Hindawi
Mobile Information Systems
Volume 2021, Article ID 8847099, 25 pages
https://doi.org/10.1155/2021/8847099

Review Article

Current Research Trends in IoT Security: A Systematic Mapping Study

Jee Young Lee and Jungwoo Lee

Graduate School of Information, Yonsei University, Seoul 037222, Republic of Korea

Correspondence should be addressed to Jee Young Lee; j.ann.lee@yonsei.ac.kr

Received 26 September 2020; Revised 29 January 2021; Accepted 27 February 2021; Published 13 March 2021

Academic Editor: Vishal Sharma

The smart mobile Internet-of-things (IoT) network lays the foundation of the fourth industrial revolution, the era of hyperconnectivity, hyperintelligence, and hyperconvergence. As this revolution gains momentum, the security of smart mobile IoT networks becomes an essential research topic. This study aimed to provide comprehensive insights on IoT security. To this end, we conducted a systematic mapping study of the literature to identify evolving trends in IoT security and determine research subjects. We reviewed the literature from January 2009 to August 2020 to identify influential researchers and trends of keywords. We additionally performed structural topic modeling to identify current research topics and the most promising ones via topic trend estimation. We synthesized and interpreted the results of the systematic mapping study to devise future research directions. The results obtained from this study are useful to understand current trends in IoT security and provide insights into research and development of IoT security.

1. Introduction

The era of hyper-connectivity, hyper-intelligence, and hyperconvergence established by the fourth industrial revolution is continuing in earnest as smart mobile Internet-of-things (M-IoT) environments are developing. The Internet of things (IoT) establishes a new networking paradigm in which various devices (e.g., network devices, sensors, and actuators) become essential elements for communication. Various objects can be considered as "smart" because they are equipped with microprocessors and network transceivers, enabling communication and the provision of autonomous services. IoT is a promising field of research related to building device networks connected to the Internet and promotes smart environments. IoT is associated with many research areas and new computing paradigms. The M-IoT cloud-computing domain, which lies at the intersection of the cloud, mobile, and IoT domains, provides new paradigms of fog computing, edge computing, mobile-edge computing (MEC), the semantic web of things, and mobile crowdsensing. Elazhary [1] summarized various related concepts. The Internet of mobile things (i.e., M-IoT) is a special case of IoT concerned with mobile IoT devices. Such devices include smartphones, vehicles, and wearable devices [2]. The IoT paradigm is also evolving into smart M-IoT devices, which in turn provide smart services and computing functions.

IoT-based smart systems and services are being developed in various fields, such as home automation, energy management, healthcare, and financial transaction management [3–6]. It is also branching into new domains, such as social IoT, in which smart objects are transformed into social objects; industrial IoT, which converges with different industries; smart-wearable IoT, which combines deep learning and wearable technologies; and medical IoT, which is integrated with medical applications [3–6].

Smart M-IoT provides smart convergence services to users of IoT environments. Accordingly, many researchers in various fields are now involved with IoT development. For the continued spread and development of smart M-IoT, it is necessary to consider security, as the devices and platforms of smart M-IoT mainly remain threatened [7]. The emphasis on security will increase, and both consolidated and new researchers need understanding and insights on IoT security.

The remainder of this paper is organized as follows. Section 2 discusses related work about the study on IoT topics and trends. Section 3 describes the conducted systematic mapping study on IoT security. Section 4 discusses the main findings. Influential authors are identified in Section 4.1, and keyword-based clusters and keyword trends are presented in Section 4.2. Research topics related to IoT security are categorized in Section 4.3, and the trend of topics is discussed in Section 4.4. Section 4.5 provides future perspectives by synthesizing the keyword and topic trends. Finally, conclusions are drawn in Section 5.

2. Related Work

2.1. Research Methodology. One of the first challenges before conducting research in any field of study is identifying relevant previous studies and establishing the need for new research [8]. Secondary research analyzes existing studies (primary research) and seeks to provide relevant insights to researchers and guide the design of future research. Secondary research methodologies include the review, systematic literature review (SLR), and systematic mapping study.

In the review or survey, researchers select important literature according to their expertise. Then, they synthesize and organize the contents. The review provides new understanding and insights about the content through in-depth content comparison analyses. However, as the content should be analyzed closely, there is a limit to the number of documents that can be included in the study due to time and cost constraints [8, 9].

The SLR applies an explicit and systematic protocol for collecting, selecting, and analyzing research literature [10]. It provides quantitative and statistical insights on the subject by analyzing primary studies to answer research questions while providing aggregate result data [11]. Therefore, SLRs can be performed with studies that can quantitatively extract information meeting the aggregation criteria.

The relatively recently developed systematic mapping study is a more open form of SLR, which aims to organize a research area [9]. This method uses the same protocol as the SLR to find and select research literature. Unlike the SLR, the systematic mapping study classifies subfields of a research area [11, 12] and focuses on identifying and classifying themes by collecting as many studies as possible [13]. The categories used are generally based on publication information (e.g., author name, author affiliation, publication source, publication type, and publication date) and/or information about the adopted research method [13]. A systematic mapping study is sometimes conducted as a preliminary study before the SLR [14, 15]. It classifies subject areas and identifies those requiring detailed content comparisons. Research on text mining and visualization tools that can be used to efficiently perform this type of analysis is ongoing [14, 16, 17]. Petersen et al. [9, 15] noted that performing a systematic mapping study before an SLR provided valuable research design criteria. Kitchenham et al. [13, 18] stated that systematic mapping can provide input data for subsequent studies. In other words, systematic mapping reduces the preparation time for subsequent research. In addition, it provides an overview of research areas and identifies research gaps. Moreover, it helps in identifying research trends and educational materials.

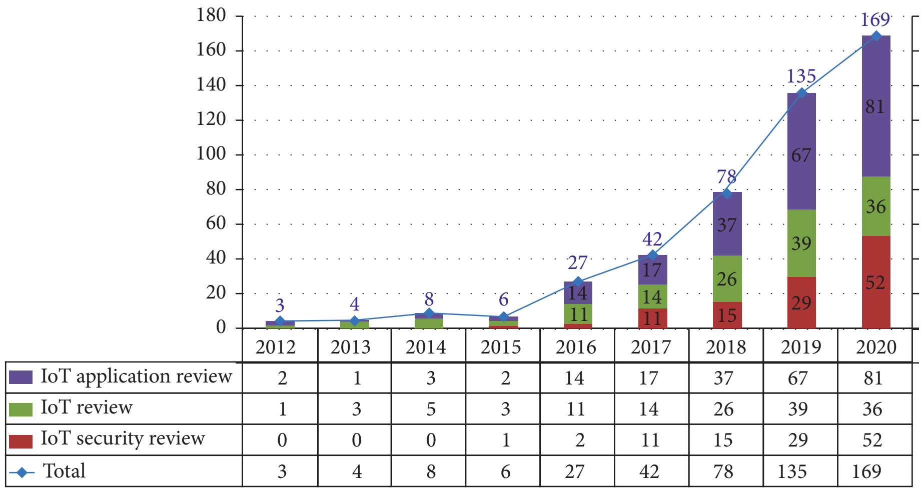
2.2. Comparison with Related Reviews. To better understand existing secondary research related to IoT, Scopus articles classified as "review" between January 2012 and October 2020 were collected, obtaining 472 review articles. These articles were then further categorized into labels "IoT security review," "IoT application review," or "IoT review," as shown in Figure 1.

Reviews related to IoT have been increasing rapidly since 2018. IoT applications including smart cities [19, 20], smart health [21, 22], smart agriculture [23, 24], and smart vehicles [25, 26] were the most frequently reviewed. In 2020, IoT security reviews were more numerous than IoT reviews. Note that we did not classify articles that have partially discussed security under label "IoT security review." Instead, we classified the articles that exclusively focus on security under this label. Table 1 compares recent reviews on IoT security from 2017 to 2020 in terms of methodology. Most of these reviews synthesized and organized contents using a review/survey method. From them, articles similar to our study are listed in Table 2.

Existing studies have some limitations. Alaba et al. [27] focused on the classification of security threats but did not cover the overall contents and did not discuss new technologies, such as machine learning (ML). Mendez Mena et al. [28] focused on IoT architectures but did not consider applications. Obaidat et al. [32] aimed to comprehensively cover IoT security but omitted related applications. In contrast, Hassija et al. [29] did not cover IoT as a whole, focusing only on applications. Hameed et al. [31] did not deal with trust as a security requirement. The major limitation of the abovementioned reviews is that they fail to provide research trends.

Sharma et al. [7] dealt with the most recent paradigm in depth, focusing on smart M-IoT, and provided a roadmap for related surveys. However, it was not a study focused on providing early insights to researchers entering from other fields. Macedo et al. [30] focused on providing insights and research trends using an SLR, but they omitted privacy. In addition, they only selected 131 articles for review. Most of the review studies not listed in Table 2 focused on specific areas of IoT security, such as layer protocols [33], intrusion detection [34], device security [35, 36], trust [37], and security of specific IoT applications [38]. Thus, a systematic mapping study is still required to determine research topics and trends in IoT security and gain insights on this field.

2.3. Contributions of This Study. For the transition to a secure, smart M-IoT, we should understand the available resources on IoT security. We aimed to provide researchers interested in IoT research with early insights on IoT security by conducting a systematic mapping study. To the best of our



	2012	2013	2014	2015	2016	2017	2018	2019	2020
🟪 IoT application review	2	1	3	2	14	17	37	67	81
🟩 IoT review	1	3	5	3	11	14	26	39	36
🟥 IoT security review	0	0	0	1	2	11	15	29	52
◆ Total	3	4	8	6	27	42	78	135	169

Figure 1: Trends in IoT-related review articles.

Table 1: Comparison of methodology used in IoT security review articles from 2017 to 2020.

Methodology	2017	2018	2019	2020
Review/Survey	11	15	25	47
SLR	0	0	4	5
Systematic mapping study	0	0	0	0

knowledge, no such studies focused on IoT security are available. We applied big data mining tools to large volumes of literature for the systematic mapping study, which is thus unbiased and replicable. We classify research on IoT security based on keywords and topics. We also explain trends and provide new understanding about keyword evolution and promising research topics. The results from this study may be used by lecturers to teach the overview, main topics, and trends related to IoT security. In addition, a qualitative content analysis provides future research directions.

In this study, we also demonstrated the application of big data mining to a systematic mapping study. The methods and findings reported in this paper may provide research opportunities by improving the overall understanding of IoT security and its research trends. In addition, the results of this study can be useful to researchers in other fields who intend to investigate IoT convergence.

3. Methods

In this study, we conducted a systematic mapping study of current research related to IoT security by mixing quantitative and qualitative approaches. The quantitative approach involves collecting literature on IoT security and conducting a systematic mapping study to identify influential researchers and concurrent keywords. We then classify the topics using an ML-based structural topic model (STM). Next, we perform qualitative content analysis to devise future research directions by synthesizing and discussing the latest keyword and topic trends. Our research aims to answer the following research questions:

RQ1. Who are influential researchers in IoT security?

RQ2. What are the major keywords in IoT security?

RQ2-1. What is the keyword-based research area?

RQ2-2. How are keywords evolving?

RQ3. What are the topics in IoT security field?

RQ3-1. What is topic-based research classification?

RQ3-2. What is the trend of topics?

RQ4. What are the most influential keywords in IoT security?

RQ5. What are promising research topics in IoT security?

Figure 2 shows the research framework that we used to understand the current status and trends in IoT security.

We selected studies according to PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [8]. We adopted a review protocol consisting of search terms, resources to be searched, study selection criteria, and study selection procedures, as listed in Table 3. We used Boolean operator AND to combine IoT and security-related terms (e.g., “secure,” “security,” “privacy,” and “trust”). We filtered the data based on the document type (e.g., “article”), source (e.g., “journal”), and language (e.g., “English”). The main research question and review protocols are listed in Table 3. Our literature search was conducted using 1,365 studies published from January 2009 to August 2020. Unlike existing review studies, we analyzed a large volume of articles to obtain comprehensive insights. To process that large volume, we used big data mining tools.

3.1. Bibliometric Mapping Study on IoT Security. In recent years, bibliometric analyses, co-citation network analyses, and keyword co-occurrence network analyses have been widely

Table 2: Comparison with related review articles.

Article	Adopted methodology	Main focus	Contribution/impact
Alaba et al. [27]	Review	IoT security threats and vulnerabilities	(i) Classification of security threats in the context of applications, architecture, communication, and data (ii) Attack analysis for security scenarios
Mendez Mena et al. [28]	Review	Security from the perspective of IoT architecture	(i) IoT architecture technology and protocol review by layer (ii) Review of privacy issues (iii) Summarize ongoing security issues of IoT
Hassija et al. [29]	Review	Security of IoT application	(i) IoT application security related issues and threat sources review (ii) Discussion of technology to increase trust in IoT applications (iii) Discussion of the latest technology to increase the level of security
Macedo et al. [30]	SLR	IoT security overall	(i) Review of literature over the last 8 years to identify security issues and trends in terms of authentication, access control, data protection, and trust
Hameed et al. [31]	Review	Requirements of IoT security	(i) Review privacy, lightweight encryption framework, security routing, internal attack detection, and resilience management as security requirements (ii) Explain the latest technology for resilience management and detection of internal attacks
Obaidat et al. [32]	Review	IoT security overall	(i) Comprehensive investigation of security, privacy, security frameworks, technologies, threats, vulnerabilities, and countermeasures. (ii) Classification of the impact of attacks according to -NIST's FIPS 199 definitions
Sharma et al. [7]	Review	Security, privacy, and trust in smart M-IoT	(i) The first survey discussing the security of smart M-IoT (ii) Describe the security framework of smart M-IoT and conduct an in-depth investigation in terms of security, privacy, and trust to provide research tasks, unresolved issues, and research directions
Our study	Systematic mapping study	IoT security overall	(i) Classify large-volume literature related to IoT security from 2009 to the present (ii) Discussion of research trends through co-occurrence keyword mapping (iii) Discussion of research trends through topic mapping (iv) Provide future research direction

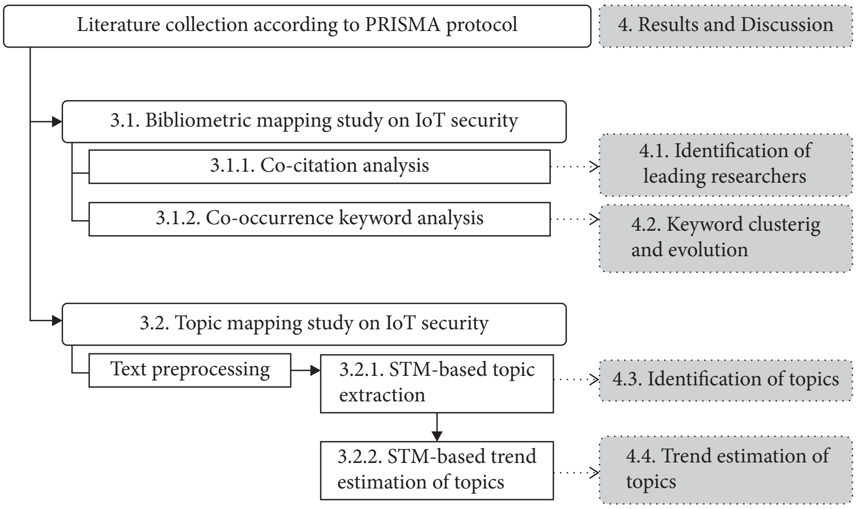

Literature collection according to PRISMA protocol
4. Results and Discussion
3.1. Bibliometric mapping study on IoT security
3.1.1. Co-citation analysis
4.1. Identification of leading researchers
3.1.2. Co-occurrence keyword analysis
4.2. Keyword clusterig and evolution
3.2. Topic mapping study on IoT security
Text preprocessing
3.2.1. STM-based topic extraction
4.3. Identification of topics
3.2.2. STM-based trend estimation of topics
4.4. Trend estimation of topics

Figure 2: Research framework adopted in this study.

used to determine research trends [39–41]. Co-citation network analysis determines the structure of scientific communications by analyzing the associations among citations. Co-occurrence keyword network analysis allows to understand the knowledge structure underlying a technical field by analyzing links between keywords found in the literature.

