A Systematic Literature Review on the Role of Big Data in IoT Security

Muna Muhammad
Department of Computer Science, Balochistan University of Information, Technology, Engineering and Management Sciences, Pakistan

Sibghat Ullah Bazai
Department of Computer Engineering, Balochistan University of Information, Technology, Engineering and Management Sciences, Pakistan

Shafi Ullah
Department of Computer Engineering, Balochistan University of Information, Technology, Engineering and Management Sciences, Pakistan

Syed Ali Asghar Shah
Department of Computer Engineering, Balochistan University of Information, Technology, Engineering and Management Sciences, Pakistan

Saad Aslam
Smart Photonics Research Laboratory, School of Engineering and Technology, Sunway University, Malaysia

Angela Amphawan
Smart Photonics Research Laboratory, School of Engineering and Technology, Sunway University, Malaysia

Tse-Kian Neo
CAMELOT, Faculty of Creative Multimedia, Multimedia University, Malaysia

Abstract: The Internet of Things (IoT) is an interconnected system of physical objects that are embedded with different sensors (for receiving information), chips, software, and other techniques, which allow connecting and transferring of data to other devices via the Internet without human involvement. Since the number of IoT devices is increasing, large amounts of data are being generated from different sources in different formats. This information needs to be used effectively to gain useful insights for enhancing IoT security. Hence, big data techniques are proposed for managing the data to overcome different issues of IoT. Despite the outstanding achievements in IoT security, a systematic literature review (SLR) on implementing big data for

http://doi.org/10.18080/jtde.v12n1.783

securing IoT is lacking. The number of existing related SLRs is limited. Hence, this paper provides a systematic literature review on the use of big data for securing IoT devices. It summarizes the relevant literature produced during the last six years and provides meaningful insights gained by these existing studies. Moreover, it provides a discussion on the sources of IoT big data, the techniques and approaches of big data for securing IoT systems. Current challenges and future research directions are discussed.

Keywords: IoT, Big data, security, big data sources, big data techniques

Introduction

The Internet of Things (IoT) is a network of interconnected devices that send and receive data across the Internet without human involvement. With the increase in the adoption of IoT devices, the amount of generated data has increased exponentially, which has led to the rise in big data (Sachindra & Rajapaksha, 2022). According to a recent report (Hassan, 2022), the number of IoT devices has passed the 14.4 billion mark in 2022, whereas it has been predicted that it will rise up to 27 billion by the year 2027, as shown in Figure 1. With the increase in the number of IoT devices, the challenges, such as security, also increase, since the data generated by these devices is enormous.

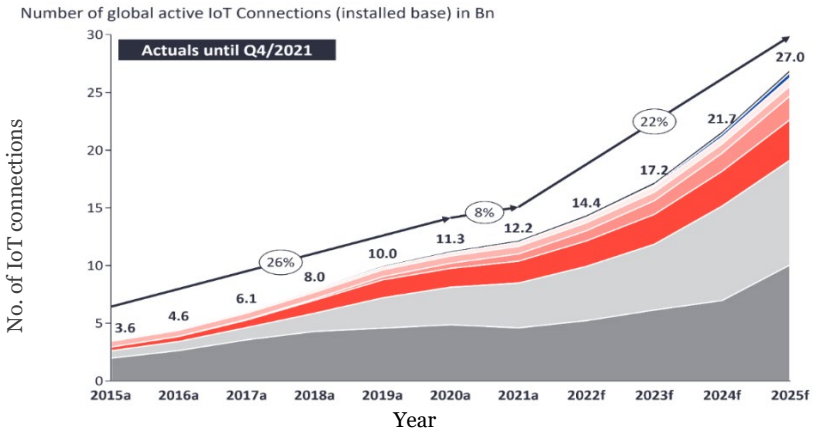

Figure 1. Rate of Increasing IoT devices (Hassan, 2022)

Securing IoT devices and networks is significant as these devices are usually deployed in sensitive environments and are more vulnerable to cyber threats, due to their heterogeneity, resource-constrained nature, low power, lack of standardization (Rao & Deebak, 2022), etc. So, the large and complex data sets produced by IoT devices can offer valuable insights into potential security threats and can help in identifying and preventing cyber-attacks.

Big data in the security of IoT refers to the collection, storage, processing, and analysis of large and complex data sets generated by IoT devices, to secure the devices and the network they are connected to. The data generated by IoT devices associates a wide range of information,

http://doi.org/10.18080/jtde.v12n1.783

such as user behaviour (Tedyyana *et al.*, 2022), device configuration, and network traffic, and that information can only be used by big data for gaining insights from it.

Big data for securing IoT includes the use of advanced analytics methods, such as machine learning (Tian, 2022) and artificial intelligence (Paraschiv *et al.*, 2022), for analyzing the large and complex data sets generated by IoT devices. These techniques can be used to detect anomalous behaviour, identify patterns and trends, and predict potential security threats (Pavithra *et al.*, 2019). It can help in improving the overall security of IoT devices and networks by providing real-time monitoring and threat detection, and improving the responsiveness of security protocols by using big data analytics in identifying security vulnerabilities, devices and networks (Hossain *et al.*, 2019).

Moreover, big data plays a vital role in securing the increasing number of IoT devices and networks. By getting insights from large and complex data sets, organizations can be helped in identifying and preventing security threats, improving security protocols, and ensuring the safety and integrity of IoT systems.

However, despite the great research achievements in IoT, in existing studies there is lack of standard and comprehensive work on IoT security using the approaches and techniques of big data. To fill this gap, this systematic literature review (SLR) paper has been written to determine the existing big-data technologies being applied for enhancing the IoT security. The purpose of this study is to review the literature by following a standard approach in reporting on existing big data technologies for IoT security since 2018 up to 2023, specifically focusing on SLRs.

IoT is being used widely in various fields for different purposes. But the security in IoT is a challenging task to solve, and big data is a potential technology to address this problem. Important concepts related to big data and IoT are discussed in the following sub-sections.

IoT security

IoT refers to the interconnected network of physical devices, vehicles, and other objects embedded with software, sensor, and network connectivity. While IoT devices can provide useful benefits, such as enhanced efficiency and convenience, they also pose newer security challenges. IoT security refers to the interventions taken to give protection to IoT devices and the data generated from the issues of cybersecurity threats and communication (Azrour *et al.*, 2021) within the IoT system.

The security risks usually included with IoT devices are many, some of which are:

http://doi.org/10.18080/jtde.v12n1.783

- **Unauthorized access**: IoT devices could be hacked and be accessed by cyber-attackers, providing access to confidential information or using the device for launching attacks on other systems (Azrour *et al.*, 2021).
- **Data privacy:** IoT devices gather large data amounts, some of which might be personal or sensitive. If this data gets into the wrong place, it can lead to financial fraud, identity theft, or other harmful consequences (Zhang *et al.*, 2022).
- **Malware attacks:** IoT devices could be infected by malware, which can be used for stealing data, causing damage to the device or network, or launching attacks on other systems (Torabi *et al.*, 2021).
- **Lack of security updates**: Some IoT devices lack proper security protocols or get infrequent security updates, or cannot update their firmware, which could make them vulnerable to known security issues.

IoT applications

IoT devices are being used in several applications in different forms, from smart industries to smart cities and wearable technology. While IoT devices provide benefits, they include significant security risks as well, and the nature of these risks varies depending on the particular application of the IoT devices. Some examples of security issues in various IoT applications are discussed in the following sub-sections.

Industrial IoT (IIoT)

Industrial IoT or IIoT refers to the use of IoT devices in industrial applications, such as in manufacturing and energy production. It includes the potential for cyber-attacks on industrial control systems (Taheri *et al.*, 2021) that could result in physical damage or disruption to critical infrastructure. These attacks can be caused by hackers or insider threats. IIoT devices may also be vulnerable to attacks that exploit software vulnerabilities, such as the Mirai botnet attack that targeted IoT devices to launch DDoS attacks (Bhayo *et al.*, 2022).

