it in four steps, which were inclusion, eligibility, screening, and identification. We reviewed around 568 articles from well-reputable journals, and after exclusion, 260 articles and 54 reports were analyzed. We performed an analysis using MAXQDA in which the nodes and themes were first identified. After the classification, a qualitative model was generated using MAXQDA. The proposed model is supported by the literature so it will be useful for the IT managers, developers, and the users of IoT.

Keywords: Internet of Things; data availability; data security; data confidentiality; data integrity

Citation: Ali, A.; Mateen, A.; Hanan, A.; Amin, F. Advanced Security Framework for Internet of Things (IoT). *Technologies* **2022**, *10*, 60. https://doi.org/10.3390/technologies10030060

Academic Editors: Manoj Gupta, Eugene Wong and Gwanggil Jeon

Received: 9 April 2022
Accepted: 10 May 2022
Published: 12 May 2022

1. Introduction

The twenty-first century is known as the era of interconnectivity and wireless communication where the world has witnessed some major technological revolutions in computer networking. The term Internet of Things (IoT) was coined by Kevin Ashton in 1999 [1]. The IoT provides a way of connectivity of things to things. The "thing" refers to all the things around us that are connected to the network. For example, the household appliances at home that are connected to the internet. IoT technology is used to share information and generate useful information between "things". It can operate without human intervention. The IoT concept is illustrated in Figure 1.

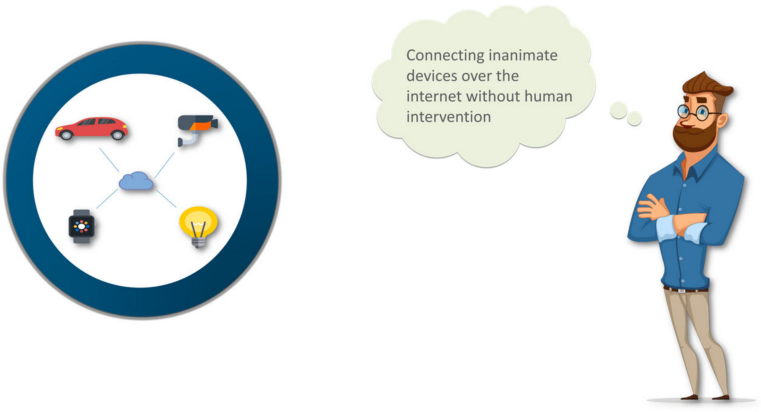

Figure 1. The concept of the Internet of Things.

In this Figure, the things are connected without human intervention. The traditional role of human command has been overpowered by the analytical capability of the IoT. Mobile phones, actuators, transceivers, protocol stacks, and microcontrollers have been developed to provide a firm connection and communication through the IoT. The data are collected and transmitted back to these devices with certain commands. The automated actions are made based on these suggested commands. The concepts of the IoT have been updated to improve the current Internet infrastructure to advanced network infrastructure, and have brought a technological revolution to the IT industry. The concept of the IoT suggests some interconnection between devices that include the facility of device autonomy, contextual awareness, sensing capability, and so on. To implement the IoT platform, many technologies and sensors, such as radiofrequency identifiers and networks of wireless sensors, are being used nowadays. However, in a conventional Internet protocol (IP), the security mechanisms need to be extended and modified to support IoT applications. The current IoT architecture is usually divided into three layers: the perception layer, the network layer, and the application layer. Figure 2 illustrates this architecture. The other forms are four-layer, five-layer, and seven-layer architecture, etc. However, we will use the three-layer architecture for illustration. The interaction of the sensors, actuators, and edge devices is the key part of this layer. The perception layer is used to identify the objects, perceive objects, collect information, and automatic control. This layer contains different types of control modules and collecting devices, such as the sound sensors, the temperature and pressure sensors, vibration sensors, etc., as shown in Figure 2. The perception layer is further divided into two parts: the perception node (controllers and sensors, etc.) and the perception network (transportation communication network) [2]. The use of the perception layer is to control data and data acquisition, while the perception network sends control instructions to the controller. The perception layers include implantable medical devices (IMDs), Global Positioning Systems (GPS), implantable medical devices (IMDs), Radio Frequency Identification (RFI), etc. The identification of abnormal sensor nodes is the one of security issues. It occurs when the node is attacked physically (e.g., destroyed or disabled). In general, these nodes are also known as faulty nodes. To ensure the standards of service, it is necessary to detect the fault codes and overcome the causes of lower standard services [3,4]. Another security concern of the perception layer is the key management mechanism and cryptography algorithms. For node authentication, public keys have been considered convenient. It is better to secure the entire network without any management protocol of complicated keys and to have large scalability [5]. According to [6], the most promising candidates for wireless sensor networks are three low-power public key encryption algorithms, namely, Rabin's Scheme, Ntru Encrypt, and the Elliptic Curve Cryptography. The network layer mainly realizes the transmission of information, routing (deciding the way of information transmission), and control (how to control the transmission of information). It is divided into two parts; one part is the communication technology and the other is the communication protocol of the Internet of Things. Communication technology is responsible for physically linking things with things to enable them to communicate. The communication protocol is responsible for establishing communication rules [7]. The application layer provides users with professional services and functional data processing and storage [8]. It has the support of the cloud and servers for the storage of data in the network. Our study is more focused on the aspect of data security in the IoT. The key data security aspects are given below:

1.1. Data Security in IoT

Currently, data security and privacy protection should be adopted equally to offer robust data security. Accessing and securing data by a static approach has become unacceptable because it fails to address the scalable data security IoT [5]. The security support is not always maintained. Consumer knowledge of IoT security is weak: security incidents can be difficult to detect or to resolve for usage [9].

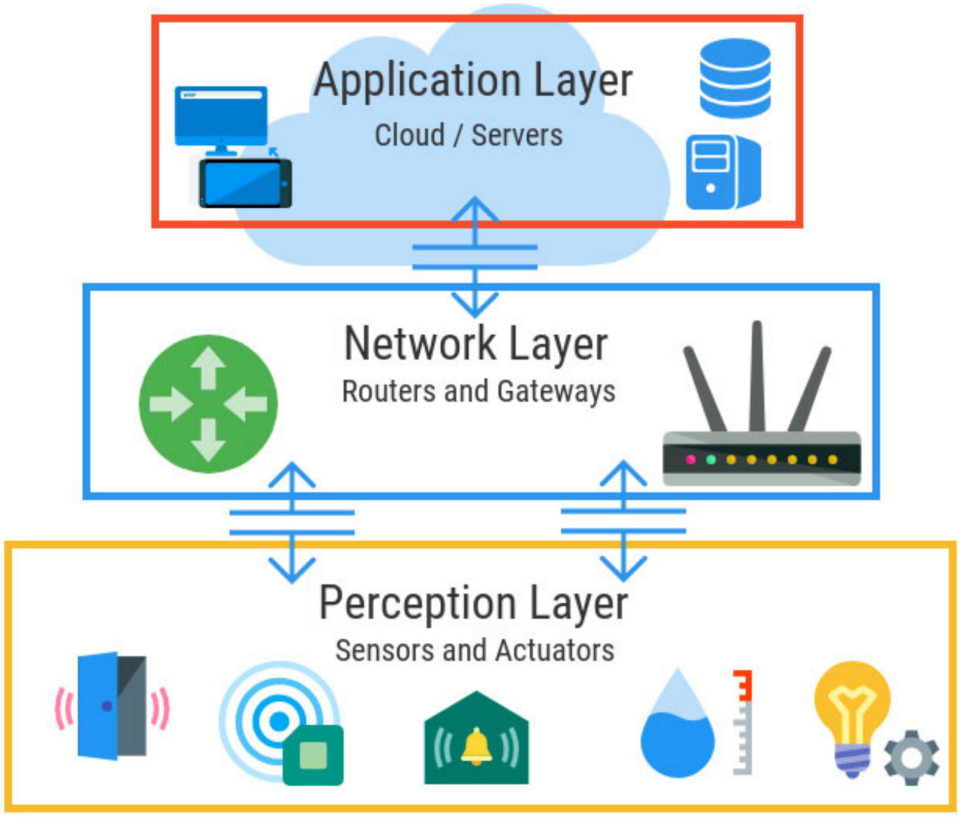

Figure 2. A three-tier IoT.