Table 3: Research question and review protocol.

Research goal		What are the research trends in IoT security?
Review protocol	Search terms	(“IoT” OR “Internet of things”) AND (“secure” OR “security” OR “privacy” OR “trust”) in title
	Resources	Scopus
	Study selection criteria	Journal articles written in English
	Study selection procedures	Two researchers searched the databases and checked each other’s work.
	No. of studies satisfying criteria	1,528
Study filtering	Duplication	−2
	Unavailable abstract	−13
	Unavailable author keywords	−148
	No. of studies after filtering	1,365

Radhakrishnan et al. [41] demonstrated the role of keyword co-occurrence networks in systematic reviews. In this current study, we conducted co-citation and co-occurrence keyword mapping studies to provide answers to RQ1 and RQ2.

3.1.1. Co-Citation Network Analysis to Identify Authors of IoT Security Research. By analyzing the co-citations of studies on IoT security, we can identify influential researchers and understand the research flow [42–44], and then we can answer RQ1. We performed author clustering by the relevance obtained from direct citation relationships. We used the quality function proposed by Traag et al. [45] and modified by Waltman and Van Eck [42] for clustering. The quality function is given by

$$\mathrm{Q}\left(x_1, \ldots, x_n\right) = \sum_{i=1}^{n} \sum_{j=1}^{n} \delta\left(x_i, x_j\right)\left(a_{ij} - \frac{\gamma}{2n}\right), \quad (1)$$

where n is the number of studies, a_{ij} measures the relation between studies i and j, γ is a resolution parameter, and x_i denotes the cluster to which study i is assigned. Function $\delta(x_i, x_j)$ is 1 if $x_i = x_j$ and 0 otherwise. The relation between studies i and j is measured as follows:

$$a_{ij} = \frac{c_{ij}}{\sum_{k=1}^{n} c_{ik}}. \quad (2)$$

In equation (2), if study i cites study j or vice versa, c_{ij} is 1, whereas it is 0 otherwise. Hence, if there is no direct citation relation between studies i and j, the relation measure, c_{ij}, is zero.

We used the CitNetExplorer tool for citation analysis [46] and set resolution parameter γ to 1 and the number of parameter optimization iterations to 10.

3.1.2. Co-Occurrence Keyword Network Analysis to Map Keyword Evolution on IoT Security. Keyword co-occurrence analysis is commonly used to determine research trends, and it has been used to conduct a systematic literature review in [41]. We adopted the method proposed by Van Eck and Waltman [47] to construct and analyze a co-occurrence keyword network that answers RQ2 and RQ4.

We performed co-occurrence analysis on keywords collected from different studies. A keyword may appear in various forms (e.g., “blockchain,” “blockchain,” “blockchain,” or “blockchains”). Therefore, after arranging a thesaurus, we applied it and grouped the keywords with the same meaning to then create a keyword co-occurrence matrix. Next, we generated a similarity matrix normalized according to the association strength of the keyword co-occurrence matrix [48]. Similarity s_{ij} between items i and j according to the association strength is given by

$$s_{ij} = \frac{c_{ij}}{c_i c_j}, \quad (3)$$

where c_{ij} represents the number of co-occurrences of items i and j, and c_i and c_j represent the total number of occurrences of items i and j, respectively.

Next, we visualized the similarities based on the similarity matrix by constructing a 2D map [49], where item 1, ..., n is allocated such that the distance between any pair of items i and j reflects similarity s_{ij} as accurately as possible. Items with high similarity were grouped closely, and those with low similarity remained distant. Specifically, we minimized the weighted sum of the squared Euclidean distances between all pairs. The higher the similarity between the two items, the higher the weight of the squared distance in the sum. The objective function for minimization is given by

$$\mathrm{V}\left(x_1, \ldots, x_n\right) = \sum_{i<j} s_{ij}\left\|x_i - x_j^2\right\|, \quad (4)$$

where vector $x_i = (x_{i1}, x_{i2})$ represents the position of item i in the 2D map and $\|\cdot\|$ represents the Euclidean norm.

From bibliometric mapping, we obtained the nodes corresponding to the keywords in the co-occurrence network, link weight, total link strength, and occurrence weights. The link weight corresponds to the number of links per node, and the total link strength is the number of links from other nodes connected to a target node. In addition, the occurrence weight represents the frequency of keyword occurrence. We then performed clustering based on the mapping results according to the method proposed by Waltman et al. [49]. To improve clustering accuracy, we applied the smart local-moving algorithm developed by Waltman and Van Eck [50].

Finally, we used the VOSviewer tool to create and visualize the bibliometric map for keyword co-occurrence network analysis [47]. We set the minimum number of occurrences of a keyword to 5 as a parameter in VOSviewer and set resolution γ to 1 with a minimum cluster size of 5. We consulted two IoT experts to analyze the clusters regarding the similarities of the co-occurrence keyword network.

3.2. Topic Mapping Study to Identify Topics in IoT Security. Regarding RQ3 and RQ5, we conducted text mining to categorize research related to IoT security and identify its trends. Text mining, also known as knowledge discovery from text, relies on various text analyses and processes to extract meaningful information from unstructured text data using natural language processing [51, 52]. In this study, we conducted STM-based topic modeling.

3.2.1. STM-Based Topic Extraction to Classify Topics in IoT Security. Topic modeling is an unsupervised learning method to determine and classify topics underlying textual data. The STM proposed by Roberts et al. [53] is a modified and extended version of the latent Dirichlet allocation, the most widely used topic modeling method. The STM determines the distribution of words constituting a topic based on the frequency of words in a document along with metadata (e.g., author's gender and age, publication year). The STM estimates the correlation between topics using the covariance matrix of the corresponding logistic normal distribution [53]. Figure 3 illustrates the STM, which can be divided into three components: a topic prevalence model that controls how words are allocated to topics as a function of covariates; a topical content model that controls the frequency of the terms in each topic as a function of the covariates; and a core language model [54].

According to Roberts et al. [53], given the number of topics (K), observed words and design matrices $\{w_{d,n}\}$, topic prevalence (X), topical content (Y), and K-dimensional hyperparameter vector (σ), data generation for document d can be modeled as

$$\gamma_k \sim \text{Normal}_p\left(0, \sigma_k^2 I_p\right), \quad \text{for } k = 1, \ldots, K-1, \tag{5}$$

$$\theta_d \sim \text{LogisticNormal}_{K-1}\left(\Gamma' \text{x}_d', \Sigma\right), \tag{6}$$

$$\text{Z}_{d,n} \sim \text{Multinominal}_K\left(\theta_d\right), \quad \text{for } n = 1, \ldots, N_d, \tag{7}$$

$$W_{d,n} \sim \text{Multinominal}_V\left(\beta_{Z_{d,n}}\right) \quad \text{for } n = 1, \ldots, N_d, \tag{8}$$

$$\beta_{d,k,v} = \frac{\exp\left(m_v + K_{k,v}^{(t)} + K_{y_d,v}^{(c)} + K_{y_d,k,v}^{(i)}\right)}{\sum_v \exp\left(m_v + K_{k,v}^{(t)} + K_{y_d,v}^{(c)} + K_{y_d,k,v}^{(i)}\right)}, \quad \text{for } v = 1, \ldots, V \text{ and } k = 1, \ldots, K, \tag{9}$$

where $\Gamma = [\gamma_1| \ldots |\gamma_K]$ is a $P \times (K-1)$ matrix of coefficients for the topic prevalence model specified by equations (5) and (6), and $\left\{K_{.,.}^{(t)}, K_{.,.}^{(c)}, K_{.,.}^{(i)}\right\}$is a collection of coefficients for the topical content model specified by equation (9). Equations (7) and (8) constitute the core language model.

In topic extraction, it is essential to determine the optimal number of topics (K) for the STM [55, 56]. To this end, the STM provides useful indicators, with the most widely used being the held-out likelihood and semantic coherence. From Figure 4, as the number of topics gradually increases from 5 to 20, we can determine the point where both the held-out likelihood and semantic coherence have high values [56], obtaining 12 as the optimal number of topics.

To interpret the topics derived according to their optimal quantity in the STM, main words representing each topic can be analyzed. We selected the main words of a topic according to four criteria: highest probability, frequency and exclusivity, lift weight, and score. Highest probability words are the upper words in the topic-word distribution. Frequency and exclusivity words are those derived using the weighted harmonic mean of the word rank, which reflects frequently used and exclusive words in a topic. Lift-weight words are derived by assigning high weights to less frequent words in other topics. The score is obtained by dividing the log frequency of a specific word in a specific topic by the log frequency of that word in other topics. To extract and analyze latent topics related to IoT security from the abstracts of the analyzed articles, we implemented the STM on the *R* software [55].

3.2.2. STM-Based Trend Estimation of Topics in IoT Security. We identified hot topics with uptrends and cold topics with downtrends in IoT security. The trend of a topic was estimated by setting the publication year as the covariate for that topic.

4. Results and Discussion

4.1. Identification of Leading Researchers in IoT Security. The results from the co-citation network analysis are shown in Figure 5. We analyzed and visualized the co-citation network using CitNetExplorer, obtaining 8 clusters of 52

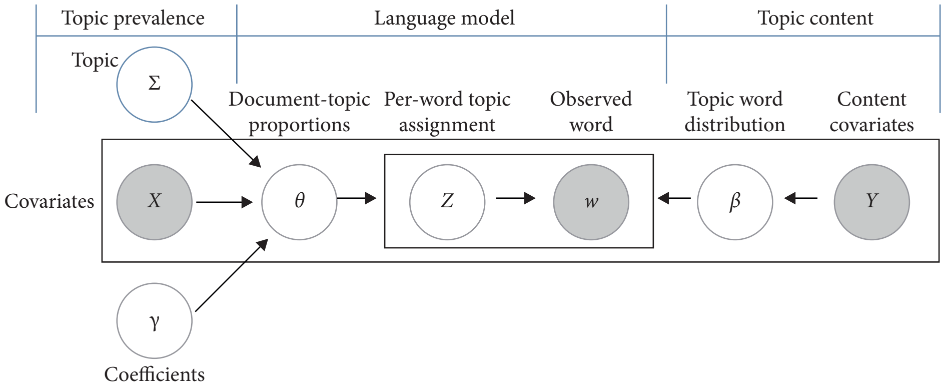
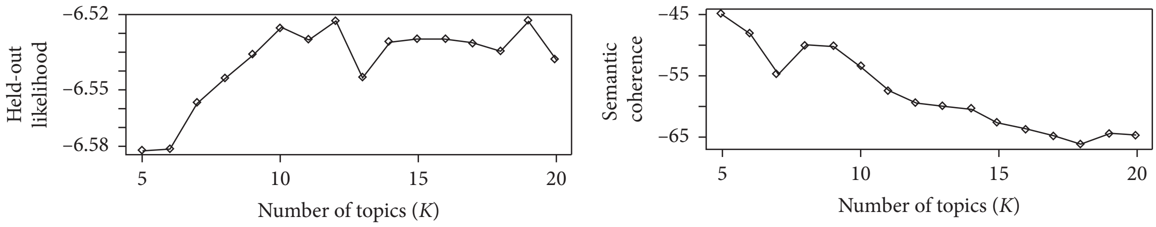


Figure 3: Diagram of STM concepts and processes.



(a)

(b)

Figure 4: Diagnostic indicators to determine the optimal number of topics. (a) Held-out likelihood. (b) Semantic coherence.

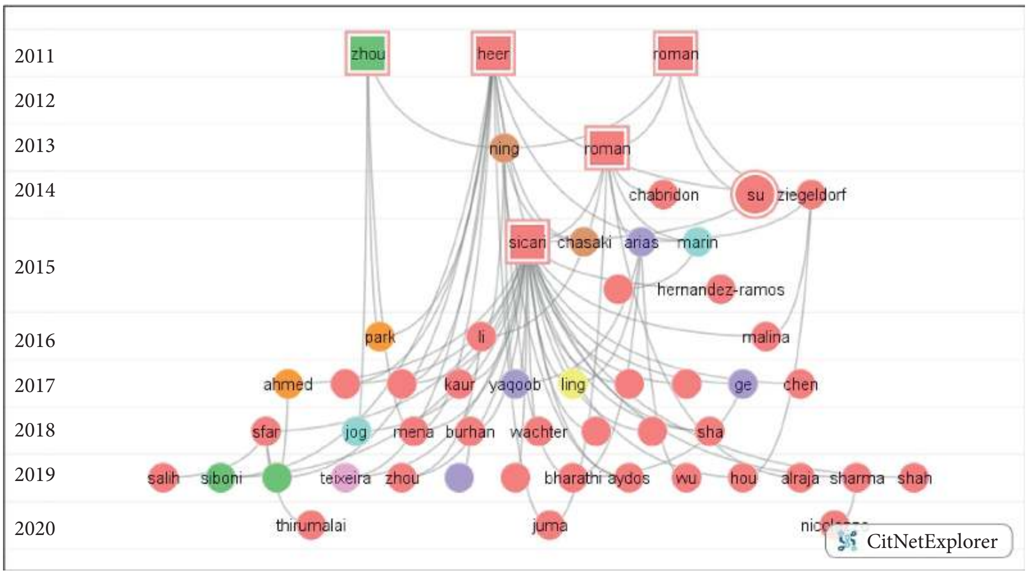


Figure 5: Co-citation network with the 52 most frequently cited publications grouped in 8 clusters (one color per cluster). The network was obtained using CitNetExplorer.

frequently cited publications. In the co-citation network, highly relevant clusters are located close together. Thus, the 8 clusters are closely related, as can be seen from the unseparated location of the nodes in the cluster. The articles on IoT security by Heer et al. [57] and Roman et al. [58] received high attention in the research community since 2011. The study with the highest citation score was authored by Sicari et al. [59] and published in 2015.

4.2. Keyword Clustering and Evolution of Research on IoT Security. From the 3,142 keywords in the 1,365 studies, 147 were derived by setting the minimum number of occurrences of a keyword to 5, and the keyword co-occurrence network analysis was performed on 146 keywords, excluding IoT, which was present in all the studies given its use with Boolean operation AND during the search.

Figure 6 shows the obtained keyword co-occurrence network with 10 clusters, and Table 4 summarizes the network and cluster information. In Figure 6, the node size is proportional to the number of occurrences of the corresponding keyword, and the link thickness is proportional to the weight of the links connecting the nodes. The node color represents the cluster containing that node.

The main keywords of cluster 1, represented by red nodes, are "sdn," "machine learning," "trust," "attacks," "ddos," and "secure routing." This cluster was summarized as the study on the introduction of artificial intelligence (e.g., ML and deep learning) to improve IoT security performance. There is increasing interest in research to improve security by introducing ML or deep learning to detect DDoS (distributed denial-of-service) attacks, malicious code, abnormal behavior, and abnormal energy consumption for IoT devices [60–66]. There was also a study aimed to ensure secure content-sharing in an IoT environment by applying ML to explore the social trust of smart device users [67, 68].

Cluster 2, represented by green nodes, consists of main keywords "ecc," "encryption," "cryptography," "aes," "energy efficiency," and "lightweight cryptography." This cluster is associated with lightweight encryption for resource-constrained IoT devices, such as those with a small size, limited computing power, and low-power consumption. Research on lightweight encryption algorithms has been conducted in relation to data and personal information security in a resource-limited environment of smart devices. The advanced encryption standard (AES) and error-correcting codes (ECC) are mainly used as basic lightweight encryption elements. Various studies have been aimed to optimize lightweight encryption while balancing security and performance management [69–76].

In cluster 3, represented by blue nodes, "privacy preservation," "cloud computing," "fog computing," "edge computing," "data privacy," and "differential privacy" are the main keywords. This cluster can be summarized with the topic of privacy preservation in IoT devices. The crowdsensing mode of smart M-IoT, a new paradigm of IoT, collects and delivers more privacy data. Thus, privacy preservation is becoming more important [77–79]. In addition, intelligent IoT applications enhanced with cloud, edge, and fog computing increasingly deal with personal information to provide intelligent services, and many studies on personal information protection and data protection are being conducted [80–83]. Among the personal information protection approaches, differential privacy is gaining attention as a mechanism to provide intelligent services by grasping user behavior patterns without infringing on personal information by adding noise to prevent the identification of personal information [81, 84–88].