Smart homes

The simpler form of the IoT ecosystem is in the smart home applications and is used as home security systems, smart thermostats, and control of smart appliances. Security risks in smart homes constitute the potential for unauthorized access to networks of home devices, which could be used for stealing personal information or launching attacks on other systems (Al Mogbil *et al.*, 2020), can be used for tracing one's location, or can enable someone to spy on one's routine and trace the complete routine and one's activities. Smart home devices might also be vulnerable to attacks that exploit software vulnerabilities or weak passwords (Khare & Totaro, 2020). Moreover, there is a risk of data breaches and cyber-attacks that could

http://doi.org/10.18080/jtde.v12n1.783

compromise home security and privacy by stealing and compromising information or IoT devices.

Smart cities

In smart-city applications, IoT is used for services such as traffic management systems, public safety systems, and environmental monitoring. Security risks in smart cities include the potential for cyber-attacks, which disrupt critical infrastructure and cause widespread disruption (Rao & Deebak, 2022). Smart-city devices may also be vulnerable to weak encryption. Moreover, there is a risk of data breaches and cyber-attacks that could compromise public safety and privacy and compromise the departmental works associated with the smart city.

Big Data

Big data refers to the huge volume of data, such as structured, semi-structured, and unstructured data, which is generated and gathered by organizations daily. The term “big data” has become famous in recent years due to the extreme growth in data volumes and the need to process, analyze, and derive insights from this data. According to a report by IDC (Reinsel *et al.*, 2017), the big data volume is predicted to reach up to 175 ZB by the year 2025, as shown in Figure 2**.**

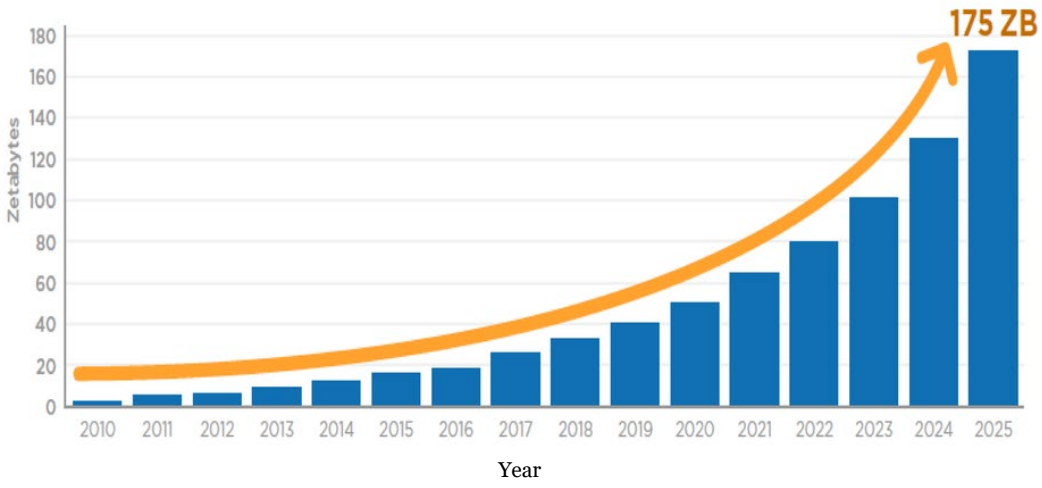

Figure 2. Data growth rate (Reinsel *et al.*, 2017)

Data is considered big data if it has certain characteristics. Big data can have a wide range of characteristics (Islam *et al.*, 2022), among which the five important can be summarized by the "5 Vs" (Figure 3): volume, velocity, variety, veracity, and value, as described in Gutta (2020):

Volume: Big data refers to datasets that are too large and complex for traditional data processing systems to handle.

http://doi.org/10.18080/jtde.v12n1.783

Velocity: Big data is generated at a very high speed and needs real-time processing to derive meaningful insights from the generated data.

Variety: Big data comes in different formats and structures, including videos, text, images social media data, and machine-generated data from IoT devices and sensors.

Veracity: This refers to the assurance of the data for quality, accuracy, credibility, and integrity, as the data is received from many sources and so its accuracy has to be assured before using it for gaining insights.

Value: Big data has to be of some value when used for insight into a business, so it is the usefulness of the data for making decisions. The value of big data has to be extracted by use of suitable big data analytics methods.

The challenges in handling big data need specialized techniques, tools, and technologies for managing, storing, processing, and analyzing these larger datasets. Big data technologies have been developed to handle the volume, velocity, and variety of big data (Sharma *et al.*, 2022), as well as to offer efficient and cost-effective solutions for managing and processing this data.

Figure 3. Characteristics of big data

One of the important technologies used for big data is distributed computing, which includes breaking down these large datasets into smaller chunks and processing them across multiple servers in parallel. This method allows for better scalability and fast processing of big data. Apache Hadoop (Li & Zhang, 2020) is one of the well-known distributed computing frameworks that is used for big data processing.

Another technique being used for big data is NoSQL databases, which are designed for handling unstructured and semi-structured data, which cannot be handled using traditional relational databases. NoSQL (Kalid *et al.*, 2017) databases are enhanced for horizontal scaling and are able to store and retrieve larger volumes of data.

http://doi.org/10.18080/jtde.v12n1.783

Data visualization is another important facet of big data, as it lets businesses gain insights and make informed decisions based on the particular data. Visualization tools like Tableau (Kumar *et al.*, 2022) and BDViewer (Li *et al.*, 2018) allow users for creating interactive charts, graphs, and dashboards for presenting and analyzing data in a meaningful way.

The importance of big data in business cannot be overstated. Big data when used with IoT, can provide many benefits, such as reducing the occurrence of security threats by gaining insights from the user behaviour or IoT devices, identifying patterns of the operations in the IoT ecosystem, and making data-driven decisions. By identifying and detecting abnormal behaviour, it can help in detecting security threats; hence, security issues can be handled or reduced importantly. Besides that, it can also solve the issue of data storage and management.

Research Contributions and Structure

In this study, a systematic literature review is being presented that contains a detailed literature review on the use of big data in IoT for securing IoT ecosystems. The contributions are as follows:

1. Current research status regarding IoT security by using big data techniques;
2. Sources of big data in IoT are identified and discussed;
3. Tools and techniques of big data for providing security solutions to IoT security challenges;
4. The main results of the contribution of research are discussed;
5. Future research directions are identified and discussed.

This paper is organized as follows. First comes a review of the existing pieces of literature. Then follows the research methodology and the research questions. A further section discusses the results of the research questions. Finally, there is a conclusion and an outline of future research directions.

Literature Review

In this section, the existing literature on the scope of big data in IoT is reviewed. The main goal is to identify the use of big data benefits in IoT, which will be undertaken to understand the existing works on the use of big data solutions for IoT applications and to identify the hidden challenges related to it, unrecognized opportunities, and the future research directions. The aim of this systematic literature review paper is to help fellow researchers better understand and implement the concepts of big data in IoT.

To achieve the aim of this study, the existing literature such as systematic reviews, survey papers, and systematic mapping studies related to the field, and published between 2017 and

http://doi.org/10.18080/jtde.v12n1.783

2023 have been gone through. The summary of the topics and main objectives of each paper is shown in Table 1**.** Out of 9 literature works, only one follows a systematic approach. More recently, in 2023, Bulatova (2023) provides a solution for strategic decision-making about the transportation system in smart cities and it is based on the concept of big data. It is based on an algorithm that uses big data and helps in making decisions for the transportation system. This paper does not follow any systematic process for the research methodology. In 2022, Zhong *et al.* (2022) provided a systematic survey on data mining and big data analysis in IoT, which is mainly focused on highlighting the main architectures of big data and data mining for IoT, the main tools of big data, the challenges of IoT when using big data and data mining, and the purpose for combining big data and IoT. In another survey by Islam *et al.* (2022), a systematic mapping study is provided that mainly concentrates on identifying the privacy attacks in IoT and big data by following a systematic approach. It identifies the main privacy attacks, identifies the measures for overcoming those privacy attacks, and the future research directions in the topic.