1.2. Data Integrity in the IoT

Data integrity is necessary for up-to-date and accurate data. It is very important to store data by any person or organization for integrity [10]. It is significant that data integrity in the IoT is measured, as data need to be secure and every transaction of data needs to be secure. Defining the integrity of data is easy but it is hard to ensure.

1.3. Data Confidentiality in the IoT

To keep data private in the public domain is called 'data privacy'. Data privacy terms can be applied to any organization or a person. Data are always limited and related to any person's life and existence [11]. He or she can keep the data private or public. An organization can also keep its data private, such as for financial statement reports or business plans. If there is no framework available for establishing personal privacy, then the privacy of any individual is very limited [12,13]. Data security and data privacy are used in many situations in the same context, but there is a distinct difference; data security is broadly thought to be about protection and saving your data from other unknown persons, whereas data privacy is to control where your data are collected, shared, and used for which, and for what, purpose.

1.4. Data Validity in the IoT

Data validity ensures that IoT services are practically available. If these services are unavailable, total progress can be decreased; it will also facilitate and provide help to hackers and attackers who are working in different smart industries, smart cities, and smart home etc. [6]. With the development of connected objects, users entrust part of their privacy to improve their environment and make their living environment more efficient and safer. There are risks to the person and his data; for example, a hacked surveillance camera lets you know if the owner is away or not from their home; a smart electricity meter: the meter can quickly become a spy if you are not careful [14].

1.5. Current IoT Security Framework

1. It consists of sensors, actuators, and other embedded systems [15].
2. Fog set of connections: A class of exchange ideas, technologies, and protocols by several IoT policies with the prerequisite to expand and enforce an entire confidence policy [16].
3. Core Complex: It provides a set of connection center platforms and IoT devices. The issues at this time are individuals confronted with conventional fundamental networks [17]. The measureless number of endpoints act together and get by to create a considerable precautions burden. Thus, based on the suggestions made in previous research papers, the current study proposes a security framework for the IoT in terms of data confidentiality, availability, and integrity.

The study has used the Systematic Literature Review (SLR) approach to find out the best security framework, which covers and identifies any problems. This study has provided a detailed analysis of prior published literature on the topic and compared the strengths and weaknesses of at least 20 security frameworks to evaluate and find out the best security framework for the IoT. This research mainly focuses on the three major security requirements, namely, data confidentiality, data availability, and data integrity. Therefore, the IoT has built a strong impact on commercial to domestic spheres of life, but besides this positive side, the IoT has introduced another darker side to the security and privacy of the person. The accessibility and interconnectivity of IoT devices have put the system at risk of being exploited by hackers [5,9].

1.6. Motivation of This Study

To the best of our knowledge, the literature still lacks research on extracting useful studies from a large pool based on the security aspects of data such as integrity, etc. Therefore, the stimulus to carry out this research was to identify and propose a secure framework for the emerging technologies.

1.7. Contribution of This Study

This study proposes a security model. In this model, the literature is reviewed from a large pool and, hence, suitable literature was extracted. We herein defined an article's inclusion and disillusion criteria and applied them to a large dataset. The model can select or discard the most relevant literature. It can easily be applied to emerging technologies such as the Internet of things (IoT). Briefly, we highlighted the different aspects and security concerns of the IoT. We also discussed recent solutions, along with comparisons and contrast. Our model is useful for IT managers, developers, and users, in extracting the most relevant literature from the databases. The rest of our study is organized as follows. In Section 2, we performed a literature review and discussed our proposed model. In Section 3, we have discussed inclusion criteria and explained that how we generate the results. In Section 4, we discuss the proposed model based on the achieved results. Finally, Section 5 offers conclusions from this study and suggests future work.

2. Literature Review and the Selection Criteria

In this study, we proposed a systematic literature review (SLR). We adopted an advanced method by Brinner and Denver. The detailed steps of the adopted methodology include the following steps. First, we performed systematic identification of the need for a systematic literature review and finalized the review protocol. On this site, we performed the election of studies and assessed their quality, and took notes to extract the relevant data. Finally, we reported and discussed the results. The details of our proposed methodology are given below.

2.1. Selection of Relevant Studies

To address the primary objective of this study, we performed a systematic literature review. This review was conducted in May 2020 without time restrictions, and the result

was updated in June 2020. In this review study, we extracted relevant literature from esteemed journals, such as Scopus, the Web of Science, Google Scholar, ScienceDirect, etc. The relevant grey literature, such as government publications and unpublished material, was searched systematically [18]. To locate the grey literature, the first 150 hits from Google Scholar were evaluated. The keyword search and alternate key work searching were used to locate the relevant studies that aligned with our objectives. The hand search reference list further locates various other sources of grey literature, particularly, committee and research documents and policy briefs from both public and private sector organizations. Accordingly, the flow chart of the strategy for locating the studies is shown in Figure 3. Furthermore, various refinement features of the Web of Science, Google Scholar, and Scopus were applied to find the most relevant studies. The articles with missing abstracts were retrieved and scrutinize for relevance. All the articles accessed through different journals were retrieved in full text.

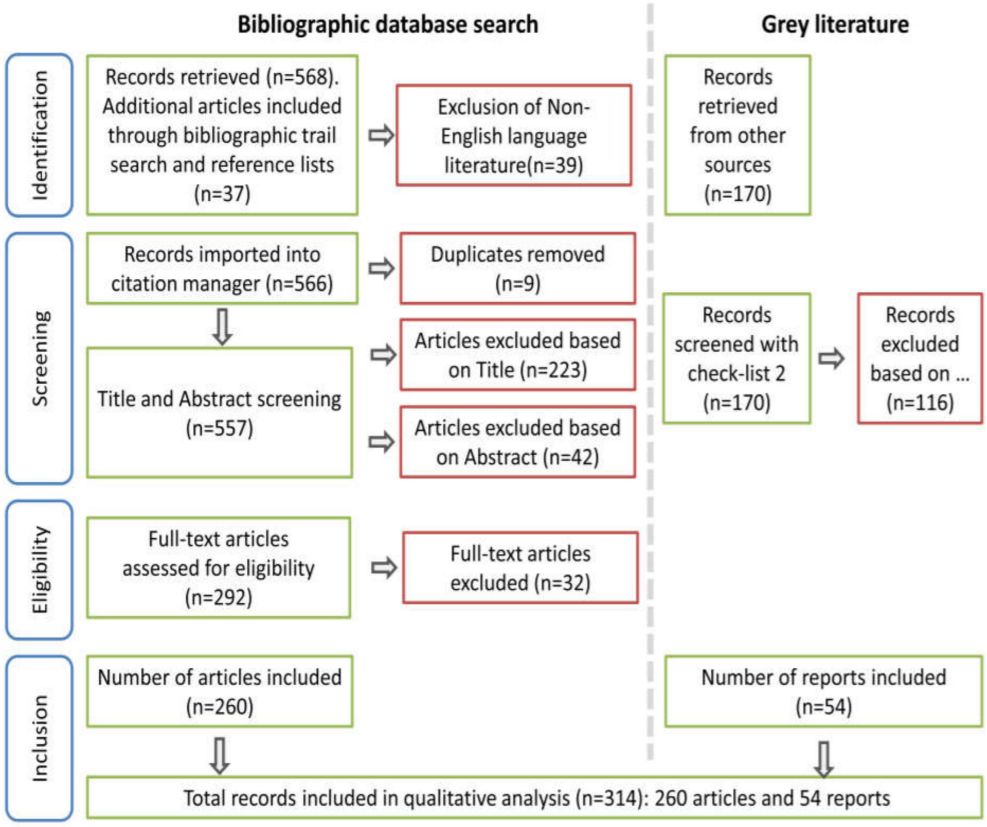

Figure 3. Flow chart of the strategy for locating the studies.