Cluster 4, represented by yellow nodes, consists of main keywords, "wsn," "cps," "coap," "6lowpan," "smart object," and "sensor node." This cluster is related to studies on secure communication of smart objects in wireless sensor networks (WSNs). To transmit the information measured by sensor nodes in smart M-IoT, security is essential [89–91]. In this regard, studies on the use of IPSec/IPv6 and OpenSSL in virtual private networks have been performed to protect smart objects and provide end-to-end security [92]. The same is true for studies on end-to-end security framework development of the Constrained Application Protocol (CoAP) [93–95] and on frameworks in which smart-object users designate privacy preferences to protect personal information generated and consumed by smart objects [96]. Smart objects that have recently attracted attention are vehicles that are equipped with various sensor devices, actuators, GPS (global positioning system) receivers, and micro-embedded computers to collect, process, and transmit vast amounts of data [97, 98]. Vehicular sensor networks provide connected sensor devices that collect data and enable safer and more fluid road traffic [99]. The Internet-of-vehicles concept supports real-time vehicle-to-everything (V2X) wireless communication based on fog and edge computing [100–102]. Therefore, safe data transmission and privacy protection in vehicles, which are now smart objects, play an essential role in their development.

In cluster 5, represented by purple nodes, the main keywords are "key management," "signcryption," "elliptic curves," and "digital signature." This cluster is thus related to digital signcryption. Digital signature encryption has been investigated on algorithms, such as the elliptic curve digital-signature algorithm, digital-signature mobile applications, and digital-signature systems, to achieve document integrity and provide nonrepudiation security services in a distributed computing environment [103–107]. It is also important to satisfy reliability and confidentiality requirements of crowdsourced data [108, 109].

Cluster 6, represented by cyan nodes, comprises keywords "smart home," "raspberry pi," "arduino," and "face detection." This cluster can be described as building safe smart homes in an IoT environment. Wireless communications and sensor technologies, key components of IoT applications, are prerequisites for the security and confidentiality of smart homes [110, 111]. Before data transmission through the Session Initiation Protocol (SIP) in a home network, mutual safety verification should be conducted between devices to block advance devices that may cause risks. To this end, a secure trust relationship should be established between smart home devices, external smart devices, and other IoT devices [112–114]. A study has been conducted to design a secure IoT microcontroller module using the Raspberry Pi platform and various IoT sensors [115–117]. To achieve flexible device utilization, heterogeneous device interoperability, security enhancement of smart homes, and software-defined networks (SDN) have been applied [118, 119].

In cluster 7, represented by orange nodes, the main keywords are "privacy," "healthcare," "information security," "e-health," and "wban." This cluster can be related to IoT-based healthcare system security. As medical information systems manage patient data, data security and privacy protection are important. In IoT-based healthcare, studies on encryption and authentication protocols for user

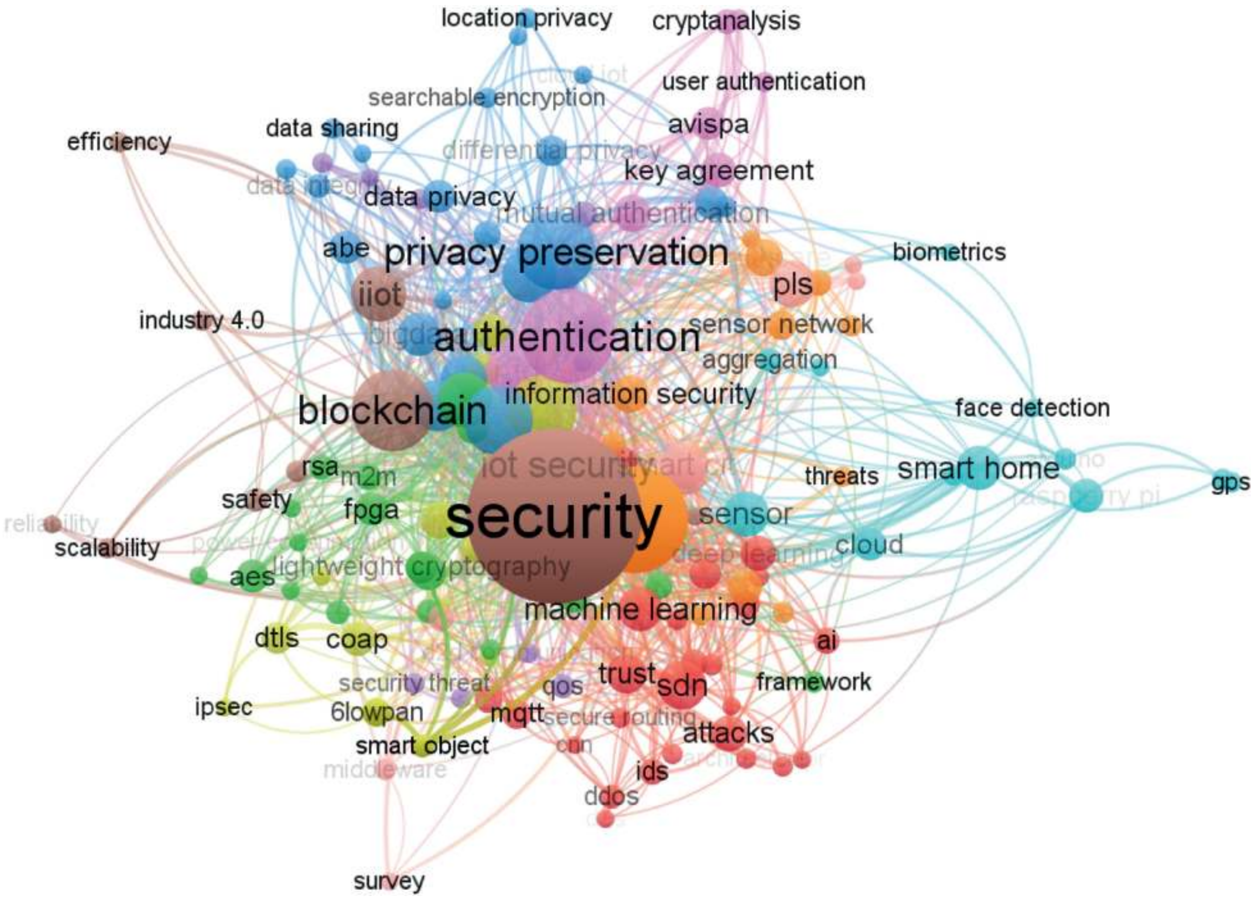


Figure 6: Keyword co-occurrence network obtained using VOSviewer.

Table 4: Specifications of keyword co-occurrence network.

Cluster	Keywords	X	Y	Weight (occurrences)	Weight (links)	Weight (total link strength)
1	SDN	0.292	−0.598	32	35	30
	Machine learning	0.178	−0.393	27	29	23
	Deep learning	0.498	−0.244	17	25	16
	Game theory	0.322	−0.537	11	17	9
	Social IoT	0.464	−0.378	11	11	8
2	ECC	−0.294	0.170	39	46	37
	5G	−0.057	−0.207	16	25	15
	Lightweight cryptography	−0.412	−0.279	12	13	10
	Lightweight encryption	−0.763	−0.342	5	9	4
3	Privacy preservation	−0.047	0.570	79	49	53
	Cloud computing	−0.203	0.114	62	46	55
	Fog computing	−0.120	0.506	39	39	35
	Edge computing	−0.296	0.228	29	38	27
4	WSN	−0.084	0.142	62	55	50
	CPS (Cyber-physical systems)	−0.363	−0.155	20	24	19
	IoT device	−0.021	−0.345	9	12	8
	Smart object	−0.409	−0.759	6	8	6
5	Key management	0.045	0.366	15	25	15
	Authentication protocol	0.029	0.668	10	10	9
	Signcryption	−0.677	0.809	6	8	6
	Digital signature	−0.549	0.769	5	10	4

Table 4: Continued.

Cluster	Keywords	X	Y	Weight (occurrences)	Weight (links)	Weight (total link strength)
6	Sensor	0.465	−0.137	28	43	27
	Smart home	1.090	−0.013	27	26	23
	Raspberry Pi	1.378	−0.086	16	10	9
	Arduino	1.323	0.012	7	10	7
7	Privacy	0.163	−0.150	138	82	126
	Healthcare	0.514	0.553	20	22	17
	Information security	0.150	0.185	20	21	14
	E-health	0.660	0.484	10	20	10
8	Security	−0.052	−0.142	360	119	306
	Blockchain	−0.487	0.141	86	57	68
	Industrial IoT	−0.525	0.456	41	37	37
	Smart contract	−0.746	−0.022	7	11	7
9	Mutual authentication	0.157	0.673	19	25	17
	Key agreement	0.391	0.789	17	21	17
	BAN (Burrows–Abadi–Needham) logic	0.441	1.195	6	11	5
	User authentication	0.512	1.028	6	9	6
10	Smart city	0.295	−0.005	31	35	27
	Cybersecurity	0.306	−0.028	23	32	20
	Mobile edge computing	0.761	0.491	5	7	5
	Secure energy efficiency	0.750	0.536	5	5	5

Note. Column keywords contain the four most representative words (from most to least important) for each cluster. Columns X and Y indicate the coordinates in the corresponding axes of the keyword node on the network shown in Figure 6.

authentication [120–123] and data encryption for patient privacy protection [124–127] are relevant. Safe and efficient medical data retrieval is important for remote medical monitoring. Given the difficulty to collect medical data safely and efficiently owing to the resource limitations of IoT devices, various studies on providing medical services by combining IoT and edge clouds have been conducted [128, 129]. In addition, to collect data, aggregate them safely and efficiently, and transmit them to a server, a study has been conducted on a system leveraging fog computing [130, 131]. There is also a growing interest in introducing unmanned aerial vehicles (UAVs) as smart objects for collecting health data. In fact, UAVs can collect health data, encrypt them, and transmit them to authenticated body sensor hives using low-power secure communications [132].

In cluster 8, represented by brown nodes, the main keywords are “blockchain,” “iiot,” “safety,” “smart contract,” and “industry 4.0.” This cluster can be described as a blockchain applied to IoT applications. It is essential to ensure the integrity of data generated in IoT environments. In this regard, research on blockchain-based encryption has been conducted [133–136]. Trust relationships must be established between disparate entities in the IoT ecosystem [137]. An analysis on the combination of blockchain and trust evaluation technologies has been conducted accordingly [138, 139]. Regarding Industry 4.0, the interest in industrial IoT (IIoT) is increasing. In particular, blockchain-based smart contracts have been studied. In addition, blockchains that provide transaction transparency, immutability, auditability, and high security for IoT-based international trade have been proposed [140, 141]. In recent years, the interest in decentralized security mechanisms based on blockchain has increased regarding the storage of important data generated by IoT systems [142, 143].

Cluster 9, represented by pink nodes, consists of main keywords “authentication,” “rfid,” “mutual authentication,” “key agreement,” and “user authentication.” This cluster is thus related to multiple forms of authentication. Smart M-IoT environments establish networks that provide smart services based on user information. Therefore, the privacy of users and the confidentiality of sensitive data must be guaranteed. Device authentication, radio-frequency identification (RFID), and user authentication are security functions that must be provided in any IoT environment [144–151].

Cluster 10, represented by coral-pink nodes, has main keywords “smart city,” “pls,” “cybersecurity,” “middleware,” and “mobile-edge computing.” This cluster can be summarized by security related to IoT-based smart cities. A smart city is an IoT application that manages a city with minimal or without human intervention and provides smart services. Beyond the smart home, it connects all sensors and smart objects at the city level to provide real-time smart services. Therefore, research on the protection of citizens’ personal information [152–154], management of IoT devices in heterogeneous device network environments [155, 156], and integrated security solutions considering the entire security stack [157, 158] has been conducted.

We also conducted a co-occurrence keyword network considering the year of publication to find answer RQ2-2. Figure 7 shows the obtained network with temporal information (publication year) encoded as a color map. Until 2017, there were many keywords related to networks, such as “6lowpan,” “dtls,” “m2m communications,” “ips,” “rfid,” “sensor networks,” and “middleware.” During the first half of 2018, many studies included keywords related to the security of data delivered over IoT applications, such as “privacy preservation,” “authentication,” and “data

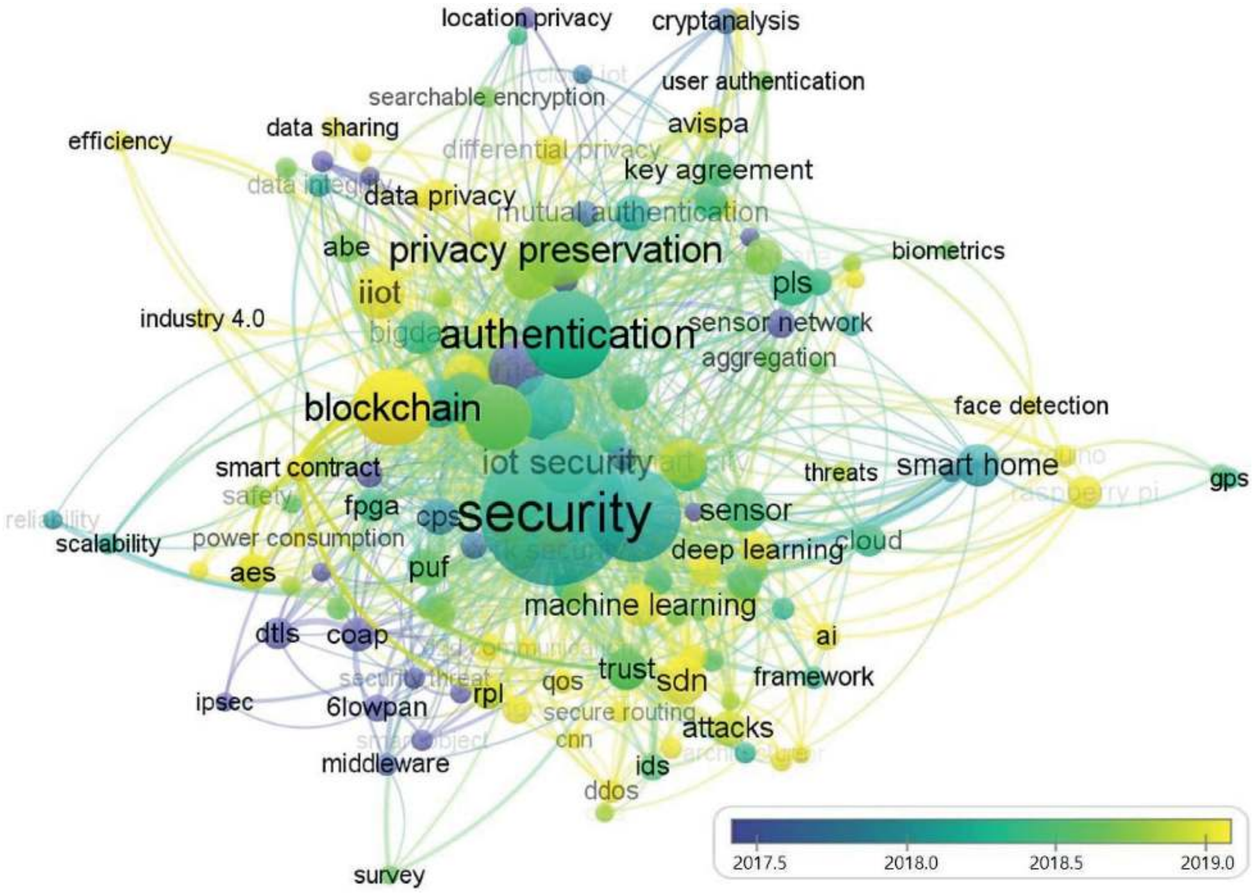


Figure 7: Keyword co-occurrence network reflecting temporal evolution. The network was obtained using VOSviewer.

integrity." During the second half of 2018, keywords, such as "trust," "fog computing," "healthcare," and "smart city," were prevalent. Since 2019, keywords related to the convergence of new technologies in the Industry 4.0 and other fields, such as "blockchain," "software-defined networking," "iiot," "machine learning," "deep learning," and "social iot," have become predominant.