In 2021, Hajjaji *et al.* (2021) performed a systematic review of big data and IoT-based applications in smart environments that puts its focus mainly on the challenges of IoT and big data in environmental applications. It discusses the main tools and technologies of big data and IoT in environmental applications as well. This survey does not contribute mainly to future research. Ageed *et al.* (2021) shows the challenges and opportunities of applying big data systems in smart cities and also gives a comparison of different smart cities and big data concepts. Also, it seeks to define criteria for the development of big data applications for innovative services in smart cities. This paper focuses only on one particular application of IoT, the smart city.

Table 1. Existing related literature

Reference	Objectives & topics	Domain	Paper type
Saeed *et al.*, 2023	It discusses IoT and big data-based applications in intelligent ecosystems for identifying challenges and future research directions.	Big data and IoT in intelligent ecosystems	Systematic Review
Bulatova, 2023	It proposes an algorithm for making strategic decisions in smart city transportation systems by using big data.	Smart cities transportation system	Algorithm-based

http://doi.org/10.18080/jtde.v12n1.783

Reference	Objectives & topics	Domain	Paper type
Zhong *et al.*, 2022	It presents a systematic survey of existing literature on data mining and big data in IoT. It aims at identifying lines of research for future works on the aforementioned topic. Provides summary of the approaches used in IoT-based data mining and big data analysis.	Big data analysis in IoT	Systematic survey
Islam *et al.*, 2022	It highlights the privacy objectives, attacks, and measures to prevent them in IoT and big data. Besides, the classification of attacks is provided.	Big data and IoT	Mapping study
Mohamad Jawad *et al.*, 2022	It is an SLR that discusses the motivations, challenges, and recommendations in smart healthcare.	IoT in healthcare	SLR
Misra *et al.*, 2022	It reviews and shows the use of big data analysis and IoT in food industry for food quality assessment, machinery monitoring.	IoT and big data in food industry	Review
Ageed *et al.*, 2021	It highlights the challenges and opportunities of applying big data systems in smart cities and provides a comparison of different smart cities and big data ideas. Besides, it seeks to define criteria for the development of big data applications for innovative services in smart cities.	Smart city	Survey
Karimi *et al.*, 2021	It reviews the use of big data for enhancing the smart city services and security.	Big data & IoT in smart city	Systematic review
Hajjaji *et al.*, 2021	It presents a systematic review of big data and IoT-based applications in smart environments focusing on the challenges of IoT and big data in environmental applications. Also, it provides the main tools and technologies of big data and IoT in environmental applications.	Smart environments	Systematic Review
Amanullah *et al.*, 2020	It provides a comprehensive survey of securing IoT by detection of security breaches using big data and deep learning.	Big data & deep learning in IoT security	Survey
Farooq *et al.*, 2020	It reviews the use of IoT technologies for addressing different domains of agriculture for improvement of food industry.	IoT in agriculture	SLR
Maswadi *et al.*, 2020	It discusses the systematic review of smart home implementation for elderly people.	Smart home	SLR

http://doi.org/10.18080/jtde.v12n1.783

Reference	Objectives & topics	Domain	Paper type
Shah *et al.*, 2019	It shows the growing role of IoT and big data analytics in disaster management applications. By the inquiry of recent studies, review on ubiquitous solutions, categorization of thematic taxonomy proposed, as well a conceptual model on big data analytics and IoT deployment in disaster management is proposed.	Disaster-management	Survey
Florence & Shyamala, 2019	It provides a survey of smart transportation systems in several applications, such as logistics, self-driving cars, traffic prediction, freight transportation, etc.	Smart transportation system	Survey
Al Mamun & Yuce, 2019	It discusses a review of current research & development for sensors and systems, such as wearables devices designed for environmental IoT applications. Provides comparison of existing wearable environment and monitoring systems.	Monitoring environment	Exploratory study
Saha *et al.*, 2018	It has provided a classification of techniques of big data used in IoT applications.	Big data techniques	Survey

From the results of these studies, it is clear that, while some reviews do cover IoT and big data concepts, these studies mainly focus on one specific application of IoT rather than talking about general IoT.

As a result, it is observed that there are still gaps in research to plan and design integrated IoT and big data technologies for IoT security. Therefore, to the best of our knowledge, this work of presenting a systematic literature review on securing IoT by using big data techniques would be the first SLR on the topic.

Methodology

The purpose of the study is to analyze the existing published studies to characterize the use of big data and approaches in IoT security, from the point of view of practitioners and researchers. To fulfill the purpose, the following research questions have been derived (Kitchenham *et al.*, 2009)

1. What is the distribution per publication venue, year, and domain of the published studies related to big data and IoT in securing IoT networks?
2. What are the sources of big data in IoT ecosystems?
3. What technologies and approaches of big data are being used for addressing security issues in IoT?

http://doi.org/10.18080/jtde.v12n1.783

To achieve this purpose, an SLR has been conducted by using the "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA)" method (Page *et al.*, 2021). By using this method, the results and methods of systematic reviews can be synthesized in appropriate detail for users to assess the applicability and trustworthiness of the review results.

The search and analysis are discussed through the following review protocol.

Planning

The planning stage of the process consists of the following subsections in which the whole planning stage is described.

Review protocol

The protocol of this study has been designed and is shown in Figure 4. The protocol consists of three phases, which are planning, conducting, and reviewing. Initially, in the planning phase, research questions need to be designed, then the selection of sources and the search strategy is formed, then inclusion and exclusion criteria are performed, and then the quality assessment criteria for selecting papers are chosen. After that, in the conducting phase, primary studies are selected by quality assessment, and the data extraction for the finalized papers is done. At last, in the reviewing phase, the results are formed from a data synthesis of the finalized papers.

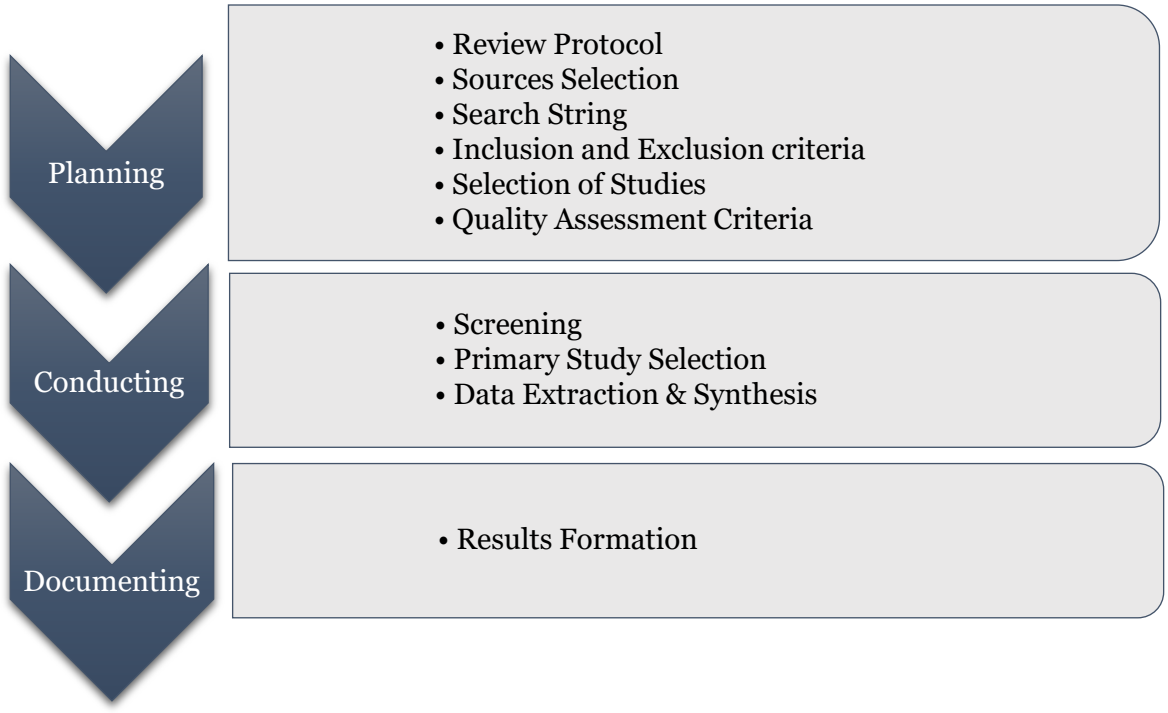

Figure 4. Review protocol

http://doi.org/10.18080/jtde.v12n1.783

Sources selection

Different online databases have been chosen as search sources. They are IEEE Xplore, SpringerLink, ScienceDirect, Scopus, and ACM digital library. These online sources have been chosen based on their quality, timeliness, availability, and versatility.