2.2. Evaluation

In this step, the selection and evaluation were performed using a systemic literature review. The eligibility of the accessed articles was examined independently based on pre-defined criteria that were outlined for inclusion and exclusion [19]. The exclusion criteria were applied especially when the search was performed in selected databases, such as custom range in terms of year, language, and subject. At first, the abstract of the paper was evaluated to determine its relevance. The studies that met the exclusion criteria were excluded and sorted by cause of exclusion. After carefully evaluating and scrutinizing the abstract of the retrieved articles, a full-text review was made and additional articles were discarded by using the exclusion criteria. The discrepancy concerning the relevance of the articles was resolved through the specific criteria for inclusion of the articles. The articles that remained out of the scope were excluded, and a refined list of articles was finalized. Articles from the Web of Science and Google Scholar that did not fit the inclusion criteria were discarded to avoid ambiguity.

2.3. Analysis and Synthesis

The retrieved and evaluated articles were finalized based on the inclusion criteria and processed through qualitative analysis software (MAXQDA11). The processing of the data results was performed in major themes. The thematic content analysis was made to determine the major theme that emerged in the selected articles. Thematic analysis is one of the commonly used qualitative research techniques; it analyses and interprets various patterns of qualitative data. In our context, the qualitative data were extracted from the selected papers [19]. Thematic analysis is a widely employed technique in contrast to most other qualitative analytic approaches, such as narrative analysis and discourse analysis, which are also widely used in a systematic literature review (SLR). The thematic analysis in a systematic literature review enables the detection of major trends and patterns in the collected papers. The significant themes remain the ones that predominate and remain prominent; after completing the thematic analysis, the coding is complete. The coding is a systematic process of indexing the text to develop a framework of major themes. The coding enables the entire process to be effective and robust. Aligned with past studies expounded in past literature, categorically, there are two types of coding that were identified; one is data-driven, and second is the concept-driven coding [20,21]. We aligned our study with past studies that used data-driven coding, and the data extracted from the selected papers were coded accordingly.

3. Reporting and Discussion of the Results

The retrieved data and articles were finalized based on the inclusion criteria. These data were processed through qualitative analysis software, i.e., MAXQDA20, which processed the data results in terms identifying different themes. The core objective of thematic content analysis is to determine various major themes. Thematic analysis is one of the commonly used qualitative research techniques. It is used to perform analyses and interprets various patterns of qualitative data. In our context, the qualitative data were extracted from the selected papers. Figure 4 illustrates how the article files were imported to the MAXQDA 20 for inferring the results. The first step in MAXQDA 20 was to conduct a quantitative analysis, whereby the file is imported and proceeded to further analysis. Once the required file has been imported, the next step is to run the auto coding. The auto code results are significant to determine which variables were reputedly used in past studies. Figure 4 illustrates the auto-coding results and confirms how many times the given variables that remain significant to the IoT remain significant. The details of the rest of the steps are given below.

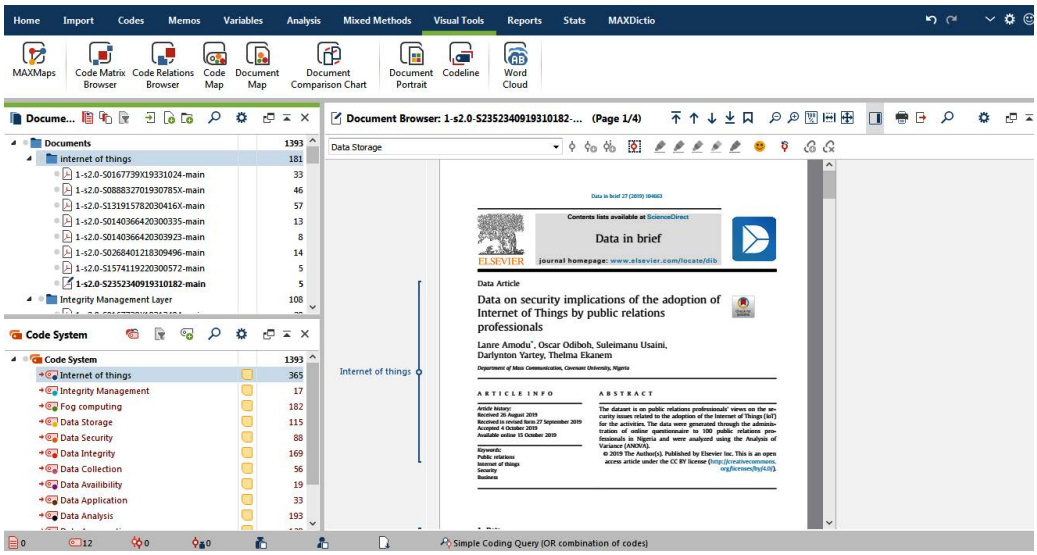

Figure 4. Data File in MAXQDA20.

3.1. Auto Codes Results from SLR

Figure 5 shows the auto-coding result. In this Figure, the auto-coding results of the selected articles reflect that articles were selected for analysis 365 times. Integrity management was used seventeen times while fog computing was used 182 times. Accordingly, data storage also remains one of the most important features of IoT as it was extensively examined and discussed 115 times in the past literature. Data security and data integrity were used 88 and 169 times, respectively. The data collection and data availability were used 56 and 19 times in articles that were selected for analysis. Data application and data analysis were used 33 and 193 times in the articles that were used for the analysis. Data aggregation and data confidentiality reflect that they were used 128 times and 28 times, respectively. Based on the auto coding, it was inferred that data analysis and data integrity along with fog computing remain the main determinants of IoT. Our efficient model contains the features of data analysis and data integrity along with fog computing to develop and implement the most robust digital system for an organization.

	Parent code	Code	Code alias	Cod. seg. (all ...
		Internet of things		365
		Integrity Manag...		17
		Fog computing		182
		Data Storage		115
		Data Security		88
		Data Integrity		169
		Data Collection		56
		Data Availibility		19
		Data Application		33
		Data Analysis		193
		Data Aggregation		128
		Data Confidentia...		28

Figure 5. Auto Codes Results from SLR.

3.2. The Codes Cloud

Based on auto coding, the codes cloud was generated. The codes cloud and auto coding are integrated. The codes cloud remains more convenient to interpret and is widely used in information technology (IT) research to make robust analyses. Figure 6 presents the phenomenon that the main codes cloud is generated based on auto coding. The codes cloud shown in this Figure state that the IoT remains one of the most significant themes appearing in the articles examined. A quantitative analysis was performed through software that enabled us to detect the major themes used in studies expounded in past literature. The codes cloud reflect that besides IoT, fog computing also remains the second major theme used in the studies analyzed. Data aggregation was also outlined as the third major theme that remains critical for effective IoT. Besides these four major themes, fog computing, and data aggregation, other minor themes were discovered through the codes of the cloud. The minor themes mainly include data collection, integrity management, data confidentiality, and data application. These minor themes all remain the key determinants of the IoT. Based on codes cloud, it remains essential to infer that collectively the IoT contains various major and minor determinants that should be considered when implementing a framework relevant to the IoT. The organization of major themes such as fog computing and data aggregation is important considering their significance, along with the other elements of IoT, such as data collection, integrity management, data confidentiality, and data application. These should be considered to be important to develop and implement effective IoT. The

IoT contains all the elements of fog computing, namely, data aggregation, data collection, integrity management, data confidentiality, and data application. These can be used to improve the effectiveness and efficiency of the system. The efficiency and effectiveness of the IoT is the main attribute that should be fulfilled to run the affairs of the organization effectively. Therefore, based on auto coding and code cloud, an analysis of the articles was selected for SLR through qualitative analysis software (MAXQDA20), it is asserted that IoT is an integrated and multifaceted phenomenon. The organizations that aim to develop and implement effective IoT should conduct internal and external analyses. The IoT remains standardized but should be aligned with organizational strategy to promote efficiency.