4.3. Identification of Topics in IoT Security. Information about the identified topics is summarized in Table 5. For each topic, 10 top words were considered under four criteria: highest probability, frequency and exclusivity, lift weight, and score. The three most meaningful keywords per criterion are included in Table 5. We also created a label explaining each topic by analyzing the five studies with the highest proportion of contents related to that topic and containing its top words. We discussed with two IoT experts the selection of the top words and topic labels.

Topic 1 is related to understanding the characteristics of IoT across a variety of aspects and the analysis and discussion of security issues and solutions for the layers of IoT networks [159–169].

Topic 2 is related to encryption and authentication for securely sharing data in an IoT-based healthcare environment considering detailed access control. With the spread of IoT applications, smart health is becoming an attractive paradigm. As it deals with user information and sensitive medical information, the security and mutual authentication of medical sensor devices for personal information protection, encryption, and real-time monitoring are key elements [125, 170–181].

Topic 3 is related to secure and lightweight encryption designs tailored for IoT applications. Lightweight encryption with low processing time and low power consumption is required to protect and secure data transmissions of resource-constrained IoT devices. Block encryption, such as AES and S-box, Galois Counter Mode, and physical unclonable functions, are being utilized, evaluated, and proposed [70, 72, 73, 182–188].

Topic 4 is related to security using ML. Considering the heterogeneity of IoT networks and devices, it has become more common for SDN technologies to be integrated into IoT applications to form flexible and manageable architecture. When a network attack occurs in an SDN, ML can be introduced as a detection technology to dynamically control and route the communication flow. Recently, studies using ML to detect and automatically respond to DDoS attacks, abnormal patterns, and data leaks against IoT networks and devices have increased [60, 189–199].

Topic 5 is related to risk assessment and prioritization of IoT security threats. For a secure IoT environment, various

Table 5: STM-based topic extraction results and top words per topic according to four criteria.

Topic (proportions)	Top words				Topic label
	Highest probability	Frequency and exclusivity	Lift weight	Score	
1 (15%)	Security	Discuss	Attitude	Layer	IoT security issues
	Issue	Issue	Society	Security	
	Challenge	Challenge	Taxonomy	WSN	
2 (9%)	Data	Patient	Biometric	Patient	Secure data sharing for healthcare
	Access	Medical	Ciphertext-policy	Medical	
	Encrypt	Healthcare	CP-ABE (Ciphertext-policy attribute-based encryption	Signature	
3 (6.5%)	Algorithm	PUF (Physical unclonable function	Scalar	PUF	Lightweight encryption
	Encrypt	FPGA (field programmable gate array)	Simeck	S-box (substitution-box)	
	Power	S-box	AES-GCM (advanced encryption standard-Galois counter mode)	FPGA	
4 (7.6%)	Device	SDN	OpenFlow	Detect	Security with ML
	Attack	Learning	SDN-IoT	Attack	
	Detect	Intrusion	Cyber-attack	SDN	
5 (9%)	Model	Risk	ANP (analytic network process)	Workforce	Risk assessment
	Develop	Assess	Casual	Risk	
	Risk	Measure	Diagram	Assess	
6 (8.5%)	Authentication	Authentication	BAN	Authentication	Mutual authentication protocol
	Protocol	Mutual	PMIPv6 (Proxy mobile IPv6)	Protocol	
	Attack	Protocol	AVISPA (automated validation of Internet security protocols)	Mutual	
7 (7.4%)	Cloud	Edge	Colluding	Fog	MEC security
	Edge	Eavesdropping	SSR (secrecy sum rate)	Eavesdropping	
	Fog	Fog	Tensor-based	Offload	
8 (8%)	Node	Rout	Acyclic	Rout	Energy-efficient routing protocol
	Energy	RPL (routing protocol for low-power and lossy networks)	Leach	Energy	
	Rout	Cluster	RPL	Cluster	
9 (6.5%)	Sensor	Camera	Burglar	Arduino	Secure home automation system
	Control	Arduino	Caution	Camera	
	Home	Raspberry	Diabetes	Gadget	
10 (6%)	Smart	City	Commerce	Blockchain	Integration of blockchain and IoT
	Blockchain	Blockchain	Campus	Smart	
	Home	Smart	Cart	City	
11 (8.5%)	Privacy	Privacy	Cyber-physics	Privacy	Privacy preservation
	User	Preserving	Mile	Preserving	
	Collect	User	Participant	Data	
12 (8%)	Device	DTLS (datagram transport layer security)	EDHOC (ephemeral Diffie-Hellman over common open software environment)	DTLS	End-to-end security
	Protocol	CoAP	Rekey	TLS	
	Key	End-end	AEAD (authenticated encryption with associated data)	CoAP	

studies have prioritized security threats by applying approaches such as product-development life cycle, decision-making trial-and-evaluation laboratory, analytic network processing, and graph theory to develop risk assessment and management frameworks [200–207].

Topic 6 corresponds to research on the development of user mutual authentication protocols for social IoT, IoT-based Long-Term Evolution (LTE), LTE-advanced networks, WSNs, and NFC (near-field communication) payment systems [144, 208–218]. In addition, the verification of authentication protocols using software tools, such as BAN and AVISPA, has gained popularity [213, 214, 217, 219–221]. Recently, the target of authentication has gained attention for mobile smart objects, such as drones and vehicles [219, 221, 222].

Topic 7 is related to MEC security. MEC integrated with IoT applications offload computationally intensive tasks at the network edge. As the edges are susceptible to cyber threats, there is a growing interest in their security. The main related studies include areas such as personal information protection and secure data collection, and transmission for MEC-supported IoT applications [223–241].

Topic 8 is related to the development of energy-efficient routing protocols that minimize the transmission power for routing between nodes in IoT networks. For instance, a routing protocol for low-power and lossy networks (RPL), a protocol for low-power and low-loss networks, and corresponding security methods have been developed [242–253].

Topic 9 is related to secure home automation systems toward automation, safety, and security through the control of home appliances and sensors. Research on this subject has two main subtopics. The first subtopic is related to security against cyberattacks in the home network [112, 254–259], and the second one is related to home automation providing safety against external physical intrusion [260–266].

Topic 10 is related to the adoption of blockchain in smart-IoT applications, such as smart contracts, smart inventory management, smart e-commerce, and smart shopping systems [140, 155, 267–279].

Topic 11 concerns privacy decisions and privacy preservation in the value chain of IoT data in environments where IoT devices collect personal data and forward them to third parties. Research on this subject has two main subtopics. The first subtopic is related to personal information security [280–283]. The second subtopic is related to the data value chain, including information related to the owner's perception of privacy protection and the right to make decisions about personal information protection [96, 284–287].

Topic 12 includes studies on transport protocols for end-to-end security [288–290]. To achieve end-to-end secure communication between an IoT back end and resource-limited smart things, various studies on communication protocols such as DTLS and CoAP [291, 292] and key setting protocols such as EDHOC have been conducted [293, 294].

4.4. Trend Estimation of Topics in IoT Security.

To answer RQ5, we estimated the trends over time for each topic by setting the year as a covariate, obtaining the results shown in Figure 8. Topics with an upward trend (increasing influence) are topics 4 (security through ML), 7 (MEC security), 8 (energy-efficient routing protocols), and 10 (blockchain and IoT integration). On the other hand, topics 1 (IoT security issues), 5 (risk assessment), 6 (mutual authentication protocol), and 12 (end-to-end security)show a decreasing trend.

4.5. Challenges and Future Perspectives.

We identify the evolution of keywords in Section 4.2. Figure 9 shows the part of Figure 6 containing the keywords (colored nodes) of clusters closely related to "blockchain," which is the core of keyword evolution, as identified in Figure 7.

In Figure 9, "blockchain" is connected to "machine learning," "deep learning," "ai," and "sdn" at the bottom-right area. Thus, there is a relation to topic 4. Node "edge computing" shown above "blockchain" can be linked to topic 7. In addition, "efficiency," which is connected to the upper-left area of "blockchain," and "rpl," which is connected at the bottom of the center area, can be related to topic 8. These results indicate that the trends obtained from keywords and topics suitably agree. Based on the analyzed studies and discussions, we summarize below challenges and future perspectives related to secure distributed smart M-IoT applications.

4.5.1. Secure Distributed Framework for Smart M-IoT Applications.

Various studies on the integration of SDN, fog and edge computing, and blockchain have been conducted aiming to improve the security of IoT applications [270, 275, 276, 278, 295–302].

Medhane et al. [295] proposed a blockchain-enabled distributed security framework for next-generation IoT applications by implementing an edge cloud security framework using an SDN. The proposed framework consists of an IoT device layer, an edge cloud layer, and a blockchain-enabled SDN. Gateway nodes in the edge cloud layer act as access points for the distributed SDN and quickly detect attacks by analyzing real-time data received from IoT devices. All roaming IoT devices and SDN servers share data through blockchain technology. The proposed security framework shows improved results in terms of packet delivery rate, throughput, and delay compared with frameworks without blockchain, edge cloud, and SDN. The framework is also effective for data confidentiality, integrity, and availability. However, energy consumption has increased.

The blockchain-based decentralized security architecture proposed by Rathore et al. [298] is a layered model consisting of sensing, edge computing, fog computing, and cloud layers. The sensing layer comprises many smart devices and widely distributed sensing nodes that monitor various environments and activities in public infrastructure. The edge computing layer consists of low-power high-performance SDN switches at the edge of the network. Each SDN switch at the edge computing layer connects to multiple sensors, and the switch processes and analyzes the data traffic of sensors. The fog computing layer with several SDN controllers is connected to the SDN switch cluster at the edge computing layer and analyzes the processed data. The SDN controller of a fog computing node consists of four components: traffic flow analyzer, traffic flow classifier, blockchain-based attack detection module, and attack mitigation module. Learning attack detection in the fog computing layer can be distributed to reduce the computational overhead and provide a fast response through simultaneous computations. Moreover, the fog computing layer transmits the traffic analysis results to the cloud layer. This decentralized architecture improves the attack detection performance by dynamically updating the attack detection model of each fog computing node using blockchain technology. It also prevents single points of failure inherent to centralized architecture. However, there is an overhead for blockchain operations.

It remains necessary to develop a secure distributed IoT framework that integrates fog and edge computing, ML-

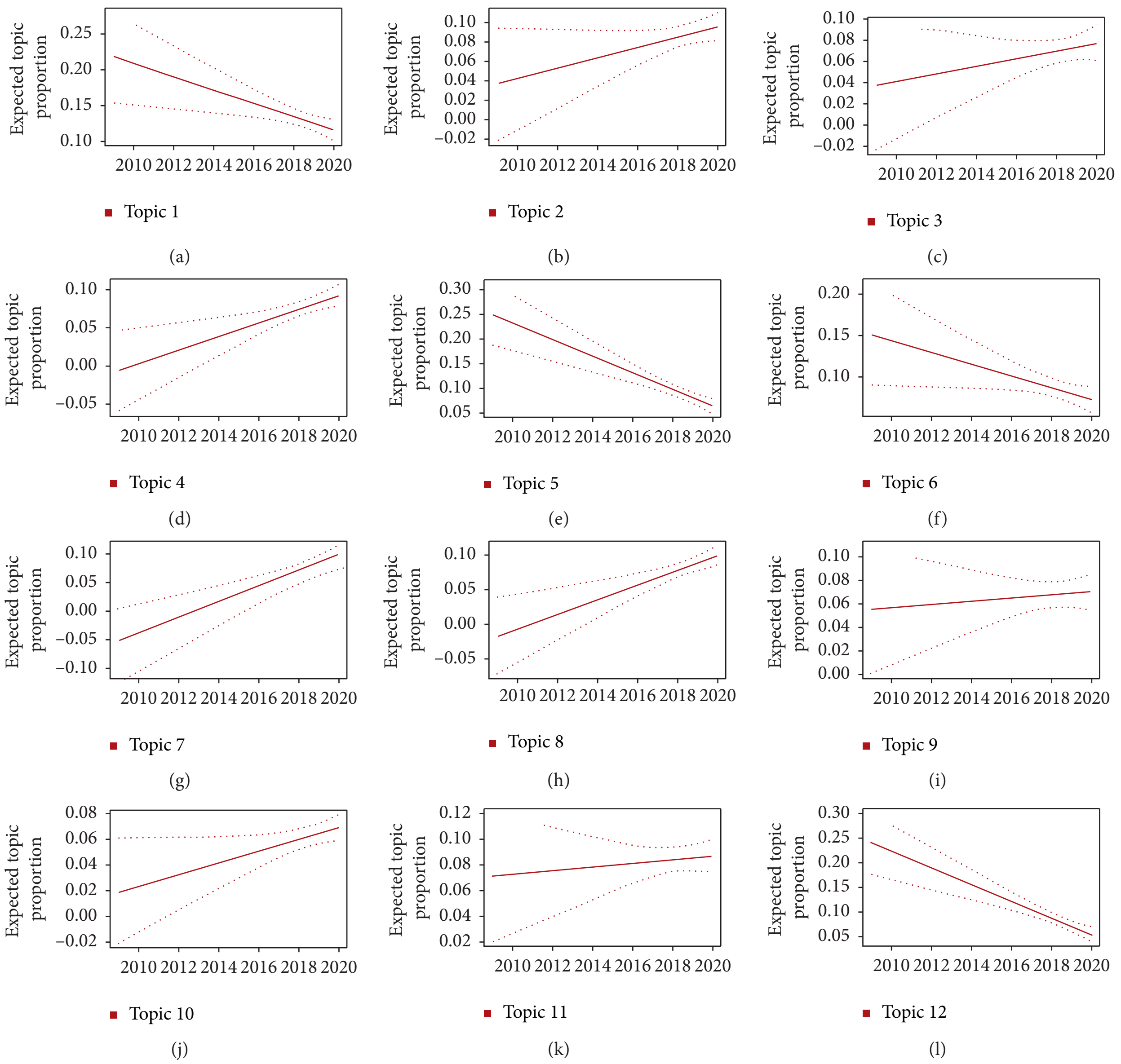


Figure 8: Topic trend estimation over time. We set the covariate to year and estimated the trends based on the change in the proportion of studies on each topic over time.

based SDN, and blockchain technology. Using fog and edge computing, the fog computing layer must analyze malicious traffic flows using ML algorithms to construct an intelligent attack detection model and dynamically update and manage traffic rules at edge computing nodes. This way, an ML-based SDN controller can enable fast attack detection. In addition, data privacy at the fog node level must be considered. The decentralized nature of blockchain supports secure distributed computing through the distributed trust concept. IoT devices and SDN servers can safely share data using blockchain [270, 295–298]. Therefore, a secure and energy-efficient blockchain-enabled architecture of ML-based SDN controllers for IoT networks is still required [303]. As new devices and applications are connected to IoT applications over time, unknown attacks can be developed. ML-based security is important to detect unknown attacks and respond properly in real time. In addition, in a secure distributed framework, IoT devices with limited resources can support routing protocols with high throughput, low latency, and low energy consumption. Thus, it remains necessary to develop a blockchain-based lightweight security protocol [281, 303].