Search string

For developing the search string, the keywords are highlighted related to the main idea of the topic of the SLR, i.e., "IoT security" and "big data". To have an effective search strategy, similar words for the two identified keywords have been produced. Based on that, the search string using specified keywords and Boolean operators (shown in Table 2) has been developed for finding as many studies as possible.

Selection of studies

The studies related to the topic of this study, "big data analytics" and "IoT", have been searched using the aforementioned digital libraries and have produced a wide range of online published studies from different sources, as shown in Table 2. The selection of studies has been done by applying the inclusion and exclusion criteria shown in Table 3. Based on that, the studies are filtered to get the most relevant and useful ones.

Table 2. Data sources and study selection

Digital Library	String	Studies
IEEE Xplore	(("big data" OR" big data approach" OR "big data techniques") AND ("IoT security" OR "Internet of things security" OR "security IoT" OR "IoT challenges"))	2232
SpringerLink	(("big data" OR" big data approaches" OR "big data techniques") AND ("IoT security" OR "Internet of things security" OR "securing IoT" OR "IoT challenges"))	6867
ACM	(("big data" OR "big data techniques") AND ("IoT security" OR "Internet of things security" OR "IoT challenges"))	1234
ResearchGate	(("big data" OR" big data approaches" OR "big data techniques") AND ("IoT security" OR "Internet of things security" OR "securing IoT" OR "IoT challenges"))	1678
ScienceDirect	(("big data" OR "big data techniques") AND ("IoT security" OR "Internet of things security" OR "IoT challenges"))	2547

Inclusion and exclusion criteria

Based on the inclusion and exclusion criteria shown in Table 3, the selected papers from the digital libraries have been screened. By applying the inclusion criteria to selected papers, title and abstract screening is done, at which point it is checked for the published dates of the

http://doi.org/10.18080/jtde.v12n1.783

papers, the topic of the paper, the written language of the paper, and the source of the published paper. There is a need to select papers that are written in the English language and are recently published (after 2019). Similarly, the exclusion criteria have been applied in the title and abstract screening for the dates, topics, and source type of the paper.

Table 3. Inclusion & exclusion criteria

Inclusion Criteria
Studies published between 2017 and 2023
Studies published only in conferences, journals, book chapters
Studies written in English language only
Studies related to big data analytics
Studies related to IoT
Exclusion Criteria
Studies written in other than the English language
Magazines, non-peer-reviewed
Studies written on fields unrelated to our topic
Studies published before 2017

Quality assessment

For filtering the primary studies to the best ones, a quality assessment has been done on the set of 102 papers based on the following 3 questions:

1. Is the motivation for studying IoT and big data mentioned?
2. Is the information given related to big data and IoT?
3. Is a proper methodology followed with results?

Based on the answers of quality assessment conducted on the set of 102 papers, 62 papers have been removed that have not followed the quality assessment criteria. So, at last, 40 papers have been selected for data extraction.

Conducting

In the conducting stage, the primary studies are screened and analyzed as described in the following subsections.

Screening

The studies retrieved and selected from different sources have been screened based on title and abstract, so that only a relevant set of primary papers will be selected for further analysis.

After that, the selected set of primary papers have been screened fully, such that full-text reading has been done so that a set of primary studies can be specified for data synthesis.

http://doi.org/10.18080/jtde.v12n1.783

Primary study selection

Title and abstract screening and full-text screening has been done on the collected papers for specifying the set of papers for primary studies' collection for data synthesis. Therefore, after the title and abstract screening, out of 7680 papers, 840 papers have been chosen (shown in Figure 5) on which full-text screening is done based on the inclusion and exclusion criteria; and, as a result, 102 primary studies have been identified on which first quality assessment and then data synthesis have been performed.

Table 4. Data extraction

Variable	Description	Research Question
V1	Title	1, 2, 3
V2	Author name	1, 2, 3
V3	Publication year	1
V4	Type of paper	1
V5	Paper methodology	3
V6	Big data approach	3
V7	Purpose of approach	3
V8	Big data sources	2
V9	Type of sources	2
V10	Big data technologies	3

Data extraction & synthesis

For extracting the data from the set of primary studies, a template has been developed as shown in Table 4. Each field of data extraction has a description and a reference to the corresponding research question number. To answer the research questions, the identified primary studies are divided into four facets. Therefore, each variable in the data extraction table is related to answering each research question.

PRISMA flow summary and phases of SLR

A total of 10549 papers have been retrieved from the aforementioned digital libraries. For further selection and filtration of the papers, the PRISMA (shown in Figure 5) method has been followed and the papers are filtered in the following way:

1. In the identification stage, 10549 papers are identified, and then, after duplicates removal, this becomes 7680.
2. In the stage of screening, by doing the title and abstract screening of the papers, 840 papers are selected and the rest of them are removed.
3. At the stage of eligibility, full-text screening has been done and 102 papers been selected for quality assessment. Out of 102 papers, only 40 papers have been finalized as quality papers.