Figure 6. Codes Cloud are generated based on auto coding.

3.3. Word Frequencies

The IoT is a relatively new concept in communication studies as it is still developing with the evolution of the IoT and its dominations. Thus, the growing influence of the IoT on commercial and domestic spheres has raised concerns regarding the availability, confidentiality, and integrity of data. For auto coding and code cloud, an analysis of the articles was selected for SLR through qualitative analysis software (MAXQDA20). Besides auto coding and code cloud, the keywords in the literature were examined to determine which keywords remain significant and had been used widely in past studies. Figure 7 reflects the most significant and insignificant keywords used in the current literature. The keyword remains dominant and widely used in past literature. Data availability remains the first prerequisite while dealing with IoT. Data availability is very important, the other determinants of IoT remain useless, as one cannot ensure the computations and processing of the data without its availability. Data availability is based on an SLR keyword search and remains one of the primary features of the IoT. Data security after data availability remains vital to keep the privacy of the information. In a connected world, data security and privacy sensitivity, and in recent times, an increase in exponential data availability, have become a big challenge. However, with the increase in security sophistication information needed for a launch, any attack decreases. That is why the security measurement and privacy protection should be adopted equally to offer robust data security and end to end. For regulating access and securing data, a static approach is not acceptable because it fails to address the necessity that a mechanism of scalable data security IoT is conceivably generally involved and an immature part of net safety. The third keyword that is significant remains critical in ensuring the effectiveness of cloud computing. Cloud computing is popular due to advancements in information and cloud technology; it remains robust to ensure data security and effective backups so that the processing and accuracy of the data are achieved effectively. The next dominant and significant keyword search that is highlighted in the above figure is known as data integrity. Data integrity is defined as

the reliability and validity of the data being used for analysis. It is the most vital feature of IoT as it is the primary concern of the entire stakeholder who uses such a system to assist their decision making through information. The information is accessed through the processing of data, which provides valuable information to the stakeholder to make a different decision. Therefore, if the data integrity remains minimal, the data reliability and validity will jeopardize the stakeholder's decision making. The information extracted, based on data that have integrity pitfalls, remains misleading and will result in economic losses. Therefore, one of the most important things that needs to be ensured during the process of the IoT is data integrity. The studies that were expounded in past literature confirmed the significance of data integrity, and it is a repeated keyword that was found to be a significant keyword search. However, it was found in the above figure that in our keyword search of the literature, confidentiality of data was found as being the least popular keyword search. These security issues have received the attention of academics, policymakers, and security experts toward ensuring the confidentiality and security of IoT devices and consumers' privacy. Hundreds of surveys were published to address these security challenges, but very limited efforts were made to design a framework that can resolve these security challenges.

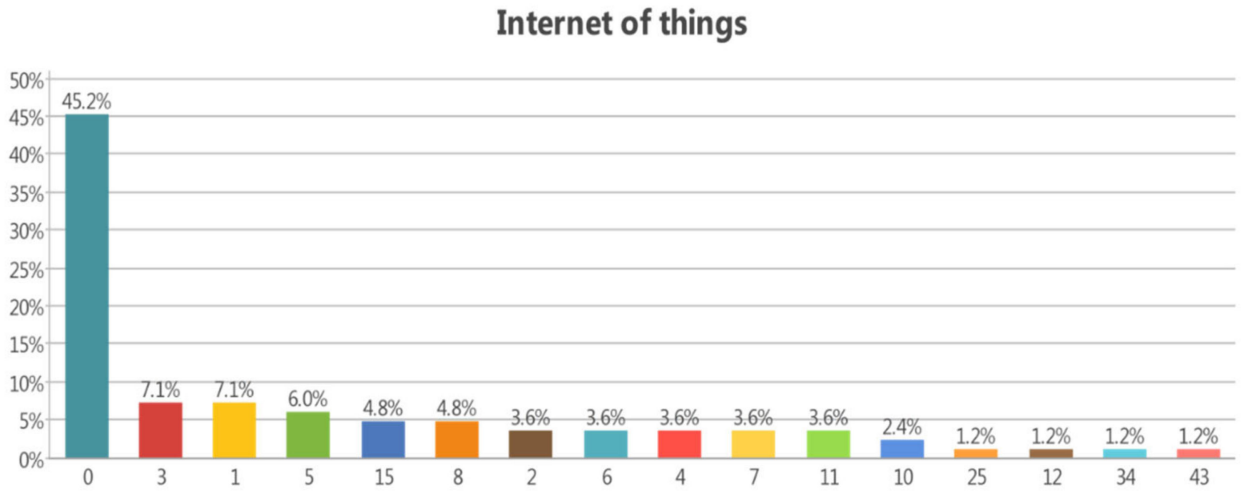

Figure 7. Significant and insignificant keywords being used in the literature.

3.3.1. Data Confidentiality

The growing influence of the IoT on commercial and domestic spheres has raised concerns regarding the availability, confidentiality, and integrity of data. By auto coding and cloud code, an analysis of the articles was selected for SLR through qualitative analysis software (MAXQDA11). Besides auto coding and code cloud, the keywords in the literature were identified. The significance of each feature of IoT was examined to determine which keywords remain significant and had been widely used by past studies expounded in literature. Figure 8 reflects the data confidentiality used in past studies. Data confidentiality remains one of the most important features of the IoT. This connection between the physical and visual world with the help of software and sensors has opened up possibilities to connect the required data or information at any time. However, these possibilities have also added certain threats to human security and confidentiality in the world of interconnected devices, where sensitive private information of users can be manipulated or leaked by hackers. As per past studies, our results also confirm the significance of data confidentiality. The studies expounded in past literature proclaim that 25% of the studies remain concerned with data confidentiality. The IoT exposes an organization to various types of risk. The information that remains private and confidential may be used by an unauthorized user to adversely affect the reputation of the business. Trust remains one of the most important elements in the IoT. Therefore, the breaching of security and privacy has introduced a

whole new degree of online privacy concerns for consumers because these devices not only can collect personal information such as users' names and telephone numbers, but can also monitor users' activities. Due to the utmost significance of data confidentiality, most organizations have separately established a cyber security system that ensures data confidentiality and prevents the data's unauthorized use. The number of studies and applied research have surged and studies have devoted their attention to developing frameworks and models that robustly contain the feature of data confidentiality. The IoT without data confidentiality remains ineffective in meeting stakeholder and organizational needs effectively.

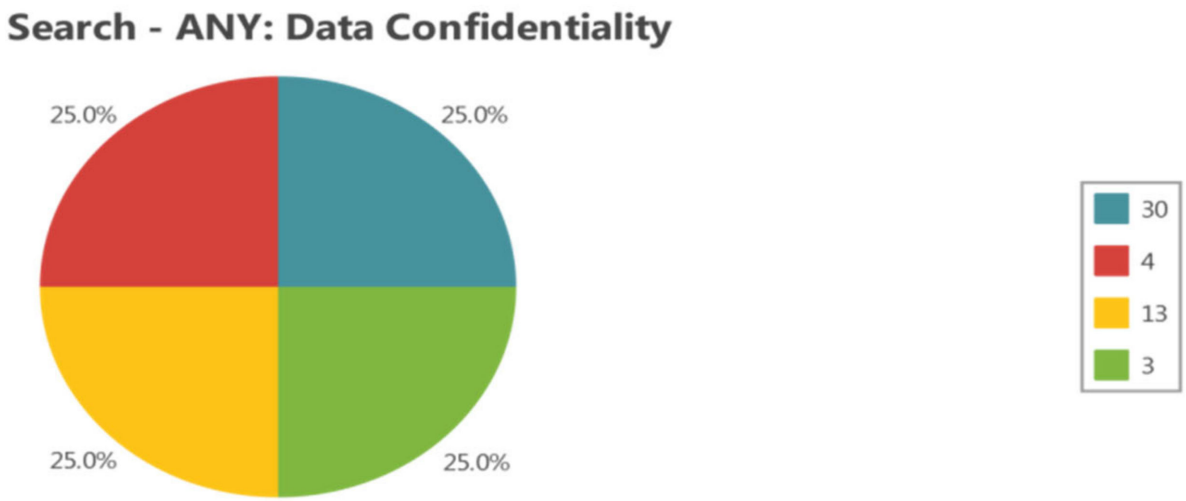

Figure 8. Data confidentiality of past studies.