4.5.2. Smart Objects in Smart M-IoT Applications. IoT devices can detect valuable data to build many intelligent applications. In addition, they can make important decisions to control their surroundings. Several IoT applications rely on end-to-end security between IoT devices and the cloud. However, realizing end-to-end security in IoT applications is difficult due to the wide variety of devices. In addition, most IoT devices have limited resources and cannot support heavy

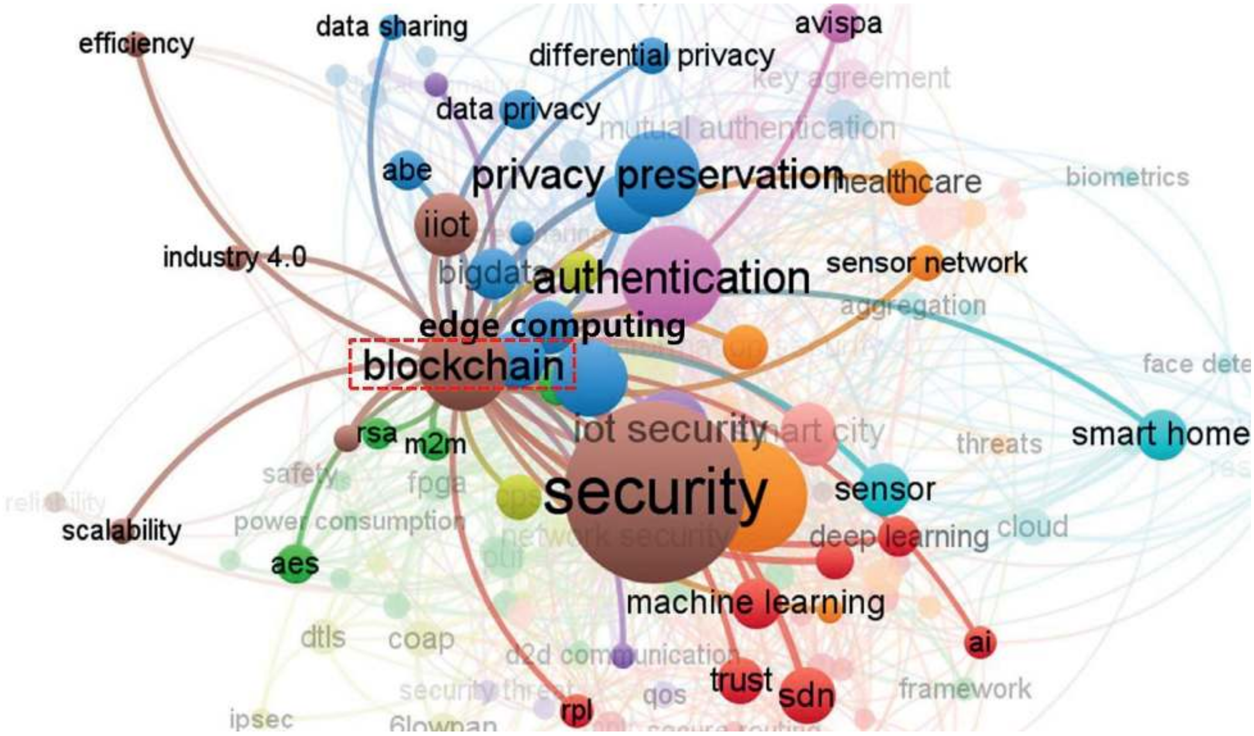


Figure 9: Keywords closely related to the keyword "blockchain" in Figure 6.

security applications such as firewalls. In [1], the introduction of edge computing into IoT device security for various applications is analyzed. Firewalls, intrusion detection systems, distributed traffic monitoring, attribute-based access control, and authentication protocols are analyzed at the edge computing layer for resource-limited IoT devices. To integrate edge computing, an algorithm and a lightweight secure communication protocol to establish trust between IoT devices and the edge should be first developed.

Talavera et al. [2] investigated security issues between the sensing layer and IoT devices and those at the IoT application layer, which involves smart homes, smart meters, smart cities, smart grids, and other solutions that directly handle end users and provide services. Therefore, unique security issues occur at this layer, such as data theft and privacy issues. Thus, a method to quantify and manage risk levels through rigorous penetration testing of IoT devices is required. Whenever IoT devices interact, a seamless authentication process must be implemented. To protect the user and environment data from being captured, mechanisms based on cryptographic techniques such as RSA, SHA256, or hash chain are needed. In addition, to increase the security level, Talavera et al. [2] recommend further development of recent technologies such as blockchain, fog and edge computing, and ML-based solutions.

Shin and Byun [3] proposed a privacy protection method for IoT devices in a smart city by applying edge computing. By processing data in near real time at the edge, they solve the heterogeneity problem of IoT devices and improve the overall performance, resulting in faster response times. Therefore, their method provides better quality of service for IoT applications.

To achieve smart applications, numerous IoT devices deployed around the world should generate large amounts of user and environment data. Consequently, much personal information can be leaked, posing a threat to individuals and the society as a whole. Therefore, IoT applications and their smart objects must be stable, secure, and robust. Smart objects that have attracted increasing interest in recent years include autonomous vehicles and UAVs. They have been combined with IoT to establish V2X communication and the Internet of drones. However, security concerns such as personal information protection, data encryption, and authentication remain to be addressed. Fog and edge computing, blockchain-based and SDN-enabled V2X communication, and Internet of drones can complete the available range of smart M-IoT services that include smart health, smart homes, smart cities, smart factories, smart agriculture, and smart transportation. As a result, more diverse smart services should be proposed, and the convergence of various fields will be promoted [101, 102, 132, 221, 302].

5. Conclusions

For the successful introduction and spread of smart M-IoT applications, security is an essential requirement. Many review studies have been conducted to understand IoT security. However, many of them have focused on specific areas of IoT security. In addition, existing studies have primarily provided in-depth professional content analysis. In contrast, we provide comprehensive initial insights in a different approach than previous studies. Our study provides IoT security keyword clusters, keyword trends, topic classification, and topic trends to interested researchers. Then, we synthesize and explain keyword evolution and topics with increasing influence. We recommend pursuing research on the development of a secure decentralized framework integrating edge computing, ML-based SDN, and blockchain, as well as research on vehicles and UAVs as smart M-IoT objects.

Our research has various limitations. For instance, when collecting articles to be analyzed, a keyword search was performed on the article titles. Therefore, articles implicitly related to IoT security may be omitted from this study. Nevertheless, our study provides new researchers with comprehensive initial insights on the security required for smart M-IoT. In addition, this study has demonstrated the application of a method to perform a systematic mapping study using big data mining to process many documents. This method can be applied to systematic reviews in other fields.

Data Availability

The list of the 1,365 research articles used in this study is available upon request to the corresponding author, at j.ann.lee@yonsei.ac.kr.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: disambiguation and research directions," *Journal of Network and Computer Applications*, vol. 128, pp. 105–140, 2019.

[2] L. E. Talavera, M. Endler, and I. Vasconcelos, "The mobile hub concept: enabling applications for the internet of mobile things," in *Proceedings of the 2015 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops)*, pp. 123–128, St. Louis, MO, USA, 2015.

[3] T. Shin and J. Byun, "Design and implementation of a vehicle social enabler based on social Internet of things," *Mobile Information Systems*, vol. 2016, Article ID 4102163, 11 pages, 2016.

[4] A. R. Dargazany, P. Stegagno, and K. Mankodiya, "WearableDL: wearable internet-of-things and deep learning for big data analytics—concept, literature, and future," *Mobile Information Systems*, vol. 2018, Article ID 8125126, 20 pages, 2018.

[5] H.-K. Ra, H. J. Yoon, S. H. Son et al., "HealthNode: software framework for efficiently designing and developing cloud-based healthcare applications," *Mobile Information Systems*, vol. 2018, Article ID 6071580, 12 pages, 2018.

[6] H.-S. Kim, S. Yun, H. Kim et al., "An efficient SDN multicast architecture for dynamic industrial IoT environments," *Mobile Information Systems*, vol. 2018, Article ID 8482467, 11 pages, 2018.

[7] V. Sharma, I. You, K. Andersson, F. Palmieri, M. H. Rehmani, and J. Lim, "Security, privacy and trust for smart mobile-internet of things (M-IoT): a survey," *IEEE Access*, vol. 8, pp. 167123–167163, 2020.

[8] S. Marcos-Pablos, A. García-Holgado, and F. J. García-Peñalvo, *Guidelines for Performing Systematic Research Projects Reviews*, 2020.

[9] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Information and Software Technology*, vol. 64, pp. 1–18, 2015.

[10] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," Technical Report, EBSE, Goyang-si, South Korea, 2007.

[11] D. Gough, J. Thomas, and S. Oliver, "Clarifying differences between review designs and methods," *Systematic Reviews*, vol. 1, no. 1, p. 28, 2012.

[12] B. Kitchenham, R. Pretorius, D. Budgen et al., "Systematic literature reviews in software engineering - a tertiary study," *Information and Software Technology*, vol. 52, no. 8, pp. 792–805, 2010.

[13] B. A. Kitchenham, D. Budgen, and O. Pearl Brereton, "Using mapping studies as the basis for further research - a participant-observer case study," *Information and Software Technology*, vol. 53, no. 6, pp. 638–651, 2011.

[14] C. Marshall and P. Brereton, "Tools to support systematic literature reviews in software engineering: a mapping study," in *Proceedings of the 2013 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement*, pp. 296–299, IEEE, Baltimore, MD, USA, 2013.

[15] K. Petersen, R. Feldt, S. Mujtaba et al., "Systematic mapping studies in software engineering," in *Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering (EASE)*, vol. 12, pp. 1–10, Trondheim, Norway, 2008.

[16] E. Zavala, X. Franch, and J. Marco, "Adaptive monitoring: a systematic mapping," *Information and Software Technology*, vol. 105, pp. 161–189, 2019.

[17] K. R. Felizardo, N. Salleh, R. M. Martins et al., "Using visual text mining to support the study selection activity in systematic literature reviews," in *Proceedings of the 2011 International Symposium on Empirical Software Engineering and Measurement*, pp. 77–86, Alberta, Canada, 2011.

[18] B. A. Kitchenham, D. Budgen, and O. P. Brereton, "The value of mapping studies–A participant-observer case study," in *Proceedings of the 14th International Conference on Evaluation and Assessment in Software Engineering (Ease)*, pp. 1–9, Ciudad Real, Spain, 2010.

[19] A. Wang, P. Wang, X. Miao et al., "A review on non-terrestrial wireless technologies for Smart City Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 16, no. 6, Article ID 1550147720936824, 2020.

[20] S. L. Ullo and G. Sinha, "Advances in smart environment monitoring systems using IoT and sensors," *Sensors*, vol. 20, no. 11, p. 3113, 2020.

[21] K. T. Kadhim, A. M. Alsahlany, S. M. Wadi et al., "An overview of patient's health status monitoring system based on internet of things (IoT)," *Wireless Personal Communications*, vol. 114, pp. 1–28, 2020.

[22] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: a survey of emerging technologies," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[23] K. L. Raju and V. Vijayaraghavan, “IoT technologies in agricultural environment: a survey,” *Wireless Personal Communications*, vol. 113, 2020.

[24] H. Farooq, H. U. Rehman, A. Javed, M. Shoukat, and S. Dudely, “A review on smart IoT based farming,” *Annals of Emerging Technologies in Computing*, vol. 4, no. 3, pp. 17–28, 2020.

[25] K. Kiela, V. Barzdenas, M. Jurgo et al., “Review of V2X-IoT standards and frameworks for ITS applications,” *Applied Sciences*, vol. 10, no. 12, p. 4314, 2020.

[26] M. A. Rahim, M. A. Rahman, M. Rahman et al., “Evolution of IoT-enabled connectivity and applications in automotive industry: a review,” *Vehicular Communications*, vol. 27, Article ID 100285, 2020.

[27] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, “Internet of Things security: a survey,” *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[28] D. Mendez Mena, I. Papapanagiotou, and B. Yang, “Internet of things: survey on security,” *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 162–182, 2018.

[29] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: application areas, security threats, and solution architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[30] E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva et al., “On the security aspects of Internet of Things: a systematic literature review,” *Journal of Communications and Networks*, vol. 21, no. 5, pp. 444–457, 2019.

[31] S. Hameed, F. I. Khan, and B. Hameed, “Understanding security requirements and challenges in Internet of Things (IoT): a review,” *Journal of Computer Networks and Communications*, vol. 2019, Article ID 9629381, 14 pages, 2019.

[32] M. A. Obaidat, S. Obeidat, J. Holst et al., “A comprehensive and systematic survey on the internet of things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures,” *Computers*, vol. 9, no. 2, 2020.

[33] R. Yugha and S. Chithra, “A survey on technologies and security protocols: reference for future generation IoT,” *Journal of Network and Computer Applications*, vol. 169, Article ID 102763, 2020.

[34] J. Arshad, M. A. Azad, R. Amad, K. Salah, M. Alazab, and R. Iqbal, “A review of performance, energy and privacy of intrusion detection systems for IoT,” *Electronics*, vol. 9, no. 4, p. 629, 2020.

[35] X. Yao, F. Farha, R. Li et al., “Security and privacy issues of physical objects in the IoT: challenges and opportunities,” *Digital Communications and Networks*, 2020, in Press.

[36] B. Liao, Y. Ali, S. Nazir, L. He, and H. U. Khan, “Security analysis of IoT devices by using mobile computing: a systematic literature review,” *IEEE Access*, vol. 8, pp. 120331–120350, 2020.

[37] A. Sharma, E. S. Pilli, A. P. Mazumdar et al., “Towards trustworthy Internet of Things: a survey on Trust Management applications and schemes,” *Computer Communications*, vol. 160, 2020.

[38] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, “Security and privacy for green IoT-based agriculture: review, blockchain solutions, and challenges,” *IEEE Access*, vol. 8, pp. 32031–32053, 2020.

[39] R. R. Braam, H. F. Moed, and A. F. J. Van Raan, “Mapping of science by combined co-citation and word analysis. I. Structural aspects,” *Journal of the American Society for Information Science*, vol. 42, no. 4, pp. 233–251, 1991.

[40] Q. He, “Knowledge discovery through co-word analysis,” *Library Trends*, vol. 48, no. 1, pp. 133–159, 1999.

[41] S. Radhakrishnan, S. Erbis, J. A. Isaacs et al., “Novel keyword co-occurrence network-based methods to foster systematic reviews of scientific literature,” *PloS One*, vol. 12, no. 3, Article ID e0172778, 2017.

[42] L. Waltman and N. J. Van Eck, “A new methodology for constructing a publication-level classification system of science,” *Journal of the American Society for Information Science and Technology*, vol. 63, no. 12, pp. 2378–2392, 2012.

[43] N. J. Van Eck and L. Waltman, “Citation-based clustering of publications using CitNetExplorer and VOSviewer,” *Scientometrics*, vol. 111, no. 2, pp. 1053–1070, 2017.

[44] R. Klavans and K. W. Boyack, “Which type of citation analysis generates the most accurate taxonomy of scientific and technical knowledge?” *Journal of the Association for Information Science and Technology*, vol. 68, no. 4, pp. 984–998, 2017.

[45] V. A. Traag, P. Van Dooren, and Y. Nesterov, “Narrow scope for resolution-limit-free community detection,” *Physical Review E*, vol. 84, no. 1, Article ID 016114, 2011.

[46] N. J. Van Eck and L. Waltman, “CitNetExplorer: a new software tool for analyzing and visualizing citation networks,” *Journal of Informetrics*, vol. 8, no. 4, pp. 802–823, 2014.

[47] N. J. Van Eck and L. Waltman, “Software survey: VOSviewer, a computer program for bibliometric mapping,” *Scientometrics*, vol. 84, no. 2, pp. 523–538, 2010.

[48] N. J. Eck and L. Waltman, “How to normalize cooccurrence data? An analysis of some well-known similarity measures,” *Journal of the American Society for Information Science and Technology*, vol. 60, no. 8, pp. 1635–1651, 2009.

[49] L. Waltman, N. J. Van Eck, and E. C. M. Noyons, “A unified approach to mapping and clustering of bibliometric networks,” *Journal of Informetrics*, vol. 4, no. 4, pp. 629–635, 2010.

[50] L. Waltman and N. J. Van Eck, “A smart local moving algorithm for large-scale modularity-based community detection,” *The European Physical Journal B*, vol. 86, no. 11, p. 471, 2013.

[51] J. Y. Lee, “Deep learning research trend analysis using text mining,” *International Journal of Advanced Culture Technology*, vol. 7, no. 4, pp. 295–301, 2019.

[52] J. Lee, “A study on research trend analysis and topic class prediction of digital transformation using text mining,” *International Journal of Advanced Smart Convergence*, vol. 8, no. 2, pp. 183–190, 2019.