http://doi.org/10.18080/jtde.v12n1.783

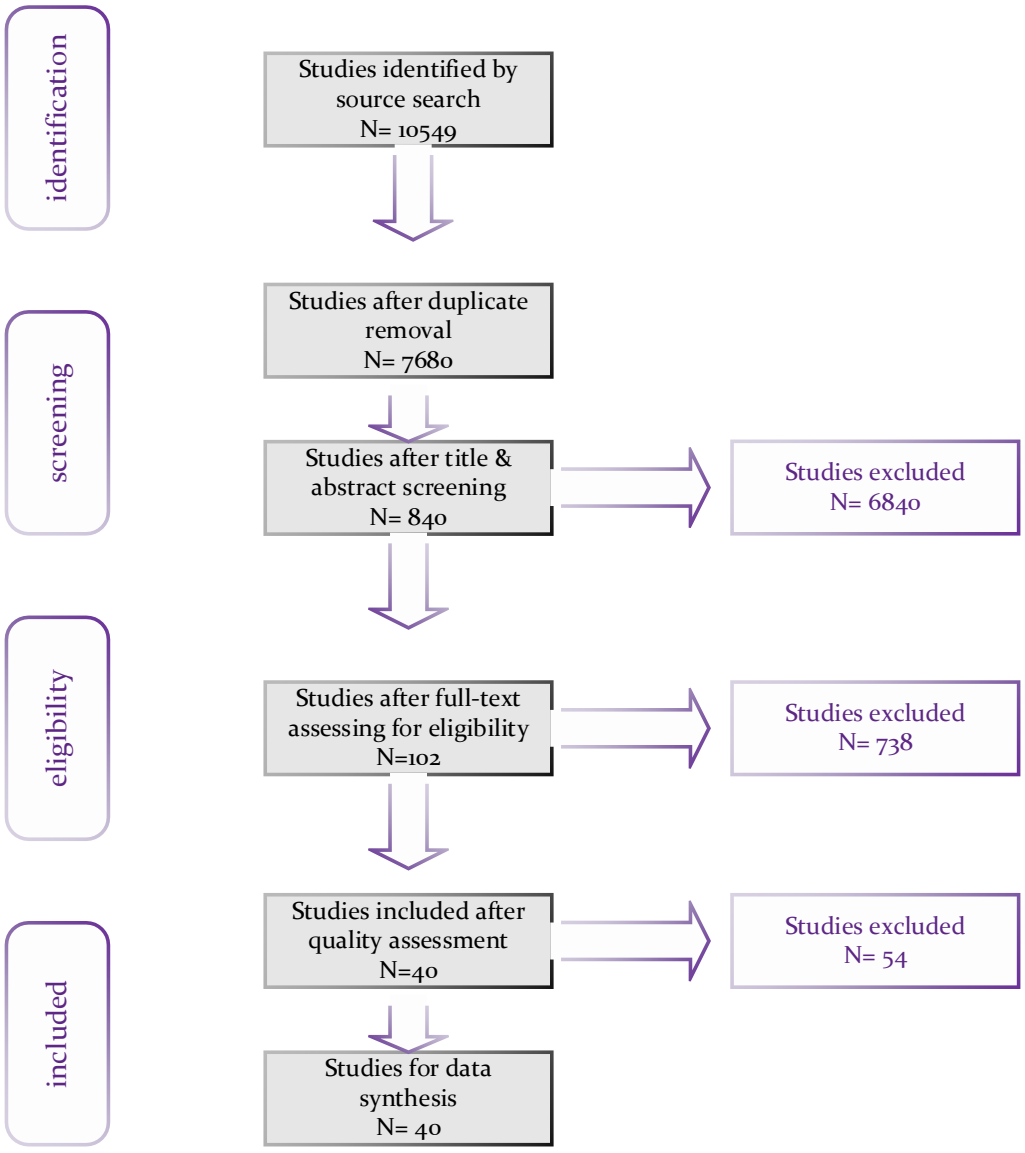

Figure 5. PRISMA flow diagram

Results and Discussion

This is the documenting stage of the SLR process. In this section, the findings are presented based on the analysis of data for each research question mentioned above. Firstly, the demographics of the papers, which have been used in the SLR, are stated. Then, the results of each research question is discussed.

Demographics of studies (RQ1)

The number of published articles on the use of big data in IoT is shown in Figure 6**.** By observing Figure 6, it can be said that the number of published articles is increasing from 2019 onwards. There is 1 article from 2017 and none from 2018. Six articles have been included from 2019 (Hossain *et al.*, 2019; Pavithra *et al.*, 2019; Chui *et al.*, 2019; Florence & Shyamala, 2019; Al Mamun & Yuce, 2019; Shah *et al.*, 2019), whereas the number of articles included

http://doi.org/10.18080/jtde.v12n1.783

from 2019 onwards are more each year, such that 8 articles are from 2020 (Wang *et al.*, 2020; Granat *et al.*, 2020; Li, *et al.*, 2020; Li & Zhang, 2020; Wu *et al.*, 2020; Al Mogbil *et al.*, 2020; Khare & Totaro, 2020; Zhaofeng *et al.*, 2020), 10 articles are from 2021 (Lv *et al.*, 2021; Wan *et al.*, 2021; Azrour *et al.*, 2021; Putra *et al.*, 2021; Ning *et al.*, 2021; Taheri *et al.*, 2021; Torabi *et al.*, 2021; Srinivas *et al.*, 2021; Hajjaji *et al.*, 2021), 12 articles are from 2022 (Tedyyana *et al.*, 2022; Yu *et al.*, 2022; Bhayo *et al.*, 2022; Rao & Deebak, 2022; Sharma *et al.*, 2022; Paraschiv *et al.*, 2022; Zhang *et al.*, 2022; Tian, 2022; Islam *et al.*, 2022; Sachindra & Rajapaksha, 2022; Zhang, Y., 2022; Zhong *et al.*, 2022), and 3 articles from 2023 (Mahmood *et al.*, 2023; Babar *et al.*, 2023; Bulatova, 2023) in the early part of the year. From that, it can be concluded that research on the use of big data in IoT security has gradually increased year by year and is in the stage where it can be said that it is not fully developed or is in its early stages, indicating emerging research.

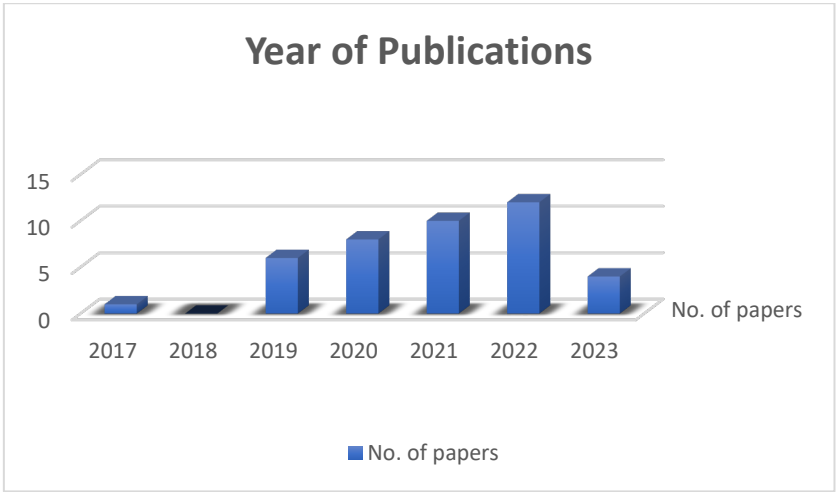

Figure 6. Rate of publications on big data and IoT

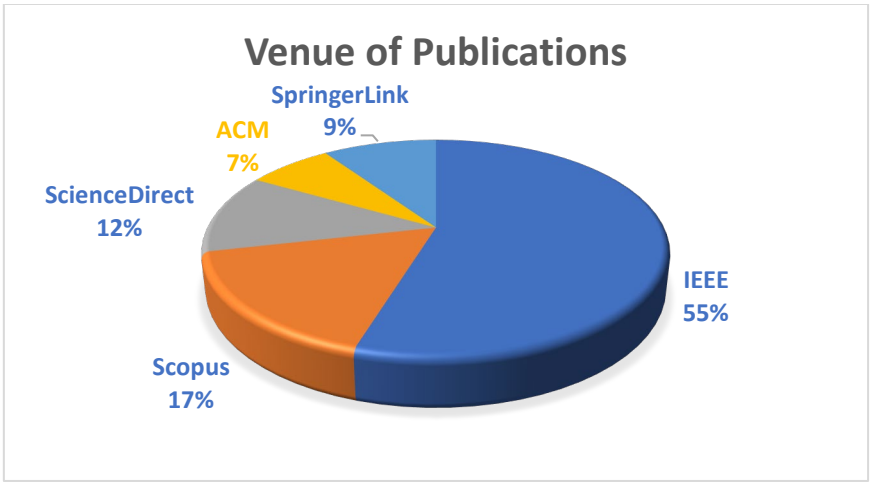

Figure 7. Distribution of venue of publications

Based on the publication venues, the primary papers selected are distributed as shown in Figure 7. It can be concluded from the distribution graph that most of the papers selected are from IEEE Xplore (55%), as Xplore is one of the top digital libraries worldwide. Papers from

http://doi.org/10.18080/jtde.v12n1.783

Scopus are (17%), then ScienceDirect (12%), and, finally, from SpringerLink (9%); very few are taken from ACM digital library (7%).

Sources of IoT Big Data (RQ2)

The sources of big data in IoT can be from the following two categories.

Device-generated data

This type of data is generated by low-end devices, sensors used in IoT environments, and machines that are part of the IoT ecosystem. These devices generate data on different aspects such as humidity, temperature, pressure, location, etc. The data generated by these devices is typically time-stamped and is high in volume. This type of data is considered the largest source of data in IoT, making up to 40% of all the sources of IoT data, according to a report by Manyika *et al.* (2015). Wireless sensor networks (WSNs) contain thousands of sensors that gather large amounts of data by monitoring a wide range of areas (Harb *et al.*, 2017). Similarly, a massive amount of data is generated by online transactions done via smart shopping, RFIDs, and many others. There is a huge amount of data being produced by IoT ecosystems but most of the data is not being used or analyzed to make it valuable (Manyika *et al.*, 2015).

User-generated data

This type of data is generated by users of IoT devices in applications like smart home services, wearables, smart parking, smart banking, smart healthcare, etc. This data can consist of information about the user's preferences, behaviour, and location. User-generated data is an important source of big data for the IoT, as most of the data is generated by users. Big data is gained by users of IoT on different platforms such as on social media (Joseph *et al.*, 2017), in the smart office, and human-computer interaction devices. Data is produced in large volume by the user-generated source and this big data can be used to gain insights from it by the use of big data analytics. It also helps in better decision-making, performance boosts, and tightening the security of an organization. One such example can be seen from the research of Joseph *et al.* (2017), where they produced results by performing data analytics on user-generated data of Twitter for discussing trends in IoT. They have used big data tools such as R and NodeXL for data analytics and have gained results like the connection of different user communities, industrial influencers, and top individuals, and security emerging in smart technologies. Similarly, another research work shows a massive amount of user-generated data is being used as a sample for training globally shared models based on federated learning (Wu *et al.*, 2020).