3.3.2. Internet of Things

This is the second major theme that remains dominant in the literature. The SLR was conducted based on selected articles and analyzed through software to predict the most significant themes being discussed in the literature. The past few decades have witnessed an increased devotion to empirical studies toward examining the role of IoT and its determinants. The analysis of the selected articles states that the IoT has been discussed most frequently in past studies and has been examined by various methods. The objectives of these studies that remain concerned with the IoT are similar. The underlying objective of these studies remains concerned with methods and frameworks that remain robust for the effectiveness and efficiency of the IoT. The IoT is relatively a new concept in communication studies as it is still developing with the evolution of the IoT and its dominations. Thus, the growing influence of the IoT on commercial and domestic spheres has raised concerns regarding the availability, confidentiality, and integrity of data. Therefore, the underlying objective of this study was to analyze the significance of SLR. The results of our study suggest that most of the literature remains devoted to the IoT. The underlying theories and framework being postulated in past studies remain robust to improve the reliability of the IoT and improve organizational capabilities. Researchers have tried to find the role of the IoT in human life along with proposed challenges to data availability, confidentiality, and integrity, but very limited data have been published on security mechanisms that can address these challenges. The adoption of the IoT appears to occur regardless of the type of organization. Figure 9 reflects the significance of IoT and its appearance in earlier studies. The studies remain devoted to understanding the phenomenon that is the IoT.

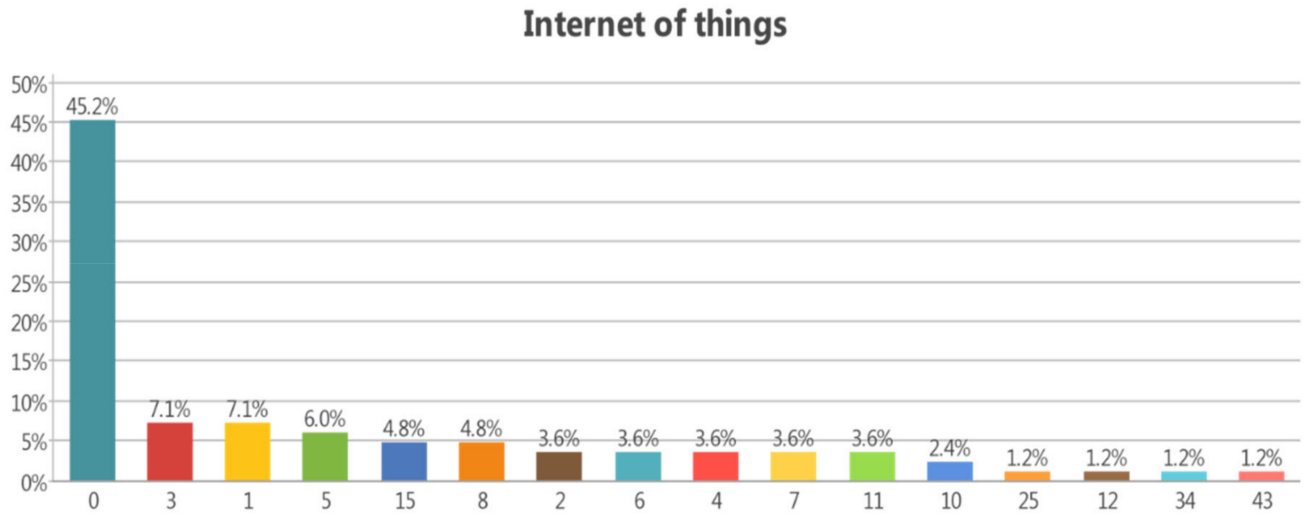

Figure 9. Significance of the IoT and its appearance in past studies.

3.3.3. Integrity Management Layer

The third major theme that appeared significant in past studies is known as the integrity management layer. This layer has become one of the most robust determinants of the IoT. The integrity management layer ensures the reliability and validity of the data. Thus, the growing influence of the IoT on commercial and domestic spheres has raised concerns regarding the availability, confidentiality, and integrity of data. Therefore, these limitations and loopholes in the security framework of the IoT have been considered during the implementation of safety mechanisms, and it is expected that this proposed research will bring new insights regarding the current security practices of the IoT and provide a solution to address any problems. Our study suggests that integrity management is considered the most pivotal and robust element of the IoT as it is essential to determine the effectiveness and efficiency as shown in Figure 10. The selected papers were chosen based on a specified threshold and reflect the past studies that remain devoted to integrity management. The integrity ensures that data input and processing and its output remain reliable and valid to ensure the effectiveness and efficiency of the IoT.

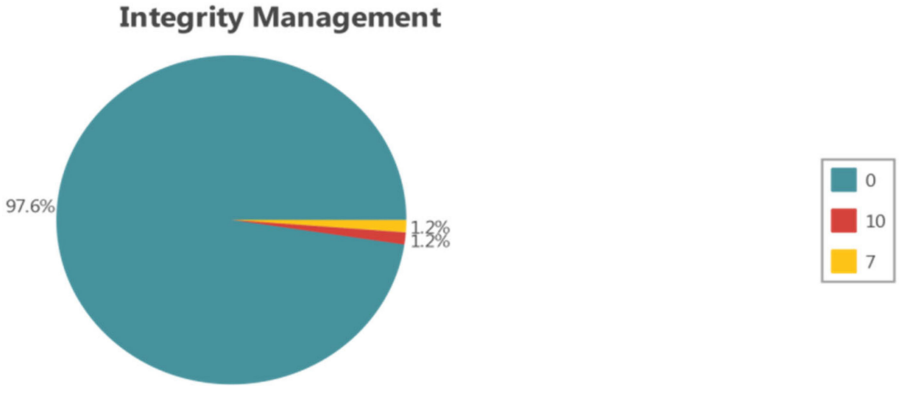

Figure 10. Effectiveness and efficiency of the IoT.

3.3.4. Fog Computing Layer

Fog computing is nowadays considered the most vital element of the IoT as it is presumed that it makes data storage and access more reliable and safer.

3.3.5. Data Storage Layer

The IoT should contain enough capacity to store the collected and processed data with an element of high privacy. The data storage should be robust so that its access can

be granted only to authorized users. The use of data storage, due to advancements in technology, has risen, and it has become convenient for companies to manage their data storage effectively. The SLR technique shown in Figure 11 reflects that 59% of the studies are being investigated. It shows that data storage is one of the most potent determinants of IoT. The traditional cryptography solutions cannot work anymore on IoT systems since these devices have limited and less space for storage. It cannot manage the heavyweight and advanced cryptography algorithm storage requirements. Therefore, alternative storage frameworks and models were developed through empirical examination to uplift the data storage, which ensures the dynamic needs of the organization.