[53] M. E. Roberts, B. M. Stewart, D. Tingley et al., “The structural topic model and applied social science,” in *Advances in Neural Information Processing Systems Workshop on Topic Models: Computation, Application, and Evaluation*Harrahs and Harveys, Lake Tahoe, NV, USA, 2013.

[54] M. E. Roberts, B. M. Stewart, and E. M. Airoldi, “A model of text for experimentation in the social sciences,” *Journal of the American Statistical Association*, vol. 111, no. 515, pp. 988–1003, 2016.

[55] M. E. Roberts, B. M. Stewart, and D. Tingley, “stm: R package for structural topic models,” *Journal of Statistical Software*, vol. 10, no. 2, pp. 1–40, 2014.

[56] H. M. Wallach, I. Murray, R. Salakhutdinov et al., “Evaluation methods for topic models,” in *Proceedings of the 26th Annual International Conference on Machine Learning*, pp. 1105–1112, Montreal, Canada, 2009.

[57] T. Heer, O. Garcia-Morchon, R. Hummen, S. L. Keoh, S. S. Kumar, and K. Wehrle, "Security challenges in the IP-based internet of things," *Wireless Personal Communications*, vol. 61, no. 3, pp. 527–542, 2011.

[58] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[59] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[60] M. V. O. de Assis, L. F. Carvalho, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença Jr, "Near real-time security system applied to SDN environments in IoT networks using convolutional neural network," *Computers & Electrical Engineering*, vol. 86, Article ID 106738, 2020.

[61] H. W. Kim and E. H. Song, "Behavior-based malware detection using deep learning for improve security of iot infrastructure," *International Journal of Advanced Science and Technology*, vol. 28, no. 5, pp. 128–134, 2019.

[62] F. Li, A. Shinde, Y. Shi, J. Ye, X.-Y. Li, and W. Song, "System statistics learning-based IoT security: feasibility and suitability," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6396–6403, 2019.

[63] F. Li, Y. Shi, A. Shinde, J. Ye, and W. Song, "Enhanced cyber-physical security in internet of things through energy auditing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 5224–5231, 2019.

[64] B. Chatterjee, D. Das, S. Maity et al., "RF-PUF: enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388–398, 2019.

[65] I. Kotenko, I. Saenko, and A. Branitskiy, "Framework for mobile internet of things security monitoring based on big data processing and machine learning," *IEEE Access*, vol. 6, pp. 72714–72723, 2018.

[66] U. Sairam and M. V. Bhanu Prakash, "Dl and ml approaches along with blockchain towards iot security," *International Journal of Advanced Science and Technology*, vol. 29, no. 4, pp. 826–832, 2020.

[67] B. Wang, Y. Sun, T. Q. Duong, L. D. Nguyen, and N. Zhao, "Security enhanced content sharing in social IoT: a directed hypergraph-based learning scheme," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4412–4425, 2020.

[68] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and federated learning for privacy-preserved data sharing in industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, 2020.

[69] A. Singh, N. Chawla, J. H. Ko et al., "Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 421–434, 2018.

[70] S. Atiewi, A. Al-Rahayfeh, M. Almiani et al., "Scalable and secure big data IoT system based on multifactor Authentication and lightweight cryptography," *IEEE Access*, vol. 8, pp. 113498–113511, 2020.

[71] L. E. Kane, J. J. Chen, R. Thomas, V. Liu, and M. Mckague, "Security and performance in IoT: a balancing act," *IEEE Access*, vol. 8, pp. 121969–121986, 2020.

[72] A. Alamer, B. Soh, and D. E. Brumbaugh, "Mickey 2.0. 85: a secure and lighter MICKEY 2.0 cipher variant with improved power consumption for smaller devices in the IoT," *Symmetry*, vol. 12, no. 1, 2020.

[73] A. Prathiba and V. S. Kanchana Bhaaskaran, "Hardware footprints of S-box in lightweight symmetric block ciphers for IoT and CPS information security systems," *Integration*, vol. 69, pp. 266–278, 2019.

[74] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3474–3484, 2020.

[75] Z. Mishra and B. Acharya, "High throughput and low area architectures of secure IoT algorithm for medical image encryption," *Journal of Information Security and Applications*, vol. 53, 2020.

[76] M. Sri Lakshmi and V. Srikanth, "A study on light weight cryptography algorithms for data security in IOT," *International Journal of Engineering & Technology*, vol. 7, no. 2.7, pp. 887–890, 2018.

[77] Q. Xu, Z. Su, M. Dai et al., "APIS: privacy-preserving incentive for sensing task allocation in cloud and edge-cooperation mobile Internet of Things with SDN," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 5892–5905, 2019.

[78] K. Janjua, M. A. Shah, A. Almogren et al., "Proactive forensics in IoT: privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies," *Electronics (Switzerland)*, vol. 9, no. 7, pp. 1–39, 2020.

[79] Z. Xu, R. Gu, T. Huang et al., "An IoT-oriented offloading method with privacy preservation for cloudlet-enabled wireless metropolitan area networks," *Sensors (Switzerland)*, vol. 18, no. 9, 2018.

[80] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[81] S. Li, Z. Liu, Z. Huang, H. Lyu, Z. Li, and W. Liu, "DynaPro: dynamic wireless sensor network data protection algorithm in IoT via differential privacy," *IEEE Access*, vol. 7, pp. 167754–167765, 2019.

[82] S. Patil and S. Joshi, "Demystifying user data privacy in the world of IOT," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 10, pp. 4412–4418, 2019.

[83] Y. S. Zhao and H. C. Chao, "A green and secure iot framework for intelligent buildings based on fog computing," *Journal of Internet Technology*, vol. 19, no. 3, pp. 837–843, 2018.

[84] K. Gai, Y. Wu, L. Zhu et al., "Differential privacy-based blockchain for industrial internet-of-things," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4156–4165, 2019.

[85] C. Yin, J. Xi, R. Sun et al., "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3628–3636, 2017.

[86] H. Cao, S. Liu, L. Wu et al., "SCRAPPOR: an efficient privacy-preserving algorithm base on sparse coding for information-centric IoT," *IEEE Access*, vol. 6, pp. 63143–63154, 2018.

[87] H. Cao, S. Liu, R. Zhao et al., "IFed: a novel federated learning framework for local differential privacy in Power Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 16, no. 5, 2020.

[88] M. Sun and W. P. Tay, "On the relationship between inference and data privacy in decentralized IoT networks," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 852–866, 2020.

[89] Y. Ju and H. J. Mun, "The research on security technology for low-performance iot sensor node," *International Journal of Engineering and Technology(UAE)*, vol. 7, no. 3, pp. 594–597, 2018.

[90] A. Yadav, A. Tripathi, N. Rakesh, and S. Pandey, "Protecting composite IoT server by secure secret key exchange for XEN intra virtual machines," *International Journal of Information and Computer Security*, vol. 12, no. 1, pp. 53–69, 2020.

[91] K. Haseeb, A. Almogren, I. U. Din et al., "SASC: secure and authentication-based sensor cloud architecture for intelligent internet of things," *Sensors (Switzerland)*, vol. 20, no. 9, 2020.

[92] M. Juma, A. A. Monem, and K. Shaalan, "Hybrid end-to-end VPN security approach for smart IoT objects," *Journal of Network and Computer Applications*, vol. 158, Article ID 102598, 2020.

[93] J. Choi, Y. In, C. In, S. Seok, H. Seo, and H. Kim, "Secure IoT framework and 2D architecture for End-To-End security," *The Journal of Supercomputing*, vol. 74, no. 8, pp. 3521–3535, 2018.

[94] R. H. Randhawa, A. Hameed, and A. N. Mian, "Energy efficient cross-layer approach for object security of CoAP for IoT devices," *Ad Hoc Networks*, vol. 92, 2019.

[95] J. D. De Hoz Diego, J. Saldana, J. Fernandez-Navajas, and J. Ruiz-Mas, "Decoupling security from applications in CoAP-based IoT devices," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 467–476, 2020.

[96] G. Sagirlar, B. Carminati, and E. Ferrari, "Decentralizing privacy enforcement for Internet of Things smart objects," *Computer Networks*, vol. 143, pp. 112–125, 2018.

[97] M. U. Aftab, Y. Munir, A. Oluwasanmi et al., "A hybrid access control model with dynamic COI for secure localization of satellite and IoT-based vehicles," *IEEE Access*, vol. 8, pp. 24196–24208, 2020.

[98] A. Patwari, P. S. S. Bhavya, and R. K. Maheswari, "NodeMCU and IoT-based safety and security ecosystem for heavy vehicles," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 5, pp. 1482–1490, 2020.

[99] F. Al-Turjman and J. P. Lemayian, "Intelligence, security, and vehicular sensor networks in internet of things (IoT)-enabled smart-cities: an overview," *Computers & Electrical Engineering*, vol. 87, p. 106776, 2020.

[100] N. A. Hussein and M. I. Shujaa, "Secure vehicle to vehicle voice chat based MQTT and coap internet of things protocol," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 1, pp. 526–534, 2020.

[101] S. Kumar and J. Singh, "Internet of vehicles over vanets: smart and secure communication using IoT," *Scalable Computing: Practice and Experience*, vol. 21, no. 3, pp. 425–440, 2020.

[102] V. Sharma, J. Kim, Y. Ko et al., "An optimal security management framework for backhaul-aware 5G-vehicle to everything (V2X)," *Journal of Internet Technology*, vol. 21, no. 1, pp. 245–260, 2020.

[103] S. Belguith, N. Kaaniche, M. Hammoudeh, and T. Dargahi, "Proud: verifiable privacy-preserving outsourced attribute based signcryption supporting access policy update for cloud assisted iot applications," *Future Generation Computer Systems*, vol. 111, pp. 899–918, 2020.

[104] A. Shahzad, K. Zhang, and A. Gherbi, "Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain," *Sensors*, vol. 20, no. 13, p. 3760, 2020.

[105] S. A. El-Rahman, D. Aldawsari, M. Aldosari, O. Alrashed, and G. Alsubaie, "A secure cloud based digital signature application for IoT," *International Journal of E-Services and Mobile Applications*, vol. 10, no. 3, pp. 42–60, 2018.

[106] M. A. Mughal, X. Luo, A. Ullah, S. Ullah, and Z. Mahmood, "A lightweight digital signature based security scheme for human-centered Internet of Things," *IEEE Access*, vol. 6, pp. 31630–31643, 2018.

[107] A. Karati, C.-I. Fan, and R.-H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10431–10440, 2019.

[108] A. Karati, S. H. Islam, G. Biswas et al., "Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of Things environments," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2904–2914, 2017.

[109] W. Liu, X. Wang, and W. Peng, "Secure remote multi-factor authentication scheme based on chaotic map zero-knowledge proof for crowdsourcing internet of things," *IEEE Access*, vol. 8, pp. 8754–8767, 2020.

[110] A. Yang, C. Zhang, Y. Chen et al., "Security and privacy of smart home systems based on the Internet of Things and stereo matching algorithms," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2521–2530, 2019.

[111] N. M. Sundaram, S. Arunkumar, and S. Kaliappan, "Smart home security monitoring system using IOT," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 2, pp. 256–258, 2018.

[112] J. Ahn, I.-G. Lee, and M. Kim, "Design and implementation of hardware-based remote attestation for a secure internet of things," *Wireless Personal Communications*, vol. 144, pp. 1–33, 2020.

[113] M. Park, H. Oh, and K. Lee, "Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective," *Sensors*, vol. 19, no. 9, p. 2148, 2019.

[114] T. Adiono, B. Tandiawan, and S. Fuada, "Device protocol design for security on internet of things based smart home," *International Journal of Online Engineering (iJOE)*, vol. 14, no. 07, pp. 161–170, 2018.

[115] K. Timur, Y. Kim, H. Cho et al., "Conception of smart home perimeter security system based on solar powered IoT solutions," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2, pp. 2056–2058, 2019.

[116] S. Snigdha and K. Haribabu, "IoT based security system using raspberry PI and mail server," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 11, pp. 1702–1704, 2019.

[117] A. Khanum and R. Shivakumar, "An enhanced security alert system for smart home using IOT," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 1, pp. 27–34, 2019.

[118] P. K. Sharma, J. H. Park, Y.-S. Jeong, and J. H. Park, "Shsec: sdn based secure smart home network architecture for internet of things," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 913–924, 2019.

[119] M. Boussard, D. T. Bui, R. Douville et al., "Future spaces: reinventing the home network for better security and automation in the IoT era," *Sensors (Switzerland)*, vol. 18, no. 9, 2018.

[120] D. Noori, H. Shakeri, and M. N. Torshiz, "Scalable, efficient, and secure RFID with elliptic curve cryptosystem for Internet of Things in healthcare environment," *EURASIP*

Journal on Information Security, vol. 2020, no. 1, 11 pages, 2020.

[121] B. A. Alzahrani, A. Irshad, K. Alsubhi et al., "A secure and efficient remote patient-monitoring authentication protocol for cloud-IoT," *International Journal of Communication Systems*, vol. 33, no. 11, 2020.

[122] S. Arunkumar, M. Vetriselvi, and S. Thanalakshmi, "Cryptography based security solutions to IoT enabled health care monitoring system," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 12, no. 7, pp. 265–272, 2020.

[123] P. Huang, L. Guo, M. Li, and Y. Fang, "Practical privacy-preserving ECG-based authentication for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9200–9210, 2019.

[124] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences*, vol. 527, pp. 493–510, 2020.

[125] X. Guo, H. Lin, Y. Wu, and M. Peng, "A new data clustering strategy for enhancing mutual privacy in healthcare IoT systems," *Future Generation Computer Systems*, vol. 113, pp. 407–417, 2020.

[126] A. A. Abd El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar et al., "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," *Optics and Laser Technology*, vol. 124, 2020.

[127] R. Boussada, B. Hamdane, M. E. Elhdhili et al., "Privacy-preserving aware data transmission for IoT-based e-health," *Computer Networks*, vol. 162, 2019.

[128] X. Wang and S. Cai, "Secure healthcare monitoring framework integrating ndn-based IoT with edge cloud," *Future Generation Computer Systems*, vol. 112, 2020.

[129] R. Ding, H. Zhong, J. Ma, X. Liu, and J. Ning, "Lightweight privacy-preserving identity-based verifiable IoT-based health storage system," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8393–8405, 2019.

[130] A. Ullah, G. Said, M. Sher, and H. Ning, "Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN," *Peer-to-Peer Networking and Applications*, vol. 13, no. 1, pp. 163–174, 2020.

[131] R. Saha, G. Kumar, M. K. Rai, R. Thomas, and S.-J. Lim, "Privacy Ensured ${e}$ -Healthcare for Fog-Enhanced IoT Based Applications," *IEEE Access*, vol. 7, pp. 44536–44543, 2019.

[132] A. Islam and S. Young Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Computers & Electrical Engineering*, vol. 84, p. 106627, 2020.

[133] Y. Liu and S. Zhang, "Information security and storage of Internet of Things based on block chains," *Future Generation Computer Systems*, vol. 106, pp. 296–303, 2020.

[134] Q. Zhao, S. Chen, Z. Liu, T. Baker, and Y. Zhang, "Blockchain-based privacy-preserving remote data integrity checking scheme for IoT information systems," *Information Processing & Management*, vol. 57, no. 6, Article ID 102355, 2020.

[135] M. Shen, H. Liu, L. Zhu et al., "Blockchain-Assisted secure device authentication for cross-domain industrial IoT," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[136] A. Gupta, B. Gupta, and K. K. Gola, "Blockchain technology for security and privacy issues in internet of things," *International Journal of Scientific and Technology Research*, vol. 9, no. 3, pp. 377–383, 2020.

[137] M. Zhaofeng, W. Lingyun, W. Xiaochang et al., "Blockchain-enabled decentralized trust management and secure usage control of IoT big data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4000–4015, 2019.

[138] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, "Blockchain and trust for secure, end-user-based and decentralized IoT service provision," *IEEE Access*, vol. 8, pp. 119961–119979, 2020.

[139] J. Chen, "Hybrid blockchain and pseudonymous authentication for secure and trusted IoT networks," *ACM SIGBED Review*, vol. 15, no. 5, pp. 22–28, 2018.