Moreover, different data is generated at different sources like the sensors in accumulating information, users interacting with the IoT devices, and many other data is being generated

http://doi.org/10.18080/jtde.v12n1.783

from IoT devices indirectly. A huge amount of data is generated by the IoT ecosystem (that is, big data) and there are many challenges associated with the huge amount of big data that needs to be addressed by combining big data with IoT technology.

Big Data techniques and approaches for securing IoT (RQ 3)

A large amount of data coming from different sources of IoT, such as sensors, actuators, and other IoT devices, need specific techniques and approaches to make the IoT system secure when handling such big data. For that purpose, different techniques and approaches (Table 5) have been proposed that can make IoT systems more secured by the use of big data concepts.

Table 5. Big data approaches to IoT Security

Reference	Main context	Advantages
Li, 2018	BDViewer	Enables processing of large data sets using web browser based on virtual cloud at back-end
Chui *et al.*, 2019	Monitoring the behaviour of the patient	Reliable and secure
Dhanasekaran *et al.*, 2019	K-mean clustering algorithm based on map-reduce	Optimized data privacy and data storage
Lavanya *et al.*, 2022	Block level security for IoT big data by using cipher security policies	Secured data storage
Tedyyana *et al.*, 2022	Framework for big data is used for providing security to IoT by using SHA-256 encryption	Prevention of external attacks
Yu *et al.*, 2021	Security analysis system for smart home	Detects and prevents security issues in smart home
Srinivas *et al.*, 2021	User Authentication Protocol	Secure communication
Granat *et al.*, 2020	Uses multicriteria approach for event detection in IoT big data analytics	Secured data storage, security, processing
Zhaofeng *et al.*, 2020	Secure Usage Control of IoT big data based on Blockchain-enabled decentralized trust management	Trusted and secure data gathering
Azrour *et al.*, 2021	Enhanced key exchange and authentication protocol	Secured user data exchange across heterogeneous sources
Li *et al.*, 2020	Online distributed security algorithm for IoT	High scalability, better detection, and monitoring of threats
Ning *et al.*, 2021	Mobile Edge Computing blockchain framework	Devices in operation are secured

Most of the time, the security issue exists due to the architecture as, through the architecture of a system or a network, the whole network is communicated among different devices involved and, hence, security can be tightened through this as well. So, for that purpose, a security analysis framework has been introduced by Yu *et al.* (2021), which designs and implements a security analysis system for a smart home for detecting and defending against mining attacks or contactless attacks by incorporating big data into it. For the big data collection in IoT, a secured mechanism has to exist that could allow for secure access to real-

http://doi.org/10.18080/jtde.v12n1.783

time data in IoT; that can be provided by using a three-factor user authentication scheme (Srinivas *et al.*, 2021) known as UAP-BCIoT, based on elliptic-curve cryptography. Similarly, another security framework has been proposed by Tedyyana *et al.* (2022) that uses a SHA-256 encryption method for providing secure data exchange and this prevents external attacks in IoT networks. Lavanya *et al.* (2022) proposes a block-level security by using cipher security policies to secure the data storage in IoT networks. The security issues can be solved to some extent by using such techniques and approaches, but there is also an issue of security and trust for IoT big data management. User authentication can also be secured by a key exchange technique (Azrour *et al.*, 2021) that can provide secure communication in IoT. This issue is solved by a blockchain-based decentralized trust management scheme (Zhaofeng *et al.*, 2020) and also it provides secure data storage, transfer, invoking, and usage.

Moreover, most of the techniques proposed are related to the authentication mechanism and framework. Some are based on encryption techniques as well. It can be said that the researchers are working at fast pace to propose effective solutions for overcoming the security challenges in IoT. Most of them have focused on the architecture of IoT networks, proposing different security frameworks, so that the security issues can be minimized to a certain level in IoT networks. Secure storage of the IoT data is also necessary, as data in storage can be at risk. Secure data exchange is necessary, since, in transit, data can be attacked and compromised. Encryption methods can be used to secure data in process. There is a further focus on securing data coming from heterogenous sources. There is still a need for more research on securing IoT networks by using different techniques of Big Data, as the technology in Big Data is advancing and using advanced technology faces other security issues. Additionally, there is a research gap in providing security solutions for the detection of unreliable data in IoT big data.

Conclusion

Today's world is known as the world of big data, but IoT technology is being further popularized and can lead to a greater explosion of data in the future. The massive IoT networks produce a new type of data called IoT big data. With the advances and progress of IoT networks, security issues arise as well. Existing big data techniques can be used to store and analyze data, so that security issues can be predicted, detected, or minimized. Certain research questions have been formulated to make meaningful conclusions about the identified problems and identify the research gaps.

To make sure of formulating a high-quality report of big data technologies in IoT security, out of 7680 papers, 802 were identified and, after full-text screening, only 40 papers were selected for data synthesis and results formation. An SLR protocol has been followed for identifying

http://doi.org/10.18080/jtde.v12n1.783

and formulating results from existing primary studies found in digital libraries. Most of the identified studies were from IEEE Xplore and the number of studies has been increasing from 2018 onwards. The sources of big data in IoT are user-generated and device-generated data. Many big data approaches and techniques are given for securing IoT systems, such as encryption-based techniques, different proposed security frameworks, and authorization and authentication methods.

Current Challenges and Future Research Directions

Information acquisition from IoT data is the main challenge that is posed by big data. Infrastructure development for analyzing IoT is vital. A large number of IoT devices generate a continuous flow of data. The researchers can use these data by using machine learning techniques for creating instruments to extract meaningful information from it. In getting information from an IoT network, scalability and security issues might be faced.

Machine learning and artificial intelligence might be additional directions in future research. Of the large amount of data produced via sensors, a model can be developed to act based on the historic data. Since the raw data and resultant data are both considered as data, big data algorithms should be used for analyzing them. There is space for the improvement of existing algorithms for the process of data analysis to be more secure and efficient, as most of the researchers do not take into consideration the response time and the energy consumption.

Combining machine learning and big data can make it possible to develop a united emergency system that could analyze the given situation and user environment and then take suitable actions based on past cases.

Acknowledgements

A version of this paper was presented at the third International Conference on Computer, Information Technology and Intelligent Computing, CITIC 2023, held in Malaysia on 26-28 July 2023.

We would like to thank the members of the Sunway FSO for Flood Communications Project (GRTIN-IGS-DCIS[S]-01-2022) for their contribution and collaboration.

We would also like to acknowledge the support of TM R&D project (RDTC/231106) and thank the members for their effort, contribution and collaboration to this study.

References

Ageed, Z. S., Zeebaree, S. R., Sadeeq, M. M., Kak, S. F., Rashid, Z. N., Salih, A. A., & Abdullah, W. M. (2021). A Survey of Data Mining Implementation in Smart City Applications. *Qubahan Academic Journal, 1*, 91–99. https://doi.org/10.48161/qaj.v1n2a52

Al Mamun, M. A., & Yuce, M. R. (2019). Sensors and systems for wearable environmental monitoring towards IOT-enabled applications: A review. *Sensors, 18*, 7771–7788. https://doi.org/10.1109/JSEN.2019.2919352

Al Mogbil, R., Al Asqah, M, & El Khediri, S. (2020). IoT: Security Challenges and Issues of Smart Homes/Cities. *2020 International Conference on Computing and Information Technology*. Tabuk, Saudi Arabia: IEEE, pp. 1–6. https://doi.org/10.1109/ICCIT-144147971.2020.9213827

Amanullah, M. A., Habeeb, R. A. A., Nasaruddin, F. H., Gani, A., Ahmed, E., Nainar, A. S. M., Akim, N. M., & Imran, M. (2020). Deep Learning and Big Data Technologies for IoT Security. *Computer Communications, 151*, 495–517. https://doi.org/10.1016/j.comcom.2020.01.016