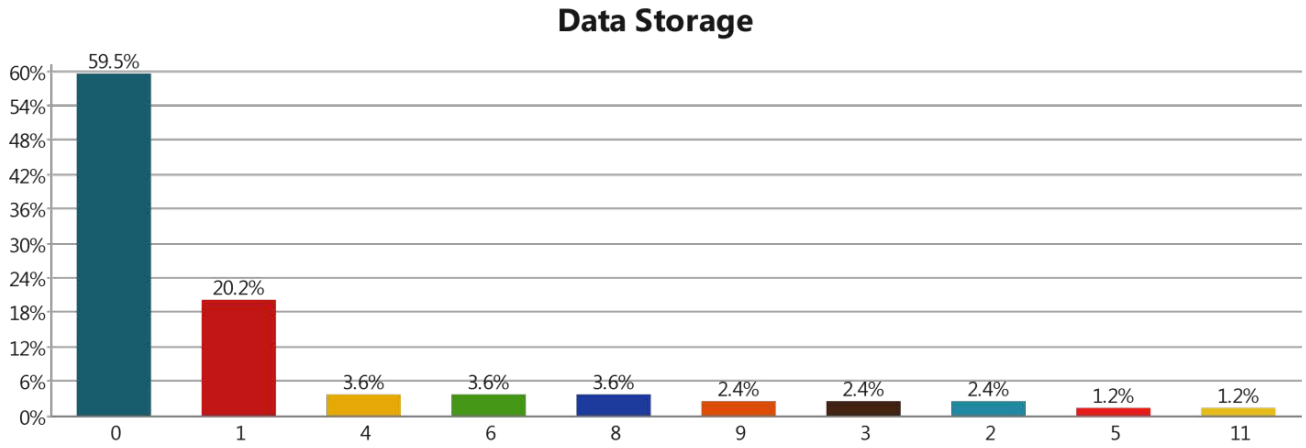

Figure 11. Potential determinants of IoT—Data storage.

3.3.6. Data Security Layer

Data security also remains very critical to ensure the effectiveness of the IoT. Data security ensures the privacy of information and safeguards it from unauthorized usage. The information system that contains loopholes in terms of data security does not meet the needs of the standard organization. Therefore, organizations have established separate arrangements to ensure data security. Figure 12 reflects the keyword search based on auto coding and it suggests that data security remains the most important determinant of the IoT. This is why security measurements and privacy protection should be adopted equally to offer robust end-to-end data security. For regulating access and securing data, a static approach is not acceptable because it fails to address the necessity that a mechanism of a scalable data security IoT is a conceivably and generally involved immature part of a net safety.

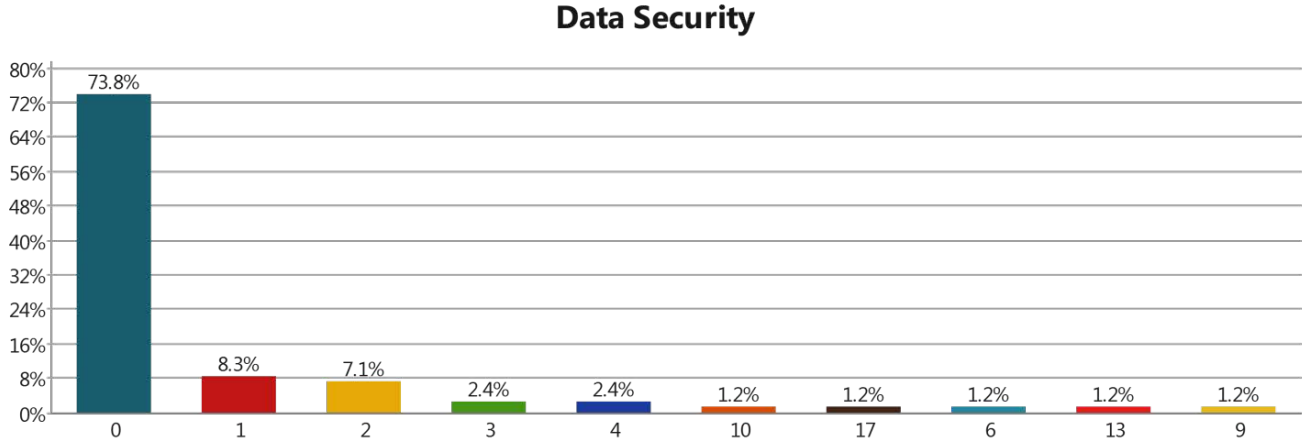

Figure 12. Data Security in IoT.

3.3.7. Data Collection Layer

The results shown in Figure 13 reflect that data collection has been widely discussed in past studies expounded in the literature. Data collection remains critical as the initial input to the IoT; the processing remains highly dependent on the data collection phase. Unless and until the data collection has been made effective, the other elements of data storage remain useless.

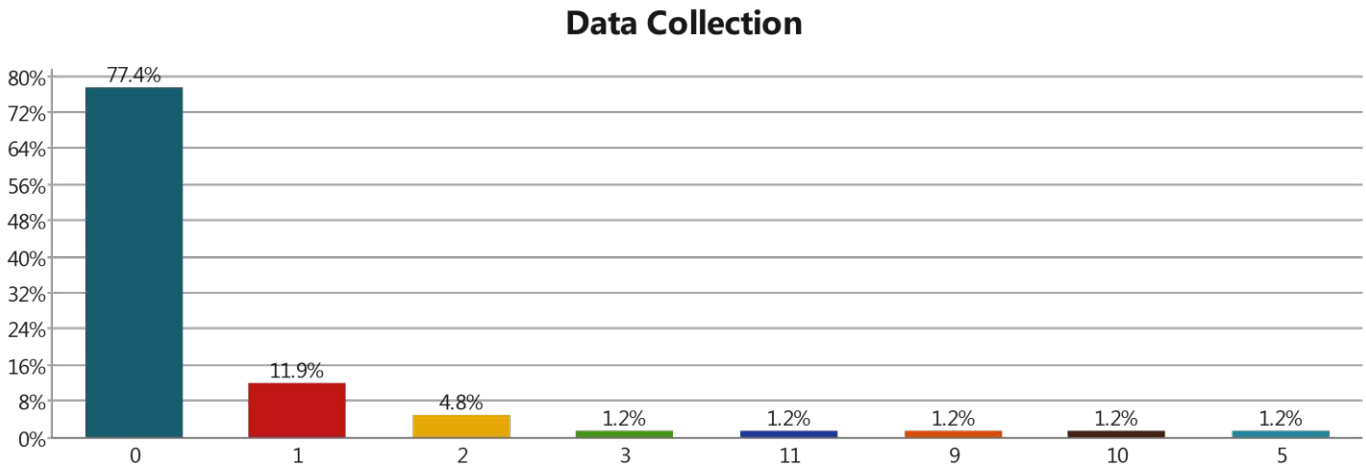

Figure 13. Data collection layer in the IoT.

3.3.8. Data Availability Layer

The data availability and the data collection are critical issues. They are used to ensure the effectiveness and efficiency of the IoT. The results shown in our study suggest that studies expounded in past literature remain concerned with data availability. It is impossible to ensure the efficient working of the information system without data availability. Therefore, besides the data collection, data availability also remains essential for the IoT to work effectively.

3.3.9. Data Application Layer

Data application is also considered as being a very important thing, which has been widely acknowledged in past studies, as shown in Figure 14. The application layer, particularly applications from the processed data, accord to the demands or requirements of the user. Therefore, the application layer should be user-friendly so that the IoT can be used with ease and convenience.