[140] M. Li, D. Hu, C. Lal et al., "Blockchain-enabled secure energy trading with verifiable fairness in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 16, 2020.

[141] R. M. Mathew, R. Suguna, and M. Shyamala Devi, "Exploration of blockchain for edifying safety and security in IoT based diamond international trade," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 8, pp. 3224–3228, 2019.

[142] C. Ge, Z. Liu, and L. Fang, "A blockchain based decentralized data security mechanism for the internet of things," *Journal of Parallel and Distributed Computing*, vol. 141, 2020.

[143] H. Rui, L. Huan, H. Yang, and Z. YunHao, "Research on secure transmission and storage of energy IoT information based on Blockchain," *Peer-to-Peer Networking and Applications*, vol. 13, no. 4, pp. 1225–1235, 2020.

[144] M. Hussain and U. Jain, "Simple and secure device authentication mechanism for smart environments using Internet of things devices," *International Journal of Communication Systems*, vol. 33, no. 16, Article ID e4570, 2020.

[145] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580–589, 2018.

[146] K. Fan, Q. Luo, K. Zhang, and Y. Yang, "Cloud-based lightweight secure RFID mutual authentication protocol in IoT," *Information Sciences*, vol. 527, pp. 329–340, 2020.

[147] J. Choi, J. Cho, H. Kim, and S. Hyun, "Towards secure and usable certificate-based authentication system using a secondary device for an industrial internet of things," *Applied Sciences*, vol. 10, no. 6, p. 1962, 2020.

[148] J. Lee, S. Yu, K. Park et al., "Secure three-factor authentication protocol for multi-gateway IoT environments," *Sensors (Switzerland)*, vol. 19, no. 10, 2019.

[149] S. Anandhi, R. Anitha, and V. Sureshkumar, "IoT enabled RFID authentication and secure object tracking system for smart logistics," *Wireless Personal Communications*, vol. 104, no. 2, pp. 543–560, 2019.

[150] S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, J. J. P. C. Rodrigues, and Y. Park, "Physically secure lightweight Anonymous user authentication protocol for internet of things using physically unclonable functions," *IEEE Access*, vol. 7, pp. 85627–85644, 2019.

[151] K. M. Renuka, S. Kumari, D. Zhao, and L. Li, "Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems," *IEEE Access*, vol. 7, pp. 51014–51027, 2019.

[152] M. Gheisari, Q.-V. Pham, M. Alazab, X. Zhang, C. Fernandez-Campusano, and G. Srivastava, "ECA: an edge computing architecture for privacy-preserving in IoT-based smart city," *IEEE Access*, vol. 7, pp. 155779–155786, 2019.

[153] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Computers & Security*, vol. 87, p. 101470, 2019.

[154] T. Sasaki, Y. Morita, and T. Kobayashi, "Security requirements and technologies for smart city IoT," *NEC Technical Journal*, vol. 13, no. 1, pp. 54–57, 2018.

[155] S. Gong, E. Tcydenova, J. Jo, Y. Lee, and J. H. Park, "Blockchain-based secure device management framework for an internet of things network in a smart city," *Sustainability*, vol. 11, no. 14, p. 3889, 2019.

[156] C. Toma, A. Alexandru, M. Popa et al., "IoT solution for smart cities' pollution monitoring and the security challenges," *Sensors (Switzerland)*, vol. 19, no. 15, 2019.

[157] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart city IoT platform respecting GDPR privacy and security aspects," *IEEE Access*, vol. 8, pp. 23601–23623, 2020.

[158] S. K. Singh, Y. S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustainable Cities and Society*, vol. 60, 2020.

[159] J. Maruthi Nagendra Prasad, C. V. Lakshmi Narayana, and B. Pandurangaraju, "An extensive study on the applications and security issues of rfid technology in iot," *International Journal of Advanced Science and Technology*, vol. 29, no. 4, pp. 694–707, 2020.

[160] D. Singh, Pushparaj, M. K. Mishra et al., "Security issues in different layers of iot and their possible mitigation," *International Journal of Scientific and Technology Research*, vol. 9, no. 4, pp. 2762–2771, 2020.

[161] S. Kamalakkannan and N. Sivasankari, "Survey on issues in authentication based iot security," *International Journal of Scientific and Technology Research*, vol. 9, no. 2, pp. 1258–1260, 2020.

[162] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: integration issues, prospects, challenges, and future research directions," *Future Generation Computer Systems*, vol. 97, pp. 512–529, 2019.

[163] S. P. Maniraj, R. Pranay Sharma, M. Venkata Siva Kumar et al., "Vulnerabilities and security issues in cps and IOT for wire less communication," *International Journal of Recent Technology and Engineering*, vol. 7, no. 5, pp. 164–167, 2019.

[164] D. Kerana Hanirex, K. P. Thooyamani, and A. Muthu Kumaravel, "A study on emerging technology internet of things (IOT): an overview of architecture and security issues," *Journal of Advanced Research in Dynamical and Control Systems*, vol. 11, no. 6, pp. 1715–1719, 2019.

[165] H. A. Khattak, M. A. Shah, S. Khan, I. Ali, and M. Imran, "Perception layer security in internet of things," *Future Generation Computer Systems*, vol. 100, pp. 144–164, 2019.

[166] N. Wang, P. Wang, A. Alipour-Fanid, L. Jiao, and K. Zeng, "Physical-layer security of 5G wireless networks for IoT: challenges and opportunities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8169–8181, 2019.

[167] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5G in the internet of things era: an overview on security and privacy challenges," *Computer Networks*, vol. 179, 2020.

[168] L. Tawalbeh, F. Muheidat, M. Tawalbeh et al., "IoT privacy and security: challenges and solutions," *Applied Sciences (Switzerland)*, vol. 10, no. 12, 2020.

[169] A. Kore and S. Patil, "Internet of things (Iot) enabled wireless sensor networks security challenges and current solutions," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 282–290, 2019.

[170] M. Amoon, T. Altameem, and A. Altameem, "Internet of things sensor assisted security and quality analysis for health care data sets using artificial intelligent based heuristic health management system," *Measurement*, vol. 161, Article ID 107861, 2020.

[171] J. Sun, H. Xiong, X. Liu et al., "Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health," *IEEE Internet of Things Journal*, vol. 7, 2020.

[172] A. Tewari and B. B. Gupta, "An internet-of-things-based security scheme for healthcare environment for robust location privacy," *International Journal of Computational Science and Engineering*, vol. 21, no. 2, pp. 298–303, 2020.

[173] K. U. K. Reddy, S. Shabbiha, and M. R. Kumar, "Design of high security smart health care monitoring system using IoT," *International Journal*, vol. 8, no. 6, 2020.

[174] P. Vijayakumar, M. S. Obaidat, M. Azees et al., "Efficient and secure anonymous authentication with location privacy for IoT-based WBANs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2603–2611, 2019.

[175] J. Mathew and R. Jemima Priyadarsini, "Enhancing security in IoT healthcare services using fog computing," *International Journal of Advanced Science and Technology*, vol. 28, no. 17, pp. 444–450, 2019.

[176] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang, and J. Han, "Toward practical privacy-preserving processing over encrypted data in IoT: an assistive healthcare use case," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10177–10190, 2019.

[177] J. John, M. S. Varkey, and M. Selvi, "Security attacks in s-wbans on iot based healthcare applications," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 2088–2097, 2019.

[178] W. Tang, J. Ren, K. Deng, and Y. Zhang, "Secure data aggregation of lightweight E-healthcare IoT devices with fair incentives," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8714–8726, 2019.

[179] X. C. Yin, Z. G. Liu, B. Ndibanje et al., "An iot-based anonymous function for security and privacy in healthcare sensor networks," *Sensors (Switzerland)*, vol. 19, no. 14, 2019.

[180] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567–592, 2019.

[181] A. M. Elmisery, S. Rho, and M. Aborizka, "A new computing environment for collective privacy protection from constrained healthcare devices to IoT cloud services," *Cluster Computing*, vol. 22, no. S1, pp. 1611–1638, 2019.

[182] A. Prathiba and V. Bhaaskaran, "Lightweight S-box Architecture for secure internet of things," *Information*, vol. 9, no. 1, p. 13, 2018.

[183] M. Qasaimeh, R. S. Al-Qassas, and S. Tedmori, "Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT security," *Multimedia Tools and Applications*, vol. 77, no. 14, pp. 18415–18449, 2018.

[184] M. A. F. Al-Husainy and B. Al-Shargabi, "Secure and lightweight encryption model for IoT surveillance camera," *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 2, pp. 1840–1847, 2020.

[185] S. S. Dhanda, B. Singh, and P. Jindal, "Lightweight cryptography: a solution to secure IoT," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947–1980, 2020.

[186] B. Seok, J. C. S. Sicato, T. Erzhena et al., "Secure D2D communication for 5G IoT network based on lightweight

cryptography," *Applied Sciences (Switzerland)*, vol. 10, no. 1, 2020.

[187] A. Ostad-Sharif, H. Arshad, M. Nikooghadam, and D. Abbasinezhad-Mood, "Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme," *Future Generation Computer Systems*, vol. 100, pp. 882–892, 2019.

[188] S. Rajesh, V. Paul, V. G. Menon et al., "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, 2019.

[189] J. Roldán, J. Boubeta-Puig, J. Luis Martínez, and G. Ortiz, "Integrating complex event processing and machine learning: an intelligent architecture for detecting IoT security attacks," *Expert Systems with Applications*, vol. 149, Article ID 113251, 2020.

[190] M. Bagaa, T. Taleb, J. B. Bernabe et al., "A machine learning security framework for iot systems," *IEEE Access*, 2020.

[191] A. Sivanathan, H. Habibi Gharakheili, and V. Sivaraman, "Managing IoT cyber-security using programmable telemetry and machine learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 60–74, 2020.

[192] X. Guo, H. Lin, Z. Li et al., "Deep Reinforcement learning based QoS-aware secure routing for SDN-IoT," *IEEE Internet of things journal*, vol. 7, no. 7, pp. 6242–6251, 2019.

[193] N. K. Kadale and J. R. Prasad, "Overview for security of internet of things using machine learning," *International Journal of Advanced Science and Technology*, vol. 29, no. 5, pp. 349–355, 2020.

[194] X. Zhang, X. Chen, J. K. Liu et al., "DeepPAR and DeepDPA: privacy preserving and asynchronous deep learning for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2081–2090, 2020.

[195] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: current solutions and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1686–1721, 2020.

[196] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for IoT security based on learning techniques," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2671–2701, 2019.

[197] A. Ferdowsi and W. Saad, "Deep learning for signal authentication and security in massive internet-of-things systems," *IEEE Transactions on Communications*, vol. 67, no. 2, pp. 1371–1387, 2019.

[198] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, "Machine learning for security and the internet of things: the good, the bad, and the ugly," *IEEE Access*, vol. 7, pp. 158126–158147, 2019.

[199] F. Ullah, H. Naeem, S. Jabbar et al., "Cyber security threats detection in internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379–124389, 2019.

[200] K. C. Park and D.-H. Shin, "Security assessment framework for IoT service," *Telecommunication Systems*, vol. 64, no. 1, pp. 193–209, 2017.

[201] G. George and S. M. Thampi, "A graph-based security framework for securing industrial IoT networks from vulnerability exploitations," *IEEE Access*, vol. 6, pp. 43586–43601, 2018.

[202] F. I. Salih, N. A. A. Bakar, N. H. Hassan et al., "IOT security risk management model for healthcare industry," *Malaysian Journal of Computer Science*, pp. 131–144, 2019.

[203] M. Aydos, Y. Vural, and A. Tekerek, "Assessing risks and threats with layered approach to Internet of Things security," *Measurement and Control (United Kingdom)*, vol. 52, no. 5-6, pp. 338–353, 2019.

[204] J. R. C. Nurse, S. Creese, and D. De Roure, "Security risk assessment in internet of things systems," *IT Professional*, vol. 19, no. 5, pp. 20–26, 2017.

[205] M. Sohail, R. Ali, M. Kashif et al., "Trustwalker: an efficient trust assessment in vehicular internet of things (viot) with security consideration," *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–22, 2020.

[206] W. Abbass, Z. Bakraouy, Z. Bakraouy, A. Baina, and M. Bella, "Assessing the internet of things security risks," *Journal of Communications*, vol. 14, no. 10, pp. 958–964, 2019.

[207] H. Yi, ""Systolic inversion algorithms for building cryptographic systems based on security measurement in IoT-based advanced manufacturing," *Journal of the International Measurement Confederation*, vol. 161, 2020.

[208] A. Ghani, K. Mansoor, S. Mehmood, S. A. Chaudhry, A. U. Rahman, and M. Najmus Saqib, "Security and key management in IoT-based wireless sensor networks: an authentication protocol using symmetric key," *International Journal of Communication Systems*, vol. 32, no. 16, Article ID e4139, 2019.

[209] S. Rostampour, M. Safkhani, Y. Bendavid et al., "ECCbAP: a secure ECC-based authentication protocol for IoT edge devices," *Pervasive and Mobile Computing*, vol. 67, Article ID 101194, 2020.

[210] J. Sanchez-Gomez, D. Garcia-Carrillo, R. Marin-Perez et al., "Secure authentication and credential establishment in narrowband IoT and 5G," *Sensors*, vol. 20, no. 3, p. 882, 2020.

[211] H. S. Trivedi and S. J. Patel, "Design of secure authentication protocol for dynamic user addition in distributed Internet-of-Things," *Computer Networks*, vol. 178, 2020.

[212] H. L. Wu, C. C. Chang, and L. S. Chen, "Secure and anonymous authentication scheme for the internet of things with pairing," *Pervasive and Mobile Computing*, vol. 67, 2020.

[213] W. I. Bae and J. Kwak, "Smart card-based secure authentication protocol in multi-server IoT environment," *Multimedia Tools and Applications*, vol. 79, no. 23-24, pp. 15793–15811, 2020.

[214] S. Garg, K. Kaur, G. Kaddoum et al., "Toward secure and provable authentication for internet of things: realizing industry 4.0," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4598–4606, 2020.

[215] P. K. Panda and S. Chattopadhyay, "A secure mutual authentication protocol for IoT environment," *Journal of Reliable Intelligent Environments*, vol. 6, no. 2, pp. 79–94, 2020.

[216] D. Sethia, D. Gupta, and H. Saran, "NFC secure element-based mutual authentication and attestation for IoT access," *IEEE Transactions on Consumer Electronics*, vol. 64, no. 4, pp. 470–479, 2018.

[217] A. A. Alamr, F. Kausar, J. Kim, and C. Seo, "A secure ECC-based RFID mutual authentication protocol for internet of things," *The Journal of Supercomputing*, vol. 74, no. 9, pp. 4281–4294, 2018.

[218] B. L. Parne, S. Gupta, and N. S. Chaudhari, "PSE-AKA: performance and security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks," *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1156–1177, 2019.

[219] K. Park, Y. Park, A. K. Das, S. Yu, J. Lee, and Y. Park, "A dynamic privacy-preserving key management protocol for V2G in social internet of things," *IEEE Access*, vol. 7, pp. 76812–76832, 2019.

[220] M. Alshahrani and I. Traore, “Secure mutual authentication and automated access control for IoT smart home using cumulative keyed-hash chain,” *Journal of Information Security and Applications*, vol. 45, pp. 156–175, 2019.

[221] B. Bera, D. Chattaraj, and A. K. Das, “Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment,” *Computer Communications*, vol. 153, pp. 229–249, 2020.

[222] W.-J. Tsaur and L.-Y. Yeh, “DANS: a secure and efficient driver-abnormal notification scheme with IoT devices over IoV,” *IEEE Systems Journal*, vol. 13, no. 2, pp. 1628–1639, 2019.

[223] X. Li, S. Liu, F. Wu et al., “Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4755–4763, 2018.

[224] A. Islam and S. Y. Shin, “BUAV: a blockchain based secure UAV-assisted data acquisition scheme in Internet of Things,” *Journal of Communications and Networks*, vol. 21, no. 5, pp. 491–502, 2019.