Azrour, M., Mabrouki, J., Guezzaz, A., & Farhaoui, Y. (2021). New enhanced authentication protocol for Internet of Things. *Big Data Mining and Analytics, 4*(1), 1–9. https://doi.org/10.26599/BDMA.2020.9020010

Babar, M., Jan, M. A., He, X., Tariq, M. U., Mastorakis, S., & Alturki, R. (2023). An Optimized IoT-Enabled Big Data Analytics Architecture for Edge–Cloud Computing. *IEEE Internet of Things Journal, 10*(5), 3995–4005. https://doi.org/10.1109/JIOT.2022.3157552

Bhayo, J., Jafaq, R., Ahmed, A., Hameed, S., & Shah, S. A. (2022). A Time-Efficient Approach Toward DDoS Attack Detection in IoT Network Using SDN. *IEEE Internet of Things Journal, 9*(5), 3612–3630. https://doi.org/10.1109/JIOT.2021.3098029

Bulatova, O. (2023). Using big data in smart cities transportation systems. *E3S Web of Conferences*. https://doi.org/10.1051/e3sconf/202337106009

Chui, K. T., Liu, R. W., Lytras, M. D., & Zhao, M. (2019). Big Data and IoT Solution for Patient Behaviour Monitoring. *Behaviour Information Technology, 38*(9), 940–949. https://doi.org/10.1080/0144929X.2019.1584245

Dhanasekaran, S., Sundarrajan, R., Murugan, B. S., Kalaivani, S., & Vasudevan, V. (2019). Enhanced Map Reduce Techniques for Big Data Analytics based on K-Means Clustering. *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing*. Tamilnadu: IEEE Xplore. https://doi.org/10.1109/INCOS45849.2019.8951368

Farooq, M. S., Riaz, S., Abid, A., Umer, T., & Zikria, Y. B. (2020). Role of IoT Technology in Agriculture: A Systematic Literature Review. *Electronics, 9(2)*, 319. https://doi.org/10.3390/electronics9020319

Florence, S., & Shyamala, K. C. (2019). Big Data and IoT in Smart Transportation System. *International Journal of Innovative Technology and Exploring Engineering, 8*(9), 1230–1232. https://doi.org/10.35940/ijitee.I7597.078919

Granat, J., Batalla, J. M., Mavromoustakis, C. X., & Mastorakis, G. (2020). Big Data Analytics for Event Detection in the IoT-Multicriteria Approach. *IEEE Internet of Things Journal, (7)*5, 4418–4430. https://doi.org/10.1109/JIOT.2019.2957320

Gutta, S. (2020, May 4). Data Science: The 5 V's of Big Data. Retrieved April 8, 2023, from https://medium.com/analytics-vidhya/the-5-vs-of-big-data-2758bfcc51d

Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I., & Hussain, A. (2021). Big data and IoT-based applications in smart environments: A systematic review. *Computer Science Review, 39*, 1–17. https://doi.org/10.1016/j.cosrev.2020.100318

Harb, H., Idrees, A. K., Jaber, A., Makhoul, A., Zahwe, O., & Taam, M. A. (2017). Wireless Sensor Networks: A Big Data Source in Internet of Things. *International Journal of Sensors Wireless Communications and Control, 7*(2), 93–109. https://doi.org/10.2174/2210327907666170906144926

Hassan, M. (2022). State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. IoT Analytics Market Insights for the Internet of Things.

Hossain, E., Khan, I., Un-Noor, F., Sikander, S. S., & Sunny, M. S. H. (2019). Application of big data and machine learning in smart grid, and associated security concerns: A review. *IEEE Access, 7*, 13960–13988. https://doi.org/10.1109/ACCESS.2019.2894819

Islam, R, Hossen, M. S., & Shin, D. (2022). A Mapping Study on Privacy Attacks in Big Data and IoT. *2022 13th International Conference on Information and Communication Technology Convergence*. (pp. 1158–1163) Jeju Island, Korea: IEEE. https://doi.org/10.1109/ICTC55196.2022.9952824

Joseph, N., Kar, A. K., Ilavarasan, P. V., & Ganesh, S. (2017). Review of Discussions on Internet of Things (IoT): Insights from Twitter Analytics. *Journal of Global Information Management, 25*(2), 38–51. https://doi.org/10.4018/JGIM.2017040103

Kalid, S., Syed, A., Mohammad, A., & Halgamuge, M. N. (2017). Big-data NoSQL databases: A comparison and analysis of "Big-Table", "DynamoDB", and "Cassandra". *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*. (pp. 89-93), Beijing, China: IEEE. https://doi.org/10.1109/ICBDA.2017.8078782

Karimi, Y., Haghi Kashani, M., Akbari, M., & Mahdipour, E. (2021). Leveraging Big Data in Smart Cities: A Systematic Review. *Concurrency and Computation: Practice and Experience, 33*(21), e6379. https://doi.org/10.1002/cpe.6379

Khare, S., & Totaro, M. (2020). Ensemble Learning for Detecting Attacks and Anomalies in IoT Smart Home. *2020 3rd International Conference on Data Intelligence and Security (ICDIS)*. South Padre Island: IEEE. https://doi.org/10.1109/ICDIS50059.2020.00014

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, *51*(1), 7–15. https://doi.org/10.1016/j.infsof.2008.09.009

Kumar, A. V., Chitumadugula, S., & Rayalacheruvu, V. T. (2022). Crime Data Analysis using Big Data Analytics and Visualization using Tableau. *2022 6th International Conference on Electronics, Communication and Aerospace Technology* (pp. 627–632). Coimbatore, India: IEEE. https://doi.org/10.1109/ICECA55336.2022.10009119

Lavanya, P., Subbareddy, I. V., & Selvakumar, V. (2022). Internet of Things enabled Block Level Security Mechanism to Big Data Environment using Cipher Security Policies. *2022 International Conference on Advances in Computing, Communication and*

Applied Informatics (ACCAI) (pp. 1–6). Chennai, India: IEEE. https://doi.org/10.1109/ACCAI53970.2022.9752603

Li, Y., & Zhang, D. (2020). Hadoop-Based University Ideological and Political Big Data Platform Design and Behavior Pattern Mining. *2020 International Conference on Advance in Ambient Computing and Intelligence (ICAACI)*. Ottawa, ON, Canada, pp. 47–51. https://doi.org/10.1109/ICAACI50733.2020.00014

Li, F., Xie, R., Wang, Z., Guo, L., Ye, J., Ma, P., & Song, W. (2020). Online Distributed IoT Security Monitoring With Multidimensional Streaming Big Data. *IEEE Internet of Things Journal, 7*(5), 4387–4394. https://doi.org/10.1109/JIOT.2019.2962788

Li, Y., Ma, J., An, B., & Cao, D. (2018). BDViewer — A Web-Based Big Data Processing and Visualization Tool. *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*. Tokyo, Japan: IEEE. https://doi.org/10.1109/COMPSAC.2018.00080

Lv, Z., Lou, R., Li, J., Singh, A. K., & Song, H. (2021). Big Data Analytics for 6G-Enabled Massive Internet of Things. *IEEE Internet of Things Journal, 8*(7), 5350–5359. https://doi.org/10.1109/JIOT.2021.3056128

Mahmood, K., Ferzund, J., Saleem, M. A., Shamshad, S., Das, A. K., & Park, Y. (2023). A Provably Secure Mobile User Authentication Scheme for Big Data Collection in IoT-Enabled Maritime Intelligent Transportation System. *IEEE Transactions on Intelligent Transport Systems, 24*(2), 2411–2421. https://doi.org/10.1109/TITS.2022.3177692

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., & Aharon, D. (2015). The Internet of Things: Mapping the value beyond the hype. McKinsey Global Institute. https://globaltrends.thedialogue.org/publication/the-internet-of-things-mapping-the-value-beyond-the-hype/:.