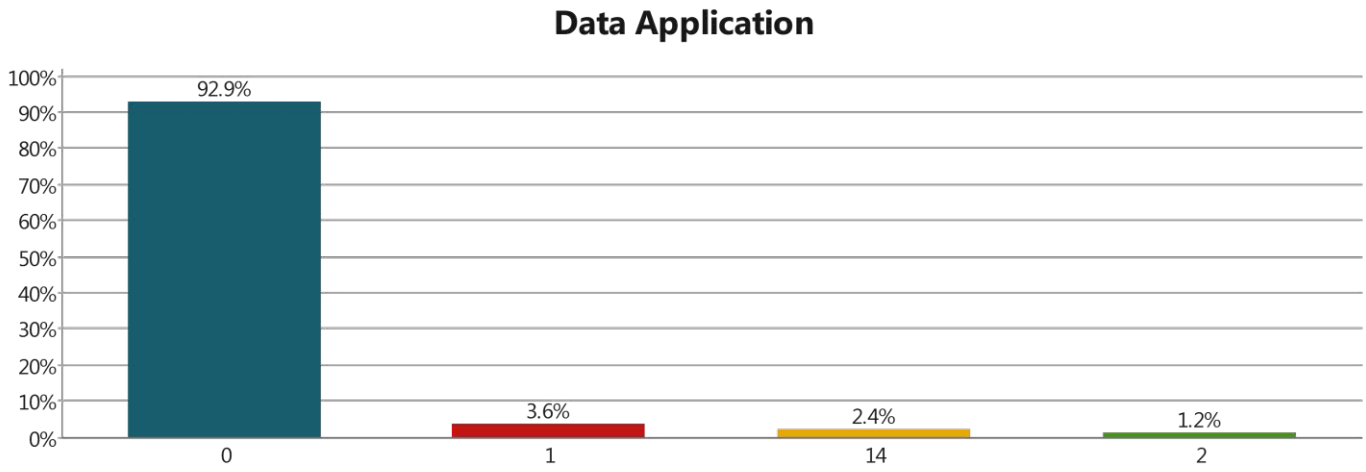

Figure 14. Data application layer.

3.3.10. Data Analysis Layer

Data analysis and the processing of the data are very important. Data analysis remains a critical challenge as it provides valuable insight to the stakeholder to issue information and decisions. Figure 15 reflects the significance of data analysis based on SLR. The SLR of the selected papers reflects that the data analysis layer gives importance to collecting the data for the development and the experimentation of smart decisions.

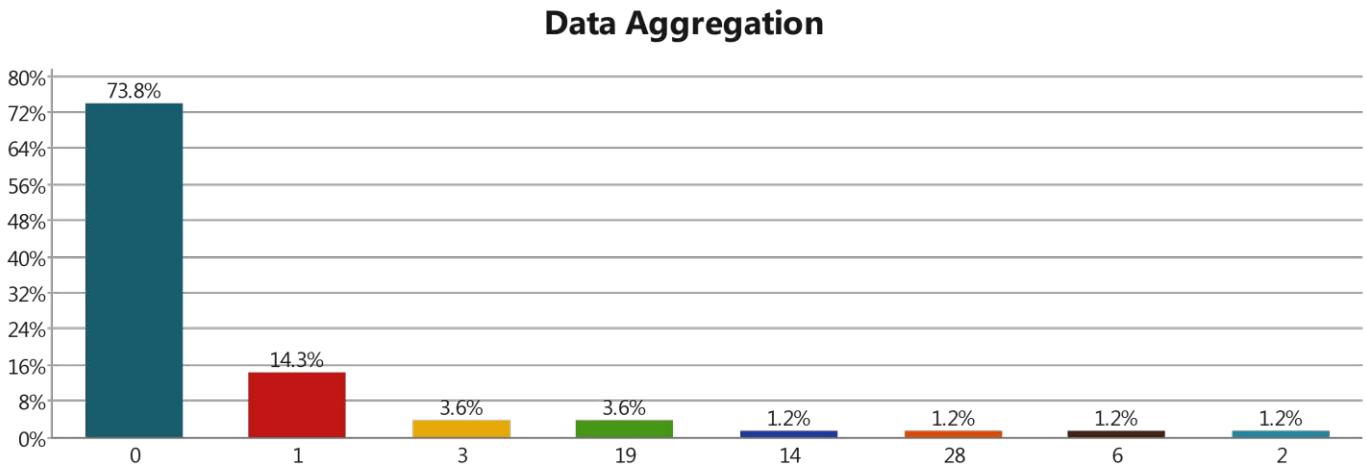

Figure 15. Data Aggregation.

3.3.11. Data Aggregation Layer

Data aggregation is one of the dominant themes that has been pointed out in past studies. Figure 15 reflects the significance of data aggregation. The storage, data supply, and the reduction size for improvement in storage and transmission of data are the major challenges of this layer. That is why the layer of these data is concentrated on merging and summarizing data. The modules that are the key to this layer are the heterogeneity, aggregation, filtering, interoperability, and transformation manager. Data that are received from the integrity management layer are more redundant, raw, and very large, as shown in Figure 15.

4. Qualitative Model

Based on the substantive SLR and the results, the following model was deduced through a deductive approach, which provides the essential elements that should be robust to build an effective and efficient IoT. The qualitative models that were deduced based on past studies are aligned with our proposed framework. The proposed model and qualitative model categorically contain nine layers, namely, computing, fog, management, integrity, security, data analysis, data aggregation, and data storage layer. Every layer of the framework contributes to the management process of the next layer. These nine layers are also considered the most robust determinants of the IoT. Each layer ensures the effectiveness and efficiency of the system to meet the individual's and organization's needs effectively. Our study aimed to design an advanced security framework for the IoT that can be used to analyze possible threats or challenges. This process began with elaborating the concept of the IoT, its characteristics, and layers of IoTs, all possible threats or challenges to the different layers of the IoT, and then moved on to find the best security framework to address these threats. The core objective of this study was to propose a security framework in terms of data confidentiality, availability, and integrity. The proposed model is shown in Figure 16. It comprises security frameworks in terms of computing layer, fog, management layer, integrity, security layer, data analysis, and data aggregation, where the data storage layer remains robust. The proposed and deduced security framework for the IoT remains to be aligned, which reflects the notion of the major determinants or features that should be an inclusive part of a security model for the IoT.

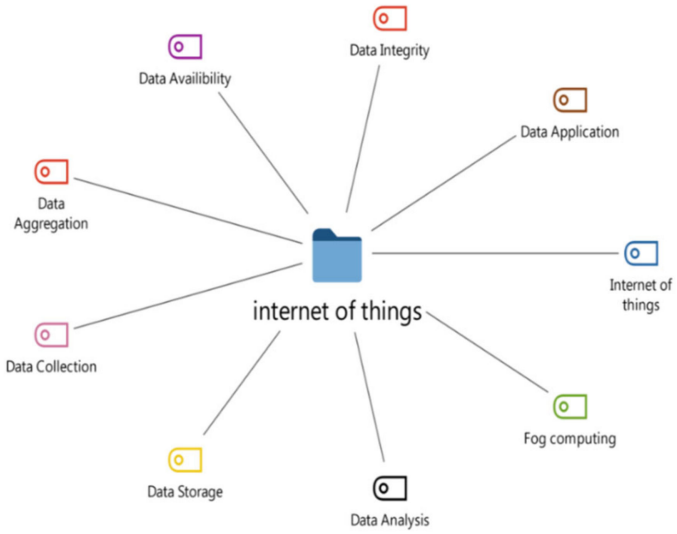

Figure 16. Security Model for the IoT.

5. Findings and Implications of This Study

In this study, we performed a thematic analysis and built a qualitative model. In this model, we extracted relevant literature from various databases using MAXQDA. The proposed security framework is completely based on different layers. These layers are data availability, data integrity, data application, IoT, fog computing, data analysis, data storage, data collection, data aggregation, etc. The research study in [22] concludes that data confidentiality in the IoT is a primary constraint that guarantees access and modification to certified entities via an access control mechanism and object authentication practice with a related identity supervision system. Our study concludes that data confidentiality is an important characteristic that needs to be included in the security framework. Similarly, the findings of [10] indicate that data integrity [23] is necessary for accurate data. Integrity is very important for storing data by any person or any organization. Data integrity is an important characteristic that needs to be included in the security framework. Hence, the key findings of our study are consistent. The results from [24] indicate that the aspects of data management should be kept in mind. The proposed model was made with a fog computing layer. This layer facilitates the devices to analyze, process, and partially store data on the node's edge. Our study also concludes that data application is an important characteristic that needs to be included in the security framework. The key findings of our study are consistent with the other findings. The studies conducted by [25–30] indicate that fog computing should also be considered as being important to develop and implement an effective IoT. One more finding concludes that data application is an important characteristic that needs to be included in the advanced security framework [31].