[225] M. I. A. Zahed, I. Ahmad, D. Habibi, and Q. V. Phung, “Green and secure computation offloading for cache-enabled IoT networks,” *IEEE Access*, vol. 8, pp. 63840–63855, 2020.

[226] B. Li, T. Chen, and G. B. Giannakis, “Secure mobile edge computing in IoT via collaborative online learning,” *IEEE Transactions on Signal Processing*, vol. 67, no. 23, pp. 5922–5935, 2019.

[227] A. Nawaz, J. P. Queralta, J. Guan et al., “Edge computing to secure iot data ownership and trade with the ethereum blockchain,” *Sensors (Switzerland)*, vol. 20, no. 14, pp. 1–17, 2020.

[228] W. Wang, P. Xu, D. Liu, L. T. Yang, and Z. Yan, “Lightweighted secure searching over public-key ciphertexts for edge-cloud-assisted industrial IoT devices,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4221–4230, 2020.

[229] J. Xia, G. Cheng, S. Gu, and D. Guo, “Secure and trust-oriented edge storage for internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4049–4060, 2020.

[230] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, “Preserving balance between privacy and data integrity in edge-assisted internet of things,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2679–2689, 2020.

[231] X. Xu, C. He, Z. Xu, L. Qi, S. Wan, and M. Z. A. Bhuiyan, “Joint optimization of offloading utility and privacy for edge computing enabled IoT,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2622–2629, 2020.

[232] P. Zhang, M. Durresi, and A. Durresi, “Multi-access edge computing aided mobility for privacy protection in Internet of Things,” *Computing*, vol. 101, no. 7, pp. 729–742, 2019.

[233] T. Wang, G. Zhang, A. Liu, M. Z. A. Bhuiyan, and Q. Jin, “A secure IoT service architecture with an efficient balance dynamics based on cloud and edge computing,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4831–4843, 2019.

[234] M. Durresi, A. Subashi, A. Durresi, L. Barolli, and K. Uchida, “Secure communication architecture for internet of things using smartphones and multi-access edge computing in environment monitoring,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 4, pp. 1631–1640, 2019.

[235] V. Sharma, I. You, D. N. K. Jayakody, and M. Atiquzzaman, “Cooperative trust relaying and privacy preservation via edge-crowdsourcing in social Internet of Things,” *Future Generation Computer Systems*, vol. 92, pp. 758–776, 2019.

[236] D. Wang, B. Bai, K. Lei, W. Zhao, Y. Yang, and Z. Han, “Enhancing information security via physical layer approaches in heterogeneous IoT with multiple access mobile edge computing in smart city,” *IEEE Access*, vol. 7, pp. 54508–54521, 2019.

[237] D. E. D. Abou-Tair, S. Büchsenstein, and A. Khalifeh, “A fog computing-based framework for privacy preserving IoT environments,” *The International Arab Journal of Information Technology*, vol. 17, no. 3, pp. 306–315, 2020.

[238] S. K. Sood, “Mobile fog based secure cloud-IoT framework for enterprise multimedia security,” *Multimedia Tools and Applications*, vol. 79, no. 15-16, pp. 10717–10732, 2020.

[239] K. Fan, H. Xu, L. Gao, H. Li, and Y. Yang, “Efficient and privacy preserving access control scheme for fog-enabled IoT,” *Future Generation Computer Systems*, vol. 99, pp. 134–142, 2019.

[240] L. Ferretti, M. Marchetti, and M. Colajanni, “Fog-based secure communications for low-power IoT devices,” *ACM Transactions on Internet Technology*, vol. 19, no. 2, 2019.

[241] Y. Yao, Z. Wang, and P. Zhou, “Privacy-preserving and energy efficient task offloading for collaborative mobile computing in IoT: an ADMM approach,” *Computers and Security*, vol. 96, 2020.

[242] V. Kiran, S. Rani, and P. Singh, “Towards a light weight routing security in IoT using non-cooperative game models and dempster-shaffer theory,” *Wireless Personal Communications*, vol. 110, no. 4, pp. 1729–1749, 2020.

[243] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security,” *Journal of Information Security and Applications*, vol. 52, Article ID 102467, 2020.

[244] D. Airehrour, J. A. Gutierrez, S. K. Ray, and “SecTrust-RPL, “SecTrust-RPL: a secure trust-aware RPL routing protocol for Internet of Things,” *Future Generation Computer Systems*, vol. 93, pp. 860–876, 2019.

[245] H. Hellaoui, M. Koudil, and A. Bouabdallah, “Energy-efficiency in security of 5G-based IoT: an end-to-end adaptive approach,” *IEEE Internet of Things Journal*, vol. 7, 2020.

[246] A. Tandon and P. Srivastava, “Location based secure energy efficient cross layer routing protocols for IOT enabling technologies,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 368–374, 2019.

[247] B. K. Dhaliwal and R. K. Datta, “Secure and energy efficient trust aware routing protocol in IoT using the optimized artificial neural network: SEETA-IoT,” *International Journal of Engineering and Advanced Technology*, vol. 8, no. 6, pp. 4341–4353, 2019.

[248] P. Reddy, R. Babu, and R. Babu, “An evolutionary secure energy efficient routing protocol in Internet of Things,” *International Journal of Intelligent Engineering and Systems*, vol. 10, no. 3, pp. 337–346, 2017.

[249] A. Anand, M. Conti, P. Kaliyar et al., “TARE: topology Adaptive Re-kEying scheme for secure group communication in IoT networks,” *Wireless Networks*, vol. 26, no. 4, pp. 2449–2463, 2020.

[250] A. Arena, P. Perazzo, C. Vallati, G. Dini, and G. Anastasi, “Evaluating and improving the scalability of RPL security in the Internet of Things,” *Computer Communications*, vol. 151, pp. 119–132, 2020.

[251] X. Fang, M. Yang, and W. Wu, “Security cost aware data communication in low-power IoT sensors with energy harvesting,” *Sensors (Switzerland)*, vol. 18, no. 12, 2018.

[252] J. M. McGinthy and A. J. Michaels, "Secure industrial internet of things critical infrastructure node design," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8021–8037, 2019.

[253] I. Batra, S. Verma, A. Malik et al., "Hybrid logical security framework for privacy preservation in the green internet of things," *Sustainability (Switzerland)*, vol. 12, no. no. 14, 2020.

[254] M. Meenakshi, R. Naresh, and S. Pradeep, "Smart home: security and acuteness in automation of IOT sensors," *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, pp. 3271–3274, 2019.

[255] H. Lee, "Home IoT resistance: extended privacy and vulnerability perspective," *Telematics and Informatics*, vol. 49, 2020.

[256] S. Bulusu, M. Krosuri, R. Koripella, and N. Sampath, "Smart and secure home automation using internet of things enabling technologies," *Journal of Computational and Theoretical Nanoscience*, vol. 17, no. 1, pp. 390–395, 2020.

[257] P. Kumar and L. Chouhan, "A secure authentication scheme for IoT application in smart home," *Peer-To-Peer Networking And Applications*, vol. 14, 2020.

[258] M. Park, H. Oh, and K. Lee, "Security risk measurement for information leakage in IoT-based smart homes from a situational awareness perspective," *Sensors (Switzerland)*, vol. 19, no. 9, 2019.

[259] B.-C. Chifor, I. Bica, V.-V. Patriciu, and F. Pop, "A security authorization scheme for smart home Internet of Things devices," *Future Generation Computer Systems*, vol. 86, pp. 740–749, 2018.

[260] H. H. Qasim, A. E. Hamza, H. H. Ibrahim, H. A. Saeed, and M. I. Hamzah, "Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IOT," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, p. 2617, 2020.

[261] G. Krishna, P. Kumar, K. Ravi et al., "Smart home authentication and security with IoT using face recognition," *International Journal of Recent Technology and Engineering*, vol. 7, pp. 705–709, 2019.

[262] S. Alani, S. N. Mahmood, S. Z. Attaallah et al., "IoT based implemented comparison analysis of two well-known network platforms for smart home automation," *International Journal of Electrical & Computer Engineering*, vol. 111 page, 2011.

[263] A. R. Syafeeza, M. K. Mohd Fitri Alif, Y. Nursyifaa Athirah et al., "IoT based facial recognition door access control home security system using raspberry pi," *International Journal of Power Electronics and Drive Systems*, vol. 11, no. 1, pp. 417–424, 2020.

[264] S. Ravikumar and D. Kavitha, "IoT based home monitoring system with secure data storage by Keccak-Chaotic sequence in cloud server," *Journal of Ambient Intelligence and Humanized Computing*, 2020.

[265] P. Gupta and M. Rajoriya, "Face recognition based home security system using IoT," *Journal of Critical Reviews*, vol. 7, no. 10, pp. 1001–1006, 2020.

[266] J. S. P. Peter, S. Selvakumar, H. Pandit et al., "Home automation and home security using arduino and ESP8266(IOT)," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 7, pp. 39–42, 2019.

[267] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 7702–7712, 2019.

[268] S. Singh, I.-H. Ra, W. Meng et al., "SH-BlockCC: a secure and efficient Internet of things smart home architecture based on cloud computing and blockchain technology," *International Journal of Distributed Sensor Networks*, vol. 15, no. 4, Article ID 1550147719844159, 2019.

[269] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[270] A. S. M. S. Hosen, S. Singh, P. K. Sharma et al., "Blockchain-based transaction validation protocol for a secure distributed IoT network," *IEEE Access*, vol. 8, pp. 117266–117277, 2020.

[271] J. Chi, Y. Li, J. Huang et al., "A secure and efficient data sharing scheme based on blockchain in industrial Internet of Things," *Journal of Network and Computer Applications*, vol. 167, 2020.

[272] A. Shahzad, K. Zhang, and A. Gherbi, "Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain," *Sensors (Switzerland)*, vol. 20, no. 13, pp. 1–27, 2020.

[273] M. Sigwart, M. Borkowski, M. Peise et al., "A secure and extensible blockchain-based data provenance framework for the internet of things," *Personal and Ubiquitous Computing*, 2020.

[274] T. A. Alghamdi, I. Ali, N. Javaid et al., "Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain," *IEEE Access*, vol. 8, 2020.

[275] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, Q. Zhang, and K.-K. R. Choo, "An energy-efficient SDN controller architecture for IoT networks with blockchain-based security," *IEEE Transactions on Services Computing*, vol. 13, no. 4, pp. 625–638, 2020.

[276] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore et al., "Blockchain-based secure storage management with edge computing for IoT," *Electronics (Switzerland)*, vol. 8, no. 8, 2019.

[277] P. Ghadekar, N. Doke, S. Kaneri et al., "Secure access control to IoT devices using blockchain," *International Journal of Recent Technology and Engineering*, vol. 8, no. 2, pp. 3064–3070, 2019.

[278] A. Muthanna, A. A. Ateya, A. Khakimov et al., "Secure and reliable IoT networks using fog computing with software-defined networking and blockchain," *Journal of Sensor and Actuator Networks*, vol. 8, no. 1, 2019.

[279] J. Ali, T. Ali, S. Musa et al., "Towards secure IoT communication with smart contracts in a Blockchain infrastructure," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 10, pp. 578–585, 2018.

[280] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati, and M. H. Alsharif, "A privacy preserving authentication scheme for roaming in IoT-based wireless mobile networks," *Symmetry*, vol. 12, no. 2, p. 287, 2020.

[281] X. Wang, M. Umehira, B. Han, H. Zhou, P. Li, and C. Wu, "An efficient privacy preserving spectrum sharing framework for internet of things," *IEEE Access*, vol. 8, pp. 34675–34685, 2020.

[282] A. R. Sfar, Y. Challal, P. Moyal et al., "A game theoretic approach for privacy preserving model in IoT-based transportation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 12, pp. 4405–4414, 2019.

[283] R. S. Apare and S. N. Gujar, "Implementing adaptive dragonfly optimization for privacy preservation in IoT,"

Journal of High Speed Networks, vol. 25, no. 4, pp. 331–348, 2019.

[284] Q. Sun, M. C. Willemsen, and B. P. Knijnenburg, "Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing," *Computers & Security*, vol. 97, p. 101924, 2020.

[285] P. Emami Naeini, M. Degeling, L. Bauer et al., "The influence of friends and experts on privacy decision making in iot scenarios," *Proceedings of the ACM on Human-Computer Interaction*, vol. 2, pp. 1–26, 2018.

[286] H. Oh, S. Park, G. M. Lee, J. K. Choi, and S. Noh, "Competitive data trading model with privacy valuation for multiple stakeholders in IoT data markets," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3623–3639, 2020.

[287] P. Menard and G. J. Bott, "Analyzing IoT users' mobile device privacy concerns: extracting privacy permissions using a disclosure experiment," *Computers & Security*, vol. 95, Article ID 101856, 2020.

[288] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca et al., "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[289] B. Mukherjee, S. Wang, W. Lu et al., "Flexible IoT security middleware for end-to-end cloud-fog communication," *Future Generation Computer Systems*, vol. 87, pp. 688–703, 2018.

[290] C. M. Latha and K. L. S. Soujanya, "Enhancing end-to-end device security of internet of things using dynamic cryptographic algorithm," *International Journal of Civil Engineering and Technology*, vol. 9, no. 9, pp. 408–415, 2018.

[291] S. Raza, T. Helgason, P. Papadimitratos, and T. Voigt, "SecureSense: end-to-end secure communication architecture for the cloud-connected Internet of Things," *Future Generation Computer Systems*, vol. 77, pp. 40–51, 2017.

[292] C.-S. Park and W.-S. Park, "A group-oriented DTLS handshake for secure IoT applications," *IEEE Transactions on Automation Science and Engineering*, vol. 15, no. 4, pp. 1920–1929, 2018.

[293] S. Pérez, J. L. Hernández-Ramos, S. Raza et al., "Application layer key establishment for end-to-end security in IoT," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2117–2128, 2019.

[294] S. Pérez, D. Garcia-Carrillo, R. Marín-López, J. L. Hernández-Ramos, R. Marín-Pérez, and A. F. Skarmeta, "Architecture of security association establishment based on bootstrapping technologies for enabling secure IoT infrastructures," *Future Generation Computer Systems*, vol. 95, pp. 570–585, 2019.

[295] D. V. Medhane, A. K. Sangaiah, M. S. Hossain, G. Muhammad, and J. Wang, "Blockchain-enabled distributed security framework for next-generation IoT: an edge cloud and software-defined network-integrated approach," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6143–6149, 2020.

[296] A. Jindal, G. S. Aujla, and N. Kumar, "SURVIVOR: a blockchain based edge-as-a-service framework for secure energy trading in SDN-enabled vehicle-to-grid environment," *Computer Networks*, vol. 153, pp. 36–48, 2019.

[297] A. H. Sodhro, S. Pirbhulal, L. Zongwei, K. Muhammad, and N. Zahid, "Towards blockchain-enabled security technique for industrial Internet of Things based decentralized applications," *Journal of Grid Computing*, vol. 18, pp. 615–628, 2020.

[298] S. Rathore, B. Wook Kwon, and J. H. Park, "BlockSecIoTNet: blockchain-based decentralized security architecture for IoT network," *Journal of Network and Computer Applications*, vol. 143, pp. 167–177, 2019.

[299] P. C. M. Arachchige, P. Bertok, I. Khalil, D. Liu, S. Camtepe, and M. Atiquzzaman, "A trustworthy privacy preserving framework for machine learning in industrial IoT systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6092–6102, 2020.

[300] S. Rathore, Y. Pan, J. H. Park, and " BlockDeepNet, "A blockchain-based secure deep learning for IoT network," *Sustainability (Switzerland)*, vol. 1114 pages, 2019.

[301] S. S. S. Sugi and S. R. Ratna, "A novel distributed training on fog node in IoT backbone networks for security," *Soft Computing*, vol. 24, no. 24, pp. 18399–18410, 2020.

[302] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in SDN-enabled 5G-VANETs," *IEEE Access*, vol. 7, pp. 56656–56666, 2019.

[303] P. Sudhakaran and M. C, "Energy efficient distributed lightweight authentication and encryption technique for IoT security," *International Journal of Communication Systems*, p. e4198, 2019.