Maswadi, K., Ghani, N. B. A., & Hamid, S. B. (2020). Systematic Literature Review of Smart Home Monitoring Technologies Based on IoT for the Elderly. *IEEE Access, 8*, 92244–92261. https://doi.org/10.1109/ACCESS.2020.2992727

Misra, N. N., Dixit, Y., Al-Mallahi, A., Bhullar, M. S., Upadhyay, R., & Martynenko, A. (2022). IoT, Big Data, and Artificial Intelligence in Agriculture and Food Industry. *IEEE Internet of Things Journal, 9*(9), 6305–6324. https://doi.org/10.1109/JIOT.2020.2998584

Mohamad Jawad, H. H., Bin Hassan, Z., Zaidan, B. B., Mohammed Jawad, F. H., Mohamed Jawad, D. H., & Alredany, W. H. D. (2022). A Systematic Literature Review of Enabling IoT in Healthcare: Motivations, Challenges, and Recommendations. *Electronics (Switzerland), 11*(9). https://doi.org/10.3390/electronics11193223

Ning, Z., Dong, P., Wen, M., Wang, X., Guo, L., Kwok, R. Y., & Poor, H. V. (2021). 5-G Enabled UAV-to-Community Offloading: Joint Trajectory Design and Task Scheduling. *IEEE Journal on Selected Areas in Communications, 39*(11), 3306–3320. https://doi.org/10.1109/JSAC.2021.3088663

Page, M. J., McKenzie, J. E., Bossuyt, P. M., *et al.* (2021). The PRISMA 2020 Statement: An Updated Guideline for Reporting Systematic Reviews. *Systematic Reviews. 372(n71)*, 1–11. https://doi.org/10.1136/bmj.n71

Paraschiv, E. A., Petrache, C. M., & Bica, O. (2022). On the continuous development of IoT in Big Data Era in the context of Remote Healthcare Monitoring & Artificial Intelligence. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. Ploiesti, Romania. pp. 1–6 https://doi.org/10.1109/ECAI54874.2022.9847503

Pavithra, A., Anandhakumar, C., & Meenashisundharam, V. N. (2019). Internet of Things with BIG DATA Analytics – A Survey. *International Journal of Scientific Research in Computer Science Applications and Management Studies, 8*(1).

Putra, G. D., Dedeoglu, V., Kanhere, S. S., Jurdak, R., & Ignjatovic, A. (2021). Trust-Based Blockchain Authorization for IoT. *IEEE Transactions on Network and Service Management, 18*(2), 1646–1658. https://doi.org/10.1109/TNSM.2021.3077276

Rao, P. M., & Deebak, B. D. (2022). Security and Privacy Issues in Smart Cities/Industries: Technologies, Applications, and Challenges. *Journal of Ambient Intelligence and Humanized Computing 14*, 1-37. https://doi.org/10.1007/s12652-022-03707-1

Reinsel, D., Gantz, J., & Rydning, J. (2017). Data Age 2025: The Evolution of Data to Life-Critical: Don't Focus on Big Data; Focus on the Data That's Big. *An IDC White Paper*. Retrieved from https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf

Sachindra, U. G. T., & Rajapaksha, U. U. S. (2022). Security Architecture Development in Internet of Things Operating Systems. *2022 International Research Conference on Smart Computing and Systems Engineering*. Colombo, Sri Lanka: IEEE. https://doi.org/10.1109/SCSE56529.2022.9905160

Saeed, N., Malik, H., Naeem, A., & Bashir, U. (2023). Incorporating big data and IoT in intelligent ecosystems: state-of-the-arts, challenges and opportunities, and future directions. *Multimedia Tools and Applications*. https://doi.org/10.1007/s11042-023-16328-3

Saha, A. K., Kumar, A., Tyagi, V., & Das, S. (2018). Big data for Internet of Things: a survey. 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 150–156. https://doi.org/10.1109/ICACCCN.2018.8748630

Shah, S. A., Seker, D. Z., Hameed, S., & Draheim, D. (2019). The rising role of big data analytics and IoT in disaster management: Recent advances, taxonomy and prospects. *IEEE Access, 7*, 54595–54614. https://doi.org/10.1109/ACCESS.2019.2913340

Sharma, M., Hagar, A. A., Murthy, G. R. K., Beyane, K., Gawali, B. W., & Pant, B. (2022). A Study on Recognising the Application of Multiple Big Data Technologies and its Related Issues, Difficulties and Opportunities. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. Greater Noida, India, pp. 341–344. https://doi.org/10.1109/ICACITE53722.2022.9823623

Srinivas, J., Das, A. K., Wazid, M., & Vasilakos, A. V. (2021). Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System. *IEEE Internet of Things Journal, 8*(9), 7727–7744. https://doi.org/10.1109/JIOT.2020.3040938

Taheri, R., Shojafar, M., Alazab, M., & Tafazolli, R. (2021). Fed-IIoT: A Robust Federated Malware Detection Architecture in Industrial IoT. *IEEE Transactions on Industrial Informatics, 17*(12), 8442–8452. https://doi.org/10.1109/TII.2020.3043458

Tedyyana, A., Sivakumar, G., Kumar, A., Velayudham, A., Pavithra, M., & Gangodkar, D. (2022). A Framework for Big Data Analytics with Wireless Communication of Network, Internet of Things and Cyber Security. *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*. Greater Noida, India: IEEE. https://doi.org/10.1109/ICACITE53722.2022.9823802

Tian, D. (2022). Simulation of Distributed Big Data Intelligent Fusion Algorithm Based on Machine Learning. *2022 International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS)*. IEEE. https://doi.org/10.1109/AIARS57204.2022.00101

Torabi, S., Dib, M., Bou-Harb, E., Assi, C., & Debbabi, M. (2021). A Strings-Based Similarity Analysis Approach for Characterizing IoT Malware and Inferring Their Underlying Relationships. *IEEE Networking Letters, 3*(3), 161–165. https://doi.org/10.1109/LNET.2021.3076600

Wan, W., Du, X., Zhao, X., Yang, Z. (2021). A Cloud-Enabled Collaborative Hub for Analysis of Geospatial Big Data. *2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics,* pp. 1–5. https://doi.org/10.1109/ICCCBDA51879.2021.9442514

Wang, T., Liang, Y., Zhang, Y., Zheng, X., Arif, M., Wang, J., & Jin, Q. (2020). An Intelligent Dynamic Offloading From Cloud to Edge for Smart IoT Systems With Big Data. *IEEE Transactions on Network Science and Engineering, 7*(4), 2598–2607. https://doi.org/10.1109/TNSE.2020.2988052

Wu, Q., He, K., & Chen, X. (2020). Personalized Federated Learning for Intelligent IoT Applications: A Cloud-Edge Based Framework. *IEEE Open Journal of the Computer Society, 1*, 35–44. https://doi.org/10.1109/OJCS.2020.2993259

Yu, R., Zhang, X., & Zhang, M. (2021). Smart Home Security Analysis System Based on The Internet of Things. *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*. Nanchang, China: IEEE. https://doi.org/10.1109/ICBAIE52039.2021.9389849

Yu, W., Liu, Y., Dillon, T., Rahayu, W., & Mostafa, F. (2022). An Integrated Framework for Health State Monitoring in a Smart Factory Employing IoT and Big Data Techniques. *IEEE Internet of Things Journal, 9*(3), 2443–2454. https://doi.org/10.1109/JIOT.2021.3096637

Zhang, P., Wang, Y., Kumar, N., Jiang, C., & Shi, G. (2022). A Security- and Privacy-Preserving Approach Based on Data Disturbance for Collaborative Edge Computing in Social IoT Systems. *IEEE Transactions on Computational Social Systems, 9*(1), 97–108. https://doi.org/10.1109/TCSS.2021.3092746

Zhang, Y. (2022). Countermeasures for the Development of the Industrial Chain of the Internet of Things Based on Big Data. *2022 International Joint Conference on Information and Communication Engineering (JCICE)*. Seoul: IEEE. https://doi.org/10.1109/JCICE56791.2022.00016

Zhaofeng, M., Lingyun, W., Xiaochang, W., Zhen, W., & Weizhe, Z. (2020). Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data. *IEEE Internet of Things Journal, 7*(5), 4000–4015. https://doi.org/10.1109/JIOT.2019.2960526

Zhong, Y., Chen, L., Dan, C., & Rezaeipanah, A. (2022). A systematic survey of data mining and big data analysis in internet of things. *The Journal of Supercomputing, 78*(15), 18405–18453. https://doi.org/10.1007/s11227-022-04594-1