6. Conclusions

This research study proposed a security framework based on the available literature by using the SLR technique, using the the current literature we first identified. The coding was performed using an extensive literature review. Thematic analysis was conducted and a qualitative model was developed. During communication, data can be altered by cybercriminals. These methods are used to ensure the accuracy and originality of the data, including methods such as Checksum and Cyclic Redundancy Check (CRC). Moreover, the continuous syncing of data for backup requires the use of features such as version control, etc. These are used to keep a record of the file changes in the system to restore the file in case of an accidental deletion of data; this can also ensure the integrity of data such that the data on IoT-based devices are in their original form when accessed by permitted users. In the future, we will extend this security framework by employing advanced CRC for errors.

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

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank our families and colleagues who provided us with moral support.

Conflicts of Interest: The authors declare they have no conflicts of interest regarding the present study.

References

1. Amin, F.; Abbasi, R.; Rehman, A.; Choi, G.S. An Advanced Algorithm for Higher Network Navigation in Social Internet of Things Using Small-World Networks. *Sensors* **2019**, *19*, 2007. [CrossRef] [PubMed]
2. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* **2018**, *72*, 266–273. [CrossRef]
3. Khattak, H.A.; Shah, M.A.; Khan, S.; Ali, I.; Imran, M. Perception layer security in Internet of Things. *Futur. Gener. Comput. Syst.* **2019**, *100*, 144–164. [CrossRef]
4. Amin, F.; Choi, G.S. Hotspots Analysis Using Cyber-Physical-Social System for a Smart City. *IEEE Access* **2020**, *8*, 122197–122209. [CrossRef]
5. Kumar, N.M.; Mallick, P.K. The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia Comput. Sci.* **2018**, *132*, 117–119. [CrossRef]
6. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and Privacy in the Medical Internet of Things: A Review. *Secur. Commun. Netw.* **2018**, *2018*, 5978636. [CrossRef]
7. Jose, D.V.; Vijyalakshmi, A. An Overview of Security in Internet of Things. *Procedia Comput. Sci.* **2018**, *143*, 744–748. [CrossRef]
8. Yang, A.; Li, Y.; Kong, F.; Wang, G.; Chen, E. Security Control Redundancy Allocation Technology and Security Keys Based on Internet of Things. *IEEE Access* **2018**, *6*, 50187–50196. [CrossRef]
9. Chen, K.; Zhang, S.; Li, Z.; Zhang, Y.; Deng, Q. Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. *J. Hardw. Syst. Secur.* **2018**, *2*, 97–110. [CrossRef]
10. Javaid, U.; Aman, M.N.; Sikdar, B. Blockpro: Blockchain based data provenance and integrity for secure IoT environments. In Proceedings of the ACM Blocksys 2018, New York, NY, USA, 4 November 2018; pp. 13–18.
11. El-Hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, 18–20 October 2017; pp. 1–13.
12. Huang, Q.; Yang, Y.; Wang, L. Secure Data Access Control with Ciphertext Update and Computation Outsourcing in Fog Computing for Internet of Things. *IEEE Access* **2017**, *5*, 12941–12950. [CrossRef]
13. Sahmim, S.; Gharsellaoui, H. Privacy and security in internet-based computing: Cloud computing, internet of things, cloud of things: A review. *Procedia Comput. Sci.* **2017**, *112*, 1516–1522. [CrossRef]
14. Meddeb, M.; Dhraief, A.; Belghith, A.; Monteil, T.; Drira, K.; Alahmadi, S. Cache Freshness in Named Data Networking for the Internet of Things. *Comput. J.* **2018**, *61*, 1496–1511. [CrossRef]
15. Angin, P.; Mert, M.B.; Mete, O.; Ramazanli, A.; Sarica, K.; Gungoren, B. A Blockchain-Based Decentralized Security Architecture for IoT. In Proceedings of the International Conference on Internet of Things, Seattle, WA, USA, 25–30 June 2018. [CrossRef]
16. Aman, M.N.; Sikdar, B.; Chua, K.C.; Ali, A. Low Power Data Integrity in IoT Systems. *IEEE Internet Things J.* **2018**, *5*, 3102–3113. [CrossRef]
17. Amin, F.; Choi, G.S. Advanced Service Search Model for Higher Network Navigation Using Small World Networks. *IEEE Access* **2021**, *9*, 70584–70595. [CrossRef]
18. Colicchia, C.; Strozzi, F. Supply chain risk management: A new methodology for a systematic literature review. *Supply Chain. Manag. Int. J.* **2012**, *17*, 403–418. [CrossRef]
19. Dziopa, F.; Ahern, K. A systematic literature review of the applications of Q-technique and its methodology. *Eur. J. Res. Methods Behav. Soc. Sci.* **2011**, *7*, 39–55. [CrossRef]
20. Si, K.; Wolfson, C.; Fi, B. A multidisciplinary systematic literature review on frailty: Overview of the methodology used by the Canadian Initiative on Frailty and Aging. *BMC Med. Res. Methodol.* **2009**, *9*, 68–72.
21. Liu, C.; Yang, C.; Zhang, X.; Chen, J. External integrity verification for outsourced big data in cloud and IoT: A big picture. *Future Gener. Comput. Syst.* **2015**, *49*, 58–67. [CrossRef]

22. Farooq, M.U.; Waseem, M.; Khairi, A.; Mazhar, P.S. A critical analysis on the security concerns of internet of things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6.
23. Amin, F.; Lee, W.-K.; Mateen, A.; Hwang, S.O. Integration of Network science approaches and Data Science tools in the Internet of Things based Technologies. In Proceedings of the 2021 IEEE Region 10 Symposium (TENSYMP), Jeju, Korea, 23–25 August 2021; pp. 1–6. [CrossRef]
24. Atlam, H.F.; Walters, R.J.; Wills, G.B. Fog computing and the internet of things: A review. *Big Data Cogn. Comput.* **2018**, *2*, 10. [CrossRef]
25. Hameed, K.; Khan, A.; Ahmed, M.; Reddy, A.G.; Rathore, M.M. Towards a formally verified zero watermarking scheme for data integrity in the Internet of Things based-wireless sensor networks. *Futur. Gener. Comput. Syst.* **2018**, *82*, 274–289. [CrossRef]
26. Bin Qaim, W.; Ometov, A.; Molinaro, A.; Lener, I.; Campolo, C.; Lohan, E.S.; Nurmi, J. Towards Energy Efficiency in the Internet of Wearable Things: A Systematic Review. *IEEE Access* **2020**, *8*, 175412–175435. [CrossRef]
27. Navas, R.E.; Cuppens, F.; Cuppens, N.B.; Toutain, L.; Papadopoulos, G.Z. MTD, Where Art Thou? A Systematic Review of Moving Target Defense Techniques for IoT. *IEEE Internet Things J.* **2020**, *8*, 7818–7832. [CrossRef]
28. Valadares, D.C.G.; Will, N.C.; Caminha, J.; Perkusich, M.B.; Perkusich, A.; Gorgonio, K.C. Systematic Literature Review on the Use of Trusted Execution Environments to Protect Cloud/Fog-Based Internet of Things Applications. *IEEE Access* **2021**, *9*, 80953–80969. [CrossRef]
29. Amjad, A.; Azam, F.; Anwar, M.W.; Butt, W.H. A Systematic Review on the Data Interoperability of Application Layer Protocols in Industrial IoT. *IEEE Access* **2021**, *9*, 96528–96545. [CrossRef]
30. Reilly, E.; Maloney, M.; Siegel, M.; Falco, G. A smart city IoT integrity-first communication protocol via an ethereum blockchain light client. In Proceedings of the SERP4IoT, Colocated with the 44th ACM/IEEE International Conference on Software Engineering ICSE 2022, Marrakech, Morocco, 19 May 2022; pp. 15–19.
31. Amin, F.; Ahmad, A.; Sang Choi, G.S. Towards Trust and Friendliness Approaches in the Social Internet of Things. *Appl. Sci.* **2019**, *9*, 166. [CrossRef]